



Documentation ONTAP 9

ONTAP 9

NetApp
September 12, 2024

This PDF was generated from <https://docs.netapp.com/fr-fr/ontap/index.html> on September 12, 2024.
Always check docs.netapp.com for the latest.

Sommaire

Documentation ONTAP 9	1
Notes de mise à jour	2
Points forts de la version ONTAP 9	2
Nouveautés d'ONTAP 9.15.1	9
Nouveautés d'ONTAP 9.14.1	13
Nouveautés d'ONTAP 9.13.1	18
Nouveautés d'ONTAP 9.12.1	24
Nouveautés d'ONTAP 9.11.1	30
Nouveautés d'ONTAP 9.10.1	35
Nouveautés d'ONTAP 9.9.1	40
Modifications des limites ONTAP et des valeurs par défaut	45
Prise en charge de la version 9 de ONTAP	49
Introduction et concepts	51
Concepts relatifs à ONTAP	51
Intégration de System Manager à BlueXP	106
Configuration, mise à niveau et restauration du logiciel et du firmware ONTAP	108
Configuration de ONTAP	108
Mettez à niveau ONTAP	126
Des mises à jour du firmware et du système	275
Restaurez la ONTAP	282
Administration du cluster	316
Gestion du cluster avec System Manager	316
Gestion des licences	333
Gestion du cluster via l'interface de ligne de commandes	343
Gestion des disques et des niveaux (agrégat)	470
Gestion des niveaux FabricPool	567
Mobilité des données des SVM	624
Gestion des paires HAUTE DISPONIBILITÉ	635
Gestion des API REST avec System Manager	661
L'administration des volumes	664
Gestion des volumes et des LUN avec System Manager	664
Gestion du stockage logique avec l'interface de ligne de commandes	688
Provisionnez le stockage NAS pour les systèmes de fichiers volumineux à l'aide de FlexGroup volumes	829
Gestion des volumes FlexGroup via l'interface de ligne de commandes	831
Gestion des volumes FlexCache	922
Gestion du réseau	956
Commencez	956
Composants réseau	960
Workflow de basculement de chemin NAS (ONTAP 9.8 et versions ultérieures)	965
Workflow de basculement de chemin NAS (ONTAP 9.7 et versions antérieures)	974
Ports réseau	988
Les IPspaces	1013
Les domaines de diffusion	1020

Groupes et règles de basculement	1048
Sous-réseaux (administrateurs du cluster uniquement)	1052
Créer des SVM	1060
Interfaces logiques	1067
Équilibrer les charges réseau	1098
Résolution du nom d'hôte	1107
Sécurisez votre réseau	1110
Marquage QoS (administrateurs du cluster uniquement)	1125
Gestion SNMP (administrateurs du cluster uniquement)	1127
Gestion du routage dans un SVM	1140
Afficher les informations sur le réseau	1144
Gestion du stockage NAS	1178
Gérez les protocoles NAS avec System Manager	1178
Configurez NFS avec l'interface de ligne de commande	1201
Gérez NFS avec l'interface de ligne de commande	1276
Gérer l'agrégation NFS	1400
Gestion de NFS sur RDMA	1411
Configurez SMB avec l'interface de ligne de commandes	1417
Gestion de SMB avec l'interface de ligne de commandes	1461
Offrez un accès client S3 aux données NAS	1825
Configuration SMB pour Microsoft Hyper-V et SQL Server	1835
Gestion du stockage SAN	1897
Concepts RELATIFS AU SAN	1897
Administration SAN	1921
Protection des données SAN	1997
Référence de configuration SAN	2018
Gestion du stockage objet S3	2063
Découvrez la prise en charge de S3 dans ONTAP 9	2063
Planification	2066
Configurer	2072
Protection des compartiments avec SnapMirror S3	2123
Audit des événements S3	2158
Authentification et contrôle d'accès	2168
Présentation de l'authentification et du contrôle d'accès	2168
Gestion de l'authentification administrateur et du RBAC	2168
Authentification et autorisation via OAuth 2.0	2269
Configurez l'authentification SAML	2291
Gérer les services Web	2298
Vérifiez l'identité des serveurs distants à l'aide de certificats	2309
Authentifier mutuellement le cluster et un serveur KMIP	2312
Sécurité et chiffrement des données	2316
À propos de la protection contre les ransomware de NetApp	2316
Protection autonome contre les ransomwares	2326
Protection antivirus avec Vscan	2353
Instructions de renforcement de la sécurité ONTAP	2395

Audit des événements NAS sur les SVM	2444
Utilisez FPolicy pour le contrôle et la gestion des fichiers sur SVM	2494
Vérifiez l'accès à l'aide du suivi de sécurité	2559
Gestion du chiffrement avec System Manager	2572
Gestion du chiffrement via l'interface de ligne de commandes	2573
Activez le modèle « zéro confiance »	2669
Protection des données et reprise d'activité	2677
Cluster et SVM peering	2677
Gérez les copies Snapshot locales	2705
Réplication de volume SnapMirror	2721
Gérer la réplication de volume SnapMirror	2743
Gérer la réplication de SVM SnapMirror	2790
Gérer la réplication de volume root SnapMirror	2828
Sauvegarder dans le cloud	2832
Détails techniques de SnapMirror	2837
Archivage et conformité grâce à la technologie SnapLock	2847
Groupes de cohérence	2893
Synchronisation active SnapMirror	2934
Service médiateur pour MetroCluster et SnapMirror actif Sync	2998
Gérez des sites MetroCluster avec System Manager	3065
Protection des données par sauvegarde sur bandes	3075
Configuration NDMP	3175
Réplication entre le logiciel NetApp Element et ONTAP	3192
Surveillance des événements, des performances et de l'état du système	3213
Contrôle des performances du cluster avec System Manager	3213
Contrôlez et gérez les performances du cluster à l'aide de l'interface de ligne de commandes	3225
Surveillez les performances des clusters avec Unified Manager	3264
Contrôle des performances du cluster avec Cloud Insights	3264
Consignation des audits	3265
AutoSupport	3271
Contrôle de l'état du système	3303
Analytique du système de fichiers	3316
Configuration EMS	3332
Référence de commande ONTAP	3350
Références des commandes pour les versions prises en charge de ONTAP	3350
Références des commandes pour les versions de support limitées de ONTAP (PDF uniquement)	3350
Outil de comparaison CLI	3350
Mentions légales	3351
Droits d'auteur	3351
Marques déposées	3351
Brevets	3351
Politique de confidentialité	3351
Source ouverte	3351

Documentation ONTAP 9

Notes de mise à jour

Points forts de la version ONTAP 9

Chaque version du logiciel de gestion des données ONTAP 9 inclut de nouvelles fonctionnalités améliorées qui améliorent les fonctionnalités, la gestion, les performances et la sécurité dans ONTAP.

En plus de ces points forts, vous trouverez une couverture complète par version de toutes les nouvelles fonctionnalités et améliorations introduites dans les dernières versions d'ONTAP.

- Découvrez ["Nouvelles fonctionnalités ONTAP MetroCluster améliorées"](#).
- Découvrez ["Prise en charge nouvelle et améliorée des plateformes FAS, ASA et AFF, ainsi que des commutateurs pris en charge"](#).
- En savoir plus sur les mises à jour du ["L'API REST DE ONTAP"](#).

Pour plus d'informations sur les problèmes connus, les limites et les mises en garde de mise à niveau dans les dernières versions de ONTAP 9, consultez le ["Notes de mise à jour de ONTAP 9"](#). Vous devez vous connecter avec votre compte NetApp ou créer un compte pour accéder aux notes de version.

Pour effectuer la mise à niveau vers la dernière version de ONTAP, reportez-vous à la section [Mise à niveau vers la dernière version de ONTAP](#) et [Quand dois-je mettre à niveau ONTAP ?](#)

Points forts de ONTAP 9.15.1

ONTAP 9.15.1 propose de nouvelles fonctionnalités améliorées dans les domaines de la gestion de la sécurité, de la protection des données et de la prise en charge des charges de travail NAS. Pour obtenir la liste complète des nouvelles fonctionnalités et améliorations, reportez-vous à la section [Nouveautés de ONTAP 9.15.1](#).

- ["Prise en charge des nouveaux systèmes AFF A-Series et du stockage conçu pour l'IA"](#)

ONTAP 9.15.1 prend en charge les nouveaux systèmes AFF A1K, AFF A90 et AFF A70 hautes performances, conçus pour les charges de travail nouvelle génération, telles que l'entraînement et l'inférence IA/ML. Ces nouveaux systèmes sont jusqu'à doubler les performances des solutions AFF A-Series existantes et offrent une efficacité du stockage améliorée « always-on » sans sacrifier les performances.

- [Applications de sauvegarde Windows et liens symboliques de style Unix](#)

Depuis ONTAP 9.15.1, vous avez également la possibilité de sauvegarder le lien symbolique lui-même au lieu des données auxquelles il pointe. Cela peut apporter plusieurs avantages, notamment une amélioration des performances de vos applications de sauvegarde. Vous pouvez activer la fonctionnalité via l'interface de ligne de commandes ou l'API REST de ONTAP.

- [Autorisation dynamique](#)

ONTAP 9.15.1 introduit un cadre initial pour l'autorisation dynamique, une fonction de sécurité qui peut déterminer si une commande émise par un compte d'administrateur doit être refusée, demandée pour une authentification supplémentaire ou autorisée à continuer. Les déterminations sont basées sur le score de confiance du compte utilisateur, en tenant compte de facteurs tels que l'heure de la journée, le lieu, l'adresse IP, l'utilisation de l'appareil de confiance et l'historique d'authentification et d'autorisation de

l'utilisateur.

- [Étendue de l'impact pour la vérification multiadministrateur](#)

ONTAP 9.15.1 RC1 ajoute plus d'une centaine de nouvelles commandes à la structure MAV pour une protection supplémentaire contre les initiés malveillants.

- [NFS sur TLS](#)

Protégez les données « sur le réseau » au niveau de la couche de protocoles en simplifiant la configuration par rapport à d'autres technologies telles que IPSec et NFS Kerberos. Cette fonctionnalité est actuellement incluse en tant qu'aperçu public. Pour plus d'informations sur cette fonctionnalité, contactez votre équipe commerciale pour plus d'informations.

- Prise en charge du chiffrement TLS 1.3 pour le peering de cluster et bien plus encore

ONTAP 9.15.1 intègre la prise en charge du chiffrement TLS 1.3 pour le stockage S3, le chiffrement FlexCache, SnapMirror et le chiffrement de peering de cluster. Des applications telles que FabricPool, le stockage des blobs Microsoft Azure page et SnapMirror Cloud continuent d'utiliser TLS 1.2 pour la version 9.15.1.

- Prise en charge du trafic SMTP sur TLS

Transfert sécurisé des données AutoSupport par e-mail avec prise en charge TLS

- [Synchronisation active SnapMirror pour des configurations actif-actif symétriques](#)

Cette nouvelle fonctionnalité offre une réplication bidirectionnelle synchrone pour la continuité de l'activité et la reprise après incident. Protégez l'accès aux données pour les workloads SAN stratégiques avec un accès simultané en lecture et en écriture aux données dans plusieurs domaines défaillants. Vous bénéficiez ainsi d'opérations sans interruption et d'une réduction des temps d'indisponibilité en cas d'incident ou de panne système.

- [Réécriture FlexCache](#)

L'écriture différée de FlexCache permet aux clients d'écrire localement sur les volumes FlexCache, réduisant ainsi la latence et améliorant les performances par rapport à l'écriture directe sur le volume d'origine. Les données nouvellement écrites sont répliquées de manière asynchrone vers le volume d'origine.

- [NFSv3 sur RDMA](#)

La prise en charge de NFSv3 over RDMA permet de répondre aux besoins en hautes performances en fournissant un accès à large bande passante et à faible latence via TCP.

Points forts de ONTAP 9.14.1

ONTAP 9.14.1 propose de nouvelles fonctionnalités améliorées dans les domaines d'FabricPool, de la protection contre les ransomware, d'OAuth, etc. Pour obtenir la liste complète des nouvelles fonctionnalités et améliorations, reportez-vous à la section [Nouveautés de ONTAP 9.14.1](#).

- [Réduction réservation WAFL](#)

ONTAP 9.14.1 augmente immédiatement de 5 % l'espace utilisable sur les systèmes FAS et Cloud Volumes ONTAP en réduisant la réserve WAFL sur les agrégats de 30 To ou plus.

- [Améliorations de FabricPool](#)

FabricPool offre un de plus en plus de [performances de lecture](#) elle permet également d'écrire directement dans le cloud, ce qui réduit les risques de manque d'espace et les coûts de stockage en déplaçant les données inactives vers un tier de stockage moins coûteux.

- ["Prise en charge d'OAuth 2.0"](#)

ONTAP prend en charge l'infrastructure OAuth 2.0, qui peut être configurée à l'aide du Gestionnaire système. Avec OAuth 2.0, vous pouvez fournir un accès sécurisé à ONTAP pour les infrastructures d'automatisation sans créer ou exposer des ID utilisateur et des mots de passe à des scripts en texte brut et des runbooks.

- ["Améliorations de la protection anti-ransomware autonome \(ARP\)"](#)

ARP vous accorde davantage de contrôle sur la sécurité des événements, ce qui vous permet d'ajuster les conditions qui créent des alertes et de réduire le risque de faux positifs.

- [Répétition de la reprise d'activité SnapMirror dans System Manager](#)

System Manager permet de tester facilement la reprise après incident sur un site distant et de la nettoyer après le test. Cette fonctionnalité permet des tests plus simples et plus fréquents, et une confiance accrue dans les objectifs de délai de restauration.

- [Prise en charge du verrouillage objet S3](#)

ONTAP S3 prend en charge la commande d'API de verrouillage objet, ce qui vous permet de protéger contre la suppression les données écrites sur ONTAP avec S3

À l'aide de commandes standard de l'API S3 et pour s'assurer que les données importantes sont protégées pendant la durée appropriée.

- [Cluster et volumétrie](#) balisage

Ajoutez des balises de métadonnées aux volumes et aux clusters, qui suivent et suivent le déplacement des données depuis l'environnement sur site vers le cloud, et inversement.

Points forts de ONTAP 9.13.1

ONTAP 9.13.1 inclut de nouvelles fonctionnalités améliorées dans les domaines de la protection contre les ransomware, des groupes de cohérence, de la qualité de service, de la gestion de la capacité des locataires, etc. Pour obtenir la liste complète des nouvelles fonctionnalités et améliorations, reportez-vous à la section [Nouveautés de ONTAP 9.13.1](#).

- Améliorations de la protection anti-ransomware autonome (ARP) :

- [Activation automatique](#)

Avec ONTAP 9.13.1, ARP passe automatiquement du mode de formation au mode de production dès lors qu'il dispose de données d'apprentissage suffisantes, ce qui évite à un administrateur de l'activer au bout de 30 jours.

- [Prise en charge de la vérification multiadministrateur](#)

Les commandes de désactivation du protocole ARP sont prises en charge par la vérification multiadministrateur, ce qui permet de s'assurer qu'aucun administrateur ne peut désactiver le protocole

ARP pour exposer les données à d'éventuelles attaques par ransomware.

- [Prise en charge de FlexGroup](#)

ARP prend en charge FlexGroups à partir de ONTAP 9.13.1. ARP peut contrôler et protéger les FlexGroups couvrant plusieurs volumes et nœuds du cluster, ce qui permet de protéger même les datasets les plus volumineux avec ARP.

- [Contrôle des performances et de la capacité pour les groupes de cohérence dans System Manager](#)

Le contrôle des performances et de la capacité fournit des informations détaillées pour chaque groupe de cohérence. Il vous permet d'identifier et de signaler rapidement les problèmes potentiels au niveau de l'application plutôt qu'au niveau de l'objet de données.

- [Gestion de la capacité des locataires](#)

Les clients et fournisseurs de services mutualisés peuvent fixer une limite de capacité sur chaque SVM, ce qui permet aux locataires d'effectuer un provisionnement en libre-service sans risque de consommation excessive de la capacité d'un locataire sur le cluster.

- [Plafonds et étages de qualité de service](#)

ONTAP 9.13.1 vous permet de regrouper des objets, tels que des volumes, des LUN ou des fichiers, et d'attribuer un plafond de QoS (IOPS maximales) ou un seuil (IOPS minimales), ce qui améliore les attentes en matière de performance des applications.

Points forts de ONTAP 9.12.1

ONTAP 9.12.1 offre de nouvelles fonctionnalités améliorées dans les domaines du renforcement de la sécurité, de la conservation, des performances, etc. Pour obtenir la liste complète des nouvelles fonctionnalités et améliorations, reportez-vous à la section [Nouveautés de ONTAP 9.12.1](#).

- [Instantanés inviolables](#)

Avec la technologie SnapLock, les copies Snapshot ne peuvent pas être supprimées à la source ou à la destination.

Conservez davantage de points de restauration en protégeant les snapshots sur le stockage primaire et secondaire contre la suppression par des attaquants de ransomware ou des administrateurs peu scrupuleux.

- [Améliorations de la protection anti-ransomware autonome \(ARP\)](#)

Activez immédiatement une protection anti-ransomware autonome intelligente sur le stockage secondaire, en fonction du modèle de filtrage déjà effectué pour le stockage primaire.

Après un basculement, identifiez instantanément les attaques par ransomware sur le stockage secondaire. Une copie Snapshot est immédiatement prise des données qui commencent à être affectées, et les administrateurs sont avertis, ce qui contribue à arrêter une attaque et à améliorer la restauration.

- [FPolicy](#)

Activation en un clic de ONTAP FPolicy pour activer le blocage automatique des fichiers malveillants connus l'activation simplifiée aide à se protéger contre les attaques de ransomware classiques qui utilisent des extensions de fichiers connues communes.

- **Renforcement de la sécurité : consignment sécurisée**

Consignation à toute épreuve dans ONTAP pour s'assurer que les comptes d'administrateur compromis ne peuvent pas masquer les actions malveillantes. L'administrateur et l'historique des utilisateurs ne peuvent pas être modifiés ou supprimés sans la connaissance des systèmes.

Consigner et auditer toutes les actions d'administration, quelle que soit leur origine, pour garantir la collecte de toutes les actions ayant un impact sur les données. Une alerte est générée chaque fois que les journaux d'audit du système ont été modifiés, de quelque manière que ce soit, pour prévenir les administrateurs de la modification.

- **Renforcement de la sécurité : authentification multifacteur étendue**

L'authentification multifacteur (MFA) pour la CLI (SSH) prend en charge les dispositifs physiques à jetons Yubikey, garantissant ainsi qu'un attaquant ne peut pas accéder au système ONTAP à l'aide d'informations d'identification volées ou d'un système client compromis. Cisco DUO est pris en charge pour MFA avec System Manager.

- **Dualité fichier/objet (accès multiprotocole)**

La dualité fichier/objet permet un accès en lecture et en écriture natif du protocole S3 à la même source de données qui dispose déjà d'un accès au protocole NAS. Vous pouvez accéder simultanément à votre stockage en tant que fichiers ou en tant qu'objets à partir de la même source de données, ce qui vous évite d'avoir à dupliquer des copies des données pour les utiliser avec différents protocoles (S3 ou NAS), comme pour l'analytique qui utilise des données d'objet.

- **Rééquilibrage FlexGroup**

Si les composants FlexGroup sont déséquilibrés, le FlexGroup peut être rééquilibré et géré sans interruption à partir du

CLI, API REST et System Manager. Pour des performances optimales, la capacité utilisée des membres d'un FlexGroup doit être répartie de façon égale.

- **Amélioration de la capacité de stockage**

La réservation d'espace WAFL a été considérablement réduite, ce qui donne jusqu'à 400 Tio de capacité utilisable supplémentaire par agrégat.

Points forts de ONTAP 9.11.1

ONTAP 9.11.1 propose de nouvelles fonctionnalités améliorées dans les domaines de la sécurité, de la conservation, des performances, etc. Pour obtenir la liste complète des nouvelles fonctionnalités et améliorations, reportez-vous à la section [Nouveautés de ONTAP 9.11.1](#).

- **Vérification multi-administrateurs**

La vérification multiadministrateur est une approche native de vérification unique sur le marché qui requiert plusieurs approbations pour les tâches administratives sensibles telles que la suppression d'un Snapshot ou d'un volume. Les approbations requises dans une implémentation MAV empêchent les attaques malveillantes et les modifications accidentelles des données.

- **Améliorations de la protection anti-ransomware autonome**

La protection anti-ransomware autonome (ARP) utilise le machine learning pour détecter les menaces de ransomware avec une granularité accrue. Vous pouvez ainsi identifier les menaces rapidement et

accélérer la restauration en cas de violation.

- [Conformité SnapLock pour les volumes FlexGroup](#)

Sécurisez des datasets de plusieurs pétaoctets pour des charges de travail telles que l'automatisation de la conception électronique, les médias et le divertissement en protégeant les données à l'aide du verrouillage des fichiers WORM afin qu'elles ne puissent pas être modifiées ou supprimées.

- [Suppression du répertoire asynchrone](#)

Avec ONTAP 9.11.1, la suppression des fichiers a lieu en arrière-plan du système ONTAP. Vous pouvez ainsi supprimer facilement les répertoires volumineux tout en éliminant les impacts sur les performances et la latence des E/S hôtes

- [Améliorations de S3](#)

Simplifiez et étendez les fonctionnalités de gestion des données d'objet S3 avec ONTAP, ainsi que des terminaux d'API supplémentaires et la gestion des versions d'objet au niveau du compartiment. Vous pouvez ainsi stocker plusieurs versions d'un objet dans le même compartiment.

- Améliorations apportées à System Manager

System Manager prend en charge des fonctionnalités avancées d'optimisation des ressources de stockage et d'amélioration de la gestion des audits. Ces mises à jour incluent des capacités améliorées de gestion et de configuration des agrégats de stockage, une meilleure visibilité sur l'analytique système et la visualisation matérielle des systèmes FAS.

Points forts de ONTAP 9.10.1

ONTAP 9.10.1 inclut de nouvelles fonctionnalités améliorées dans les domaines du renforcement de la sécurité, de l'analytique des performances, de la prise en charge du protocole NVMe et des options de sauvegarde du stockage objet. Pour obtenir la liste complète des nouvelles fonctionnalités et améliorations, reportez-vous à la section [Nouveautés de ONTAP 9.10.1](#).

- [Protection autonome contre les ransomwares](#)

La protection autonome contre les ransomware crée automatiquement une copie Snapshot de votre volume et alerte les administrateurs en cas d'activité anormale, ce qui vous permet de détecter rapidement les attaques par ransomware et de restaurer vos données plus rapidement.

- Améliorations apportées à System Manager

System Manager télécharge automatiquement les mises à jour de firmware pour les disques, les tiroirs et les processeurs de service, en plus de proposer de nouvelles intégrations avec NetApp Active IQ Digital Advisor, BlueXP et la gestion des certificats. Ces améliorations simplifient l'administration et assurent la continuité de l'activité.

- [Améliorations de l'analyse du système de fichiers](#)

L'analytique du système de fichiers fournit des outils de télémétrie supplémentaires pour identifier les principaux fichiers, répertoires et utilisateurs de votre partage de fichiers. Vous pouvez ainsi identifier les problèmes de performances des workloads afin d'améliorer la planification des ressources et l'implémentation de la QoS.

- [Prise en charge de NVMe over TCP \(NVMe/TCP\) pour les systèmes AFF](#)

Obtenez une haute performance et réduisez le TCO de votre SAN d'entreprise et des workloads modernes sur un système AFF lorsque vous utilisez NVMe/TCP sur votre réseau Ethernet existant.

- [Prise en charge de NVMe over Fibre Channel \(NVMe/FC\) pour les systèmes NetApp FAS](#)

Utilisez le protocole NVMe/FC sur vos baies hybrides pour permettre une migration uniforme vers NVMe.

- [Sauvegarde native dans le cloud hybride pour le stockage objet](#)

Protégez vos données ONTAP S3 avec les cibles de stockage objet de votre choix. Utilisez la réplication SnapMirror pour sauvegarder vos données dans un stockage sur site avec StorageGRID, dans le cloud avec Amazon S3 ou dans un autre compartiment ONTAP S3 sur des systèmes NetApp AFF et FAS.

- [Verrouillage global des fichiers avec FlexCache](#)

Assurez la cohérence des fichiers aux emplacements du cache lors des mises à jour des fichiers source à l'origine avec un verrouillage global des fichiers à l'aide de FlexCache. Cette amélioration permet d'activer des verrouillages exclusifs de lecture de fichiers dans une relation origine-cache pour les charges de travail qui nécessitent un verrouillage amélioré.

Points forts de ONTAP 9.9.1

ONTAP 9.9.1 inclut de nouvelles fonctionnalités améliorées dans les domaines de l'efficacité du stockage, de l'authentification multifacteur, de la reprise d'activité, etc. Pour obtenir la liste complète des nouvelles fonctionnalités et améliorations, reportez-vous à la section [Nouveautés de ONTAP 9.9.1](#).

- [Sécurité renforcée pour la gestion des accès à distance via l'interface de ligne de commande](#)

La prise en charge du hachage de mot de passe SHA512 et SSH A512 protège les informations d'identification des comptes d'administrateur contre les agents malveillants qui tentent d'accéder au système.

- ["Améliorations MetroCluster IP : prise en charge des clusters à 8 nœuds"](#)

La nouvelle limite est deux fois plus importante que la précédente. Elle prend en charge les configurations MetroCluster et assure la disponibilité continue des données.

- [Synchronisation active SnapMirror](#)

Offre davantage d'options de réplication pour la sauvegarde et la reprise d'activité pour les conteneurs de données volumineux pour workloads NAS.

- [Performances SAN améliorées](#)

Délivre des performances SAN jusqu'à quatre fois supérieures pour les applications à LUN uniques, telles que les datastores VMware, afin que vous puissiez atteindre les performances élevées dans votre environnement SAN.

- [Nouvelle option de stockage objet pour le cloud hybride](#)

StorageGRID peut être utilisé comme destination pour NetApp Cloud Backup Service afin de simplifier et d'automatiser la sauvegarde de vos données ONTAP sur site.

Étapes suivantes

- [Mise à niveau vers la dernière version de ONTAP](#)
- [Quand dois-je mettre à niveau ONTAP ?](#)

Nouveautés d'ONTAP 9.15.1

Découvrez les nouvelles fonctionnalités disponibles dans ONTAP 9.15.1.

Pour plus d'informations sur les problèmes connus, les limites et les mises en garde de mise à niveau dans les dernières versions de ONTAP 9, consultez le ["Notes de mise à jour de ONTAP 9"](#). Vous devez vous connecter avec votre compte NetApp ou créer un compte pour accéder aux notes de version.

Découvrez les nouveautés et les améliorations ["Fonctionnalités ONTAP MetroCluster"](#).

Découvrez les nouveautés et les améliorations de la prise en charge de ["Plateformes FAS, ASA et AFF, ainsi que les commutateurs pris en charge"](#).

En savoir plus sur les mises à jour du ["L'API REST DE ONTAP"](#).

Pour effectuer la mise à niveau vers la dernière version de ONTAP, reportez-vous à la section ["Préparez la mise à niveau de ONTAP"](#).

Protection des données

Mise à jour	Description
Applications de sauvegarde Windows et liens symboliques de style Unix	Lorsqu'une application de sauvegarde Windows rencontre un lien symbolique de style Unix (symlink), le lien est suivi et les données réelles sont renvoyées par ONTAP et sauvegardées. Depuis ONTAP 9.15.1, vous avez également la possibilité de sauvegarder le lien symbolique lui-même au lieu des données auxquelles il pointe. Cela peut apporter plusieurs avantages, notamment une amélioration des performances de vos applications de sauvegarde. Vous pouvez activer la fonctionnalité via l'interface de ligne de commandes ou l'API REST de ONTAP.
La synchronisation active SnapMirror prend en charge les déploiements actif-actif symétriques	La synchronisation active SnapMirror (anciennement SnapMirror Business Continuity) prend désormais en charge les déploiements actifs-actifs symétriques. Vous pouvez ainsi effectuer des opérations d'E/S en lecture et écriture à partir des deux copies d'une LUN protégée grâce à la réplication synchrone bidirectionnelle.
Augmentation de la limite pour les volumes d'un groupe de cohérence à l'aide de la réplication asynchrone SnapMirror	Les groupes de cohérence qui utilisent la protection asynchrone SnapMirror prennent désormais en charge jusqu'à 80 volumes dans le groupe de cohérence.

Mise à jour	Description
Prise en charge du niveau de privilège admin pour les opérations de l'API REST et de l'interface de ligne de commandes avec groupes de cohérence	Les opérations de l'API CLI et REST pour les groupes de cohérence sont désormais prises en charge au niveau des privilèges d'administration.
Réserves persistantes pour les volumes virtuels VMware avec le clustering avec basculement sur incident Windows Server	ONTAP prend actuellement en charge les volumes virtuels VMware (vVols) ainsi que les réservations persistantes avec les LUN classiques. Depuis la version ONTAP 9.15.1, vous pouvez également créer une réservation persistante avec un vVol. Cette fonctionnalité est prise en charge dans les outils ONTAP pour VMware vSphere 9. Il n'est pris en charge que dans un cluster de basculement Windows Server (WSFC) qui est un groupe de machines virtuelles Windows en cluster.

Sécurité

Mise à jour	Description
Création et configuration simplifiées de stockage persistant FPolicy	<p>Vous pouvez créer le stockage persistant FPolicy et automatiser la création et la configuration de son volume en même temps à l'aide de <code>persistent-store create</code> commande.</p> <p>Le modèle amélioré <code>persistent-store create</code> permet également d'utiliser le paramètre <code>auto-size-mode</code>, qui permet au volume d'augmenter ou de réduire sa taille en fonction de la quantité d'espace utilisé.</p>
Prise en charge de NFSv3 avec RDMA	Les configurations NFS over RDMA prennent désormais en charge NFSv3.
FPolicy prend en charge le protocole NFS 4.1	FPolicy prend en charge le protocole NFS 4.1.
Prise en charge des formats de moteur Protobuf pour FPolicy	<p>Protobuf est le mécanisme de sérialisation des données structurées, neutre en langage de Google. Il est plus petit, plus rapide et plus simple que XML, ce qui contribue à améliorer les performances FPolicy.</p> <p>Vous pouvez utiliser le format de moteur externe protobuf. Lorsqu'ils sont définis sur protobuf, les messages de notification sont codés sous forme binaire à l'aide de Google Protobuf. Avant de définir le format du moteur externe sur protobuf, assurez-vous que le serveur FPolicy prend également en charge la désérialisation des protobuf.</p>

Mise à jour	Description
Autorisation dynamique pour les connexions SSH	ONTAP 9.15.1 fournit le cadre initial pour l'autorisation dynamique, qui offre une sécurité améliorée pour la gestion du système ONTAP en vous permettant d'attribuer un score de confiance de sécurité aux utilisateurs administrateurs et de les contester par des vérifications d'autorisation supplémentaires lorsque leur activité semble suspecte. Vous pouvez utiliser l'autorisation dynamique dans le cadre d'une architecture de sécurité Zero Trust axée sur les données.
Prise en charge de TLS 1.3 pour le stockage S3, le chiffrement FlexCache et de cluster peering	TLS 1.3 est pris en charge depuis ONTAP 9.11.1 pour la gestion de l'accès, mais il est désormais pris en charge dans ONTAP 9.15.1 pour le stockage S3, le chiffrement FlexCache et le chiffrement de cluster peering. Certaines applications, telles que FabricPool, le stockage des blobs Microsoft Azure page et SnapMirror Cloud, continuent de se limiter à l'utilisation de TLS 1.2 pour la version 9.15.1.
Prise en charge TLS des connexions NFS	<p>NFS over TLS est disponible dans ONTAP 9.15.1 en tant que préversion publique. À titre de préversion, NFS over TLS n'est pas pris en charge pour les workloads de production dans ONTAP 9.15.1.</p> <p>NFS over TLS assure le chiffrement en transit des données du système de stockage vers le client. TLS est plus récent et plus pratique que Kerberos, ce qui permet une configuration et une administration plus simples.</p>
Jeu éligible de commandes protégées par des règles étendu pour la vérification multiadministrateur	Les administrateurs peuvent créer des règles de vérification multiadministrateur pour protéger la configuration du cluster, la suppression de LUN, la configuration du système, la configuration de la sécurité pour IPsec et SAML, les opérations de snapshot de volume, la configuration du vServer et d'autres commandes.
Envoi de messages AutoSupport à l'aide de SMTP avec TLS	Bien que le transport recommandé des messages AutoSupport vers NetApp soit HTTPS, SMTP non chiffré est également disponible. Avec ONTAP 9.15.1, les clients peuvent désormais utiliser TLS avec SMTP. Le protocole SMTPS établit un canal de transport sécurisé en cryptant le trafic de messagerie ainsi que les informations d'identification facultatives du serveur de messagerie. Le protocole TLS explicite est utilisé et le protocole TLS est activé après la création de la connexion TCP. Si des copies des messages sont envoyées à des adresses e-mail locales, la même configuration est utilisée.

Efficacité du stockage

Mise à jour	Description
Modifications apportées au reporting des metrics d'espace de volume	Deux nouveaux compteurs ont été introduits et affichent uniquement les métadonnées utilisées. De plus, plusieurs des compteurs existants ont été ajustés pour supprimer les métadonnées et afficher uniquement les données utilisateur. Ensemble, ces changements offrent une vue plus claire des mesures séparées dans les deux types de données. Ces compteurs permettent aux clients de mettre en œuvre des modèles de facturation interne plus précis en actualisant les métadonnées du total et en tenant compte uniquement des données utilisateur réelles.
Efficacité du stockage avec processeur ou processeur de déchargement dédié	ONTAP assure l'efficacité du stockage et la compaction des données sur les plateformes AFF A70, AFF A90 et AFF A1K. Selon la plate-forme, la compression s'effectue à l'aide du processeur principal ou d'un processeur de déchargement dédié. L'efficacité du stockage est activée automatiquement, sans configuration.

Améliorations de la gestion des ressources de stockage

Mise à jour	Description
Prise en charge de l'écriture FlexCache	Lorsque l'écriture différée est activée sur le volume du cache, les demandes d'écriture sont envoyées vers le cache local plutôt que vers le volume d'origine, ce qui améliore les performances des environnements d'informatique en périphérie et des caches avec des charges de travail très exigeantes en écriture.
Amélioration des performances pour l'analytique de système de fichiers	ONTAP applique que 5 à 8 % de la capacité d'un volume doit être disponible lors de l'activation de l'analytique du système de fichiers, ce qui réduit les problèmes de performance potentiels pour les volumes et l'analytique du système de fichiers.
Clés de chiffrement des volumes FlexClone	Une clé de chiffrement dédiée est attribuée à un volume FlexClone, indépendamment de la clé de chiffrement (hôte) du volume FlexVol.

System Manager

Mise à jour	Description
Prise en charge de System Manager pour la configuration des relations de coffre-fort SnapLock	Les relations de coffre-fort SnapLock peuvent être configurées à l'aide de System Manager lorsque la source et la destination exécutent ONTAP 9.15.1 ou une version ultérieure.
Améliorations des performances du tableau de bord System Manager	Le tableau de bord de System Manager présente des informations détaillées sur les vues intégrité, capacité, réseau et performances. Vous y trouverez des descriptions plus complètes, notamment des améliorations des mesures de performances qui vous aideront à identifier et à résoudre les problèmes de latence ou de performances.

Mise à niveau

Mise à jour	Description
Prise en charge de la migration de LIF vers le nœud partenaire haute disponibilité lors de la mise à niveau automatisée sans interruption	Si la migration de LIF vers l'autre groupe de batchs échoue lors d'une mise à niveau automatisée sans interruption, les LIF sont migrées vers le nœud partenaire haute disponibilité dans le même groupe de batchs.

Nouveautés d'ONTAP 9.14.1

Découvrez les nouvelles fonctionnalités disponibles dans ONTAP 9.14.1.

Pour plus d'informations sur les problèmes connus, les limites et les mises en garde de mise à niveau dans les dernières versions de ONTAP 9, consultez le ["Notes de mise à jour de ONTAP 9"](#). Vous devez vous connecter avec votre compte NetApp ou créer un compte pour accéder aux notes de version.

Découvrez les nouveautés et les améliorations ["Fonctionnalités ONTAP MetroCluster"](#).

Découvrez les nouveautés et les améliorations de la prise en charge de ["Plateformes FAS, ASA et AFF, ainsi que les commutateurs pris en charge"](#).

En savoir plus sur les mises à jour du ["L'API REST DE ONTAP"](#).

Pour effectuer la mise à niveau vers la dernière version de ONTAP, reportez-vous à la section [Préparez la mise à niveau de ONTAP](#).

Protection des données

Mise à jour	Description
NVE pris en charge sur les volumes root du SVM	Les volumes root SVM peuvent être chiffrés à l'aide de clés uniques à l'aide de NetApp Volume Encryption.
Possibilité de définir le verrouillage des copies Snapshot sur des copies Snapshot de conservation à long terme et Pour réinitialiser l'horloge de conformité	Sur les clusters disposant d'une licence SnapLock, le verrouillage inviolable des copies Snapshot pour les copies Snapshot avec conservation à long terme peut être défini pour les copies Snapshot créées sur des volumes de destination non SnapLock SnapMirror et l'horloge de conformité peut être initialisée lorsqu'aucun volume SnapLock n'est présent.
La synchronisation active SnapMirror prend en charge les réservations persistantes SCIS3 et le clustering avec basculement Windows	Les réservations persistantes SCSI3 et le clustering avec basculement de fenêtre pour SnapMirror la synchronisation active prend en charge plusieurs nœuds qui accèdent à un périphérique tout en bloquant l'accès à d'autres nœuds. Ainsi, la mise en cluster de différents environnements applicatifs reste cohérente et stable.
Copiez les copies Snapshot granulaires de volume avec des groupes de cohérence	Vous pouvez utiliser des groupes de cohérence pour répliquer les copies Snapshot SnapMirror asynchrones et les copies Snapshot granulaires de volume vers les groupes de cohérence de destination afin d'ajouter une couche de reprise après incident.

Mise à jour	Description
Prise en charge de la protection des données asynchrone pour les groupes de cohérence au sein de la relation de reprise d'activité de SVM	Les SVM configurés pour la reprise d'activité SVM peuvent répliquer les informations sur le groupe de cohérence vers le site secondaire si le SVM contient un groupe de cohérence.
"Prise en charge asynchrone de SnapMirror pour 20 cibles en éventail"	Le nombre de cibles de ventilateur SnapMirror asynchrones prises en charge sur les systèmes A700 et supérieurs passe de 16 à 20 lors de l'utilisation de ONTAP 9.14.1.
Création de cache non chiffrée à partir d'une source chiffrée	Depuis ONTAP 9.14.0, FlexCache prend en charge la création d'un volume FlexCache non chiffré à partir d'une source chiffrée. Dans les versions précédentes de ONTAP, la création de FlexCache a échoué lorsque la source du cache était chiffrée.
Prise en charge de l'interface de ligne de commandes pour les groupes	Gérer les groupes de cohérence à l'aide de l'interface de ligne de commandes de ONTAP

Protocoles d'accès aux fichiers

Mise à jour	Description
Agrégation de sessions NFSv4.1	L'agrégation de session permet de créer plusieurs chemins vers un datastore exporté. Cela simplifie la gestion et améliore les performances à mesure que les charges de travail évoluent en scale-up. Elle est particulièrement adaptée aux environnements avec des workloads VMware.

MetroCluster

Mise à jour	Description
Prise en charge du stockage objet S3 sur les agrégats en miroir et sans miroir	Activez un serveur de stockage objet S3 sur une SVM dans un agrégat en miroir ou sans miroir dans les configurations MetroCluster IP et FC.
Prise en charge du provisionnement d'un compartiment S3 sur des agrégats en miroir et sans miroir dans un cluster MetroCluster	Dans les configurations MetroCluster, vous pouvez créer un compartiment sur un agrégat en miroir ou sans miroir.

Pour en savoir plus sur les améliorations apportées à la configuration des commutateurs et des plateformes pour les configurations MetroCluster, consultez ["Notes de mise à jour de ONTAP 9"](#).

Stockage objet S3

Mise à jour	Description
Le redimensionnement automatique a été activé sur les volumes FlexGroup S3 afin d'éliminer l'allocation de capacité excessive lorsque des compartiments sont créés	Lorsque des compartiments sont créés sur ou supprimés de volumes FlexGroup nouveaux ou existants, les volumes sont redimensionnés à une taille minimale requise. La taille minimale requise correspond à la taille totale de tous les compartiments S3 d'un volume FlexGroup.
Prise en charge du stockage objet S3 sur les agrégats en miroir et sans miroir	Vous pouvez activer un serveur de stockage objet S3 sur une SVM dans un agrégat en miroir ou sans miroir dans des configurations MetroCluster IP et FC.
Verrouillage des objets en fonction des rôles utilisateur et de la période de conservation des verrous	Les objets des compartiments S3 peuvent être verrouillés et ne pas être remplacés ou supprimés. La possibilité de verrouiller des objets dépend d'utilisateurs ou d'une heure spécifiques.
Configuration de l'accès pour les groupes d'utilisateurs LDAP afin de prendre en charge les services d'annuaire externes et d'ajouter une période de validité pour les clés d'accès et les clés secrètes	Les administrateurs ONTAP peuvent configurer l'accès au stockage objet ONTAP S3 pour des groupes d'utilisateurs LDAP (Lightweight Directory Access Protocol) ou Active Directory, avec la possibilité d'activer l'authentification en mode de liaison rapide LDAP. Les utilisateurs de groupes locaux ou de domaines, ou de groupes LDAP peuvent générer leurs propres clés d'accès et secrètes pour les clients S3. Vous pouvez définir une période de validité pour les clés d'accès et les clés secrètes des utilisateurs S3. ONTAP prend en charge des variables telles que <code>\$aws:username</code> pour les politiques de compartiment et les règles de groupe.

SAN

Mise à jour	Description
Découverte automatisée d'hôtes NVMe/TCP	La détection des contrôleurs hôte via le protocole NVMe/TCP est automatisée par défaut.
Reporting et résolution de problèmes côté hôte NVMe/FC	Par défaut, ONTAP prend en charge la possibilité pour les hôtes NVMe/FC d'identifier les machines virtuelles à l'aide d'un identifiant unique, et pour les hôtes NVMe/FC de surveiller l'utilisation des ressources des machines virtuelles. Cela améliore le reporting et la résolution des problèmes côté hôte.
Hiérarchisation des hôtes NVMe	Vous pouvez configurer votre sous-système NVMe de manière à hiérarchiser l'allocation des ressources pour des hôtes spécifiques. L'hôte affecté à une priorité élevée se voit attribuer un plus grand nombre de files d'attente d'E/S et des profondeurs de files d'attente plus importantes.

Sécurité

Mise à jour	Description
Prise en charge de l'authentification multifacteur Cisco DUO pour les utilisateurs SSH	Les utilisateurs SSH peuvent s'authentifier en utilisant Cisco DUO comme deuxième facteur d'authentification lors de la connexion.

Mise à jour	Description
"Améliorations apportées à la prise en charge d'OAuth 2.0"	ONTAP 9.14.1 étend la prise en charge de l'authentification basée sur les jetons de base et de l'authentification OAuth 2.0 initialement fournie avec ONTAP 9.14.0. L'autorisation peut être configurée à l'aide d'Active Directory ou LDAP avec un mappage groupe-rôle. Les jetons d'accès limités par l'expéditeur sont également pris en charge et sécurisés sur la base de MTLS (Mutual TLS). Outre Auth0 et Keycloak, Microsoft Windows Active Directory Federation Service (ADFS) est pris en charge en tant que fournisseur d'identité (IDP).
"OAuth 2.0 cadre d'autorisation"	Le framework d'autorisation ouverte (OAuth 2.0) est ajouté et fournit une authentification basée sur jeton pour les clients de l'API REST ONTAP. Cela permet une gestion et une administration plus sécurisées des clusters ONTAP à l'aide de workflows d'automatisation optimisés par des scripts d'API REST ou Ansible. Les fonctionnalités standard d'OAuth 2.0 sont prises en charge, notamment l'émetteur, le public, la validation locale, l'introspection à distance, demande d'utilisateur à distance et prise en charge du proxy. L'autorisation du client peut être configurée à l'aide des étendues OAuth 2.0 autonomes ou en mappant les utilisateurs ONTAP locaux. Les fournisseurs d'identités pris en charge incluent Auth0 et Keycloak utilisant plusieurs serveurs simultanés.
Alertes réglables pour la protection anti-ransomware autonome	Configurez la protection anti-ransomware autonome pour recevoir des notifications lorsqu'une nouvelle extension de fichier est détectée ou lorsqu'une copie Snapshot ARP est prise, et recevoir un avertissement préalable concernant d'éventuels événements de ransomware.
FPolicy prend en charge les magasins persistants pour réduire la latence	FPolicy vous permet de configurer un magasin persistant pour capturer les événements d'accès aux fichiers pour des règles asynchrones non obligatoires dans la SVM. Les magasins persistants peuvent aider à découpler le traitement des E/S client du traitement des notifications FPolicy afin de réduire la latence du client. Les configurations obligatoires synchrones et asynchrones ne sont pas prises en charge.
FPolicy prend en charge les volumes FlexCache sur SMB	FPolicy est pris en charge pour les volumes FlexCache avec NFS ou SMB. Auparavant, FPolicy n'était pas pris en charge pour les volumes FlexCache avec SMB.

Efficacité du stockage

Mise à jour	Description
Suivi des analyses dans File System Analytics	Suivez l'analyse d'initialisation de l'analyse du système de fichiers avec des informations en temps réel sur la progression et l'accélération.
Augmentation de l'espace utilisable dans l'agrégat sur les plateformes FAS	Pour les plateformes FAS, la réserve WAFL pour les agrégats de plus de 30 To est réduite de 10 % à 5 %, ce qui entraîne une augmentation de l'espace utilisable dans l'agrégat.

Mise à jour	Description
Modification de la génération de rapports sur l'espace physique utilisé dans les volumes TSSE	<p>Sur les volumes sur lesquels l'efficacité du stockage sensible à la température est activée, la mesure de la CLI ONTAP qui indique la quantité d'espace utilisée dans le volume inclut les économies d'espace réalisées grâce à la technologie TSSE. Cette mesure est reflétée dans les commandes <code>volume show -physique-used</code> et <code>volume show-space -physique Used</code>.</p> <p>Pour FabricPool, la valeur de <code>-physical-used</code> est une combinaison du tier de capacité et du tier de performance.</p> <p>Pour des commandes spécifiques, voir lien: https://docs.netapp.com/us-en/ontap-cli-9141/volume-show.html[<code>volume show^</code>] et <code>volume show space</code>.</p>

Améliorations de la gestion des ressources de stockage

Mise à jour	Description
Rééquilibrage proactif des FlexGroup	Les volumes FlexGroup prennent en charge le déplacement automatique des fichiers croissants d'un répertoire vers un composant distant afin de réduire les goulets d'étranglement d'E/S sur le composant local.
Balisage des copies Snapshot dans les volumes FlexGroup	Vous pouvez ajouter, modifier et supprimer des balises et des libellés (commentaires) dans pour identifier les copies Snapshot et éviter de supprimer accidentellement des copies Snapshot dans des volumes FlexGroup.
Écrivez directement dans le cloud avec FabricPool	FabricPool permet en outre d'écrire des données sur un volume dans FabricPool. Celles-ci sont ainsi envoyées directement vers le cloud sans attendre l'analyse du Tiering.
Une lecture anticipée agressive avec FabricPool	FabricPool fournit des fichiers à lecture anticipée agressive, comme les flux de films sur les volumes FabricPool, pour garantir qu'aucune image n'est supprimée.

Améliorations de la gestion des SVM

Mise à jour	Description
Prise en charge de la mobilité des données des SVM pour la migration des SVM contenant les quotas d'utilisateurs et de groupes et les qtrees	La mobilité des données par SVM permet de prendre en charge la migration des SVM contenant les quotas d'utilisateurs et de groupes et les qtrees.
Prise en charge d'un maximum de 400 volumes par SVM, d'un maximum de 12 paires HA et de pNFS avec NFS 4.1 en utilisant la mobilité des données SVM	Le nombre maximal de volumes pris en charge par SVM avec la mobilité des données SVM augmente à 400 et le nombre de paires haute disponibilité prises en charge passe à 12.

System Manager

Mise à jour	Description
Prise en charge du basculement de test SnapMirror	Vous pouvez utiliser System Manager pour effectuer des répétitions de basculement de test SnapMirror sans interrompre les relations SnapMirror existantes.
Gestion des ports dans un domaine de diffusion	Vous pouvez utiliser System Manager pour modifier ou supprimer les ports attribués à un broadcast domain.
Activation du basculement automatique non planifié assisté par Mediator (MAUSO)	Vous pouvez utiliser System Manager pour activer ou désactiver le basculement automatique non planifié (MAUSO) assisté par le Mediator lors d'un basculement et d'un rétablissement IP MetroCluster.
Cluster et volumétrie balisage	Vous pouvez utiliser System Manager pour utiliser des balises afin de catégoriser les clusters et les volumes de différentes manières, par exemple, par objectif, propriétaire ou environnement. Ceci est utile lorsqu'il existe de nombreux objets du même type. Les utilisateurs peuvent rapidement identifier un objet spécifique en fonction des balises qui lui ont été attribuées.
Prise en charge améliorée du contrôle de groupe de cohérence	System Manager affiche les données historiques relatives à l'utilisation des groupes de cohérence.
Authentification intrabande NVMe	Vous pouvez utiliser System Manager pour configurer l'authentification sécurisée, unidirectionnelle et bidirectionnelle entre un hôte et un contrôleur NVMe via les protocoles NVMe/TCP et NVMe/FC à l'aide du protocole d'authentification DH-HMAC-CHAP.
Prise en charge de la gestion du cycle de vie des compartiments S3 étendue à System Manager	Vous pouvez utiliser System Manager pour définir des règles de suppression d'objets spécifiques d'un compartiment et, par le biais de ces règles, pour expirer ces objets de compartiment.

Nouveautés d'ONTAP 9.13.1

Découvrez les nouvelles fonctionnalités disponibles dans ONTAP 9.13.1.

Pour plus d'informations sur les problèmes connus, les limites et les mises en garde de mise à niveau dans les dernières versions de ONTAP 9, consultez le ["Notes de mise à jour de ONTAP 9"](#). Vous devez vous connecter avec votre compte NetApp ou créer un compte pour accéder aux notes de version.

Découvrez les nouveautés et les améliorations ["Fonctionnalités ONTAP MetroCluster"](#).

Découvrez les nouveautés et les améliorations de la prise en charge de ["Plateformes FAS, ASA et AFF, ainsi que les commutateurs pris en charge"](#).

En savoir plus sur les mises à jour du ["L'API REST DE ONTAP"](#).

Pour mettre à niveau ONTAP, voir [Préparez la mise à niveau de ONTAP](#).

Protection des données

Mise à jour	Description
"Vérification multi-administrateurs"	L'administrateur du cluster peut explicitement activer la vérification multiadministrateur sur un cluster afin de demander l'approbation du quorum avant l'exécution de certaines opérations SnapLock.
"Prise en charge améliorée de la gestion des groupes de cohérence, notamment le déplacement de volumes et la géométrie"	Vous pouvez déplacer des volumes entre des groupes de cohérence, modifier la géométrie des groupes de cohérence hiérarchiques et obtenir des informations sur la capacité des groupes de cohérence. System Manager prend en charge la création d'un groupe de cohérence avec de nouveaux volumes NAS ou des espaces de noms NVME.
"Restauration NDMP avec SnapMirror synchrone"	La restauration NDMP est prise en charge avec SnapMirror synchrone.
Amélioration de la synchronisation active SnapMirror	<ul style="list-style-type: none"> • "Ajoutez des volumes à un groupe de cohérence sans interruption avec une relation active SnapMirror." • "Utilisation de la restauration NDMP avec SnapMirror actif Sync".
"Prise en charge asynchrone de SnapMirror avec un seul groupe de cohérence"	Les groupes de cohérence prennent en charge les configurations SnapMirror asynchrones, ce qui permet l'archivage des sauvegardes SnapMirror pour les groupes de cohérence uniques.

Protocoles d'accès aux fichiers

Mise à jour	Description
"Prise en charge des pools de stockage NFSv4.x"	Quelques clients consomment trop de ressources de pool de stockage NFSv4.x, ce qui entraîne le blocage d'autres clients NFSv4.x en raison de l'indisponibilité des ressources de pool de stockage NFSv4.x. Vous pouvez activer le refus et le blocage des clients qui consomment une grande ressource de pool de stockage NFSv4.x dans leurs environnements.

MetroCluster

Mise à jour	Description
"Transition de MetroCluster FC vers MetroCluster IP à l'aide d'un commutateur partagé pour le stockage MetroCluster IP et le stockage connecté Ethernet"	Vous pouvez passer d'une configuration FC MetroCluster à une configuration IP MetroCluster (ONTAP 9.8 et versions ultérieures) sans interruption grâce à un commutateur partagé.
"Transitions sans interruption entre une configuration FC MetroCluster à huit nœuds et une configuration IP MetroCluster"	Vous pouvez migrer vos charges de travail et vos données sans interruption à partir d'une configuration MetroCluster FC à huit nœuds vers une nouvelle configuration MetroCluster IP.

Mise à jour	Description
"Mise à niveau de la configuration IP MetroCluster à quatre nœuds via le basculement et le rétablissement"	Mettez à niveau les contrôleurs d'une configuration IP MetroCluster à quatre nœuds en utilisant le basculement et le rétablissement avec <code>system controller replace</code> commandes.
"Le basculement automatique non planifié (MAUSO) assisté par un médiateur est déclenché en cas d'arrêt de l'environnement"	Si un site s'arrête normalement en raison d'un arrêt environnemental, MAUSO est déclenché.
"Prise en charge des configurations IP MetroCluster à 8 nœuds"	Vous pouvez mettre à niveau les contrôleurs et le stockage dans une configuration IP MetroCluster à huit nœuds en développant la configuration pour devenir une configuration temporaire à douze nœuds, puis en supprimant les anciens groupes DR.
"Conversion de la configuration IP de MetroCluster en une configuration de commutateur MetroCluster de stockage partagé"	Vous pouvez convertir une configuration IP MetroCluster en une configuration de commutateur MetroCluster de stockage partagé.

Pour en savoir plus sur les améliorations apportées à la configuration des commutateurs et des plateformes pour les configurations MetroCluster, consultez ["Notes de mise à jour de ONTAP 9"](#).

Mise en réseau

Mise à jour	Description
Prise en charge matérielle étendue pour l'interconnexion de cluster RDMA	ONTAP prend en charge les systèmes AFF A900, ASA A900 et FAS9500 pour le RDMA d'interconnexion de cluster avec une carte réseau de cluster X91153A, ce qui contribue à réduire la latence, les temps de basculement et à accélérer la communication entre les nœuds.
Augmentation des limites LIF de données	ONTAP améliore la flexibilité en augmentant les limites d'évolutivité des LIF de données pour les paires haute disponibilité et les clusters.
Prise en charge d'IPv6 lors de la configuration de clusters sur les plateformes A800 et FAS8700	Sur les plateformes A800 et FAS8700, vous pouvez utiliser l'interface de ligne de commandes ONTAP pour créer et configurer de nouveaux clusters dans des environnements réseau IPv6 uniquement.

Stockage objet S3

Mise à jour	Description
Gestion du cycle de vie des compartiments S3	Les actions d'expiration des objets S3 définissent la date d'expiration des objets d'un compartiment. Cette fonctionnalité vous permet de gérer les versions d'objets afin de répondre aux exigences de conservation et de gérer efficacement le stockage objet S3 global.

SAN

Mise à jour	Description
Prise en charge de NVMe/FC sur les hôtes AIX	ONTAP prend en charge le protocole NVMe/FC sur des hôtes AIX. Voir la "Outil d'interopérabilité NetApp" pour les configurations prises en charge.

Sécurité

Fonction	Description
Protection autonome contre les ransomwares	<ul style="list-style-type: none">• Fonctionnalité de vérification multiadministrateur avec la protection anti-ransomware autonome• Passage automatique du mode d'apprentissage au mode actif• Prise en charge de FlexGroup, Notamment les analyses et la création de rapports pour les volumes FlexGroup et les opérations, notamment l'extension d'un volume FlexGroup, les conversions FlexVol vers FlexGroup et le rééquilibrage FlexGroup.
Authentification de clé publique SSH avec Active Directory	Vous pouvez utiliser une clé publique SSH comme méthode d'authentification principale avec un utilisateur Active Directory (AD), ou vous pouvez utiliser une clé publique SSH comme méthode d'authentification secondaire après un utilisateur AD.
Certificats X.509 avec clés publiques SSH	ONTAP vous permet d'associer un certificat X.509 à la clé publique SSH d'un compte, ce qui vous offre la sécurité supplémentaire des vérifications d'expiration et de révocation des certificats lors de la connexion SSH.
Notification d'échec d'accès aux fichiers FPolicy	FPolicy prend en charge les notifications pour les événements d'accès refusé. Les notifications sont générées pour l'opération de fichier ayant échoué en raison d'un manque d'autorisation, ce qui inclut : échec dû aux autorisations NTFS, échec dû aux bits du mode Unix et échec dû aux ACL NFSv4.
Authentification multifacteur avec TOTP (mots de passe à usage unique basés sur le temps)	Configurez des comptes utilisateur locaux avec authentification multifacteur à l'aide d'un mot de passe à usage unique (TOTP). Le TOTP est toujours utilisé comme deuxième méthode d'authentification. Vous pouvez utiliser une clé publique SSH ou un mot de passe utilisateur comme méthode d'authentification principale.

Efficacité du stockage

Mise à jour	Description
Modification des rapports concernant le taux de réduction des données primaires dans System Manager	Le taux de réduction des données primaires affiché dans System Manager n'inclut plus les économies d'espace de la copie Snapshot dans le calcul. Il ne représente que le rapport entre l'espace logique utilisé et l'espace physique utilisé. Dans les versions précédentes d'ONTAP, le taux de réduction des données primaires incluait une réduction d'espace considérable des copies Snapshot. Par conséquent, lorsque vous effectuez une mise à niveau vers ONTAP 9.13.1, vous constatez un ratio primaire significativement inférieur. Vous pouvez toujours voir les taux de réduction des données avec les copies Snapshot dans la vue de détails capacité .
Efficacité du stockage sensible à la température	L'efficacité du stockage sensible à la température ajoute la compaction séquentielle de blocs physiques contigus pour améliorer l'efficacité du stockage. Sur les volumes dont l'efficacité du stockage sensible à la température est activée, la compression séquentielle est automatiquement activée lorsque les systèmes sont mis à niveau vers ONTAP 9.13.1.
Application de l'espace logique	La mise en œuvre d'espace logique est prise en charge sur les destinations SnapMirror.
Limites de capacité des VM de stockage prises en charge	Vous pouvez définir des limites de capacité sur une machine virtuelle de stockage (SVM) et activer des alertes lorsque la SVM approche un seuil de pourcentage.

Améliorations de la gestion des ressources de stockage

Mise à jour	Description
Augmentation du nombre maximum d'inodes	ONTAP continuera à ajouter automatiquement des inodes (à raison de 1 inode par 32 Ko d'espace volume) même si le volume dépasse les 680 Go. ONTAP continuera d'ajouter des inodes jusqu'à ce qu'il atteigne le maximum de 2,147,483,632.
Prise en charge de la spécification d'un type de SnapLock lors de la création de FlexClone	Vous pouvez spécifier l'un des trois types de SnapLock suivants : conformité, entreprise ou non SnapLock, lors de la création d'un volume FlexClone en lecture/écriture.
Activer l'analyse du système de fichiers par défaut	Définissez l'option analyse du système de fichiers sur activée par défaut sur les nouveaux volumes.
Relations de type « fan-out » pour la reprise d'activité SVM avec les volumes FlexGroup	La restriction de fanout du SVM DR avec des volumes FlexGroup est supprimée. La solution SVM DR avec FlexGroup prend en charge les relations de ventilateur SnapMirror vers huit sites.
Opération de rééquilibrage d'une seule baie FlexGroup	Vous pouvez planifier le début d'une opération de rééquilibrage FlexGroup à une date et une heure que vous spécifiez à l'avenir.

Mise à jour	Description
Performances de lecture FabricPool	FabricPool offre une meilleure performance de lecture séquentielle pour les charges de travail à flux unique et multiples pour les données hébergées dans le cloud, ainsi qu'un débit de Tiering amélioré. Cette amélioration peut envoyer un taux plus élevé d'objets et de transferts vers le magasin d'objets back-end. Dans le cas de référentiels de stockage en mode objet sur site, il est conseillé de tenir compte de la marge de performance du service de magasin d'objets pour déterminer si une régulation des FabricPool PUT est nécessaire.
Modèles de règles de QoS adaptative	Les modèles de règles de QoS adaptative vous permettent de définir des étages de débit au niveau des SVM.

Améliorations de la gestion des SVM

Mise à jour	Description
Mobilité des données des SVM	Prise en charge accrue de la migration des SVM contenant jusqu'à 200 volumes.
Prise en charge de la recréation des répertoires des SVM	Nouvelle commande CLI <code>debug vservers refresh-vservers-dir -node node_name</code> recrée les répertoires et fichiers manquants. Pour plus d'informations sur la syntaxe des commandes, reportez-vous à la section "Référence des commandes ONTAP" .

System Manager

Depuis ONTAP 9.12.1, System Manager est intégré à BlueXP. En savoir plus sur [Intégration de System Manager à BlueXP](#).

Mise à jour	Description
Modification du rapport sur le taux de réduction des données primaires	Le taux de réduction des données primaires affiché dans System Manager n'inclut plus les économies d'espace de la copie Snapshot dans le calcul. Il ne représente que le rapport entre l'espace logique utilisé et l'espace physique utilisé. Dans les versions précédentes d'ONTAP, le taux de réduction des données primaires incluait une réduction d'espace considérable des copies Snapshot. Par conséquent, lorsque vous effectuez une mise à niveau vers ONTAP 9.13.1, vous constatez un ratio primaire significativement inférieur. Vous pouvez toujours voir les taux de réduction des données avec les copies Snapshot dans la vue Détails sur la capacité.
Verrouillage inviolable des copies Snapshot	Vous pouvez utiliser System Manager pour verrouiller une copie Snapshot sur un volume non SnapLock afin de vous protéger contre les attaques par ransomware.
Prise en charge des gestionnaires de clés externes	System Manager vous permet de gérer des gestionnaires de clés externes afin de stocker et de gérer les clés d'authentification et de chiffrement.

Mise à jour	Description
Dépannage des problèmes matériels	<p>Les utilisateurs de System Manager peuvent afficher des représentations visuelles de plates-formes matérielles supplémentaires dans la page « matériel », y compris les plates-formes ASA et AFF série C.</p> <p>La prise en charge des plates-formes AFF C-Series est également incluse dans les dernières versions de correctifs de ONTAP 9.12.1, ONTAP 9.11.1 et ONTAP 9.10.1.</p> <p>Les visualisations identifient les problèmes ou les problèmes liés aux plates-formes, fournissant ainsi aux utilisateurs une méthode rapide pour résoudre les problèmes matériels.</p>

Nouveautés d'ONTAP 9.12.1

Découvrez les nouvelles fonctionnalités disponibles dans ONTAP 9.12.1.

Pour plus d'informations sur les problèmes connus, les limites et les mises en garde de mise à niveau dans les dernières versions de ONTAP 9, consultez le ["Notes de mise à jour de ONTAP 9"](#). Vous devez vous connecter avec votre compte NetApp ou créer un compte pour accéder aux notes de version.

Découvrez les nouveautés et les améliorations ["Fonctionnalités ONTAP MetroCluster"](#).

Découvrez les nouveautés et les améliorations de la prise en charge de ["Plateformes FAS, ASA et AFF, ainsi que les commutateurs pris en charge"](#).

En savoir plus sur les mises à jour du ["L'API REST DE ONTAP"](#).

Pour mettre à niveau ONTAP, voir [Préparez la mise à niveau de ONTAP](#).

Protection des données

Mise à jour	Description
Prise en charge de volumes FlexVol plus importants avec SnapMirror synchrone	La taille maximale du volume FlexVol pris en charge dans les configurations SnapMirror synchrone est passée de 100 To à 300 To. Les clusters source et destination doivent tous deux exécuter <i>ONTAP 9.12.1P2 ou ultérieure</i> .
Prise en charge de fichiers et de LUN de plus grande taille dans SnapMirror synchrone	La taille maximale de fichier et de LUN prise en charge dans les configurations SnapMirror synchrone est passée de 16 To à 128 To. Le cluster source et le cluster destination doivent tous deux exécuter ONTAP 9.12.1 P2 ou une version ultérieure.
Prise en charge améliorée des groupes de cohérence	<ul style="list-style-type: none"> Vous pouvez ajouter et supprimer des volumes d'un groupe de cohérence et cloner un groupe de cohérence (y compris à partir d'une copie Snapshot). Les groupes de cohérence prennent en charge le balisage des applications pour rationaliser les processus de protection et de gestion des données. L'API REST ONTAP prend en charge la configuration des groupes de cohérence avec des volumes NFS/SMB ou des espaces de noms NVMe.

Mise à jour	Description
CONTINUITÉ DE L'ACTIVITÉ SnapMirror synchrone	SnapMirror synchrone prend en charge la CONTINUITÉ de L'ACTIVITÉ (NDO) des basculements et retours HA, du déplacement de volumes et d'autres opérations de maintenance. Cette fonctionnalité est uniquement disponible sur les plateformes AFF/ASA.
Le médiateur ONTAP 1.5 prend en charge la continuité de l'activité SnapMirror	Le médiateur ONTAP 1.5 est disponible pour la surveillance des relations de synchronisation active SnapMirror.
Amélioration de la continuité de la synchronisation active SnapMirror	La synchronisation active SnapMirror prend en charge la restauration partielle de LUN à partir des snapshots. De plus, la synchronisation active SnapMirror étend la qualité de service aux volumes qui ne font pas partie de la relation SnapMirror.
Indicateur de reconstruction d'entrepôt de données pour SnapMirror asynchrone	SnapMirror asynchrone fournit un indicateur indiquant la durée de reconstruction d'un entrepôt de données après une répétition de reprise d'activité en affichant le pourcentage effectué.
Option SnapLock pour définir une durée de rétention absolue « non spécifiée »	SnapLock inclut une option permettant de définir une durée de conservation minimale lorsque la durée de conservation absolue est définie sur « non spécifiée ».
Copies Snapshot inviolables	Vous pouvez verrouiller une copie Snapshot sur un volume non SnapLock afin de protéger les données contre les attaques par ransomware. Le verrouillage des copies Snapshot permet de s'assurer qu'elles ne sont pas supprimées accidentellement ou de manière malveillante.

Protocoles d'accès aux fichiers

Mise à jour	Description
Désactivez les types de cryptage faibles pour les communications Kerberos	Une nouvelle option de sécurité SMB vous permet de désactiver RC4 et DES en faveur DES types de cryptage AES (Advanced Encryption Standard) pour les communications Kerberos avec le KDC Active Directory (AD).
Accès client S3 aux données NAS	Les clients S3 peuvent accéder aux mêmes données NAS que les clients NFS et SMB sans reformatage, ce qui facilite le service des applications S3 qui nécessitent des données d'objet.
Attributs étendus NFS	Les serveurs NFS activés pour NFSv4.2 peuvent stocker et récupérer des attributs étendus NFS (xattrs) à partir de clients compatibles xattr.
Prise en charge des fichiers éparses NFSv4.2 et de la réservation d'espace	Le client NFSv4.2 peut réserver de l'espace pour un fichier fragmenté. L'espace peut également être désalloué et non réservé à partir d'un fichier.

MetroCluster

Mise à jour	Description
ONTAP Mediator 1.5 est pris en charge dans une configuration MetroCluster IP	Le Mediator 1.5 de ONTAP est disponible pour la surveillance des configurations IP de MetroCluster.

Mise à jour	Description
La prise en charge IPSec pour le protocole hôte frontal (tel que NFS et iSCSI) est disponible dans les configurations FAS MetroCluster IP et MetroCluster.	La prise en charge IPSec pour le protocole hôte frontal (tel que NFS et iSCSI) est disponible dans les configurations FAS MetroCluster IP et MetroCluster.
"Fonction de basculement forcé automatique MetroCluster dans une configuration MetroCluster IP"	Vous pouvez activer la fonction de basculement automatique forcé MetroCluster dans une configuration MetroCluster IP. Cette fonction est une extension de la fonction de basculement non planifié assisté par un médiateur (MAUSO).
"S3 sur un SVM sur un agrégat sans miroir en configuration MetroCluster IP"	Vous pouvez activer la fonction de basculement automatique forcé MetroCluster dans une configuration MetroCluster IP. Cette fonction est une extension de la fonction de basculement non planifié assisté par un médiateur (MAUSO).

Pour en savoir plus sur les améliorations apportées à la configuration des commutateurs et des plateformes pour les configurations MetroCluster, consultez ["Notes de mise à jour de ONTAP 9"](#).

Mise en réseau

Mise à jour	Description
Services LIF	Vous pouvez utiliser le <code>management-log-forwarding</code> Service permettant de contrôler les LIF utilisées pour transférer les journaux d'audit à un service syslog distant

Stockage objet S3

Mise à jour	Description
Prise en charge étendue des actions S3	Les actions de l'API Amazon S3 suivantes sont prises en charge : <ul style="list-style-type: none"> • <code>CopyObject</code> • <code>UploadPartCopy</code> • <code>BucketPolicy</code> (OBTENIR, PLACER, SUPPRIMER)

SAN

Mise à jour	Description
Taille maximale de LUN augmentée pour les plateformes AFF et FAS	À partir de ONTAP 9.12.1P2, la taille maximale de LUN prise en charge sur les plateformes AFF et FAS est passée de 16 To à 128 To.

Mise à jour	Description
"Augmentation des limites NVMe"	Le protocole NVMe prend en charge les éléments suivants : <ul style="list-style-type: none"> • Sous-systèmes de 8 Ko dans une VM de stockage unique et un cluster unique • Clusters de 12 nœuds NVMe/FC prend en charge 256 contrôleurs par port et NVMe/TCP prend en charge 2 contrôleurs par nœud.
Prise en charge de NVMe/TCP pour l'authentification sécurisée	L'authentification sécurisée, unidirectionnelle et bidirectionnelle entre un hôte et un contrôleur NVMe est prise en charge via NVMe/TCP à l'aide du protocole d'authentification DHHMAC-CHAP.
Prise en charge de MetroCluster IP pour NVMe	Le protocole NVMe/FC est pris en charge dans les configurations IP MetroCluster à 4 nœuds.

Sécurité


En octobre 2022, NetApp a mis en œuvre des modifications pour rejeter les transmissions de messages AutoSupport qui ne sont pas envoyées par HTTPS avec TLSv1.2 ou SMTP sécurisé. Pour plus d'informations, voir "SU484 : NetApp rejette les messages AutoSupport transmis avec une sécurité de transport insuffisante".

Fonction	Description
Améliorations de l'interopérabilité de la protection anti-ransomware autonome	La protection anti-ransomware autonome est disponible pour les configurations suivantes : <ul style="list-style-type: none"> • Volumes protégés par SnapMirror • Les SVM sont protégés par SnapMirror • SVM activé pour la migration (mobilité des données des SVM)
Prise en charge de l'authentification multifacteur (MFA) pour SSH avec FIDO2 et PIV (tous deux utilisés par Yubikey)	SSH MFA peut utiliser l'échange de clés publiques/privées assisté par matériel avec le nom d'utilisateur et le mot de passe. Yubikey est un dispositif à jeton physique connecté au client SSH afin d'améliorer la sécurité MFA.
Enregistrement inviolable	Tous les journaux internes de ONTAP sont inviolables par défaut, ce qui permet de s'assurer que les comptes d'administrateur compromis ne peuvent pas masquer les actions malveillantes.
Transport TLS pour les événements	Les événements EMS peuvent être envoyés à un serveur syslog distant à l'aide du protocole TLS, améliorant ainsi la protection sur le réseau pour la journalisation d'audit externe centrale.

Efficacité du stockage

Mise à jour	Description
Efficacité du stockage sensible à la température	L'efficacité du stockage sensible à la température est activée par défaut sur les nouveaux volumes et plates-formes AFF C250, AFF C400 et AFF C800. Le TSSE n'est pas activé par défaut sur les volumes existants mais peut être activé manuellement à l'aide de l'interface de ligne de commande ONTAP.
Augmentation de l'espace utilisable dans l'agrégat	Pour les plateformes FAS 100 % Flash (AFF) et FAS500f, la réserve WAFL pour les agrégats de plus de 30 To est réduite de 10 % à 5 %, ce qui entraîne une augmentation de l'espace utilisable dans l'agrégat.
Analyse du système de fichiers : les meilleurs répertoires par taille	L'analyse du système de fichiers identifie désormais les répertoires d'un volume qui consomment le plus d'espace.

Améliorations de la gestion des ressources de stockage

Mise à jour	Description
Rééquilibrage FlexGroup	<p>Vous pouvez activer le rééquilibrage automatique des volumes FlexGroup sans interruption pour redistribuer les fichiers entre des composants FlexGroup.</p> <div>  <p>Il est recommandé de ne pas utiliser le rééquilibrage automatique des FlexGroup après une conversion de FlexVol en FlexGroup. Vous pouvez utiliser la fonctionnalité de déplacement de fichier avec effet rétroactif disruptive disponible dans ONTAP 9.10.1 et versions ultérieures, en entrant le volume rebalance file-move commande. Pour plus d'informations sur la syntaxe des commandes, reportez-vous à la section "Référence des commandes ONTAP".</p> </div>
Prise en charge de SnapLock pour SnapVault pour les volumes FlexGroup	Prise en charge de SnapLock pour SnapVault pour les volumes FlexGroup

Améliorations de la gestion des SVM

Mise à jour	Description
Amélioration de la mobilité des données SVM	<p>Les administrateurs de cluster peuvent déplacer un SVM d'un cluster source vers un cluster de destination sans interruption à l'aide de FAS, de plateformes AFF, sur des agrégats hybrides.</p> <p>La prise en charge du protocole SMB perturbateur et la protection anti-ransomware autonome ont été ajoutées.</p>

System Manager

Depuis ONTAP 9.12.1, System Manager est intégré à BlueXP. Avec BlueXP, les administrateurs peuvent gérer

l'infrastructure multicloud hybride à partir d'un seul plan de contrôle, tout en conservant le tableau de bord familier de System Manager. Lors de la connexion à System Manager, les administrateurs peuvent accéder à l'interface System Manager dans BlueXP ou accéder directement à System Manager. En savoir plus sur [Intégration de System Manager à BlueXP](#).

Mise à jour	Description
Prise en charge de System Manager pour SnapLock	System Manager prend en charge les opérations SnapLock, notamment l'initialisation Compliance Clock, la création de volume SnapLock et la mise en miroir de fichiers WORM.
Visualisation matérielle du câblage	Les utilisateurs de System Manager peuvent afficher des informations de connectivité sur le câblage entre les périphériques matériels de leur cluster afin de résoudre les problèmes de connectivité.
Prise en charge de l'authentification multifacteur avec Cisco DUO lors de la connexion à System Manager	Vous pouvez configurer Cisco DUO en tant que fournisseur d'identités SAML, ce qui permet aux utilisateurs de s'authentifier à l'aide de Cisco DUO lorsqu'ils se connectent à System Manager.
Améliorations de la mise en réseau de System Manager	System Manager offre un contrôle accru sur le sous-réseau et le choix du port de départ lors de la création de l'interface réseau. System Manager prend également en charge la configuration de NFS sur les connexions RDMA.
Thèmes d'affichage du système	Les utilisateurs de System Manager peuvent sélectionner un thème clair ou foncé pour l'affichage de l'interface de System Manager. Ils peuvent également choisir le thème par défaut utilisé pour leur système d'exploitation ou leur navigateur. Cette fonction permet aux utilisateurs de spécifier un paramètre plus confortable pour la lecture de l'affichage.
Améliorations des détails de capacité du niveau local	Les utilisateurs de System Manager peuvent afficher les détails de capacité de niveaux locaux spécifiques afin de déterminer si l'espace est sur-alloué. Cela peut indiquer qu'ils doivent ajouter de la capacité pour s'assurer que l'espace n'est pas insuffisant au niveau local.
Recherche améliorée	La fonctionnalité de recherche améliorée de System Manager permet aux utilisateurs de rechercher et d'accéder aux informations de support pertinentes et contextuelles, ainsi qu'aux documents relatifs à System Manager depuis le site du support NetApp, directement via l'interface du gestionnaire système. Les utilisateurs peuvent ainsi acquérir les informations dont ils ont besoin pour prendre les mesures appropriées sans avoir à effectuer de recherche à différents emplacements sur le site du support.
Amélioration du provisionnement de volumes	Les administrateurs du stockage peuvent choisir une règle de copie Snapshot lors de la création d'un volume à l'aide de System Manager plutôt que d'utiliser la règle par défaut.
Augmenter la taille d'un volume	Les administrateurs du stockage peuvent visualiser l'impact sur l'espace de données et la réserve de copies Snapshot lorsqu'ils utilisent System Manager pour redimensionner un volume.
Pool de stockage et Flash Pool gestion	Les administrateurs du stockage peuvent utiliser System Manager pour ajouter des disques SSD à un pool de stockage SSD, créer des niveaux locaux Flash Pool (agrégat) à l'aide d'unités d'allocation de pools de stockage SSD et créer des niveaux locaux Flash Pool à l'aide de disques SSD physiques.

Mise à jour	Description
Prise en charge de NFS sur RDMA dans System Manager	System Manager prend en charge les configurations d'interface réseau pour NFS sur RDMA et identifie les ports compatibles RoCE.

Nouveautés d'ONTAP 9.11.1

Découvrez les nouvelles fonctionnalités disponibles dans ONTAP 9.11.1.

Pour plus d'informations sur les problèmes connus, les limites et les mises en garde de mise à niveau dans les dernières versions de ONTAP 9, consultez le ["Notes de mise à jour de ONTAP 9"](#). Vous devez vous connecter avec votre compte NetApp ou créer un compte pour accéder aux notes de version.


Découvrez les nouveautés et les améliorations ["Fonctionnalités ONTAP MetroCluster"](#).

Découvrez les nouveautés et les améliorations de la prise en charge de ["Plateformes FAS, ASA et AFF, ainsi que les commutateurs pris en charge"](#).

En savoir plus sur les mises à jour du ["L'API REST DE ONTAP"](#).

Pour effectuer la mise à niveau vers la dernière version de ONTAP, reportez-vous à la section [Préparez la mise à niveau de ONTAP](#).

Protection des données

Mise à jour	Description
Mettre en cluster des serveurs de clés externes	La prise en charge des serveurs de gestion externe des clés en cluster est ajoutée pour les partenaires NetApp qui proposent une solution de serveur KMIP en cluster. Cela permet d'ajouter des serveurs KMIP principaux et secondaires afin d'éviter la duplication des données de clé de chiffrement. Pour les partenaires pris en charge, consultez le "Matrice d'interopérabilité" .
Règle asynchrone SnapMirror dans System Manager	<p>Vous pouvez utiliser System Manager pour ajouter des règles de miroir et de copie pré-crées et personnalisées, afficher des règles héritées et remplacer les planifications de transfert définies dans une règle de protection lors de la protection des volumes et des machines virtuelles de stockage. Vous pouvez également utiliser System Manager pour modifier vos relations de protection de volumes et de machines virtuelles de stockage.</p> <div>  <p>Si vous exécutez ONTAP 9.8P12 ou une version ultérieure de ONTAP 9.8, avez configuré SnapMirror à l'aide de System Manager et envisagez une mise à niveau vers ONTAP 9.9.1 ou ONTAP 9.10.1, utilisez ONTAP 9.9.1P13 ou version ultérieure et ONTAP 9.10.1P10 ou version ultérieure pour votre mise à niveau.</p> </div>

Mise à jour	Description
Restauration du répertoire unique de SnapMirror Cloud	Permet au cluster d'administrer au niveau de privilège d'administration d'effectuer une opération de restauration de répertoire unique à partir d'un terminal cloud. L'UUID du point de terminaison source doit être fourni pour identifier le point de terminaison de sauvegarde à partir duquel vous effectuez la restauration. Car plusieurs sauvegardes peuvent utiliser la même <code>cloud_endpoint_name</code> . En tant que destination, l'UUID associé à la sauvegarde doit être fourni pour la commande <code>restore</code> . Vous pouvez utiliser le <code>snapmirror show</code> pour obtenir le <code>source_endpoint_uuid</code> .
Prise en charge améliorée de la synchronisation active SnapMirror	<ul style="list-style-type: none"> La synchronisation active SnapMirror prend en charge AIX en tant qu'hôte La synchronisation active SnapMirror prend en charge l'SnapRestore à fichier unique, ce qui vous permet de restaurer un LUN individuel ou un fichier normal dans une configuration de synchronisation active SnapMirror.
Resynchronisation rapide de la réplication des données SVM	La resynchronisation rapide de la réplication des données d'un SVM permet aux administrateurs du stockage d'éviter la reconstruction complète d'un data warehouse et de restaurer plus rapidement ces données après une répétition de la reprise d'activité.
Prise en charge de la réplication des données SVM avec MetroCluster	La source SVM-DR est supportée des deux côtés d'une configuration MetroCluster.
Groupe de cohérence en deux phases création de la copie Snapshot	Dans l'API REST, les groupes de cohérence prennent en charge une procédure Snapshot en deux phases, ce qui vous permet d'effectuer un précontrôle avant de valider le Snapshot.

Protocoles d'accès aux fichiers

Mise à jour	Description
Prise en charge de TLSv1.3	ONTAP prend en charge TLS 1.3 pour les protocoles de gestion HTTPS et REST. TLS 1.3 n'est pas pris en charge avec SP/BMC ou avec le chiffrement de peering de cluster.
Prise en charge de la liaison rapide LDAP	S'il est pris en charge par le serveur LDAP, vous pouvez utiliser la liaison rapide LDAP pour authentifier rapidement et simplement les utilisateurs admin de ONTAP.

MetroCluster

Mise à jour	Description
Prise en charge du Mediator 1.4 de ONTAP	La version 1.4 du logiciel Mediator de ONTAP est prise en charge dans les configurations IP de MetroCluster.
Prise en charge des groupes de cohérence	Les groupes de cohérence sont pris en charge dans les configurations MetroCluster.

Mise à jour	Description
"Passer d'une configuration FC MetroCluster à une configuration IP AFF A250 ou FAS500f MetroCluster"	Vous pouvez passer d'une configuration FC MetroCluster à une configuration IP MetroCluster AFF A250 ou FAS500f.

Pour en savoir plus sur les améliorations apportées à la configuration des commutateurs et des plateformes pour les configurations MetroCluster, consultez ["Notes de mise à jour de ONTAP 9"](#).

Mise en réseau

Mise à jour	Description
Protocole LLDP (Link Layer Discovery Protocol)	Le réseau de clusters prend en charge LLDP pour permettre à ONTAP de fonctionner avec des commutateurs de cluster ne prenant pas en charge le protocole CDP (Cisco Discovery Protocol).
Services LIF	Les nouveaux services LIF côté client permettent de mieux contrôler les LIF utilisées pour les requêtes AD, DNS, LDAP et NIS sortantes.

Stockage objet S3

Mise à jour	Description
Prise en charge supplémentaire des actions d'objets S3	Les actions suivantes sont supportées par les API ONTAP : CreateBucket, DeleteBucket, DeleteObjects. En outre, ONTAP S3 prend en charge la gestion des versions d'objets et les actions associées avec PutBucketVersioning, GetBucketVersioning, ListBucketVersions.

SAN

Mise à jour	Description
Basculement de LIF iSCSI	La nouvelle fonctionnalité de basculement LIF iSCSI prend en charge la migration automatique et manuelle des LIF iSCSI dans un basculement partenaire SFO ainsi que dans un basculement local. Le basculement de LIF iSCSI est disponible sur toutes les plateformes de baies SAN (ASA).
Migration non destructive d'une LUN vers un namespace NVMe et d'un namespace NVMe vers une LUN	Utilisez l'interface de ligne de commandes de ONTAP pour convertir un système sur place LUN existante dans un namespace NVMe ou un Namespace NVMe existant vers une LUN .

Sécurité

Mise à jour	Description
Améliorations de la protection anti-ransomware autonome (ARP)	L'algorithme de détection ARP a été amélioré pour détecter d'autres menaces de programmes malveillants. Par ailleurs, une nouvelle clé de licence est utilisée pour activer la protection anti-ransomware autonome. Pour les mises à niveau de systèmes ONTAP à partir de ONTAP 9.10.1, la clé de licence précédente offre toujours les mêmes fonctionnalités.
Vérification multi-administrateurs	Lorsque la vérification multiadministrateur est activée, certaines opérations, telles que la suppression de volumes ou de copies Snapshot, ne peuvent être exécutées qu'après approbation par les administrateurs désignés. Cela empêche les administrateurs compromis, malveillants ou peu expérimentés d'effectuer des modifications ou de supprimer des données indésirables.

Efficacité du stockage

Mise à jour	Description
Afficher les économies en termes d'encombrement physique	Lorsque l'efficacité du stockage sensible à la température est activée sur un volume, vous pouvez utiliser la commande volume show-Footprint pour afficher les économies d'encombrement physique.
Prise en charge SnapLock des volumes FlexGroup	SnapLock inclut la prise en charge des données stockées sur des volumes FlexGroup. La prise en charge des volumes FlexGroup est disponible avec les modes SnapLock Compliance et SnapLock Enterprise.
Mobilité des données des SVM	Augmente le nombre de baies AFF prises en charge à trois et ajoute la prise en charge des relations SnapMirror lorsque la source et la destination exécutent ONTAP 9.11.1 ou une version ultérieure. La gestion externe des clés (KMIP) est également introduite et disponible pour les installations cloud et sur site.

Améliorations de la gestion des ressources de stockage


Mise à jour	Description
Suivi de l'activité au niveau des SVM dans File System Analytics	Le suivi des activités est agrégé au niveau des SVM, qui assure le suivi des IOPS et des débits de lecture/écriture afin de fournir des informations instantanées et exploitables sur les données.
Activer les mises à jour des temps d'accès aux fichiers	Lorsqu'elle est activée, la durée d'accès est mise à jour au niveau du volume d'origine FlexCache uniquement si l'âge de l'heure d'accès actuelle est supérieur à la durée spécifiée par l'utilisateur.
Suppression du répertoire asynchrone	La suppression asynchrone est disponible pour les clients NFS et SMB lorsque l'administrateur du stockage leur accorde des droits sur le volume. Lorsque la suppression asynchrone est activée, les clients Linux peuvent utiliser la commande mv et les clients Windows peuvent utiliser la commande rename pour supprimer un répertoire et le déplacer vers un répertoire masqué .ontaptrashbin répertoire.


Mise à jour	Description
Prise en charge SnapLock des volumes FlexGroup	SnapLock inclut la prise en charge des données stockées sur des volumes FlexGroup. La prise en charge des volumes FlexGroup est disponible avec les modes SnapLock Compliance et SnapLock Enterprise. SnapLock ne prend pas en charge les opérations suivantes sur les volumes FlexGroup : SnapLock pour SnapVault, la conservation basée sur les événements et la conservation à des fins juridiques.

Améliorations de la gestion des SVM

Mise à jour	Description
Mobilité des données des SVM	Augmente le nombre de baies AFF prises en charge à trois et ajoute la prise en charge des relations SnapMirror lorsque la source et la destination exécutent ONTAP 9.11.1 ou une version ultérieure. La gestion externe des clés (KMIP) est également introduite et disponible pour les installations dans le cloud et sur site.

System Manager

Mise à jour	Description
Gérer les règles asynchrones de SnapMirror	<p>Utilisez System Manager pour ajouter des règles de miroir et de copie pré-crées et personnalisées, afficher les règles héritées et remplacer les planifications de transfert définies dans une règle de protection lors de la protection des volumes et des machines virtuelles de stockage. Vous pouvez également utiliser System Manager pour modifier vos relations de protection de volumes et de machines virtuelles de stockage.</p> <div>  <p>Si vous utilisez ONTAP 9.8P12 ou une version ultérieure du correctif ONTAP 9.8 et que vous avez configuré SnapMirror à l'aide de System Manager et que vous prévoyez de mettre à niveau vers ONTAP 9.9.1 ou ONTAP 9.10.1, vous devez utiliser ONTAP 9.9.1P13 ou une version ultérieure et ONTAP 9.10.1P10 ou une version ultérieure du correctif pour votre mise à niveau.</p> </div>
Visualisation matérielle	La fonction de visualisation matérielle de System Manager prend en charge toutes les plateformes AFF et FAS actuelles.
Informations exploitables sur l'analytique système	Sur la page Insights, System Manager vous aide à optimiser votre système en affichant des informations supplémentaires sur la capacité et la sécurité, ainsi que de nouvelles informations sur la configuration des clusters et des machines virtuelles de stockage.

Mise à jour	Description
Amélioration de la facilité d'utilisation	<ul style="list-style-type: none"> • Les volumes nouvellement créés ne peuvent pas être partagés par défaut : Vous pouvez spécifier les autorisations d'accès par défaut, telles que l'exportation via NFS ou le partage via SMB/CIFS et la spécification du niveau d'autorisation. • Simplification du SAN : Lors de l'ajout ou de la modification d'un groupe initiateur, les utilisateurs de System Manager peuvent afficher l'état de connexion des initiateurs du groupe et s'assurer que les initiateurs connectés sont inclus dans le groupe afin que les données des LUN soient accessibles.
Des opérations de niveau local (agrégat) avancées	<p>Les administrateurs System Manager peuvent spécifier la configuration d'un niveau local s'ils ne souhaitent pas accepter la recommandation de System Manager. Les administrateurs peuvent également modifier la configuration RAID d'un niveau local existant.</p> <div>  <p>Si vous utilisez ONTAP 9.8P12 ou une version ultérieure du correctif ONTAP 9.8 et que vous avez configuré SnapMirror à l'aide de System Manager et que vous prévoyez de mettre à niveau vers ONTAP 9.9.1 ou ONTAP 9.10.1, vous devez utiliser ONTAP 9.9.1P13 ou une version ultérieure et ONTAP 9.10.1P10 ou une version ultérieure du correctif pour votre mise à niveau.</p> </div>
Gestion des journaux d'audit	System Manager vous permet d'afficher et de gérer les journaux d'audit ONTAP.

Nouveautés d'ONTAP 9.10.1

Découvrez les nouvelles fonctionnalités disponibles dans ONTAP 9.10.1.

Pour plus d'informations sur les problèmes connus, les limites et les mises en garde de mise à niveau dans les dernières versions de ONTAP 9, consultez le ["Notes de mise à jour de ONTAP 9"](#). Vous devez vous connecter avec votre compte NetApp ou créer un compte pour accéder aux notes de version.

Découvrez les nouveautés et les améliorations ["Fonctionnalités ONTAP MetroCluster"](#).

Découvrez les nouveautés et les améliorations de la prise en charge de ["Plateformes FAS, ASA et AFF, ainsi que les commutateurs pris en charge"](#).

En savoir plus sur les mises à jour du ["L'API REST DE ONTAP"](#).

Pour mettre à niveau ONTAP, voir [Préparez la mise à niveau de ONTAP](#).

Protection des données

Mise à jour	Description
Définissez une période de conservation SnapLock jusqu'à 100 ans	Dans les versions antérieures à ONTAP 9.10.1, la durée de conservation maximale prise en charge est le 19 janvier 2071. Depuis ONTAP 9.10.1, SnapLock entreprise et conformité prend en charge une durée de conservation jusqu'au 26 octobre 3058 et une période de conservation jusqu'à 100 ans. Les anciennes règles sont automatiquement converties lorsque vous prolongez les dates de conservation.
Possibilité de créer des volumes SnapLock et non SnapLock sur le même agrégat	Depuis ONTAP 9.10.1, les volumes SnapLock et non SnapLock peuvent exister sur le même agrégat. Il n'est donc plus nécessaire de créer un agrégat SnapLock distinct pour les volumes SnapLock.
Groupes de cohérence	Organisez les volumes et les LUN par groupes de cohérence pour gérer les règles de protection des données et assurer la fidélité à l'ordre des écritures des charges de travail réparties sur plusieurs volumes de stockage.
Archivez les sauvegardes avec le cloud public	SnapMirror Cloud prend en charge le Tiering des sauvegardes ONTAP vers des classes de stockage objet de cloud public à moindre coût dans AWS et MS Azure pour la conservation à long terme.
Prise en charge AES pour la communication sécurisée des canaux Netlogon	Si vous vous connectez à des contrôleurs de domaine Windows à l'aide du service d'authentification Netlogon, vous pouvez utiliser AES (Advanced Encryption Standard) pour sécuriser les communications de canal.
Kerberos pour SMB domain-tunnel Authentication	L'authentification Kerberos est disponible pour les authentifications de tunnel de domaine pour la gestion ONTAP en plus de NTLM. Ainsi, les connexions sont plus sécurisées vers l'interface de ligne de commande ONTAP et l'interface graphique de System Manager à l'aide des informations d'identification Active Directory.
Liaison de canal pour une sécurité accrue des communications LDAP	La liaison de canal LDAP est prise en charge par défaut pour les connexions LDAP Active Directory et des services de noms. Cela offre une meilleure protection contre les attaques de l'homme du milieu.

Protocoles d'accès aux fichiers

Mise à jour	Description
NFS over RDMA (NVIDIA uniquement)	NFS sur RDMA utilise des adaptateurs RDMA. Il permet de copier directement les données entre la mémoire du système de stockage et la mémoire du système hôte, ce qui évite les interruptions du processeur et la surconsommation. NFS over RDMA permet d'utiliser le stockage NVIDIA GPUDirect pour les workloads accélérés par processeur graphique sur des hôtes dotés de processeurs graphiques NVIDIA pris en charge.

MetroCluster

Mise à jour	Description
"Configuration de l'adresse IP MetroCluster de couche 3 dans les configurations MetroCluster IP"	Vous pouvez modifier l'adresse IP, le masque de réseau et la passerelle MetroCluster des nœuds dans une configuration de couche 3.

Mise à jour	Description
"Mise à niveau simplifiée des nœuds du contrôleur dans une configuration MetroCluster FC"	La procédure de mise à niveau du processus de mise à niveau via le basculement et le rétablissement a été simplifiée.

Pour en savoir plus sur les améliorations apportées à la configuration des commutateurs et des plateformes pour les configurations MetroCluster, consultez ["Notes de mise à jour de ONTAP 9"](#).

Mise en réseau

Mise à jour	Description
Interconnexion de cluster RDMA	Avec le système de stockage A400 ou ASA A400 et une carte réseau en cluster X1151A, vous pouvez accélérer les charges de travail hautes performances dans un cluster à plusieurs nœuds en exploitant RDMA pour le trafic intra-cluster
Une confirmation est requise avant de définir le statut admin à down pour une LIF dans un SVM système	Cela vous protège contre la panne accidentelle de LIF qui sont essentielles au bon fonctionnement du cluster. Si vous avez des scripts qui invoquent ce comportement au niveau de l'interface de ligne de commande, vous devez les mettre à jour pour tenir compte de l'étape de confirmation.
Recommandations de détection et de réparation automatiques en cas de problème de câblage réseau	Lorsqu'un problème d'accessibilité de port est détecté, ONTAP System Manager recommande une opération de réparation pour résoudre le problème.
Certificats IPsec (Internet Protocol Security)	Les stratégies IPsec prennent en charge les clés prépartagées (PSK) en plus des certificats d'authentification.
Règles de service LIF	Les politiques de pare-feu sont obsolètes et remplacées par des politiques de service LIF. Une nouvelle politique de service de LIF NTP a également été ajoutée afin de renforcer le contrôle sur les LIFs utilisées pour les requêtes NTP sortantes.

Stockage objet S3

Mise à jour	Description
Protection des données en mode objet S3, sauvegarde et reprise d'activité	S3 SnapMirror fournit des services de protection des données pour le stockage objet ONTAP S3, notamment la mise en miroir des compartiments vers des configurations ONTAP S3 et la sauvegarde des compartiments vers des destinations NetApp et non NetApp.
Audit S3	Vous pouvez effectuer un audit des données et des événements de gestion dans les environnements ONTAP S3. La fonctionnalité d'audit S3 est similaire aux fonctionnalités d'audit NAS existantes, et l'audit S3 et NAS peut coexister dans un cluster.

SAN

Mise à jour	Description
Namespace NVMe	Vous pouvez utiliser l'interface de ligne de commandes de ONTAP pour augmenter ou réduire la taille d'un namespace. System Manager vous permet d'augmenter la taille d'un namespace.
Prise en charge du protocole NVMe pour TCP	Le protocole NVMe (non-volatile Memory Express) est disponible pour les environnements SAN sur un réseau TCP.

Sécurité

Mise à jour	Description
Protection autonome contre les ransomwares	À l'aide de l'analyse des workloads dans les environnements NAS, la protection anti-ransomware autonome vous alerte en cas d'activité anormale susceptible d'indiquer une attaque par ransomware. La protection autonome contre les ransomware crée également des sauvegardes Snapshot automatiques lorsqu'une attaque est détectée, en plus de la protection existante contre les copies Snapshot planifiées.
Une norme de gestion des clés de cryptage	Utilisez Azure Key Vault et le service de gestion des clés Google Cloud Platform pour stocker, protéger et utiliser les clés ONTAP, rationalisant ainsi la gestion des clés et l'accès.

Efficacité du stockage

Mise à jour	Description
Efficacité du stockage sensible à la température	Vous pouvez activer l'efficacité du stockage sensible à la température en mode « par défaut » ou en mode « efficace » sur des volumes AFF nouveaux ou existants.
Possibilité de déplacer des SVM entre les clusters sans interruption	Vous pouvez déplacer des SVM entre des clusters AFF physiques, d'une source à une destination, pour l'équilibrage de la charge, l'amélioration des performances, les mises à niveau d'équipement et les migrations du data Center.

Améliorations de la gestion des ressources de stockage

Mise à jour	Description
Suivi de l'activité pour les objets sensibles avec File System Analytics (FSA)	Pour améliorer l'évaluation des performances du système, FSA peut identifier les objets sensibles : fichiers, répertoires, utilisateurs et clients ayant le plus de trafic et de débit.
Verrouillage global de la lecture des fichiers	Activez un verrouillage en lecture à partir d'un point unique sur tous les caches et l'article d'origine affecté dans la migration.
Prise en charge de NFSv4 pour FlexCache	Les volumes FlexCache prennent en charge le protocole NFSv4.
Créez des clones à partir de volumes FlexGroup existants	Vous pouvez créer un volume FlexClone à l'aide de volumes FlexGroup existants.

Mise à jour	Description
Conversion d'un volume FlexVol en FlexGroup dans une source de reprise d'activité SVM	Vous pouvez convertir des volumes FlexVol en volumes FlexGroup sur une source de reprise d'activité SVM.

Améliorations de la gestion des SVM

Mise à jour	Description
Possibilité de déplacer des SVM entre les clusters sans interruption	Vous pouvez déplacer des SVM entre des clusters AFF physiques, d'une source à une destination, pour l'équilibrage de la charge, l'amélioration des performances, les mises à niveau d'équipement et les migrations du data Center.

System Manager

Mise à jour	Description
Activez la journalisation de la télémétrie des performances dans les journaux System Manager	Les administrateurs peuvent activer la journalisation de télémétrie en cas de problèmes de performances avec System Manager, puis contacter le support pour analyser le problème.
Fichiers de licence NetApp	Toutes les clés de licence sont fournies sous forme de fichiers de licence NetApp au lieu de clés de licence individuelles à 28 caractères, ce qui permet de concéder plusieurs fonctions à l'aide d'un seul fichier.
Mise à jour automatique du micrologiciel	Les administrateurs System Manager peuvent configurer ONTAP pour mettre automatiquement à jour le micrologiciel.
Examiner les recommandations en matière d'atténuation des risques et prendre connaissance des risques signalés par Active IQ	Les utilisateurs de System Manager peuvent afficher les risques signalés par Active IQ et examiner les recommandations relatives à la réduction des risques. À partir de la version 9.10.1, les utilisateurs peuvent également reconnaître les risques.
Configurer la réception par l'administrateur des notifications d'événements EMS	Les administrateurs System Manager peuvent configurer la manière dont les notifications d'événements du système de gestion des événements (EMS) sont envoyées pour être avertis des problèmes système nécessitant leur attention.
Gérer les certificats	Les administrateurs System Manager peuvent gérer les autorités de certification approuvées, les certificats client/serveur et les autorités de certification locales (intégrées).
Utilisez System Manager pour afficher l'historique d'utilisation de la capacité et prévoir les besoins futurs	Grâce à l'intégration entre Active IQ et System Manager, les administrateurs peuvent afficher des données sur les tendances historiques d'utilisation de la capacité pour les clusters.
Utilisez System Manager pour sauvegarder les données dans StorageGRID à l'aide de Cloud Backup Service	En tant qu'administrateur Cloud Backup Service, vous pouvez sauvegarder sur StorageGRID si Cloud Manager est déployé sur site. Vous pouvez également archiver des objets à l'aide de Cloud Backup Service avec AWS ou Azure.

Mise à jour	Description
Amélioration de la facilité d'utilisation	<p>À partir de ONTAP 9.10.1, vous pouvez :</p> <ul style="list-style-type: none"> • Attribuez des règles de QoS aux LUN au lieu du volume parent (VMware, Linux, Windows) • Modifiez la « policy group » QoS de la LUN • Déplacer une LUN • Mettez une LUN hors ligne • Effectuer une mise à niveau d'image ONTAP en déploiement • Créez un ensemble de ports et liez-le à un groupe initiateur • Recommandations de détection et de réparation automatiques en cas de problème de câblage réseau • Activez ou désactivez l'accès client au répertoire de copie Snapshot • Calculer l'espace récupérable avant de supprimer les copies Snapshot • Accédez aux modifications de terrain en permanence disponibles dans les partages SMB • Afficher les mesures de capacité à l'aide d'unités d'affichage plus précises • Gestion d'utilisateurs et de groupes spécifiques à un hôte pour Windows et Linux • Gérer les paramètres AutoSupport • Redimensionner les volumes en tant qu'action séparée

Nouveautés d'ONTAP 9.9.1

Découvrez les nouvelles fonctionnalités disponibles dans ONTAP 9.9.1.

Pour plus d'informations sur les problèmes connus, les limites et les mises en garde de mise à niveau dans les dernières versions de ONTAP 9, consultez le ["Notes de mise à jour de ONTAP 9"](#). Vous devez vous connecter avec votre compte NetApp ou créer un compte pour accéder aux notes de version.

Découvrez les nouveautés et les améliorations ["Fonctionnalités ONTAP MetroCluster"](#).

Découvrez les nouveautés et les améliorations de la prise en charge de ["Plateformes FAS, ASA et AFF, ainsi que les commutateurs pris en charge"](#).

En savoir plus sur les mises à jour du ["L'API REST DE ONTAP"](#).

Pour effectuer la mise à niveau vers la dernière version de ONTAP, reportez-vous à la section [Préparez la mise à niveau de ONTAP](#).

Protection des données

Mise à jour	Description
"Prise en charge de l'efficacité du stockage sur les volumes et les agrégats SnapLock"	Les fonctionnalités d'efficacité du stockage pour les volumes et les agrégats SnapLock ont été étendues pour inclure la compaction des données, la déduplication entre volumes, la compression adaptative et l'efficacité du stockage TSSE (Temperature Sensitive Storage Efficiency), permettant ainsi de réaliser des économies d'espace plus importantes pour les données WORM.
"Prise en charge de la configuration de différentes règles Snapshot sur la source et la destination du SVM DR"	Les configurations des SVM DR peuvent utiliser la règle mirror-vault pour configurer différentes règles Snapshot sur la source et la destination. De plus, les règles sur la destination ne sont pas écrasées par les règles sur la source.
"Prise en charge de System Manager pour SnapMirror Cloud"	SnapMirror Cloud est désormais pris en charge dans System Manager.
SVM avec audit activé	Le nombre maximal de SVM avec audit pris en charge dans un cluster est passé de 50 à 400.
SnapMirror synchrone	Le nombre maximal de terminaux SnapMirror synchrones pris en charge par paire haute disponibilité est passé de 80 à 160.
Topologie de FlexGroup SnapMirror	Les volumes FlexGroup prennent en charge au moins deux relations de type « fanout », par exemple A→B, A→C. Tout comme les volumes FlexVol, FlexGroup Fout prend en charge un maximum de 8 pieds en éventail et en cascade jusqu'à deux niveaux, par exemple, A→B→C.

Protocoles d'accès aux fichiers

Mise à jour	Description
"Améliorations de la recherche de références LDAP"	La recherche de références LDAP est prise en charge avec la signature et le chiffrement LDAP, les connexions TLS cryptées et les communications sur le port LDAPS 636.
"Prise en charge LDAPS sur n'importe quel port"	LDAPS peut être configuré sur n'importe quel port ; le port 636 reste le port par défaut.
"Versions NFSv4.x activées par défaut"	NFSv4.0, NFSv4.1 et NFSv4.2 sont activés par défaut.
"Prise en charge de NFSv4.2 avec libellé"	Le contrôle d'accès obligatoire (MAC) nommé NFS est pris en charge lorsque NFSv4.2 est activé. Grâce à cette fonctionnalité, les serveurs NFS ONTAP prennent en charge les adresses MAC, le stockage et la récupération <code>sec_label</code> attributs envoyés par les clients.

MetroCluster

Mise à jour	Description
"Prise en charge IP de la liaison partagée au niveau de la couche 3"	Les configurations IP de MetroCluster peuvent être implémentées grâce à des connexions internes routées par IP (couche 3).

Mise à jour	Description
"Prise en charge des clusters à 8 nœuds"	Les clusters à 8 nœuds permanents sont pris en charge dans les configurations IP et FAS. En outre, les plateformes AFF ASA prennent en charge les configurations MCC IP à 8 nœuds.

Pour en savoir plus sur les améliorations apportées à la configuration des commutateurs et des plateformes pour les configurations MetroCluster, consultez ["Notes de mise à jour de ONTAP 9"](#).

Mise en réseau

Mise à jour	Description
"Résilience du cluster"	<ul style="list-style-type: none"> • Surveillance et évitement des ports pour les clusters à 2 nœuds sans commutateur (auparavant disponible uniquement dans les configurations avec commutateur) • Basculement automatique des nœuds lorsqu'un nœud ne peut pas transmettre de données sur son réseau de cluster • Nouveaux outils permettant d'afficher les chemins de clusters qui subissent une perte de paquets
"Extension de la LIF Virtual IP (VIP)"	<ul style="list-style-type: none"> • Le numéro de système autonome (ASN) pour le protocole BGP (Border Gateway Protocol) prend en charge un entier non négatif de 4 octets. • Le discriminateur multi-exit (MED) permet des sélections d'itinéraire avancées avec prise en charge de la hiérarchisation des chemins. MED est un attribut facultatif dans le message de mise à jour BGP. • VIP BGP offre une automatisation de routage par défaut grâce au regroupement de pairs BGP pour une configuration simplifiée.

Stockage objet S3

Mise à jour	Description
"Prise en charge des métadonnées S3 et des balises"	Le serveur ONTAP S3 offre des fonctionnalités d'automatisation améliorées aux clients et aux applications S3 avec prise en charge des métadonnées d'objet définies par l'utilisateur et du balisage d'objets.

SAN

Mise à jour	Description
Importation de LUN étrangères (FLI)	L'application SAN LUN Migrate sur le site de support NetApp peut être utilisée pour qualifier une baie étrangère qui n'est pas répertoriée dans la matrice d'interopérabilité FLI.
Accès au chemin à distance NVMe-of	En cas de perte de l'accès direct au chemin en cas de basculement, les E/S distantes permettent au système de basculer vers un chemin distant et de continuer l'accès aux données.
Prise en charge des clusters à 12 nœuds sur les baies ASA	Les clusters à 12 nœuds sont pris en charge dans les configurations AFF ASA. Les clusters ASA peuvent inclure divers types de systèmes ASA.

Mise à jour	Description
Protocole NVMe-of sur les baies ASA	La prise en charge du protocole NVMe-of est également disponible avec un système AFF ASA.
Améliorations apportées aux groupes initiateurs	<ul style="list-style-type: none"> • Vous pouvez créer un groupe initiateur composé de groupes initiateurs existants. • Vous pouvez ajouter une description à un groupe initiateur ou à des initiateurs hôtes qui servent d'alias pour ce groupe initiateur ou cet initiateur hôte. • Vous pouvez mapper des groupes initiateurs sur deux ou plusieurs LUN simultanément.
Amélioration des performances d'une seule LUN	Les performances des LUN uniques pour AFF ont été considérablement améliorées, ce qui en fait la solution idéale pour simplifier les déploiements dans les environnements virtuels. Par exemple, l'A800 peut offrir jusqu'à 400 % d'IOPS en lecture aléatoire en plus.

Sécurité

Mise à jour	Description
Prise en charge de l'authentification multifacteur avec Cisco DUO lors de la connexion à System Manager	À partir de ONTAP 9.9.1P3, vous pouvez configurer Cisco DUO en tant que fournisseur d'identité SAML, ce qui permet aux utilisateurs de s'authentifier à l'aide de Cisco DUO lorsqu'ils se connectent au Gestionnaire système.

Efficacité du stockage

Mise à jour	Description
"Définissez le nombre de fichiers au maximum pour le volume"	Automatise les valeurs maximales de fichier avec le paramètre de volume <code>-files-set-maximum</code> , éliminant la nécessité de surveiller les limites des fichiers.

Améliorations de la gestion des ressources de stockage

Mise à jour	Description
Améliorations de la gestion de l'analytique de système de fichiers (FSA) dans System Manager	FSA offre des fonctionnalités supplémentaires de System Manager pour la recherche et le filtrage, ainsi que pour prendre des mesures en fonction des recommandations de FSA.
Prise en charge du cache de recherche négative	Met en cache une erreur « fichier introuvable » sur le volume FlexCache pour réduire le trafic réseau provoqué par les appels vers l'origine.
Reprise d'activité FlexCache	Permet la migration sans interruption des clients d'un cache à un autre.
Prise en charge de SnapMirror en cascade et en éventail pour les volumes FlexGroup	Prend en charge les relations SnapMirror en cascade et les relations SnapMirror en mode « fan out » pour les volumes FlexGroup.

Mise à jour	Description
Prise en charge de la reprise d'activité SVM pour les volumes FlexGroup	La prise en charge de la reprise d'activité SVM pour les volumes FlexGroup assure la redondance en utilisant SnapMirror pour répliquer et synchroniser la configuration et les données d'un SVM.
Reporting et application de l'espace logique pour les volumes FlexGroup	Vous pouvez afficher et limiter la quantité d'espace logique consommée par les utilisateurs du volume FlexGroup.
Prise en charge de l'accès SMB dans les qtrees	L'accès SMB est pris en charge par les qtrees dans les volumes FlexVol et FlexGroup sur lesquels SMB est activé.

System Manager

Mise à jour	Description
System Manager affiche les risques signalés par Active IQ	Utilisez System Manager pour établir un lien vers NetApp Active IQ, qui signale les opportunités de réduction des risques et d'amélioration des performances et de l'efficacité de votre environnement de stockage.
Affecter manuellement des niveaux locaux	Les utilisateurs de System Manager peuvent attribuer manuellement un niveau local lors de la création et de l'ajout de volumes et de LUN.
Suppression rapide du répertoire	Vous pouvez supprimer des répertoires dans System Manager grâce à une fonctionnalité de suppression rapide des répertoires à faible latence.
Générez des playbooks Ansible	Les utilisateurs de System Manager peuvent générer des playbooks Ansible à partir de l'interface pour quelques workflows spécifiques et les utiliser dans un outil d'automatisation pour ajouter ou modifier à plusieurs reprises des volumes ou des LUN.
Visualisation du matériel	Introduite pour la première fois dans ONTAP 9.8, la fonctionnalité de visualisation du matériel prend désormais en charge toutes les plates-formes AFF.
Intégration avec Active IQ	Les utilisateurs de System Manager peuvent consulter les dossiers de demande de support associés au cluster et les télécharger. Ils peuvent également copier les informations dont ils ont besoin pour ouvrir de nouveaux dossiers de demande de support sur le site du support NetApp. Les utilisateurs de System Manager peuvent recevoir des alertes de la part de Active IQ afin de les informer de la disponibilité de nouvelles mises à jour de firmware. Ils peuvent ensuite télécharger l'image du firmware et la télécharger à l'aide de System Manager.
Intégration de Cloud Manager	Les utilisateurs de System Manager peuvent configurer la protection pour sauvegarder les données sur des terminaux de cloud public à l'aide de Cloud Backup Service.
Amélioration du flux de travail de provisionnement de protection des données	Lors de la configuration de la protection des données, les utilisateurs de System Manager peuvent nommer manuellement une destination SnapMirror et un nom de groupe initiateur.
Gestion améliorée des ports réseau	Les fonctionnalités améliorées de la page interfaces réseau permettent d'afficher et de gérer les interfaces de leurs ports d'accueil.

Mise à jour	Description
Améliorations de la gestion du système	<ul style="list-style-type: none"> • Prise en charge des igroups imbriqués • Mappez plusieurs LUN sur un groupe initiateur en une seule tâche et pouvez utiliser un alias WWPN pour filtrer les données pendant le processus. • Lors de la création de LIF NVMe-of, il n'est plus nécessaire de sélectionner des ports identiques sur les deux contrôleurs. • Désactivez les ports FC à l'aide d'un bouton à bascule pour chaque port.
Affichage amélioré dans System Manager des informations relatives aux copies Snapshot	<ul style="list-style-type: none"> • Les utilisateurs de System Manager peuvent afficher la taille des copies Snapshot et le libellé SnapMirror. • La réserve de copies Snapshot est définie sur zéro si les copies Snapshot sont désactivées.
Affichage amélioré dans System Manager des informations de capacité et d'emplacement pour les niveaux de stockage	<ul style="list-style-type: none"> • Une nouvelle colonne tiers identifie les niveaux locaux (agrégats) dans lesquels réside chaque volume. • System Manager affiche la capacité physique utilisée, la capacité logique utilisée au niveau du cluster et le niveau local (agrégat). • Les nouveaux champs d'affichage de la capacité permettent de surveiller la capacité, de suivre les volumes proches de la capacité ou qui sont sous-utilisés.
Affichage dans System Manager des alertes d'urgence EMS et d'autres erreurs et avertissements	Le nombre d'alertes EMS reçues en 24 heures, ainsi que d'autres erreurs et avertissements, sont indiqués sur la carte Santé dans System Manager.

Modifications des limites ONTAP et des valeurs par défaut

En savoir plus sur les modifications apportées aux limites et aux valeurs par défaut mises en œuvre dans les versions ONTAP 9. NetApp s'efforce d'aider ses clients à comprendre les valeurs par défaut les plus importantes et à limiter les modifications apportées à chaque version de ONTAP.

Permet de modifier les valeurs par défaut de ONTAP

Avant de procéder à une mise à niveau vers une nouvelle version de ONTAP, vous devez tenir compte de toute modification des paramètres par défaut de ONTAP susceptible d'affecter l'automatisation ou les opérations de l'entreprise.

Fonction	Modification par défaut	Modifié dans la version...
vserver object-store-server user show commande	Dans les versions antérieures à ONTAP 9.15.1, le vserver object-store-server user show Renvoie les clés secrètes de l'utilisateur S3. La commande ne renvoie plus les données de clé secrète pour les utilisateurs S3.	ONTAP 9.15.1
Audit NAS	La configuration d'audit NAS permet de conserver tous les enregistrements de journal d'audit par défaut. Une valeur révisée pour le paramètre de limite de rotation garantit que le journal d'audit est correctement dimensionné pour le volume qui le prend en charge.	ONTAP 9.15.1
Allocation d'espace	L'allocation d'espace est activée par défaut pour les nouvelles LUN créées. L'allocation d'espace avait été désactivée par défaut dans les versions précédentes de ONTAP (9.14.1 et antérieures).	ONTAP 9.15.1
Découverte automatisée d'hôtes NVMe/TCP	La détection des contrôleurs hôte via le protocole NVMe/TCP est automatisée par défaut.	ONTAP 9.14.1
Cryptage AES pour les communications Kerberos	Le chiffrement AES pour l'authentification est activé par défaut pour les communications Kerberos avec les serveurs SMB. Vous pouvez désactiver manuellement le chiffrement AES si votre environnement ne le prend pas en charge.	ONTAP 9.13.1
Agrégat RAID	À partir de ONTAP 9.12.1, le contrôleur système ne s'arrête pas par défaut au bout de 24 heures si un agrégat est dégradé. Si un utilisateur modifie le raid.timeout en option, le contrôleur système continuera à s'arrêter après l'expiration du raid.timeout heures.	ONTAP 9.12.1
TLS 1.1 désactivé par défaut	TLS 1.1 est désactivé par défaut pour les nouvelles installations de ONTAP. Les systèmes mis à niveau vers ONTAP 9.12.0 et versions ultérieures sur lesquels TLS 1.1 est déjà activé ne sont pas concernés car la mise à niveau laissera TLS 1.1 dans un état activé. Toutefois, si vous mettez à niveau des clusters avec FIPS activé, TLS 1.1 n'est pas pris en charge avec FIPS à partir de ONTAP 9.11.1, donc TLS 1.1 sera automatiquement désactivé. Lorsqu'il est désactivé par défaut, TLS 1.1 peut être activé manuellement selon les besoins.	ONTAP 9.12.0

Fonction	Modification par défaut	Modifié dans la version...
TLS 1.0 désactivé par défaut	TLS 1.0 est désactivé par défaut pour les nouvelles installations de ONTAP. Les systèmes mis à niveau vers ONTAP 9.8 et versions ultérieures sur lesquels TLS 1.0 est déjà activé ne sont pas concernés car la mise à niveau laissera TLS 1.0 dans un état activé. Toutefois, si vous mettez à niveau des clusters avec FIPS activé, TLS 1.0 n'est pas pris en charge avec FIPS à partir de ONTAP 9.8, donc TLS 1.0 sera automatiquement désactivé. Lorsqu'il est désactivé par défaut, TLS 1.0 peut être activé manuellement selon les besoins.	ONTAP 9.8

Modifications des limites ONTAP

Avant de procéder à une mise à niveau vers une nouvelle version de ONTAP, vous devez être conscient de toute modification des limites de ONTAP qui pourrait affecter l'automatisation ou les opérations de l'entreprise.

Fonction	Modification de limite	Modifié dans la version...
Synchronisation active SnapMirror	La synchronisation active SnapMirror prend en charge 80 volumes au sein d'un groupe de cohérence	ONTAP 9.15.1
Réplication asynchrone SnapMirror	Les groupes de cohérence qui utilisent la protection asynchrone SnapMirror prennent en charge jusqu'à 80 volumes dans un groupe de cohérence.	ONTAP 9.15.1
Analytique du système de fichiers	Pour limiter les problèmes de performance, ONTAP veille à ce que 5 à 8 % de la capacité d'un volume soit libre lors de l'activation de l'analytique du système de fichiers.	ONTAP 9.15.1
Mobilité des données des SVM	Le nombre maximal de volumes pris en charge par SVM avec la mobilité des données SVM augmente à 400 et le nombre de paires haute disponibilité prises en charge passe à 12.	ONTAP 9.14.1
Rééquilibrage FlexGroup	La taille minimale des fichiers configurables pour les opérations de rééquilibrage FlexGroup passe de 4 Ko à 20 Mo.	<ul style="list-style-type: none"> • ONTAP 9.14.1 • ONTAP 9.13.1P1 • ONTAP 9.12.1P10
Taille maximale des volumes FlexVol et FlexGroup	La taille maximale des composants de volume FlexVol et FlexGroup pris en charge sur les plateformes AFF et FAS est passée de 100 To à 300 To.	ONTAP 9.12.1P2
Taille maximale de la LUN	La taille maximale de LUN prise en charge sur les plateformes AFF et FAS est passée de 16 To à 128 To. La taille maximale de LUN prise en charge dans les configurations SnapMirror (synchrone et asynchrone) est passée de 16 To à 128 To.	ONTAP 9.12.1P2

Fonction	Modification de limite	Modifié dans la version...
Taille maximale du volume FlexVol	La taille maximale du volume pris en charge sur les plateformes AFF et FAS est passée de 100 To à 300 To. La taille maximale du volume FlexVol pris en charge dans les configurations SnapMirror synchrones est passée de 100 To à 300 To.	ONTAP 9.12.1P2
Taille maximale du fichier	La taille maximale de fichier prise en charge pour les systèmes de fichiers NAS sur les plateformes AFF et FAS est passée de 16 To à 128 To. La taille maximale de fichier prise en charge dans les configurations SnapMirror synchrones est passée de 16 To à 128 To.	ONTAP 9.12.1P2
Limite de volume du cluster	Les contrôleurs peuvent mieux exploiter le processeur et la mémoire et augmenter le nombre maximal de volumes d'un cluster de 15,000 à 30,000.	ONTAP 9.12.1
Relations SVM-DR pour les volumes FlexVol	Pour les volumes FlexVol, le nombre maximal de relations SVM-DR est passé de 64 à 128 (128 SVM par cluster).	ONTAP 9.11.1
SnapMirror synchrone	Le nombre maximal d'opérations SnapMirror synchrones autorisées par paire haute disponibilité est passé de 200 à 400.	ONTAP 9.11.1
Volumes FlexVol NAS	La limite des clusters pour les volumes FlexVol NAS est passée de 12,000 à 15,000.	ONTAP 9.10.1
Volumes SAN FlexVol	La limite des clusters pour les volumes FlexVol SAN est passée de 12,000 à 15,000.	ONTAP 9.10.1
SVM-DR avec les volumes FlexGroup	<ul style="list-style-type: none"> • Un maximum de 32 relations SVM-DR est pris en charge avec les volumes FlexGroup. • Le nombre maximum de volumes pris en charge par un seul SVM dans une relation SVM-DR est de 300, ce qui inclut le nombre de volumes FlexVol et de composants FlexGroup. • Le nombre maximum de composants dans un FlexGroup ne peut pas dépasser 20. • Les limites du volume SVM-DR sont de 500 par nœud, 1000 par cluster (y compris les volumes FlexVol et les composants FlexGroup). 	ONTAP 9.10.1
SVM avec audit activé	Le nombre maximal de SVM avec audit pris en charge dans un cluster est passé de 50 à 400.	ONTAP 9.9.1
SnapMirror synchrone	Le nombre maximal de terminaux SnapMirror synchrones pris en charge par paire haute disponibilité est passé de 80 à 160.	ONTAP 9.9.1

Fonction	Modification de limite	Modifié dans la version...
Topologie de FlexGroup SnapMirror	Les volumes FlexGroup prennent en charge au moins deux relations de type « éventail », par exemple, De A à B, De A à C. Tout comme les volumes FlexVol, la sortie FlexGroup prend en charge un maximum de 8 pieds en éventail et une cascade jusqu'à deux niveaux, par exemple, De A à B à C.	ONTAP 9.9.1
Transfert simultané SnapMirror	Le nombre maximal de transferts simultanés asynchrones au niveau des volumes est passé de 100 à 200. Les transferts SnapMirror de cloud à cloud sont passés de 32 à 200 sur les systèmes haut de gamme et de 6 à 20 transferts SnapMirror sur les systèmes bas de gamme.	ONTAP 9.8
La limite des volumes FlexVol	L'espace consommé par les volumes FlexVol est passé de 100 To à 300 To pour les plateformes ASA.	ONTAP 9.8

Prise en charge de la version 9 de ONTAP

À partir de la version ONTAP 9.8, NetApp publie deux fois par an les versions ONTAP. Bien que les plans soient susceptibles d'être modifiés, l'objectif est de fournir de nouvelles versions de ONTAP au cours des deuxième et quatrième trimestres de chaque année civile. Utilisez ces informations pour planifier la durée de votre mise à niveau et bénéficier de la dernière version de ONTAP.

Version	Date de sortie
9.15.1	Mai 2024
9.14.1	Janvier 2024
9.13.1	Juin 2023
9.12.1	Février 2023
9.11.1	Juillet 2022
9.10.1	Janvier 2022
9.9.1	Juin 2021

Niveaux de support

Le niveau de support disponible pour une version spécifique de ONTAP varie en fonction du moment où le logiciel a été commercialisé.

Niveau de support	Support complet			Prise en charge limitée		Support en libre-service		
Année	1	2	3	4	5	6	7	8
Accès à la documentation en ligne	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.
Support technique	Oui.	Oui.	Oui.	Oui.	Oui.			
Analyse de la cause première	Oui.	Oui.	Oui.	Oui.	Oui.			
Téléchargements de logiciels	Oui.	Oui.	Oui.	Oui.	Oui.			
Mises à jour de service (correctifs [versions P])	Oui.	Oui.	Oui.					
Alertes concernant les vulnérabilités	Oui.	Oui.	Oui.					

Pour effectuer la mise à niveau vers la dernière version de ONTAP, reportez-vous à la section [Mise à niveau vers la dernière version de ONTAP](#) et [Quand dois-je mettre à niveau ONTAP ?](#)

Introduction et concepts

Concepts relatifs à ONTAP

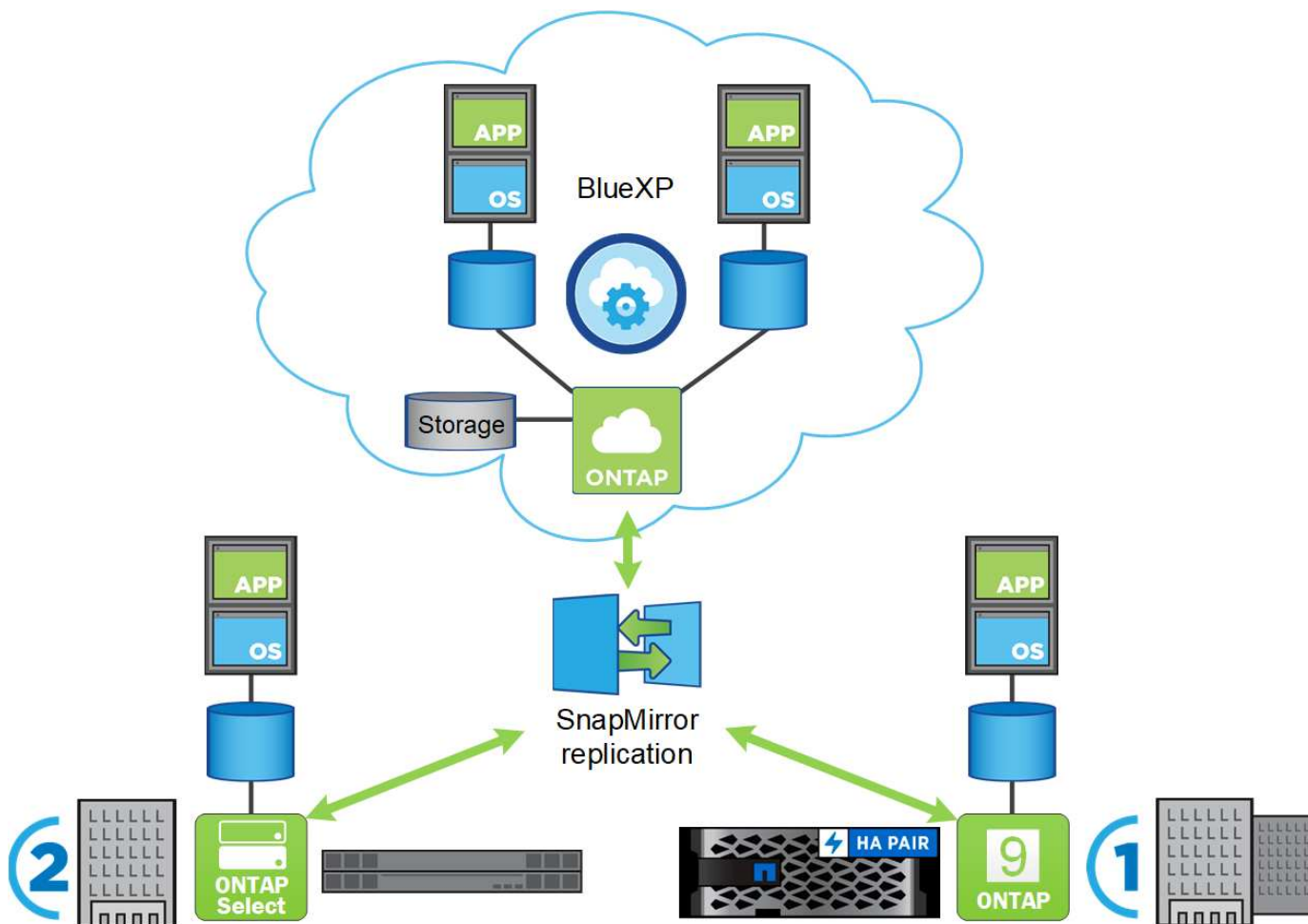
Plateformes ONTAP

Le logiciel de gestion des données ONTAP offre un stockage unifié pour les applications qui lisent et écrivent des données de blocs ou de fichiers. Les options de configuration de stockage vont du Flash ultra-rapide aux supports rotatifs à moindre coût au stockage objet basé dans le cloud.

Les implémentations ONTAP s'exécutent sur les éléments suivants :

- **Systèmes NetApp** : "Les systèmes Flash hybrides FAS, les systèmes FAS 100 % Flash (AFF) A-Series et C-Series, ainsi que les plateformes ASA (baies SAN 100 % Flash)"
- **Matériel de base** : "ONTAP Select"
- **Clouds privés, publics ou hybrides** : "Cloud Volumes ONTAP"
- **Implémentations spécialisées**, y compris "Data Center FlexPod", qui offre la meilleure infrastructure convergée de sa catégorie

Ensemble, ces implémentations forment la structure de base de la structure de données *NetApp*, à l'aide d'une approche Software-defined commune de la gestion des données et d'une réplication rapide et efficace entre les plateformes.



Interfaces utilisateur ONTAP

Le logiciel de gestion des données ONTAP offre plusieurs interfaces que vous pouvez utiliser pour gérer vos clusters ONTAP. Ces options d'interface proposent différents niveaux d'accès et de fonctionnalité et vous offrent la flexibilité nécessaire pour gérer vos clusters ONTAP en fonction de votre environnement.

Vous pouvez utiliser l'une de ces interfaces pour administrer vos clusters ONTAP et effectuer des opérations de gestion des données

ONTAP System Manager

ONTAP System Manager est une interface utilisateur web qui vous offre une gestion simplifiée et intuitive de votre cluster. Vous pouvez gérer les opérations courantes, telles que la configuration du stockage, la protection des données ainsi que la configuration et la gestion du réseau. System Manager contrôle également les risques et les performances du cluster, et vous aide à réagir aux problèmes du cluster et à anticiper les problèmes. ["En savoir plus >>"](#).

L'interface de ONTAP System Manager a été repensée dans ONTAP 9.7, et l'expérience utilisateur est plus simple et plus intuitive. Les procédures décrites dans cette documentation décrivent la nouvelle interface de System Manager, qui propose davantage d'options à chaque version de ONTAP.



L'ancienne interface de System Manager est appelée System Manager Classic dans la documentation de ONTAP. La dernière version de ONTAP dans laquelle l'interface System Manager Classic est disponible est ONTAP 9.7.

BlueXP

Depuis ONTAP 9.12.1, vous pouvez utiliser l'interface web BlueXP pour gérer votre infrastructure multicloud hybride à partir d'un seul plan de contrôle tout en conservant le tableau de bord familier de System Manager. BlueXP vous permet de créer et de gérer du stockage cloud (par exemple, Cloud Volumes ONTAP), d'utiliser les services de données NetApp (par exemple, sauvegarde dans le cloud) et de contrôler de nombreux périphériques de stockage sur site et en périphérie. L'ajout de systèmes ONTAP sur site à BlueXP vous permet de gérer l'ensemble de vos ressources de stockage et de données à partir d'une interface unique. ["En savoir plus >>"](#).

Interface de ligne de commande ONTAP

Le ["Interface de ligne de commande ONTAP"](#) Est une interface texte qui vous permet d'interagir avec un cluster, un nœud, un SVM, et bien plus encore en utilisant ["commandes"](#). Les commandes CLI sont disponibles sur la base de ["type de rôle"](#). Vous pouvez accéder à l'interface de ligne de commandes de ONTAP via une connexion SSH ou une connexion console à un nœud du cluster.

L'API REST DE ONTAP

À partir de ONTAP 9.6, vous pouvez accéder à une API RESTful qui vous permet de gérer et d'automatiser par programmation les opérations du cluster. Vous pouvez utiliser l'API pour effectuer diverses tâches d'administration ONTAP, telles que la création et la gestion de volumes, de snapshots et d'agrégats, ou encore le contrôle des performances du cluster. Vous pouvez accéder à l'API REST ONTAP directement à l'aide d'un utilitaire tel que curl ou de tout langage de programmation qui prend en charge un client REST, comme Python, PowerShell et Java. ["En savoir plus >>"](#).



ONTAPI est une API ONTAP propriétaire antérieure à l'API REST ONTAP. L'interface ONTAPI sera désactivée dans les prochaines versions de ONTAP. Si vous utilisez ONTAPI, vous devez planifier votre ["Migration vers l'API REST ONTAP"](#).

Frameworks et kits d'outils NetApp

NetApp fournit des kits d'outils client pour des langages et des environnements de développement spécifiques qui extraient l'API REST de ONTAP et facilitent la création du code d'automatisation.

["En savoir plus >>"](#).

En plus de ces kits d'outils, vous pouvez créer et déployer du code d'automatisation à l'aide de frameworks.

["En savoir plus >>"](#).

Stockage en cluster

L'itération actuelle de ONTAP a été développée à l'origine pour notre architecture de stockage scale-out *cluster*. C'est l'architecture que vous trouvez généralement dans les implémentations de data Center de ONTAP. Comme cette implémentation met en œuvre la plupart des fonctionnalités d'ONTAP, il est judicieux de commencer par comprendre les concepts qui la technologie ONTAP.

Les architectures de data Center déploient généralement des contrôleurs FAS ou AFF dédiés qui exécutent le

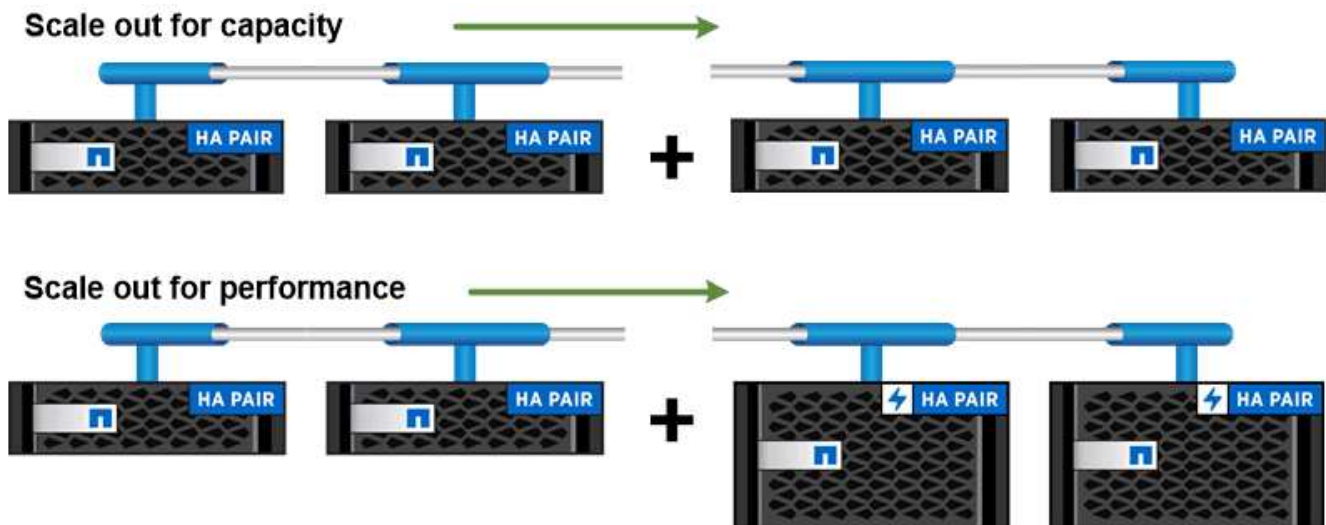
logiciel de gestion des données ONTAP. Chaque contrôleur, son stockage, sa connectivité réseau et l'instance d'ONTAP exécutée sur le contrôleur sont appelés « nœud_._ »

Les nœuds sont jumelés pour la haute disponibilité (HA). Ensemble, ces paires (jusqu'à 12 nœuds pour les SAN, jusqu'à 24 nœuds pour les NAS) constituent le cluster. Les nœuds communiquent les uns avec les autres via une interconnexion de cluster dédiée et privée.

Selon le modèle de contrôleur, le stockage des nœuds se compose de disques Flash, de disques haute capacité ou des deux. Les ports réseau du contrôleur permettent d'accéder aux données. Les ressources de stockage physique et de connectivité réseau sont virtualisées, visibles uniquement pour les administrateurs du cluster, et non pour les clients NAS ou les hôtes SAN.

Les nœuds d'une paire haute disponibilité doivent utiliser le même modèle de baie de stockage. Vous pouvez également utiliser toute combinaison de contrôleurs prise en charge. Vous pouvez faire évoluer horizontalement la capacité par l'ajout de nœuds avec des modèles de baie de stockage similaires ou pour la performance en ajoutant des nœuds aux baies de stockage plus haut de gamme.

Vous pouvez bien sûr évoluer verticalement comme vous le souhaitez, en mettant à niveau les disques et les contrôleurs selon vos besoins. L'infrastructure de stockage virtualisée d'ONTAP permet de déplacer facilement les données sans interrompre l'activité. Ainsi, vous pouvez évoluer verticalement ou horizontalement sans interruption.



You can scale out for capacity by adding nodes with like controller models, or for performance by adding nodes with higher-end storage arrays, all while clients and hosts continue to access data.

Pairs haute disponibilité

Les nœuds de cluster sont configurés sous forme de paires haute disponibilité_ pour la tolérance aux pannes et la continuité de l'activité. Si un nœud tombe en panne ou si vous devez arrêter un nœud pour assurer la maintenance de routine, son partenaire peut *reprendre* son stockage et continuer à transmettre les données à partir de celui-ci. Le partenaire *fournit* du stockage supplémentaire lorsque le nœud est revenu en ligne.

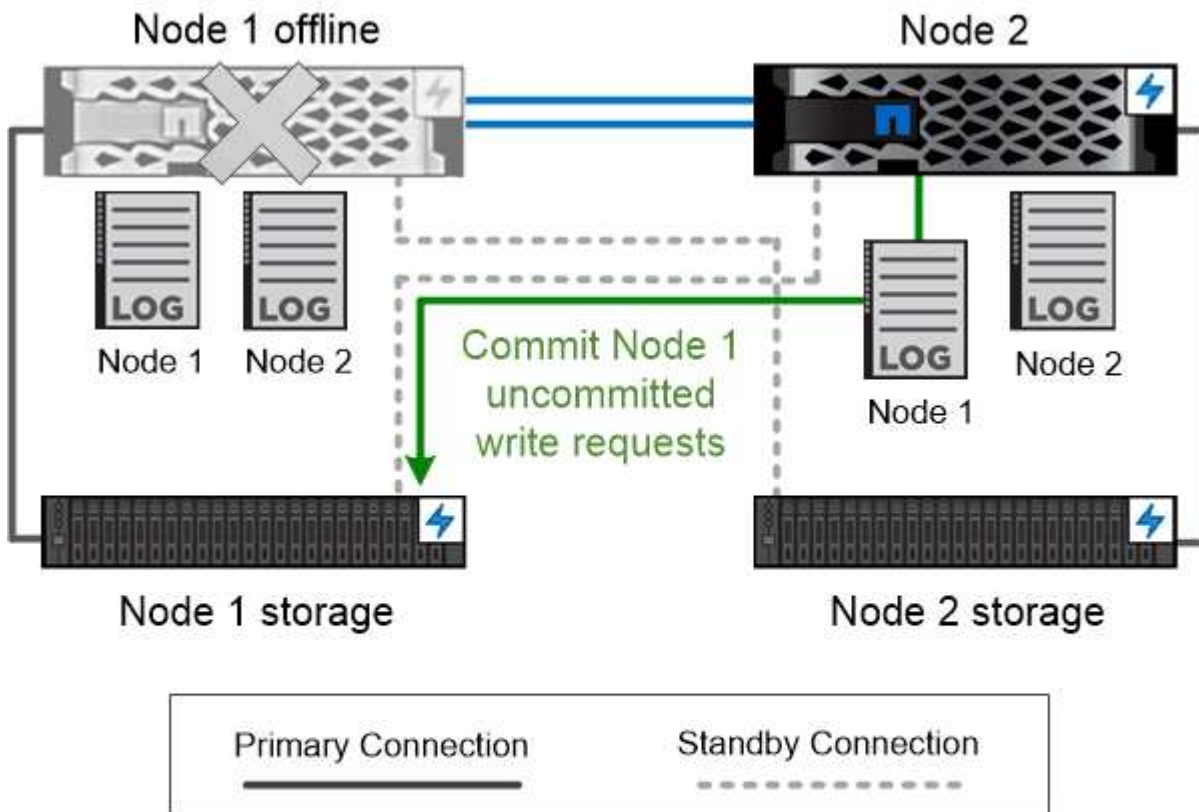
Les paires HAUTE DISPONIBILITÉ se composent toujours de modèles de contrôleurs similaires. Les contrôleurs se trouvent généralement dans le même châssis avec des blocs d'alimentation redondants.

Les paires haute disponibilité sont des nœuds tolérants aux pannes qui peuvent communiquer entre eux de

différentes manières, ce qui permet à chaque nœud de vérifier en permanence si son partenaire fonctionne et de mettre en miroir les données des journaux pour la mémoire non volatile de l'autre nœud. Lorsqu'une requête d'écriture est formulée sur un nœud, celle-ci est connectée en NVRAM sur les deux nœuds avant qu'une réponse ne soit renvoyée au client ou à l'hôte. Lors du basculement, le partenaire survivant engage les demandes d'écriture non validées du nœud défaillant vers le disque, pour assurer la cohérence des données.

Des connexions au support de stockage des autres contrôleurs permettent à chaque nœud d'accéder au stockage de l'autre contrôleur en cas de basculement. Les mécanismes de basculement de chemin réseau garantissent que les clients et les hôtes continuent de communiquer avec le nœud survivant.

Pour assurer la disponibilité, vous devez continuer à utiliser la capacité de performance sur l'un des nœuds à 50 % pour gérer les charges de travail supplémentaires en cas de basculement. Pour la même raison, il peut être préférable de ne pas configurer plus de 50 % du nombre maximal d'interfaces de réseau virtuel NAS pour un nœud.



On failover, the surviving partner commits the failed node's uncommitted write requests to disk, ensuring data consistency.

Le basculement et le retour dans les implémentations ONTAP virtualisées

Le stockage n'est pas partagé entre les nœuds dans les implémentations ONTAP virtualisées « sans partage » telles que Cloud Volumes ONTAP pour AWS ou ONTAP Select. Lorsqu'un nœud tombe en panne, son partenaire continue de transmettre des données à partir d'une copie en miroir synchrone des données du nœud. Il ne prend pas le relais du stockage du nœud, mais uniquement sa fonction de service des données.

Conseiller digital AutoSupport et Active IQ

ONTAP propose un contrôle et un reporting basés sur l'intelligence artificielle via un portail Web et une application mobile. Le composant AutoSupport de ONTAP envoie une télémétrie analysée par le conseiller digital Active IQ.

Active IQ vous permet d'optimiser votre infrastructure de données dans l'ensemble de votre cloud hybride grâce à un portail cloud et à une application mobile qui offrent des analyses prédictives et un support proactif. Les informations et les recommandations basées sur les données de Active IQ sont accessibles à tous les clients NetApp qui possèdent un contrat SupportEdge actif (les fonctionnalités varient selon le produit et le niveau de support).

Voici quelques avantages que vous pouvez faire avec Active IQ :

- Planification des mises à niveau. Active IQ identifie les problèmes qui peuvent être résolus dans votre environnement en effectuant une mise à niveau vers la plus récente version d'ONTAP et le composant Upgrade Advisor vous aide à planifier une mise à niveau réussie.
- Voir le bien-être du système. Votre tableau de bord Active IQ signale tout problème éventuel et vous aide à le corriger. Surveillez la capacité du système pour vous assurer que votre espace de stockage est insuffisant.
- Gestion des performances. Active IQ affiche les performances du système sur une période plus longue que ce que vous pouvez voir dans System Manager. Identifiez les problèmes de configuration et de système qui ont un impact sur les performances.
- Optimisez l'efficacité. Affichez les mesures de l'efficacité du stockage et identifiez des moyens de stocker plus de données dans moins d'espace.
- Voir l'inventaire et la configuration. Active IQ affiche des informations complètes sur l'inventaire et la configuration logicielle et matérielle. Voyez quand les contrats de service arrivent à expiration pour vous assurer de rester couverts.

Informations associées

["Documentation NetApp : conseiller digital Active IQ"](#)

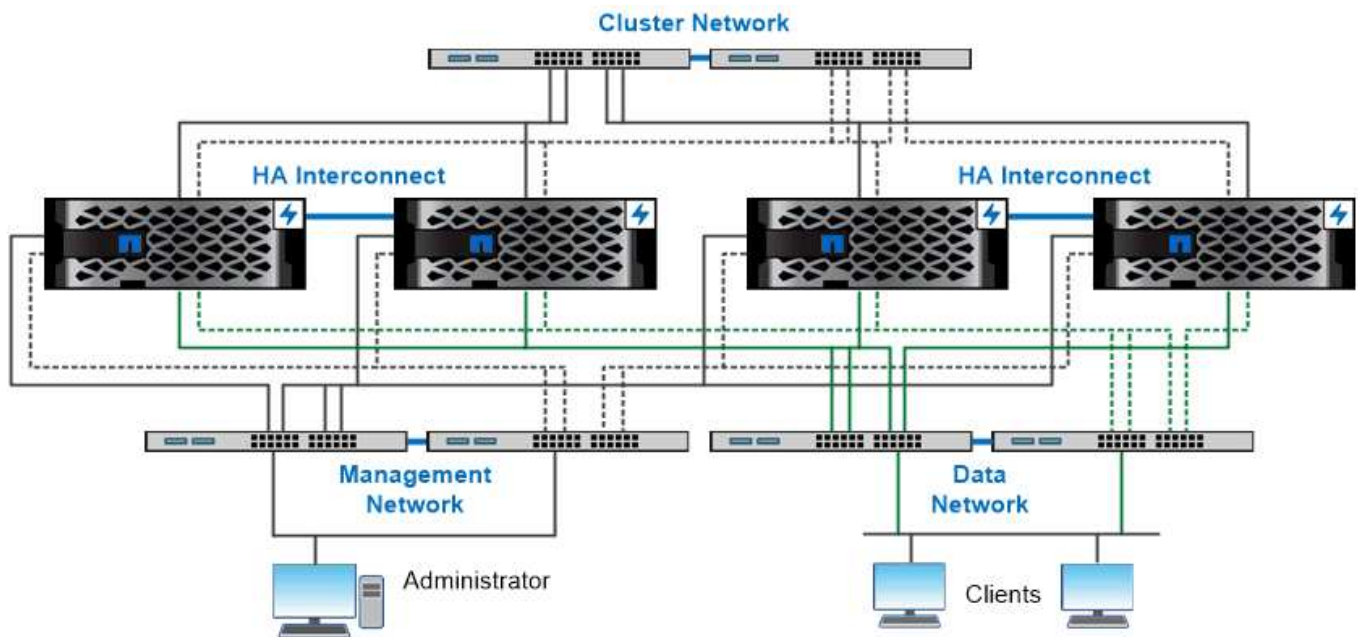
["Lancez Active IQ"](#)

["Services SupportEdge"](#)

Architecture du réseau

Présentation de l'architecture réseau

L'architecture réseau d'une implémentation de data Center ONTAP se compose généralement d'une interconnexion de cluster, d'un réseau de gestion pour l'administration de clusters et d'un réseau de données. Les cartes réseau (cartes d'interface réseau) fournissent des ports physiques pour les connexions Ethernet. Les HBA (adaptateurs de bus hôte) fournissent des ports physiques pour les connexions FC.



The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network.

Ports logiques

Outre les ports physiques fournis sur chaque nœud, vous pouvez utiliser *Logical ports* pour gérer le trafic réseau. Les ports logiques sont des groupes d'interfaces ou des VLAN.

Groupes d'interface

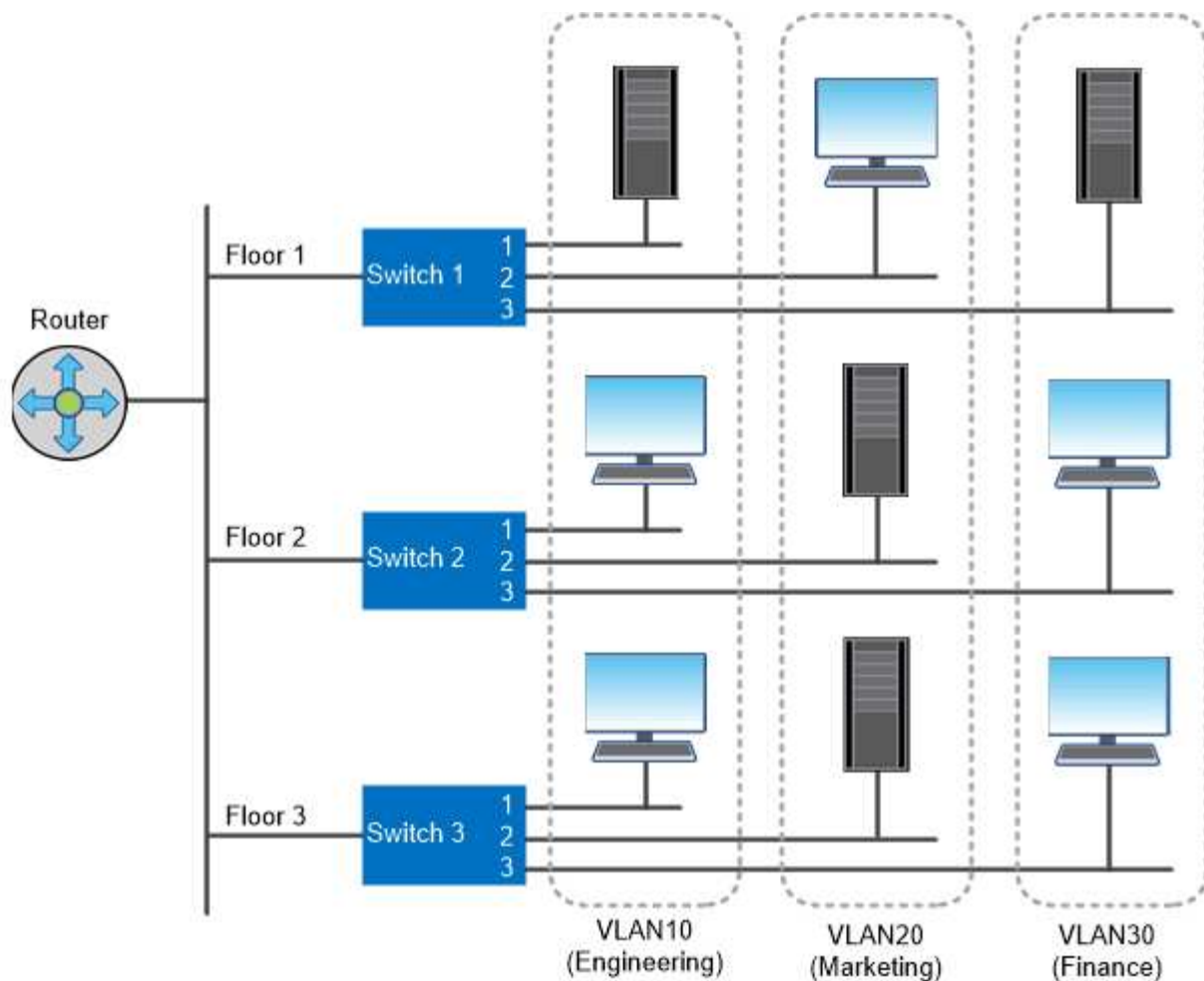
Interface Groups combine plusieurs ports physiques en un seul « port de jonction » logique. Vous pourriez vouloir créer un groupe d'interface composé de ports de cartes réseau dans différents emplacements PCI pour vous assurer qu'en cas de défaillance d'un slot, le trafic stratégique est réduit.

Un groupe d'interface peut être multimode ou dynamique en mode unique. Chaque mode offre différents niveaux de tolérance aux pannes. Vous pouvez utiliser l'un ou l'autre type de groupe d'interface multimode pour équilibrer la charge du trafic réseau.

VLAN

VLAN séparer le trafic d'un port réseau (qui peut être un groupe d'interfaces) en segments logiques définis sur une base de port de commutateur, plutôt que sur des limites physiques. Les *end-stations* appartenant à un VLAN sont liés par fonction ou application.

Vous pouvez regrouper les postes finaux par service, comme Ingénierie et Marketing, ou par projet, comme release1 et release2. Étant donné que la proximité physique des terminaux radio n'est pas pertinente dans un VLAN, les terminaux radio peuvent être géographiquement éloignés.



You can use VLANs to segregate traffic by department.

Prise en charge des technologies réseau standard

ONTAP prend en charge l'ensemble des principales technologies réseau standard de l'industrie. Les technologies clés sont les IPspaces, l'équilibrage de la charge DNS et les interruptions SNMP.

Les domaines de diffusion, les groupes de basculement et les sous-réseaux sont décrits dans le [Basculement de chemin NAS](#).

Les IPspaces

Vous pouvez utiliser un *IPspace* pour créer un espace d'adresse IP distinct pour chaque serveur de données virtuel dans un cluster. Ainsi, les clients se trouvant dans des domaines réseau distincts d'un point de vue administratif peuvent accéder aux données du cluster tout en utilisant des adresses IP redondantes à partir de la même plage de sous-réseaux.

Par exemple, un fournisseur de services peut configurer des IPspaces différents pour les locataires à l'aide des mêmes adresses IP pour accéder à un cluster.

Équilibrage de charge DNS

Vous pouvez utiliser *DNS load balancing* pour distribuer le trafic réseau des utilisateurs à travers les ports disponibles. Un serveur DNS sélectionne dynamiquement une interface réseau pour le trafic en fonction du nombre de clients montés sur l'interface.

Interruptions SNMP

Vous pouvez utiliser *SNMP traps* pour vérifier périodiquement la présence de seuils ou d'échecs opérationnels. Les interruptions SNMP capturent les informations de surveillance système envoyées de façon asynchrone d'un agent SNMP à un gestionnaire SNMP.

Conformité FIPS

ONTAP est conforme à la norme FIPS (Federal information Processing Standards) 140-2 pour toutes les connexions SSL. Vous pouvez activer et désactiver le mode SSL FIPS, définir globalement les protocoles SSL et désactiver tout chiffrement faible tel que RC4.

Présentation de RDMA

Les offres RDMA (Remote Direct Memory Access) d'ONTAP prennent en charge les charges de travail à large bande passante et sensibles à la latence. RDMA permet de copier directement les données entre la mémoire du système de stockage et la mémoire du système hôte, ce qui évite les interruptions du processeur et la surcharge.

NFS sur RDMA

Vous pouvez le configurer avec ONTAP 9.10.1 ["NFS sur RDMA"](#) Pour permettre l'utilisation du stockage NVIDIA GPUDirect pour les workloads avec accélération par processeur graphique sur des hôtes équipés de processeurs graphiques NVIDIA pris en charge.

Interconnexion de cluster RDMA

L'interconnexion de cluster RDMA réduit la latence, réduit les temps de basculement et accélère la communication entre les nœuds d'un cluster.

À partir de ONTAP 9.10.1, le protocole RDMA d'interconnexion de cluster est pris en charge pour certains systèmes matériels lorsqu'il est utilisé avec des cartes réseau de cluster X1151A. À partir de ONTAP 9.13.1, les cartes réseau X91153A prennent également en charge le protocole RDMA d'interconnexion de cluster. Consultez le tableau pour connaître les systèmes pris en charge dans les différentes versions de ONTAP.

Systèmes	Versions de ONTAP prises en charge
<ul style="list-style-type: none">AFF A400ASA A400	ONTAP 9.10.1 et versions ultérieures
<ul style="list-style-type: none">AFF A900ASA A900FAS9500	ONTAP 9.13.1 et versions ultérieures

Étant donné la configuration appropriée du système de stockage, aucune configuration supplémentaire n'est nécessaire pour utiliser l'interconnexion RDMA.

Protocoles clients

ONTAP prend en charge tous les principaux protocoles clients standard du secteur : NFS, SMB, FC, FCoE, iSCSI, NVMe et S3.

NFS

NFS est le protocole d'accès classique aux fichiers pour les systèmes UNIX et LINUX. Les clients peuvent accéder aux fichiers des volumes ONTAP à l'aide des protocoles suivants.

- NFSv3
- NFSv4
- NFSv4.2
- NFSv4.1
- PNFS

Vous pouvez contrôler l'accès aux fichiers à l'aide d'autorisations de style UNIX, d'autorisations de style NTFS ou d'une combinaison des deux.

Les clients peuvent accéder aux mêmes fichiers à l'aide des protocoles NFS et SMB.

PME

SMB est le protocole d'accès aux fichiers traditionnel pour les systèmes Windows. Les clients peuvent accéder aux fichiers des volumes ONTAP à l'aide des protocoles SMB 2.0, SMB 2.1, SMB 3.0 et SMB 3.1.1. Tout comme avec NFS, plusieurs styles d'autorisation sont pris en charge.

SMB 1.0 est disponible mais désactivé par défaut dans les versions ONTAP 9.3 et ultérieures.

FC

Fibre Channel est le protocole de bloc en réseau d'origine. Au lieu de fichiers, un protocole de bloc présente l'ensemble d'un disque virtuel à un client. Le protocole FC traditionnel utilise un réseau FC dédié avec des commutateurs FC spécialisés et requiert que l'ordinateur client possède des interfaces réseau FC.

Une LUN représente le disque virtuel et une ou plusieurs LUN sont stockées dans un volume ONTAP. La même LUN est accessible via les protocoles FC, FCoE et iSCSI, mais plusieurs clients ne peuvent accéder à la même LUN que s'ils font partie d'un cluster qui empêche les collisions d'écriture.

FCoE

FCoE est en gros le même protocole que FC, mais utilise un réseau Ethernet de data Center à la place du transport FC classique. Le client requiert toujours une interface réseau spécifique à FCoE.

iSCSI

iSCSI est un protocole de bloc capable de s'exécuter sur les réseaux Ethernet standard. La plupart des systèmes d'exploitation clients proposent un initiateur logiciel qui fonctionne sur un port Ethernet standard. iSCSI est un bon choix pour quand un protocole de bloc est nécessaire pour une application particulière, mais ne dispose pas d'une mise en réseau FC dédiée.

NVMe/FC et NVMe/TCP

Le nouveau protocole en mode bloc, NVMe, est spécialement conçu pour le stockage Flash. Dotée de sessions évolutives, d'une réduction considérable de la latence et d'une augmentation du parallélisme, cette solution convient parfaitement aux applications à faible latence et à haut débit, telles que les bases de données en mémoire et les analyses.

Contrairement à FC et iSCSI, NVMe n'utilise pas de LUN. Il utilise plutôt des espaces de noms, qui sont stockés dans un volume ONTAP. Les espaces de noms NVMe sont uniquement accessibles via le protocole NVMe.

S3

À partir de ONTAP 9.8, vous pouvez activer un serveur ONTAP simple Storage Service (S3) dans un cluster ONTAP, qui vous permet d'accéder aux données du stockage objet à l'aide des compartiments S3.

ONTAP prend en charge deux scénarios d'utilisation sur site pour la gestion du stockage objet S3 :

- FabricPool Tiering dans un compartiment du cluster local (Tier vers un compartiment local) ou du cluster distant (Tier cloud)
- L'application client S3 permet d'accéder à un compartiment sur le cluster local ou à distance.



ONTAP S3 est adapté si vous souhaitez utiliser des fonctionnalités S3 dans les clusters déjà en place, sans nécessiter de matériel ni de gestion supplémentaire. Pour des déploiements de plus de 300 To, le logiciel NetApp StorageGRID continue à être la solution phare de NetApp pour le stockage objet. Découvrez "[StorageGRID](#)".

Disques et agrégats

Présentation des disques et des niveaux locaux (agrégats)

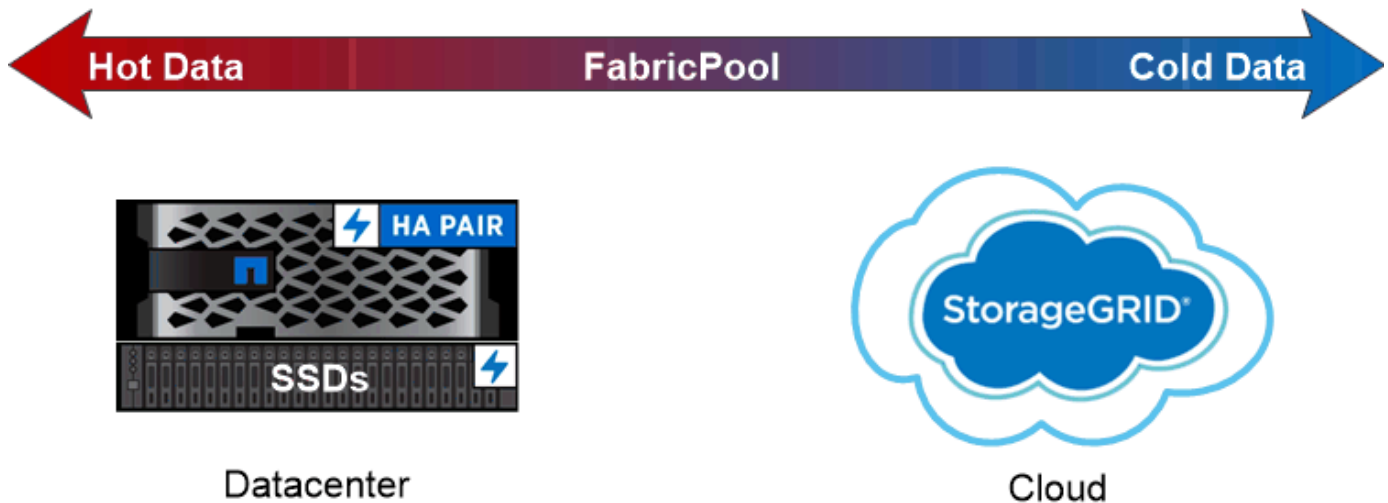
System Manager et l'interface de ligne de commandes vous permettent de gérer le stockage physique ONTAP. Vous pouvez créer, développer et gérer des niveaux locaux (agrégats), travailler avec les niveaux locaux Flash Pool (agrégats), gérer les disques et gérer les règles RAID.

De quels niveaux locaux (agrégats) sont-ils

Local tiers (également appelé *Aggregates*) sont des conteneurs pour les disques gérés par un nœud. Vous pouvez utiliser des niveaux locaux pour isoler des charges de travail présentant différents besoins en performances, hiérarchiser les données selon différents modèles d'accès ou isoler les données à des fins réglementaires.

- Vous pouvez créer un niveau local composé exclusivement de SSD pour les applications stratégiques qui nécessitent une latence la plus faible et des performances maximales.
- Pour hiérarchiser les données selon différents modèles d'accès, vous pouvez créer un *niveau local hybride* en déployant Flash comme cache haute performance pour un jeu de données de travail, tout en utilisant des disques durs à moindre coût ou un stockage objet pour les données moins fréquemment utilisées.
 - *Flash Pool* est composé à la fois de SSD et de disques durs.
 - Un *FabricPool* consiste en un niveau local tout SSD avec un magasin d'objets attaché.
- Si vous devez isoler les données archivées de données actives à des fins réglementaires, vous pouvez

utiliser un niveau local composé de disques durs haute capacité ou encore une combinaison de disques durs performants et haute capacité.



You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed “hot” data and object storage for rarely accessed “cold” data.

Utilisation des niveaux locaux (agrégats)

Vous pouvez effectuer les tâches suivantes :

- ["Gestion des niveaux locaux \(agrégats\)"](#)
- ["Gérer les disques"](#)
- ["Gérer les configurations RAID"](#)
- ["Gestion des niveaux Flash Pool"](#)

Vous pouvez effectuer ces tâches si les conditions suivantes sont vraies :

- Vous ne souhaitez pas utiliser un outil de script automatique.
- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.
- Vous disposez d'une configuration MetroCluster et vous suivez les procédures décrites dans ["MetroCluster"](#) documentation sur la configuration initiale et les instructions relatives aux niveaux locaux (agrégats) et à la gestion des disques.

Informations associées

- ["Gérer les niveaux clouds FabricPool"](#)

Niveaux locaux (agrégats) et groupes RAID

Les technologies RAID modernes protègent contre les défaillances de disque en reconstruisant les données d'un disque défaillant sur un disque de secours. Le système compare les informations d'index sur un « disque de parité » avec les données des disques restants en bonne santé pour reconstruire les données manquantes, le tout sans

temps d'arrêt ni coûts de performances significatifs.

Un niveau local (agrégat) se compose d'un ou plusieurs *RAID Groups*. Le *RAID type* du niveau local détermine le nombre de disques de parité du groupe RAID et le nombre de pannes de disque simultanées que la configuration RAID protège contre.

Le type RAID par défaut, RAID-DP (RAID-double parité), requiert deux disques de parité par groupe RAID et protège contre les pertes de données en cas de défaillance simultanée de deux disques. Pour le RAID-DP, la taille de groupe RAID recommandée est comprise entre 12 et 20 disques durs et entre 20 et 28 disques SSD.

Vous pouvez répartir le coût supplémentaire des disques de parité en créant des groupes RAID à la partie supérieure des recommandations de dimensionnement. Ceci est particulièrement vrai pour les disques SSD, qui sont bien plus fiables que les disques haute capacité. Pour les niveaux locaux utilisant des disques durs, il est conseillé de choisir entre l'optimisation du stockage sur disque et les facteurs compensatoires, comme le délai de reconstruction plus long requis pour les groupes RAID plus volumineux.

Niveaux locaux en miroir et sans mise en miroir (agrégats)

ONTAP dispose d'une fonction optionnelle appelée *SyncMirror* que vous pouvez utiliser pour mettre en miroir les données de niveau local (agrégat) de manière synchrone dans des copies, ou *plex*, stockées dans différents groupes RAID. Les plexes permettent d'éviter les pertes de données en cas de panne de l'ensemble des disques de type RAID, ou en cas de perte de connectivité aux disques du groupe RAID.

Lorsque vous créez un niveau local avec System Manager ou depuis l'interface de ligne de commandes, vous pouvez spécifier que le niveau local est mis en miroir ou non.

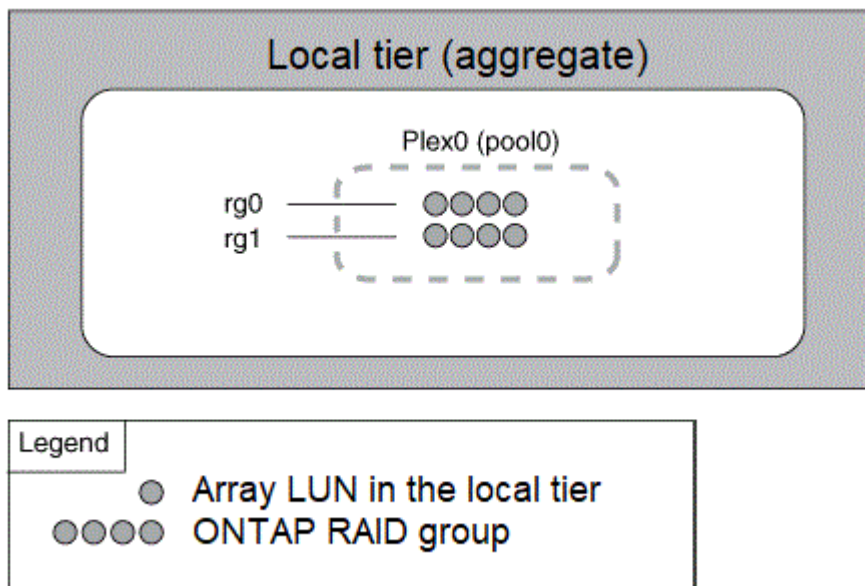
Fonctionnement des niveaux locaux non mis en miroir (agrégats)

Si vous ne spécifiez pas que les niveaux locaux sont mis en miroir, ils sont créés en tant que niveaux locaux non mis en miroir (agrégats). Les niveaux locaux non mis en miroir ne possèdent qu'un seul *plex* (une copie de leurs données), qui contient tous les groupes RAID appartenant à ce niveau local.

Le schéma suivant montre un niveau local non mis en miroir composé de disques, avec son plex unique. Le niveau local a quatre groupes RAID : rg0, rg1, rg2 et rg3. Chaque groupe RAID comporte six disques de données, un disque de parité et un disque de parité (double parité). Tous les disques utilisés par le niveau local proviennent du même pool, ""pool0"".



Le schéma suivant présente un niveau local non mis en miroir avec des LUN de matrice, avec son plex unique. Il dispose de deux groupes RAID, rg0 et rg1. Toutes les LUN de baie utilisées par le niveau local proviennent du même pool, « pool0 ».



Fonctionnement des niveaux locaux en miroir (agrégats)

Les agrégats en miroir possèdent deux plexes_ (copies de leurs données), qui exploitent la fonctionnalité SyncMirror pour dupliquer les données pour assurer la redondance.

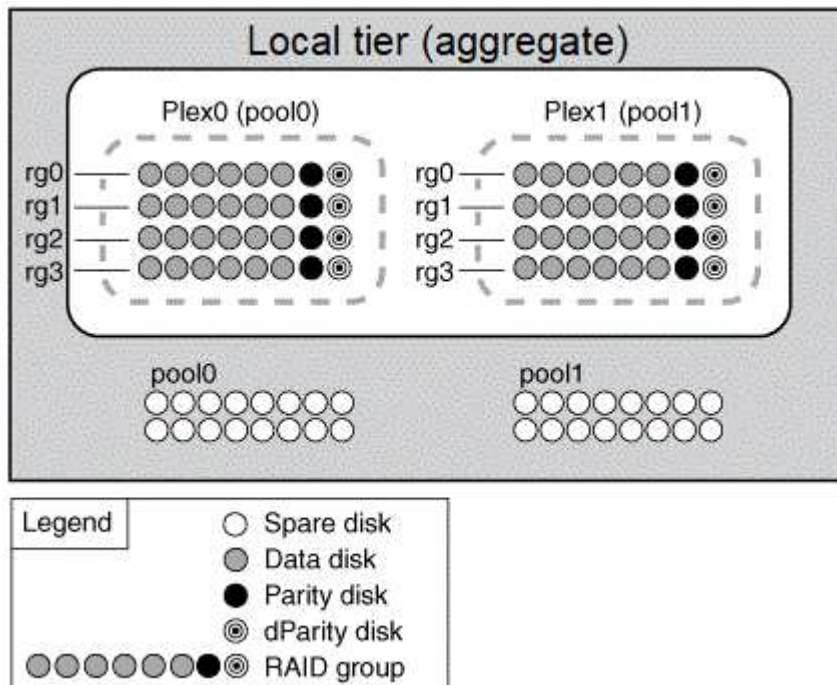
Lorsque vous créez un niveau local, vous pouvez spécifier qu'il s'agit d'un niveau local mis en miroir. En outre, vous pouvez ajouter un second plex à un niveau local non mis en miroir existant pour en faire un niveau en miroir. Grâce à la fonctionnalité SyncMirror, ONTAP copie les données du plex d'origine (plex0) sur le nouveau plex (plex1). Les plexes sont séparés physiquement (chaque plex dispose de ses propres groupes RAID et de

son propre pool), et les plex sont mis à jour simultanément.

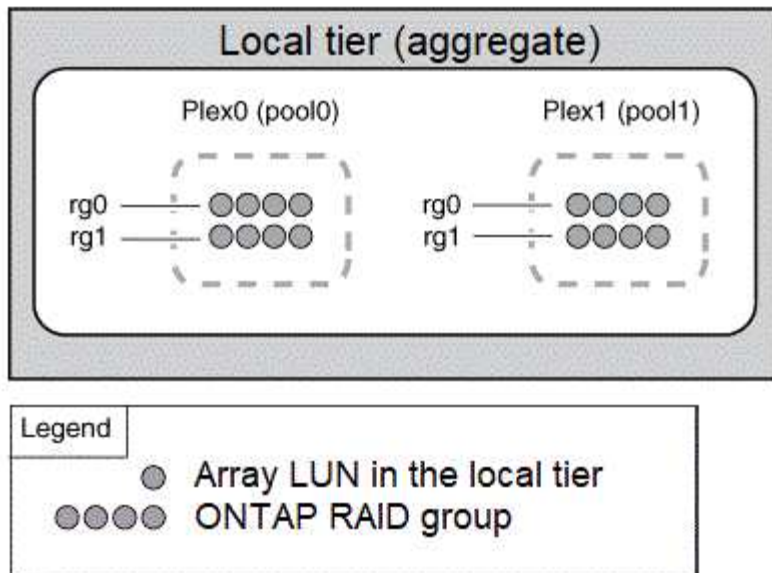
Cette configuration renforce la protection contre la perte de données en cas de défaillance de plus de disques que le niveau RAID de l'agrégat assure la protection contre ou en cas de perte de connectivité, car le plex non affecté continue de transmettre les données pendant que vous corrigez la cause de la défaillance. Une fois le plex qui avait un problème résolu, les deux plexes se synchronisaient et rétablissent la relation du miroir.

Les disques et les unités logiques de baie du système sont répartis en deux pools : « pool0 » et « pool1 ». Plex0 obtient son stockage de pool0 et plex1 obtient son stockage de pool1.

Le schéma suivant présente un niveau local composé de disques pour que la fonctionnalité SyncMirror soit activée et implémentée. Un second plex a été créé pour le niveau local, « plex1 ». Les données dans le plex1 sont une copie des données dans le plex0 et les groupes RAID sont également identiques. Les 32 disques de réserve sont alloués à pool0 ou pool1 en utilisant 16 disques par pool.



Le schéma suivant présente un niveau local composé de LUN de baie dont la fonctionnalité SyncMirror est activée et implémentée. Un second plex a été créé pour le niveau local, « plex1 ». Plex1 est une copie de plex0 et les groupes RAID sont également identiques.



Pour optimiser les performances et la disponibilité du stockage, il est recommandé de conserver au moins 20 % d'espace libre pour les agrégats en miroir. Bien que la recommandation soit de 10 % pour les agrégats non mis en miroir, le système de fichiers peut utiliser 10 % d'espace supplémentaire pour absorber les modifications incrémentielles. Les modifications incrémentielles augmentent l'utilisation de l'espace pour les agrégats en miroir grâce à l'architecture Snapshot d'ONTAP basée sur la copie en écriture. Le non-respect de ces meilleures pratiques peut avoir un impact négatif sur les performances.

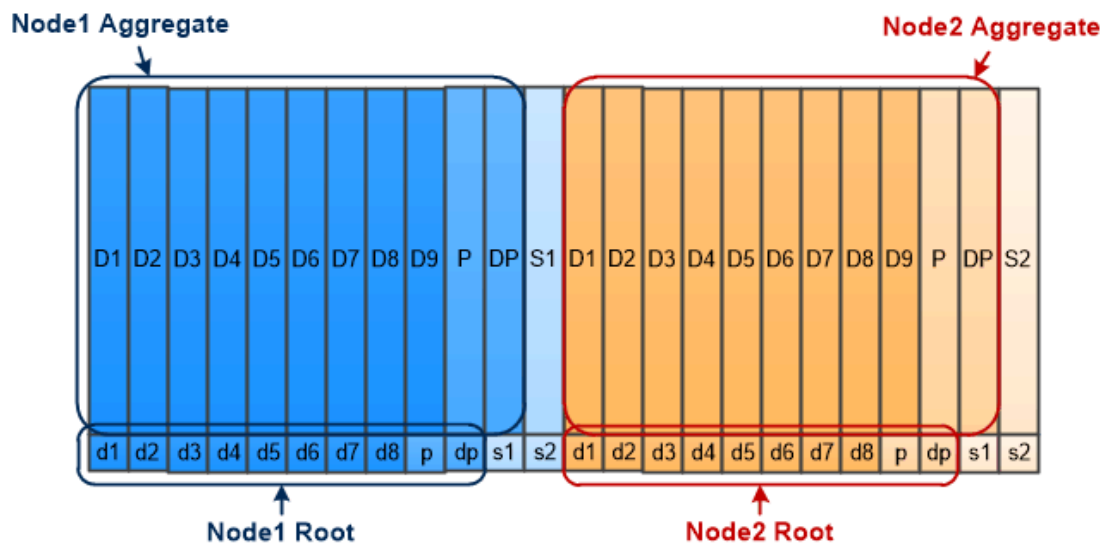
Partitionnement données-racines

Chaque nœud doit disposer d'un agrégat racine pour les fichiers de configuration du système de stockage. L'agrégat root dispose du type RAID de l'agrégat de données.

System Manager ne prend pas en charge le partitionnement données-racines ou données-racines.

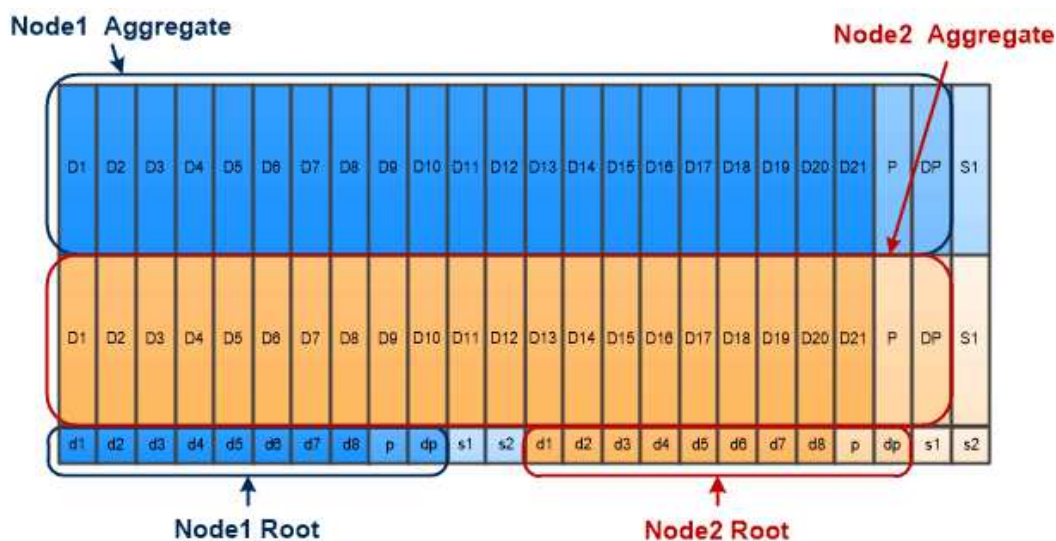
Un agrégat racine de type RAID-DP se compose généralement d'un disque de données et de deux disques de parité. Il s'agit là d'un surcoût important « parité » pour payer les fichiers du système de stockage, lorsque le système réserve déjà deux disques en tant que disques de parité pour chaque groupe RAID de l'agrégat.

Root-Data partition réduit les taxes sur les parité en répartissant l'agrégat racine sur les partitions de disque, en réservant une petite partition sur chaque disque en tant que partition racine et une grande partition pour les données.



Root-data partitioning creates one small partition on each disk as the root partition and one large partition on each disk for data.

Comme l'indique l'illustration, plus le nombre de disques utilisés pour stocker l'agrégat racine est important, plus la partition racine est petite. C'est également le cas d'une forme de partitionnement données-racines appelée *root-data-partition*, qui crée une petite partition comme partition racine et deux partitions de taille égale pour les données.



Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.

Les deux types de partitionnement données-racines font partie de la fonctionnalité ONTAP *Advanced Drive Partitionnement (ADP)*. Les deux sont configurés en usine : partitionnement données-racines pour les systèmes d'entrée de gamme FAS2xxx, FAS9000, FAS8200, FAS80xx et AFF, partitionnement données-racines uniquement pour les systèmes AFF.

En savoir plus sur ["Partitionnement de disque avancé"](#).

Disques partitionnés et utilisés pour l'agrégat racine

Les disques partitionnés à utiliser dans l'agrégat racine dépendent de la configuration du système.

Connaître le nombre de disques utilisés pour l'agrégat racine vous aide à déterminer la capacité des disques consacrée à la partition racine, et la quantité disponible pour un agrégat de données.

La fonctionnalité de partitionnement données-racines est prise en charge pour les plateformes d'entrée de gamme, les plateformes FAS 100 % Flash et les plateformes FAS uniquement associées à des disques SSD.

Pour les plateformes d'entrée de gamme, seuls les disques internes sont partitionnés.

Pour toutes les plateformes FAS Flash et FAS avec uniquement des disques SSD connectés, tous les disques reliés au contrôleur lors de l'initialisation du système sont partitionnés, dans la limite de 24 par nœud. Les disques ajoutés après la configuration du système ne sont pas partitionnés.

Volumes, qtrees, fichiers et LUN

ONTAP fournit les données aux clients et aux hôtes à partir des conteneurs logiques appelés *FlexVol volumes*. ces volumes étant associés uniquement à leur agrégat contenant, ils offrent une plus grande flexibilité de gestion des données que les volumes traditionnels.

Vous pouvez attribuer plusieurs volumes FlexVol à un agrégat, chacun dédié à une autre application ou service. Vous pouvez étendre et réduire un volume FlexVol, déplacer un volume FlexVol et effectuer des copies efficaces d'un volume FlexVol. Vous pouvez utiliser des qtrees_ pour partitionner un volume FlexVol en unités plus gérables et quotas pour limiter l'utilisation des ressources des volumes.

Les volumes contiennent des systèmes de fichiers dans un environnement NAS et des LUN dans un environnement SAN. Une LUN (numéro d'unité logique) est un identifiant pour un périphérique appelé une unité logique_adressée par un protocole SAN.

Les LUN sont l'unité de stockage de base dans une configuration SAN. L'hôte Windows considère que des LUN de votre système de stockage sont des disques virtuels. Vous pouvez déplacer des LUN vers d'autres volumes sans interruption.

Outre les volumes de données, vous devez connaître quelques volumes spéciaux :

- Un *node root volume* (en général « vol0 ») contient des informations sur la configuration du nœud et des journaux.
- Un *SVM root volume* sert de point d'entrée au namespace fourni par le SVM et contient des informations sur le répertoire d'espace de noms.
- *System volumes* contient des métadonnées spéciales telles que les journaux d'audit de service.

Vous ne pouvez pas utiliser ces volumes pour stocker des données.



Volumes contain files in a NAS environment and LUNs in a SAN environment.

volumes FlexGroup

Dans certaines entreprises, un seul namespace peut nécessiter plusieurs pétaoctets de stockage, voire même une capacité de 100 To d'un volume FlexVol.

Un *FlexGroup volume* prend en charge jusqu'à 400 milliards de fichiers avec 200 volumes de membres constitutifs qui travaillent en collaboration afin d'équilibrer de façon dynamique la charge et l'allocation d'espace entre les différents membres.

Les volumes FlexGroup ne nécessitent aucune surcharge administrative ou de maintenance. Il vous suffit de créer le volume FlexGroup et de le partager avec vos clients NAS. ONTAP se charge du reste.

Virtualisation du stockage

Présentation de la virtualisation du stockage

Utilisez *Storage Virtual machines (SVM)* pour fournir des données aux clients et aux hôtes. À l'instar d'une machine virtuelle fonctionnant sur un hyperviseur, un SVM est une entité logique qui extrait les ressources physiques. L'accès aux données via la SVM n'est pas limité à un emplacement de stockage. L'accès réseau au SVM n'est pas lié à un port physique.



Les SVM étaient auparavant appelés « vservers ». L'interface de ligne de commande de ONTAP utilise toujours le terme « vserver ».

Un SVM fournit des données aux clients et hôtes depuis un ou plusieurs volumes via une ou plusieurs interfaces logiques réseau (LIF). Les volumes peuvent être affectés à n'importe quel agrégat de données du cluster. Les LIFs peuvent être hébergées par n'importe quel port physique ou logique. Les volumes et les LIF peuvent être déplacés sans interrompre le service de données, que vous travailliez pour des mises à niveau

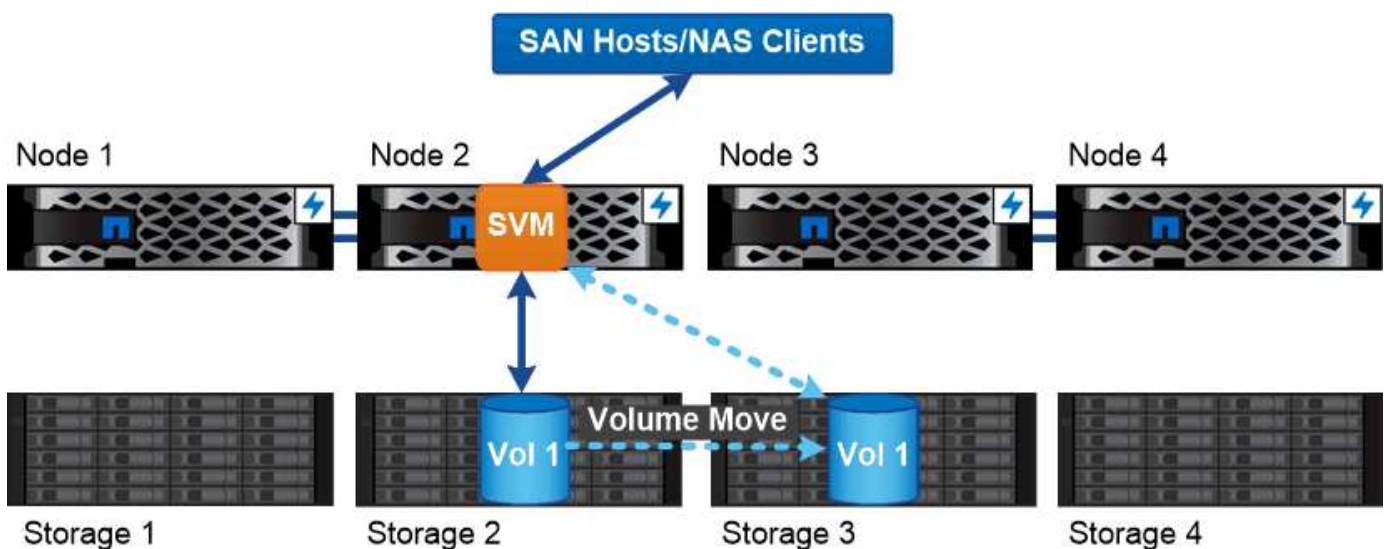
matérielles, des nœuds, des équilibrer les performances ou optimiser la capacité entre les agrégats.

La même SVM peut disposer d'une LIF pour le trafic NAS et d'une LIF pour le trafic SAN. Les clients et les hôtes ont uniquement besoin de l'adresse de la LIF (adresse IP pour NFS, SMB ou iSCSI ; WWPN pour FC) pour accéder à la SVM. Les LIF conservent leur adresse lors de leur déplacement. Les ports peuvent héberger de multiples LIFs. Chaque SVM possède son propre système de sécurité, d'administration et de namespace.

En plus des SVM de données, ONTAP déploie des SVM spéciaux pour l'administration :

- Un SVM *admin* est créé lorsque le cluster est configuré.
- Un *node SVM* est créé lorsqu'un nœud rejoint un cluster nouveau ou existant.
- Un SVM_System_ est automatiquement créé pour les communications au niveau du cluster dans un IPspace.

Vous ne pouvez pas utiliser ces SVM pour fournir des données. Il existe également des LIF spéciales permettant le trafic au sein des clusters et entre eux, et pour la gestion du cluster et des nœuds.



Data accessed through an SVM is not bound to a physical storage location. You can move a volume without disrupting data service.

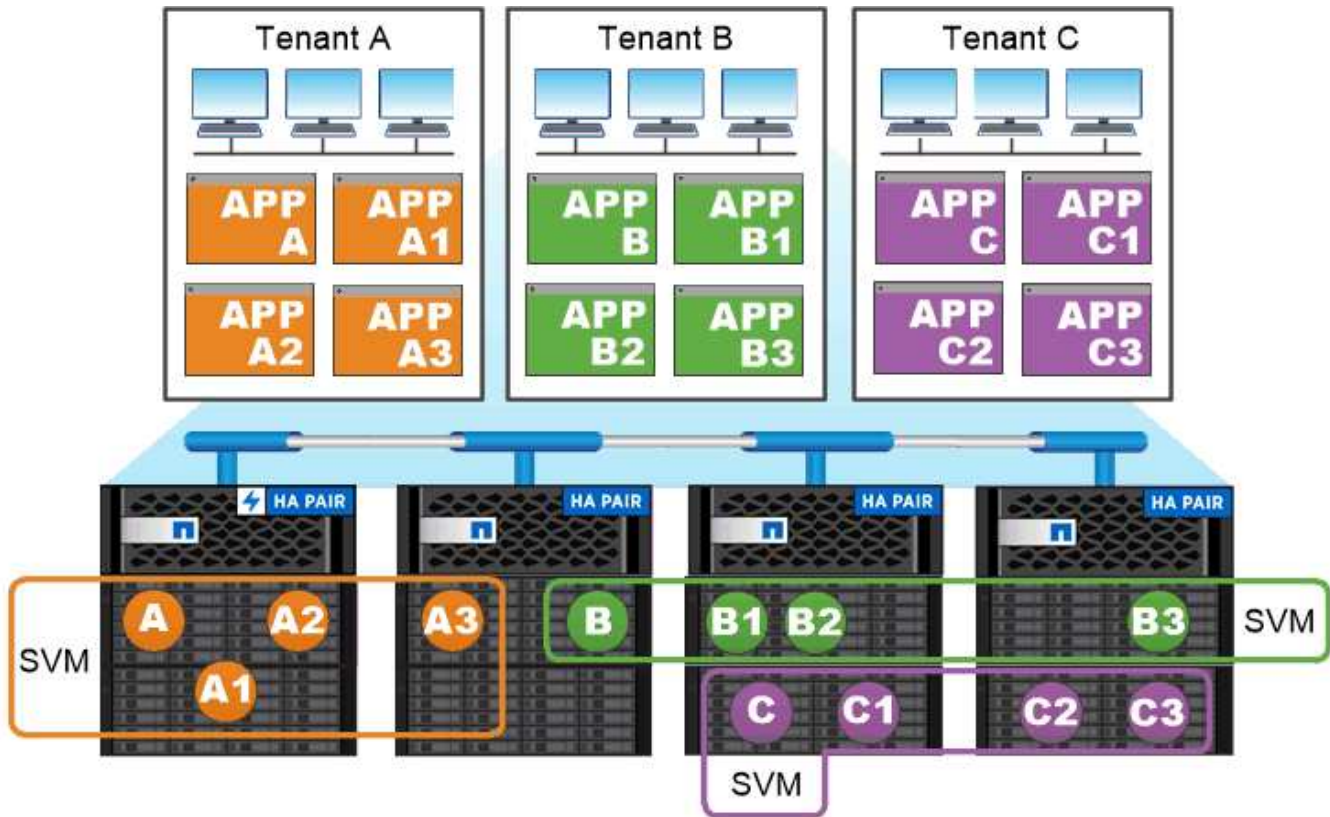
Pourquoi ONTAP est comme le middleware

Les objets logiques utilisés par ONTAP pour les tâches de gestion du stockage servent les objectifs familiers d'un paquet de middleware bien conçu : protéger l'administrateur des détails de mise en œuvre de bas niveau et isoler la configuration des modifications de caractéristiques physiques telles que les nœuds et les ports. De base, l'administrateur doit pouvoir déplacer facilement des volumes et des LIF en reconfigurer quelques champs au lieu de l'intégralité de l'infrastructure de stockage.

Cas d'utilisation de SVM

Les Service Providers utilisent des SVM dans le cadre d'accords de colocation sécurisée afin d'isoler les données de chaque locataire, de fournir à chacun d'eux ses propres fonctionnalités d'authentification et d'administration, et de simplifier la refacturation. Vous pouvez attribuer plusieurs LIF à la même SVM afin de répondre aux différents besoins des clients et utiliser la qualité de service pour vous protéger des charges de travail mutualisées et « brider » les charges de travail des autres locataires.

Les administrateurs utilisent des SVM à des fins similaires dans l'entreprise. Vous pouvez isoler les données de différents départements ou préserver l'accès aux volumes de stockage des hôtes dans un SVM et les volumes de partage d'utilisateurs dans un autre. Certains administrateurs placent les LUN iSCSI/FC et les datastores NFS dans un partage SVM et SMB dans un autre.



Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.

Administration des clusters et des SVM

Un *cluster Administrator* accède au SVM d'admin pour le cluster. La SVM d'admin et un administrateur du cluster avec le nom réservé `admin` sont automatiquement créées lorsque le cluster est configuré.

Un administrateur de cluster avec la valeur par défaut `admin` le rôle peut administrer l'ensemble du cluster et ses ressources. L'administrateur du cluster peut créer d'autres administrateurs de cluster disposant de différents rôles selon les besoins.

Un *administrateur SVM* accède à un SVM de données. L'administrateur du cluster crée des SVM de données et des administrateurs SVM si nécessaire.

Les administrateurs du SVM sont affectés à `vsadmin` rôle par défaut. L'administrateur du cluster peut attribuer différents rôles aux administrateurs du SVM si nécessaire.

contrôle d'accès basé sur les rôles (RBAC)

Le *role* attribué à un administrateur détermine les commandes auxquelles l'administrateur a accès. Vous attribuez le rôle lorsque vous créez le compte pour l'administrateur. Vous pouvez attribuer un autre rôle ou définir des rôles personnalisés selon vos besoins.

Espaces de noms et points de jonction

Un NAS *namespace* est un regroupement logique de volumes regroupés à *Junction points* pour créer une seule hiérarchie de système de fichiers. Un client disposant des autorisations suffisantes peut accéder aux fichiers dans l'espace de noms sans spécifier l'emplacement des fichiers dans le stockage. Des volumes regroupés dans le cluster peuvent se trouver n'importe où.

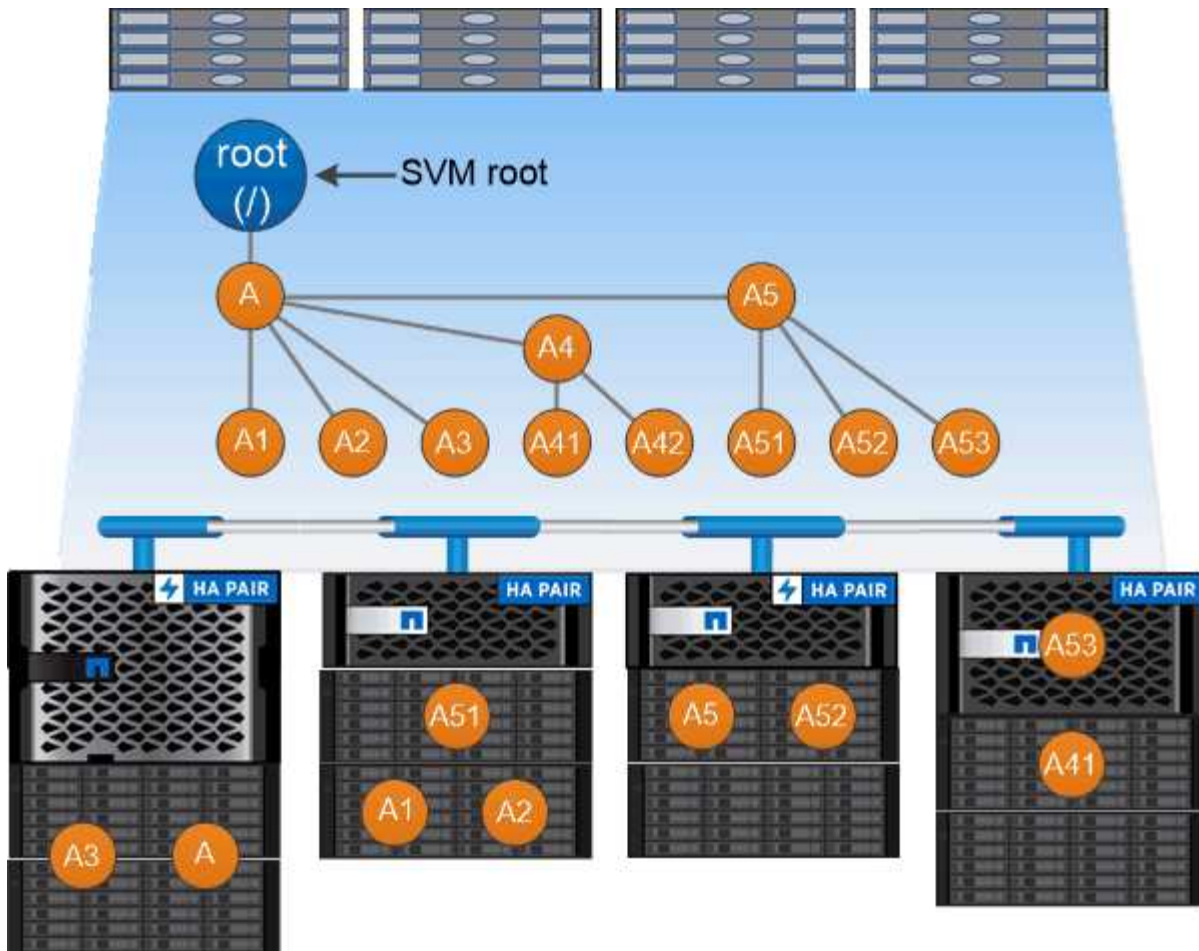
Plutôt que de monter chaque volume contenant un fichier d'intérêt, les clients NAS monter un NFS *export* ou accéder à un partage SMB. L'exportation ou le partage représente l'intégralité de l'espace de noms ou un emplacement intermédiaire dans l'espace de noms. Le client n'accède qu'aux volumes montés sous son point d'accès.

Vous pouvez ajouter des volumes au namespace selon vos besoins. Vous pouvez créer des points de jonction directement en-dessous d'une jonction de volume parent ou sur un répertoire au sein d'un volume. Il se peut qu'un chemin vers une jonction de volume pour un volume nommé « vol3 » soit possible /vol1/vol2/vol3, ou /vol1/dir2/vol3, ou même /dir1/dir2/vol3. Le chemin est appelé *Junction path*.

Chaque SVM possède un espace de noms unique. Le volume root du SVM est le point d'entrée de la hiérarchie de l'espace de noms.



Pour garantir la disponibilité des données en cas de panne du nœud ou de basculement, vous devez créer une copie *load-sharing mirror* pour le volume root du SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Exemple

L'exemple suivant crée un volume nommé « maison 4 » situé sur le SVM vs1 qui a une Junction path /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

Basculement de chemin

Présentation du basculement de chemin

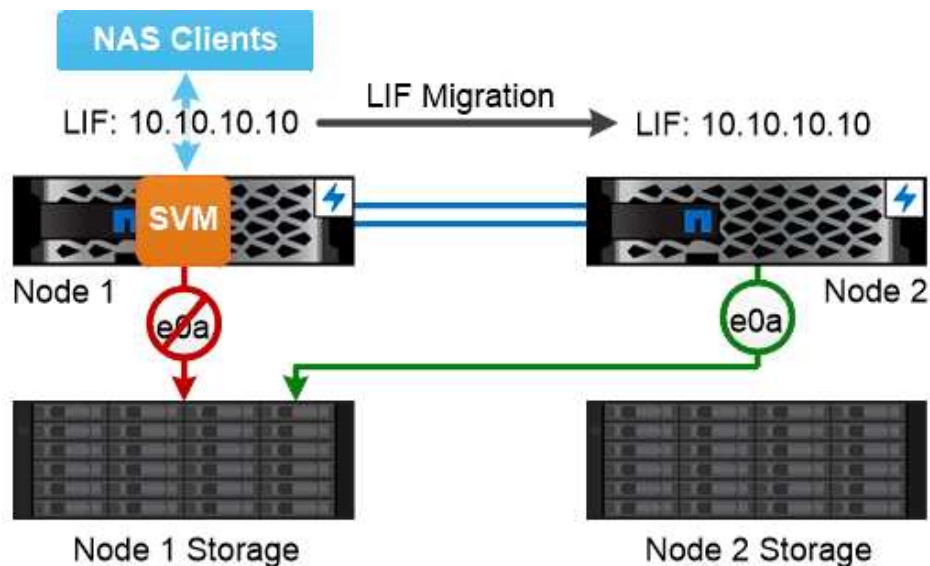
La gestion du basculement de chemin dans les topologies NAS et SAN est deux différences importantes dans la façon dont ONTAP gère ce basculement. Une LIF NAS migre automatiquement vers un autre port réseau après une panne de liaison. Une LIF SAN ne migre pas (sauf si vous la déplacez manuellement après la panne). La technologie de chemins d'accès multiples sur l'hôte transfère le trafic vers une autre LIF—sur le même SVM, mais vers un autre port réseau.

Basculement de chemin NAS

Une LIF NAS migre automatiquement vers un port réseau survivant après une panne de liaison sur son port actuel. Le port vers lequel la LIF migre doit être membre de la *failover group* pour la LIF. La *failover group policy* permet de rétrécir les cibles de basculement pour une LIF de données vers les ports sur le nœud qui possède les données et son partenaire de haute disponibilité.

Pour des raisons de commodité administrative, ONTAP crée un groupe de basculement pour chaque *broadcast domain* dans l'architecture réseau. Les domaines de diffusion regroupent des ports appartenant au même réseau de couche 2. Si vous utilisez des VLAN, par exemple, pour isoler le trafic par département (ingénierie, marketing, finance, etc.), chaque VLAN définit un domaine de diffusion distinct. Le groupe de basculement associé au domaine de diffusion est automatiquement mis à jour chaque fois que vous ajoutez ou supprimez un port de broadcast domain.

Il est presque toujours bon d'utiliser un domaine de diffusion pour définir un groupe de basculement pour s'assurer que le groupe de basculement reste à jour. Toutefois, vous pouvez parfois définir un groupe de basculement qui n'est pas associé à un domaine de diffusion. Par exemple, vous pouvez vouloir que les LIFs échouent uniquement en cas de ports d'un sous-ensemble des ports définis dans le broadcast domain.



A NAS LIF automatically migrates to a surviving network port after a link failure on its current port.

sous-réseaux

A *subnet* réserve un bloc d'adresses IP dans un domaine de diffusion. Ces adresses appartiennent au même réseau de couche 3 et sont allouées aux ports du broadcast domain lorsque vous créez une LIF. Il est généralement plus facile et moins sujette aux erreurs pour spécifier un nom de sous-réseau lorsque vous définissez une adresse LIF qu'il ne doit spécifier une adresse IP et un masque réseau.

Basculement de chemin SAN

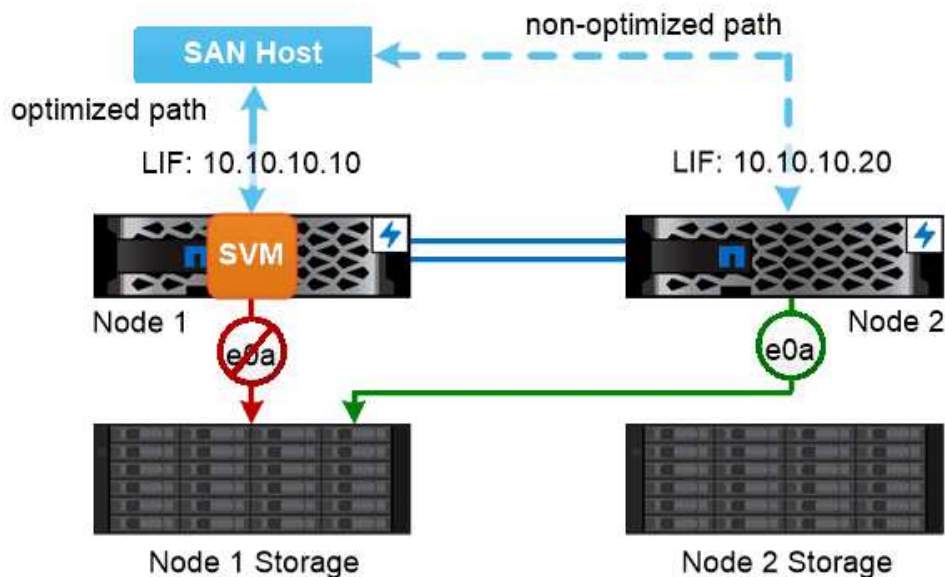
Un hôte SAN utilise le protocole ALUA (Asymmetric Logical Unit Access) et MPIO

(chemins d'accès E/S multiples) pour rediriger le trafic vers un LIF survivant après une défaillance de liaison. Les chemins prédéfinis déterminent les voies possibles vers la LUN desservie par la SVM.

Dans un environnement SAN, les hôtes sont considérés comme des *initiateurs* des requêtes vers des LUN *Targets*. MPIO active plusieurs chemins d'accès des initiateurs aux cibles. ALUA identifie les chemins les plus directs, appelés « chemins optimisés »._

Vous configurez généralement plusieurs chemins optimisés vers les LIF sur le nœud propriétaire de la LUN, ainsi que plusieurs chemins non optimisés vers ceux-ci sur son partenaire haute disponibilité. Si un port tombe en panne sur le nœud propriétaire, l'hôte achemine le trafic vers les ports survivants. Si tous les ports échouent, l'hôte achemine le trafic sur les chemins non optimisés.

Par défaut, ONTAP Selective LUN Map (SLM) limite le nombre de chemins d'accès de l'hôte à une LUN. Une LUN nouvellement créée est accessible uniquement via des chemins vers le nœud qui possède la LUN ou son partenaire de haute disponibilité. Vous pouvez également limiter l'accès à une LUN en configurant des LIFs dans un *port set* pour l'initiateur.



A SAN host uses multipathing technology to reroute traffic to a surviving LIF after a link failure.

déplacement de volumes dans des environnements SAN

Par défaut, ONTAP *Selective LUN Map (SLM)* limite le nombre de chemins d'accès à une LUN à partir d'un hôte SAN. Une LUN nouvellement créée n'est accessible qu'via des chemins vers le nœud qui possède la LUN ou son partenaire de haute disponibilité, le *node reporting* pour la LUN.

En effet, lorsque vous déplacez un volume vers un nœud d'une autre paire haute disponibilité, vous devez ajouter des nœuds de reporting pour la paire haute disponibilité de destination au mappage de LUN. Vous pouvez ensuite spécifier les nouveaux chemins dans la configuration de MPIO. Une fois le déplacement de volume terminé, vous pouvez supprimer des nœuds de reporting de la paire haute disponibilité source du mappage.

Équilibrage de la charge

Les performances des charges de travail commencent à être affectées par la latence lorsque le volume de travail d'un nœud dépasse les ressources disponibles. Vous pouvez gérer un nœud surchargé en augmentant les ressources disponibles (mise à niveau des disques ou du processeur) ou en réduisant la charge (déplacement de volumes ou de LUN vers des nœuds différents selon les besoins).

Vous pouvez également utiliser la qualité de service (QoS) du stockage ONTAP_ pour garantir que les performances des workloads stratégiques ne sont pas dégradées par des charges de travail concurrentes :

- Vous pouvez fixer un plafond de débit QoS pour une charge de travail concurrente afin de limiter son impact sur les ressources système (QoS Max).
- Vous pouvez définir un débit QoS *so/* pour une charge de travail stratégique, afin de vous assurer qu'il répond aux objectifs de débit minimaux indépendamment de la demande des charges de travail concurrentes (QoS min).
- Vous pouvez définir un plafond et un sol QoS pour la même charge de travail.

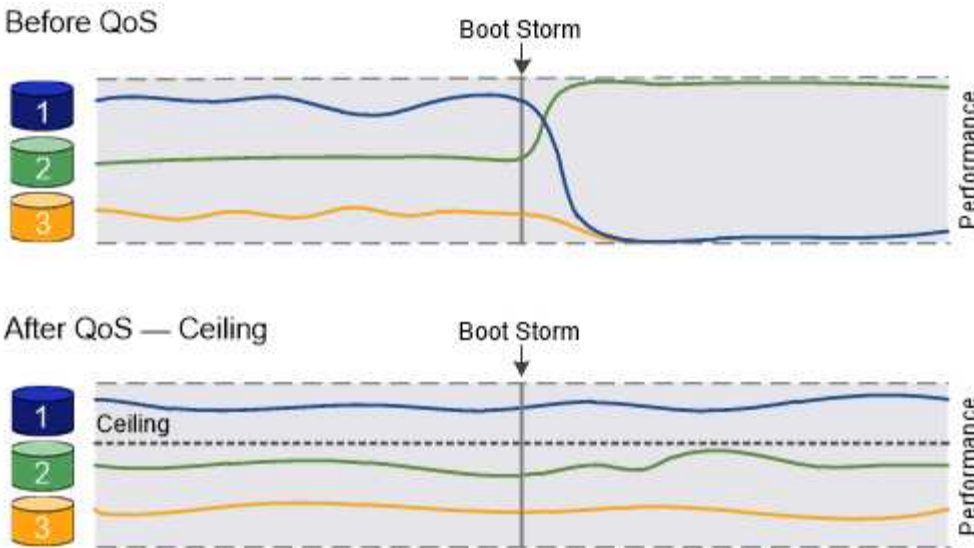
Plafonds de débit

Un plafond de débit limite le débit d'une charge de travail à un nombre maximal d'IOPS ou de Mo/s. Dans la figure ci-dessous, le plafond de débit pour la charge de travail 2 garantit qu'il ne s'agit pas de charges de travail « dominantes » 1 et 3.

Un *policy group* définit le plafond de débit pour une ou plusieurs charges de travail. Une charge de travail représente les opérations d'E/S pour un objet de *stockage* : un volume, un fichier ou une LUN, ou tous les volumes, fichiers ou LUN d'un SVM. Vous pouvez spécifier le plafond lorsque vous créez le groupe de règles ou attendre jusqu'à ce que vous contrôdiez les charges de travail pour les spécifier.



Le débit des charges de travail peut dépasser jusqu'à 10 % le plafond spécifié, en particulier si une charge de travail a des variations rapides du débit. Le plafond peut être dépassé de 50 % pour gérer les rafales.



The throughput ceiling for workload 2 ensures that it does not “bully” workloads 1 and 3.

Le niveau de débit

Un étage de débit garantit que le débit d’une charge de travail ne se trouve pas en dessous du nombre minimal d’IOPS. Dans la figure ci-dessous, les niveaux de débit pour la charge de travail 1 et la charge de travail 3 s’assurent qu’ils répondent aux objectifs de débit minimum, indépendamment de la demande par charge de travail 2.



Comme le suggèrent les exemples, un plafond de débit accélère directement le débit. Un plancher de débit accélère indirectement le débit en donnant la priorité aux charges de travail pour lesquelles le sol a été défini.

Une charge de travail représente les opérations d’E/S d’un volume, d’une LUN ou, en commençant par un fichier ONTAP 9.3. Un groupe de règles qui définit un étage de débit ne peut pas être appliqué à un SVM. Vous pouvez spécifier l’étage lors de la création du groupe de règles ou attendre jusqu’à ce que vous surveilliez les charges de travail pour le spécifier.



Le débit d’une charge de travail peut tomber en dessous du seuil spécifié si la capacité de performance est insuffisante (marge) sur le nœud ou l’agrégat, ou lors des opérations stratégiques comme `volume move trigger-cutover`. Même lorsque vous disposez d’une capacité suffisante et que vos opérations stratégiques ne sont pas effectuées, le débit d’une charge de travail peut tomber en dessous du seuil spécifié de 5 %.



The throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.

La QoS adaptative

En principe, la valeur du groupe de règles que vous attribuez à un objet de stockage est fixe. Vous devez modifier la valeur manuellement lorsque la taille de l'objet de stockage change. Une augmentation de l'espace utilisé sur un volume, par exemple, nécessite généralement une augmentation correspondante du plafond de débit spécifié pour le volume.

Adaptive QoS ajuste automatiquement la valeur du groupe de règles en fonction de la taille de la charge de travail, en maintenant le rapport IOPS/To|Go en fonction de la taille des modifications de la charge de travail. C'est un avantage considérable pour la gestion de centaines, voire de milliers de charges de travail dans le cadre d'un déploiement à grande échelle.

Généralement, vous utilisez la QoS adaptative pour ajuster les plafonds de débit, mais vous pouvez également l'utiliser pour gérer le débit (en cas d'augmentation de la taille des charges de travail). La taille du workload est exprimée en espace alloué à l'objet de stockage ou en espace utilisé par l'objet de stockage.



L'espace utilisé est disponible pour les étages de débit dans ONTAP 9.5 et versions ultérieures. Elle n'est pas prise en charge pour les étages de débit dans ONTAP 9.4 et les versions antérieures.

À partir de la ONTAP 9.13.1, vous pouvez utiliser la QoS adaptative pour définir des planchers et des plafonds de débit au niveau des SVM.

- Une politique *Allocated space* maintient le ratio IOPS/To|Go en fonction de la taille nominale de l'objet de stockage. Si le rapport est de 100 IOPS/Go, un volume de 150 Go plafonné à 15,000 IOPS, tant que la taille du volume reste celle-ci. Si le volume a été redimensionné de façon à 300 Go, la QoS adaptative ajuste le débit au plafond à 30,000 000 IOPS.
- Une règle *Used space* (par défaut) maintient le ratio IOPS/To|Go en fonction de la quantité de données réelles stockées avant le stockage efficace. Si le rapport est de 100 IOPS/Go, un volume de 150 Go contenant 100 Go de données stockées aurait un débit plafond de 10,000 000 IOPS. À mesure que la quantité d'espace utilisée change, la QoS adaptative ajuste le plafond de débit en fonction du rapport.

La réplication

Copies Snapshot

Les technologies de réplication ONTAP exigeaient les reprises après incident et les archivages. Avec l'avènement des services cloud, la réplication ONTAP a été adaptée au transfert des données entre les terminaux dans l'environnement NetApp Data Fabric. Ces utilisations reposent sur la technologie Snapshot de ONTAP.

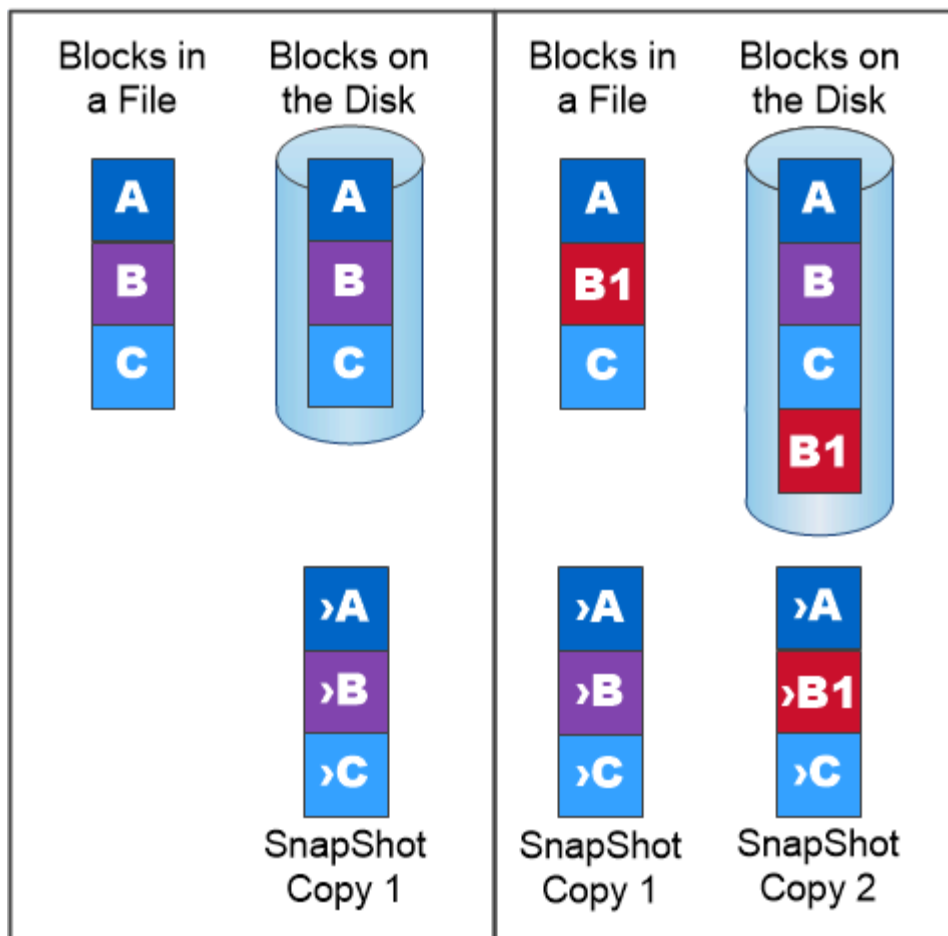
Une *copie snapshot* est une image ponctuelle en lecture seule d'un volume. Après la création d'une copie Snapshot, le système de fichiers actif et la copie Snapshot pointent vers les mêmes blocs de disque. Ainsi, la copie Snapshot n'utilise pas d'espace disque supplémentaire. Au fil du temps, l'image consomme un espace de stockage minimal et implique un impact négligeable sur les performances, car elle n'enregistre que les modifications apportées aux fichiers depuis la dernière copie Snapshot.

Les copies Snapshot doivent leur efficacité à la technologie de virtualisation du stockage principale d'ONTAP, sa *WAFL (Write Anywhere File Layout)*. Comme une base de données, WAFL utilise des métadonnées pour pointer les blocs de données réels du disque. Contrairement à une base de données, WAFL ne remplace pas les blocs existants. Il écrit les données mises à jour sur un nouveau bloc et modifie les métadonnées.

Les copies Snapshot sont efficaces car, au lieu de copier des blocs de données, ONTAP référence les métadonnées lors de la création d'une copie Snapshot. Ainsi, vous éliminez à la fois le temps de recherche que d'autres systèmes impliquent pour localiser les blocs à copier et le coût lié à la copie.

Vous pouvez utiliser une copie Snapshot pour restaurer des fichiers ou des LUN individuels, ou pour restaurer l'ensemble du contenu d'un volume. ONTAP compare les informations du pointeur de la copie Snapshot aux données d'un disque pour reconstruire l'objet manquant ou endommagé, sans temps d'indisponibilité ni coûts de performance significatifs.

Une règle *Snapshot* définit la façon dont le système crée des copies Snapshot de volumes. La règle indique quand créer les copies Snapshot, le nombre de copies à conserver, comment les nommer et comment les étiqueter pour la réplication. Par exemple, un système peut créer une copie Snapshot tous les jours à 12 h 10, conserver les deux copies les plus récentes, les nommer « diotidienne » (ajoutée avec un horodatage) et les étiqueter « dootidienne » pour la réplication.



A SnapShot copy records only changes to the active file system since the last SnapShot copy.

Reprise sur incident et transfert de données SnapMirror

SnapMirror est une technologie de reprise après incident conçue pour le basculement du stockage primaire vers le stockage secondaire sur un site distant. Comme son nom l'indique, SnapMirror crée une réplique ou *mirror* de vos données de travail dans un stockage secondaire à partir duquel vous pouvez continuer à transmettre des données en cas de catastrophe sur le site primaire.

Les données sont mises en miroir au niveau du volume. La relation entre le volume source du stockage primaire et le volume de destination du stockage secondaire est appelée « relation *protection des données* ». les clusters dans lesquels résident les volumes et les SVM qui fournissent des données à partir de ces volumes doivent être *peered*. Une relation de pairs permet l'échange de clusters et de SVM sécurité des données.



Vous pouvez également créer une relation de protection des données entre les SVM. Dans ce type de relation, toute ou partie de la configuration du SVM, depuis les exportations NFS et les partages SMB vers le RBAC, est répliquée, ainsi que les données au sein des volumes dont est propriétaire le SVM.

Depuis la version ONTAP 9.10.1, vous pouvez créer des relations de protection des données entre les

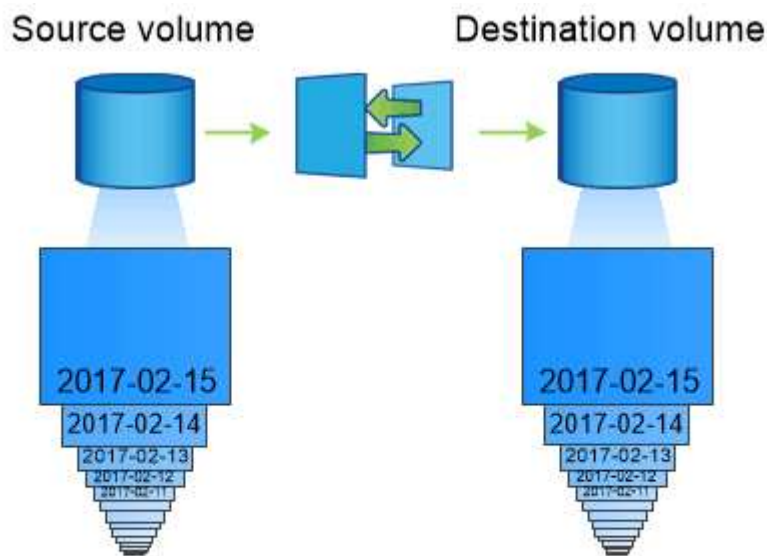
compartiments S3 à l'aide de SnapMirror S3. Les compartiments de destination peuvent être sur les systèmes ONTAP locaux ou distants, ou sur les systèmes non ONTAP tels qu'StorageGRID et AWS.

La première fois que vous appelez SnapMirror, il effectue un *transfert de base* du volume source vers le volume de destination. Le transfert de base implique généralement les étapes suivantes :

- Créer une copie Snapshot du volume source.
- Transférez la copie Snapshot et tous les blocs de données qu'elle référence vers le volume de destination.
- Transférez les copies Snapshot restantes et moins récentes sur le volume source vers le volume de destination pour toute utilisation en cas de corruption du miroir « actif ».

Une fois le transfert de base terminé, SnapMirror transfère uniquement les nouvelles copies Snapshot vers le miroir. Les mises à jour sont asynchrones, en fonction du planning que vous configurez. La conservation met en miroir la règle Snapshot sur la source. Vous pouvez activer le volume de destination en cas d'incident au niveau du site primaire et réactiver le volume source une fois le service restauré.

Étant donné que SnapMirror transfère uniquement les copies Snapshot après la création de la copie de base, la réplication est rapide et sans interruption. Comme l'indique le cas de basculement, les contrôleurs du système secondaire doivent être équivalents ou presque équivalents aux contrôleurs du système primaire pour assurer un service efficace des données à partir du stockage en miroir.



A SnapMirror data protection relationship mirrors the Snapshot copies available on the source volume.

utilisation de SnapMirror pour le transfert de données

Vous pouvez également utiliser SnapMirror pour répliquer les données entre les terminaux de NetApp Data Fabric. Lorsque vous créez la règle SnapMirror, vous avez le choix entre une réplication ponctuelle ou une réplication récurrente.

Sauvegardes cloud SnapMirror vers le stockage objet

SnapMirror Cloud est une technologie de sauvegarde et de restauration conçue pour les utilisateurs ONTAP qui souhaitent migrer leurs workflows de protection des données vers

le cloud. Les entreprises qui se détournent de leurs architectures de sauvegarde sur bande existantes peuvent utiliser le stockage objet comme référentiel alternatif pour la conservation et l'archivage des données à long terme. Le cloud SnapMirror offre une réplication du stockage ONTAP vers objet dans le cadre d'une stratégie de sauvegarde incrémentielle permanente.

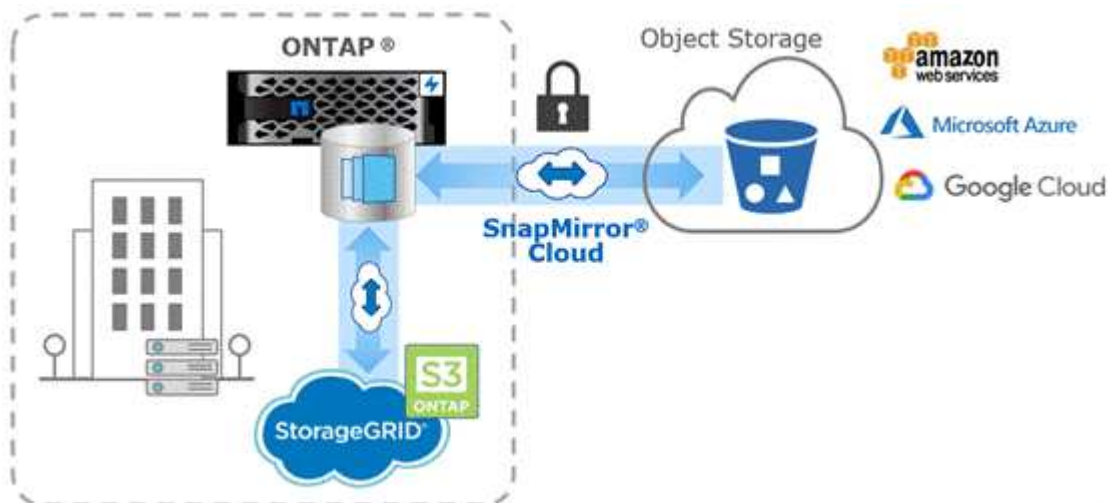
Le cloud SnapMirror a été introduit dans ONTAP 9.8 comme extension de la gamme de technologies de réplication SnapMirror. Tandis que SnapMirror est fréquemment utilisé pour les sauvegardes ONTAP à ONTAP, le cloud SnapMirror utilise le même moteur de réplication pour transférer les copies Snapshot d'ONTAP vers des sauvegardes de stockage objet compatibles S3.

Conçu pour les cas d'usage de sauvegarde, le cloud SnapMirror prend en charge à la fois les workflows d'archivage et la conservation à long terme. Comme pour SnapMirror, la sauvegarde cloud SnapMirror initiale effectue un transfert de base d'un volume. Dans le cas des sauvegardes suivantes, le cloud SnapMirror génère une copie Snapshot du volume source et transfère la copie Snapshot avec uniquement les blocs de données modifiés vers une cible de stockage objet.

Les relations cloud SnapMirror peuvent être configurées entre les systèmes ONTAP et certaines cibles de stockage objet sur site et dans le cloud public, notamment Amazon S3, Google Cloud Storage et Microsoft Azure Blob Storage. Des cibles supplémentaires de stockage objet sur site incluent StorageGRID et ONTAP S3.

La réplication cloud SnapMirror est une fonctionnalité ONTAP sous licence qui nécessite une application approuvée pour orchestrer les workflows de protection des données. Plusieurs options d'orchestration sont disponibles pour la gestion des sauvegardes cloud SnapMirror :

- Plusieurs partenaires de sauvegarde tiers qui prennent en charge la réplication cloud SnapMirror. Les fournisseurs participants sont disponibles sur le ["Blog NetApp"](#).
- Sauvegarde et restauration BlueXP pour une solution NetApp native pour les environnements ONTAP
- API pour développer des logiciels personnalisés pour les workflows de protection des données ou exploiter les outils d'automatisation



Archivage SnapVault

La licence SnapMirror permet la prise en charge des relations SnapVault pour la sauvegarde et des relations SnapMirror pour la reprise sur incident. À partir de ONTAP

9.3, les licences SnapVault sont obsolètes et les licences SnapMirror peuvent être utilisées pour configurer les relations Vault, mirror et mirror-and-vault. La réplication SnapMirror est utilisée pour la réplication ONTAP vers ONTAP des copies Snapshot, et prend en charge à la fois des opérations de sauvegarde et de reprise d'activité.

SnapVault est une technologie d'archivage conçue pour la réplication de copie Snapshot disque à disque à des fins de conformité aux normes et autres pour la gouvernance. Contrairement à une relation SnapMirror, dans laquelle la destination contient généralement uniquement les copies Snapshot actuellement dans le volume source, la destination SnapVault conserve en général les copies Snapshot instantanées créées sur une période bien plus longue.

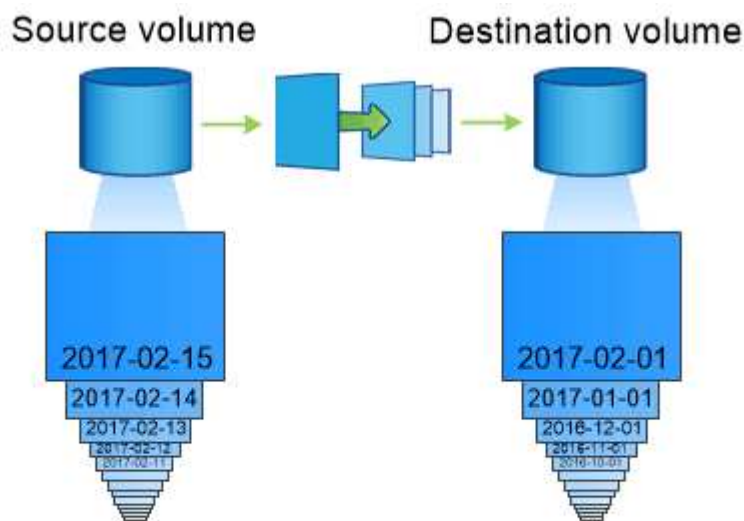
Vous pouvez conserver tous les mois des copies Snapshot de vos données sur une période de 20 ans, par exemple, pour vous conformer aux réglementations gouvernementales relatives à la comptabilité de votre entreprise. Etant donné qu'il n'est pas nécessaire de transmettre des données à partir du stockage Vault, vous pouvez utiliser des disques plus lents et moins coûteux sur le système de destination.

Tout comme SnapMirror, SnapVault effectue un transfert de base dès la première fois que vous l'appellez. Il effectue une copie Snapshot du volume source, puis transfère la copie et les blocs de données qu'il renvoie vers le volume de destination. Contrairement à SnapMirror, SnapVault n'inclut pas d'anciennes copies Snapshot dans la configuration de base.

Les mises à jour sont asynchrones, en fonction du planning que vous configurez. Les règles que vous définissez dans la règle pour la relation identifient les nouvelles copies Snapshot à inclure dans les mises à jour et le nombre de copies à conserver. Les libellés définis dans la politique (« mensuel », par exemple) doivent correspondre à un ou plusieurs libellés définis dans la politique Snapshot de la source. Dans le cas contraire, la réplication échoue.



SnapMirror et SnapVault partagent la même infrastructure de commandes. Vous spécifiez la méthode à utiliser lors de la création d'une stratégie. Les deux méthodes exigent des clusters de peering et des SVM.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Sauvegarde dans le cloud et prise en charge des sauvegardes classiques

Outre les relations de protection des données SnapMirror et SnapVault, qui étaient disque à disque uniquement pour ONTAP 9.7 et les versions antérieures, plusieurs solutions de sauvegarde offrent une alternative moins onéreuse pour la conservation à long terme des données.

De nombreuses applications tierces de protection des données proposent des sauvegardes classiques pour les données gérées par ONTAP. Veeam, Veritas et CommVault entre autres proposent une sauvegarde intégrée pour les systèmes ONTAP.

À partir de ONTAP 9.8, le cloud SnapMirror offre une réplication asynchrone des copies Snapshot entre des instances ONTAP et des terminaux de stockage objet. La réplication cloud SnapMirror nécessite une application sous licence pour l'orchestration et la gestion des workflows de protection des données. Les relations cloud SnapMirror sont prises en charge par les systèmes ONTAP pour sélectionner des cibles de stockage objet sur site et dans le cloud public, y compris AWS S3, Google Cloud Storage Platform ou Microsoft Azure Blob Storage, pour une efficacité améliorée avec les logiciels de sauvegarde des fournisseurs. Contactez votre conseiller NetApp pour obtenir une liste des fournisseurs d'applications certifiées et de stockage objet pris en charge.

Si la protection des données native du cloud vous intéresse, BlueXP peut être utilisé pour configurer les relations SnapMirror ou SnapVault entre les volumes sur site et les instances Cloud Volumes ONTAP dans le cloud public.

BlueXP fournit également des sauvegardes d'instances Cloud Volumes ONTAP à l'aide d'un modèle SaaS. Les utilisateurs peuvent sauvegarder leurs instances Cloud Volumes ONTAP dans le stockage objet de cloud public compatible S3 et S3 à l'aide de Cloud Backup disponible sur NetApp Cloud Central.

["Ressources de documentation Cloud Volumes ONTAP et BlueXP"](#)

["NetApp Cloud Central"](#)

Disponibilité sans interruption avec MetroCluster

Les configurations MetroCluster protègent les données grâce à la mise en œuvre de deux clusters en miroir séparés physiquement. Chaque cluster réplique de manière synchrone les données et la configuration SVM de l'autre. En cas d'incident sur un site, un administrateur peut activer la SVM en miroir et commencer à transférer les données depuis le site survivant.

- Les *configurations MetroCluster* reliées à la structure prennent en charge les clusters à l'échelle de la zone métropolitaine.
- *Stretch MetroCluster* configurations prennent en charge les clusters à l'échelle du campus.

Les grappes doivent être pételées dans les deux cas.

MetroCluster utilise la fonctionnalité ONTAP appelée *SyncMirror* pour mettre en miroir de manière synchrone les données d'agrégats pour chaque cluster dans des copies, ou *plex*, dans le stockage de l'autre cluster. En cas de basculement, le plex distant sur le cluster survivant est mis en ligne et le SVM secondaire commence à transmettre les données.



When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.

utilisation de SyncMirror dans des implémentations non MetroCluster

Vous pouvez, par ailleurs, utiliser SyncMirror dans une implémentation non MetroCluster pour vous protéger contre la perte de données si le nombre de disques défaillants est supérieur à la protection du type RAID ou en cas de perte de connectivité avec les disques du groupe RAID. La fonctionnalité est disponible uniquement pour les paires haute disponibilité.

Les données agrégées sont mises en miroir dans des plexes stockés sur différents tiroirs disques. Si l'un des tiroirs n'est plus disponible, le plex non affecté continue à transmettre des données pendant que vous corrigez la défaillance.

N'oubliez pas qu'un agrégat en miroir avec SyncMirror nécessite deux fois plus de stockage qu'un agrégat non mis en miroir. Chaque plex requiert autant de disques que le plex IT miroirs. Vous auriez besoin de 2,880 Go d'espace disque, par exemple pour mettre en miroir un agrégat de 1,440 Go, 1,440 Go par plex.

Avec SyncMirror, il est recommandé de conserver au moins 20 % d'espace libre pour les agrégats en miroir pour une disponibilité et des performances de stockage optimales. Bien que la recommandation soit de 10 % pour les agrégats non mis en miroir, le système de fichiers peut utiliser 10 % d'espace supplémentaire pour absorber les modifications incrémentielles. Les modifications incrémentielles augmentent l'utilisation de l'espace pour les agrégats en miroir grâce à l'architecture Snapshot d'ONTAP basée sur la copie en écriture. Le non-respect de ces bonnes pratiques peut avoir un impact négatif sur les performances de resynchronisation SyncMirror, qui a un impact indirect sur les workflows opérationnels, tels que la mise à niveau sans interruption pour les déploiements cloud non partagés et la reprise pour les déploiements MetroCluster.



SyncMirror est également disponible pour les implémentations de virtualisation FlexArray.

Efficacité du stockage

Présentation de l'efficacité du stockage ONTAP

L'efficacité du stockage mesure la manière dont un système de stockage utilise l'espace disponible en optimisant les ressources de stockage, en minimisant le gaspillage d'espace et en réduisant l'encombrement physique des données écrites. Un stockage plus efficace vous permet de stocker un maximum de données dans un minimum d'espace et à moindre coût. Par exemple, l'utilisation de technologies d'efficacité du stockage qui détectent et éliminent les blocs de données dupliqués et les blocs de données remplis de zéros réduit la quantité globale de stockage physique nécessaire et le coût global.

ONTAP propose une large gamme de technologies d'efficacité du stockage qui réduisent la quantité de matériel physique ou de stockage cloud consommée par vos données et qui améliorent considérablement les performances du système. Ces technologies incluent une lecture plus rapide des données, des copies plus rapides des jeux de données et un provisionnement plus rapide des machines virtuelles.

Les technologies ONTAP d'efficacité du stockage incluent :

- **Provisionnement fin**

Provisionnement fin Vous permet d'allouer du stockage dans un volume ou une LUN en fonction des besoins au lieu de le réserver à l'avance. Cela réduit la quantité de stockage physique nécessaire en vous permettant de surallouer vos volumes ou LUN en fonction de leur utilisation potentielle, sans réserver un

espace qui n'est pas utilisé actuellement.

- **Déduplication**

Déduplication réduit la quantité de stockage physique nécessaire pour un volume de trois manières distinctes.

- **Déduplication de blocs zéro**

La déduplication de blocs « zéro » détecte et élimine les blocs de données remplis de zéros, et met uniquement à jour les métadonnées. 100 % de l'espace généralement utilisé par les blocs « zéro » est ensuite économisé. La déduplication de blocs « zéro » est activée par défaut sur tous les volumes dédupliqués.

- **Déduplication à la volée**

La déduplication à la volée détecte les blocs de données dupliqués et les remplace par des références à un bloc partagé unique avant l'écriture des données sur le disque. La déduplication à la volée accélère le provisionnement des machines virtuelles de 20 à 30 %. Selon votre version d'ONTAP et votre plateforme, la déduplication à la volée est disponible au niveau du volume ou de l'agrégat. Il est activé par défaut sur les systèmes AFF et ASA. Vous devez activer manuellement la déduplication à la volée sur les systèmes FAS.

- **Déduplication en arrière-plan**

La déduplication en arrière-plan détecte également les blocs de données dupliqués et les remplace par des références à un bloc partagé unique. Elle améliore également l'efficacité du stockage après l'écriture des données sur le disque. Vous pouvez configurer la déduplication en arrière-plan pour qu'elle s'exécute lorsque certains critères sont remplis sur votre système de stockage. Par exemple, vous pouvez activer la déduplication en arrière-plan lorsque votre volume atteint 10 % d'utilisation. Vous pouvez également déclencher manuellement la déduplication en arrière-plan ou la configurer pour qu'elle s'exécute selon un planning spécifique. Il est activé par défaut sur les systèmes AFF et ASA. Vous devez activer manuellement la déduplication en arrière-plan sur les systèmes FAS.

La déduplication est prise en charge au sein des volumes et entre les volumes d'un agrégat. Les lectures de données dédupliquées n'entraînent en général aucun frais de performances.

- **Compression**

Compression réduit la quantité de stockage physique nécessaire pour un volume en combinant les blocs de données dans des groupes de compression, chacun étant stocké sous forme de bloc unique. Lorsqu'une demande de lecture ou de remplacement est reçue, seul un petit groupe de blocs est lu, et non le fichier entier. Ce processus optimise les performances de lecture et d'écriture et permet une plus grande évolutivité de la taille des fichiers compressés.

Elle peut être exécutée à la volée ou en post-traitement. La compression à la volée permet des gains d'espace immédiats en compressant les données dans la mémoire avant d'être écrites sur le disque. La compression post-traitement écrit d'abord les blocs sur le disque comme non compressés, puis compresse les données à un moment prédéfini. Elle est activée par défaut sur les systèmes 100 % Flash. Vous devez activer manuellement la compression sur tous les autres systèmes.

- **Compaction**

La compaction réduit la quantité de stockage physique requise pour un volume en prenant des segments de données stockés dans des blocs de 4 Ko mais dont la taille est inférieure à 4 Ko et en les combinant dans un seul bloc. La compaction a lieu lorsque les données sont encore dans la mémoire. Ainsi, l'espace

inutile n'est jamais consommé sur les disques. Il est activé par défaut sur les systèmes AFF et ASA. Vous devez activer manuellement la compaction sur les systèmes FAS.

- **Volumes FlexClone, fichiers et LUN**

Technologie FlexClone Exploite les métadonnées Snapshot pour créer des copies instantanées inscriptibles d'un volume, d'un fichier ou d'une LUN. Les copies partagent les blocs de données avec leurs parents. Elles ne consomment pas d'espace de stockage, à l'exception des éléments requis pour les métadonnées jusqu'à ce que les modifications soient écrites sur une copie ou sur son parent. Lorsqu'une modification est écrite, seul le delta est stocké.

Là où la création de copies de datasets classiques peut prendre quelques minutes, voire plusieurs heures, la technologie FlexClone vous permet de copier même les jeux de données les plus volumineux de manière quasi instantanée.

- **Efficacité de stockage sensible à la température**

ONTAP offre de "**efficacité du stockage sensible à la température**" nombreux avantages en évaluant la fréquence d'accès aux données de votre volume et en mappant cette fréquence au niveau de compression appliqué à ces données. Pour les données inactives peu utilisées, les blocs de données plus volumineux sont compressés. Pour les données fortement sollicitées qui sont fréquemment utilisées et remplacées, des blocs de données plus petits sont compressés, ce qui rend le processus plus efficace.

Introduit dans ONTAP 9.8, l'efficacité du stockage sensible à la température est automatiquement activée sur les volumes AFF nouvellement créés à provisionnement fin. Il n'est pas activé sur "**Plates-formes AFF A70, AFF A90 et AFF A1K**" qui sont introduits dans ONTAP 9.15.1, qui utilisent un processeur de déchargement matériel.

- **Efficacité de stockage du processeur ou du processeur de déchargement dédié**

À partir de ONTAP 9.15.1, ONTAP assure la "**Efficacité du stockage du processeur ou du processeur de déchargement dédié**" compaction et la compaction des données sur les plateformes AFF A70, AFF A90 et AFF A1K. L'efficacité du stockage est activée automatiquement, sans configuration.

Et si vous le souhaitez, vous pouvez tirer parti de ces technologies dans vos opérations quotidiennes en toute simplicité. Supposons par exemple que vous devez fournir à 5,000 utilisateurs du stockage pour les répertoires locaux, et que vous estimez que l'espace maximal requis par un utilisateur est de 1 Go. Vous pouvez réserver un agrégat de 5 To à l'avance pour répondre au besoin total de stockage potentiel. Cependant, vous savez également que les besoins en capacité des répertoires locaux varient considérablement dans votre organisation. Au lieu de réserver 5 To d'espace total à votre entreprise, vous pouvez créer un agrégat de 2 To. Vous pouvez ensuite utiliser le provisionnement fin pour attribuer nominale 1 Go de stockage à chaque utilisateur, mais allouer le stockage uniquement en fonction des besoins. Vous pouvez activement surveiller l'agrégat dans le temps et augmenter sa taille physique réelle si nécessaire.

Dans un autre exemple, supposons que vous utilisiez une infrastructure de postes de travail virtuels (VDI) avec une grande quantité de données dupliquées au sein de vos postes de travail virtuels. La déduplication réduit l'utilisation du stockage en éliminant automatiquement les blocs d'informations dupliqués dans l'infrastructure VDI, puis en les remplaçant par un pointeur vers le bloc d'origine. D'autres technologies d'efficacité du stockage ONTAP, telles que la compression, peuvent également s'exécuter en arrière-plan sans intervention de votre part.

La technologie de partitionnement de disque ONTAP offre également une meilleure efficacité du stockage. La technologie RAID DP protège contre les doubles défaillances de disques sans sacrifier les performances ni augmenter la surcharge liée à la mise en miroir des disques. Le partitionnement SSD avancé avec ONTAP 9 augmente la capacité exploitable de près de 20 %.

NetApp fournit les mêmes fonctionnalités d'efficacité du stockage que celles disponibles avec ONTAP sur site dans le cloud. La migration des données depuis un environnement ONTAP sur site vers le cloud préserve l'efficacité du stockage. Supposons que vous disposiez d'une base de données SQL contenant des données stratégiques que vous souhaitez déplacer d'un système sur site vers le cloud. Vous pouvez utiliser la réplication des données dans BlueXP pour migrer vos données et, dans le cadre du processus de migration, vous pouvez activer votre dernière règle sur site pour les copies Snapshot dans le cloud.

Provisionnement fin

ONTAP propose un large éventail de technologies d'efficacité du stockage, en plus des copies Snapshot. Les technologies clés sont le provisionnement fin, la déduplication, la compression, ainsi que les volumes FlexClone, les fichiers Et des LUN. À l'instar des copies Snapshot, elles reposent sur le WAFL (Write Anywhere File Layout) d'ONTAP.

Un *volume* provisionné_ ou une LUN est un volume pour lequel le stockage n'est pas réservé à l'avance. Au contraire, le stockage est alloué de manière dynamique, selon les besoins. L'espace libre est relibéré dans le système de stockage lorsque les données du volume ou de la LUN sont supprimées.

Imaginez que votre entreprise doit fournir à 5,000 utilisateurs du stockage pour les répertoires locaux. Vous estimez que les principaux répertoires locaux consommeront 1 Go d'espace.

Dans ce cas, vous pouvez acheter 5 To de stockage physique. Pour chaque volume qui stocke un home Directory, vous pouvez réserver suffisamment d'espace pour répondre aux besoins des plus grands consommateurs.

En pratique, cependant, vous savez aussi que les besoins en capacité des répertoires d'accueil varient considérablement d'un bout à l'autre de votre communauté. Pour chaque grand utilisateur du stockage, dix ne consomment que peu ou pas d'espace.

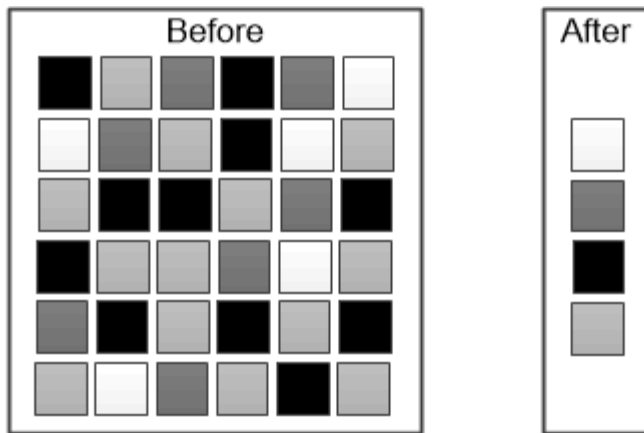
Le provisionnement fin vous permet de répondre aux besoins des grands consommateurs de stockage sans acheter de stockage que vous n'utiliserez probablement pas. L'espace de stockage n'étant pas alloué tant qu'il n'est pas consommé, vous pouvez « surallouer » un agrégat de 2 To en attribuant théoriquement une taille de 1 Go à chacun des 5,000 volumes que l'agrégat contient.

Tant que vous avez raison de ratios de lumière 10:1 pour les utilisateurs intensifs et tant que vous jouez un rôle actif dans la surveillance de l'espace libre de l'agrégat, vous pouvez compter sur le fait que les écritures de volume ne échouent pas en raison du manque d'espace.

Déduplication

Deduplication réduit le volume de stockage physique requis pour un volume (ou pour tous les volumes d'un agrégat AFF) en abandonnant les blocs dupliqués et en les remplaçant par des références à un seul bloc partagé. Les lectures de données dédupliquées n'entraînent en général aucun frais de performances. Les écritures entraînent un frais négligeable sauf sur les nœuds surchargés.

Au fur et à mesure que les données sont écrites pendant l'utilisation normale, WAFL crée un catalogue de signatures de blocs . après le démarrage de la déduplication, ONTAP compare les signatures dans le catalogue pour identifier les blocs dupliqués. Si une correspondance existe, une comparaison octet par octet est effectuée pour vérifier que les blocs candidats n'ont pas changé depuis la création du catalogue. Uniquement si tous les octets correspondent au bloc dupliqué supprimé et si son espace disque est récupéré.



Deduplication reduces the amount of physical storage required for a volume by discarding duplicate data blocks.

Compression

Compression réduit la quantité de stockage physique requise pour un volume en combinant des blocs de données dans *groupes de compression* dont chacun est stocké comme un seul bloc. Les lectures de données compressées sont plus rapides que dans les méthodes de compression traditionnelles, car ONTAP décompresse uniquement les groupes de compression contenant les données requises, et non un fichier ou une LUN entier.

Vous pouvez effectuer la compression à la volée ou post-traitement, séparément ou conjointement :

- *Inline compression* compresse les données en mémoire avant de les écrire sur le disque, ce qui réduit de manière significative la quantité d'opérations d'écriture E/S sur un volume, mais diminue potentiellement les performances d'écriture. Le cas échéant, les opérations exigeant des performances élevées sont reportées jusqu'à la prochaine opération de compression post-traitement.
- *Post-compression* compresse les données après leur écriture sur le disque, selon la même planification que la déduplication.

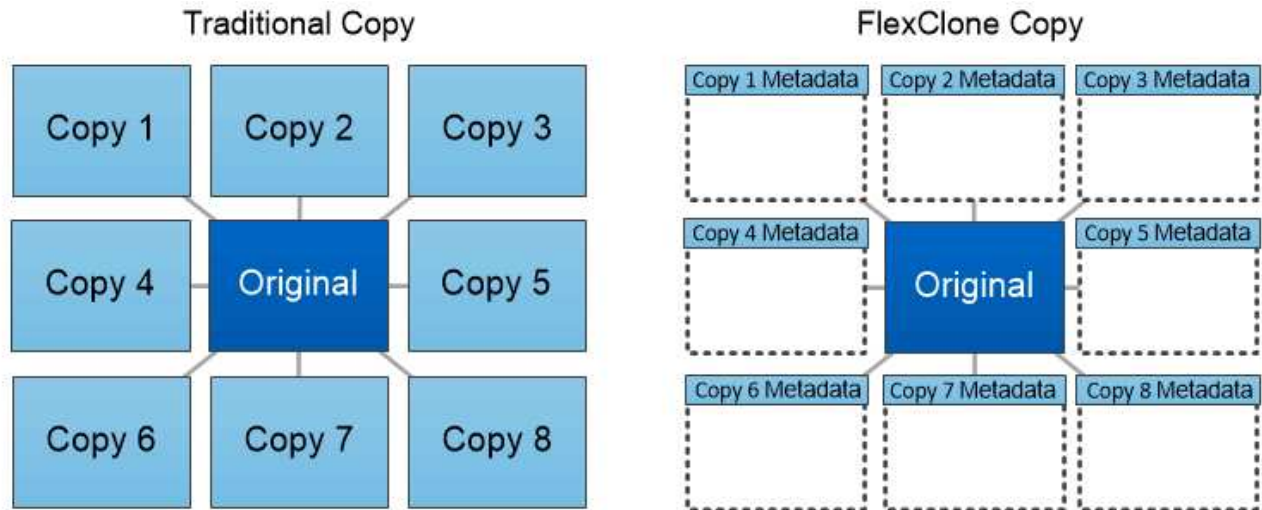
compaction des données à la volée les petits fichiers ou E/S rembourrés avec des zéros sont stockés dans un bloc de 4 Ko, qu'ils aient ou non besoin de 4 Ko de stockage physique. *La compaction des données à la volée* associe des blocs de données qui consomment normalement plusieurs blocs de 4 Ko dans un seul bloc de 4 Ko sur disque. La compaction a lieu tandis que les données sont encore dans la mémoire, il est donc recommandé d'accélérer les contrôleurs.

Volumes FlexClone, fichiers et LUN

FlexClone fait référence aux métadonnées Snapshot pour créer des copies inscriptibles instantanées d'un volume. Les copies partagent les blocs de données avec leurs parents. Aucun stockage n'est nécessaire, sauf pour les métadonnées, jusqu'à ce que les modifications soient écrites sur la copie. Les fichiers FlexClone et les LUN FlexClone utilisent une technologie identique, à la différence qu'une copie Snapshot de sauvegarde n'est pas requise.

Là où les copies classiques peuvent prendre des minutes, voire des heures, pour créer des copies, FlexClone vous permet de copier même les jeux de données les plus volumineux quasi instantanément. Cela est idéal si vous avez besoin de plusieurs copies de jeux de données identiques (par exemple, pour le déploiement de postes de travail virtuels) ou de copies temporaires d'un jeu de données (test d'une application par rapport à un jeu de données de production).

Vous pouvez cloner un volume FlexClone existant, cloner un volume contenant des clones de LUN ou cloner des données de miroir et d'archivage sécurisé. Vous pouvez *split* volume FlexClone de son parent, dans le cas où la copie lui serait allouée son propre stockage.



FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.

Mesures de la capacité dans System Manager

La capacité du système peut être mesurée soit en tant qu'espace physique, soit en tant qu'espace logique. Depuis ONTAP 9.7, System Manager mesure la capacité physique et logique.

Les différences entre les deux mesures sont expliquées dans les descriptions suivantes :

- **Capacité physique** : l'espace physique fait référence aux blocs physiques de stockage utilisés dans le volume ou le niveau local. La valeur de la capacité physique utilisée est généralement inférieure à la valeur de la capacité logique utilisée grâce à la réduction des données provenant des fonctionnalités d'efficacité du stockage (telles que la déduplication et la compression).
- **Capacité logique** : l'espace logique fait référence à l'espace utilisable (les blocs logiques) dans un volume ou un niveau local. L'espace logique désigne la manière dont l'espace théorique peut être utilisé, sans tenir compte des résultats obtenus grâce à la déduplication ou à la compression. La valeur de l'espace logique utilisé est issue de la quantité d'espace physique utilisé, plus les économies réalisées grâce aux fonctionnalités d'efficacité du stockage (telles que la déduplication et la compression) qui ont été configurées. Cette mesure est souvent supérieure à la capacité physique utilisée, car elle inclut des copies Snapshot, des clones et d'autres composants, et ne reflète pas la compression des données et autres réductions de l'espace physique. La capacité logique totale peut donc être supérieure à l'espace provisionné.



Dans System Manager, les représentations de capacité ne prennent pas en compte les capacités du niveau de stockage racine (agrégat).

Mesures de la capacité utilisée

Les mesures de la capacité utilisée s'affichent différemment en fonction de la version de System Manager que vous utilisez, comme expliqué dans le tableau ci-dessous :

Version de System Manager	Terme utilisé pour la capacité	Type de capacité visé
9.9.1 et versions ultérieures	Utilisation logique	Espace logique utilisé (si les paramètres d'efficacité du stockage ont été activés)
9.7 et 9.8	Utilisé	Espace logique utilisé (si les paramètres d'efficacité du stockage ont été activés)
9.5 et 9.6 (Vue classique)	Utilisé	Espace physique utilisé

Termes de mesure de la capacité

Les termes suivants sont utilisés pour décrire la capacité :

- **Capacité allouée** : quantité d'espace allouée aux volumes d'une machine virtuelle de stockage.
- **Disponible** : quantité d'espace physique disponible pour stocker des données ou provisionner des volumes dans une machine virtuelle de stockage ou sur un niveau local.
- **Capacité sur les volumes** : somme du stockage utilisé et du stockage disponible de tous les volumes sur une machine virtuelle de stockage.
- **Données client** : quantité d'espace utilisée par les données client (physique ou logique).
 - Depuis ONTAP 9.13.1, la capacité utilisée par les données client est appelée **logique utilisée** et la capacité utilisée par les copies Snapshot est affichée séparément.
 - Dans ONTAP 9.12.1 et versions antérieures, la capacité utilisée par les données client ajoutées à la capacité utilisée par les copies Snapshot est appelée **logique utilisée**.
- **Validé** : le montant de la capacité engagée pour un niveau local.
- **Réduction des données** :
 - À partir de ONTAP 9.13.1, les taux de réduction des données sont affichés comme suit :
 - La valeur de réduction des données affichée sur le panneau **capacité** correspond au rapport entre l'espace logique utilisé et l'espace physique utilisé, sans tenir compte des réductions significatives obtenues lors de l'utilisation de fonctionnalités d'efficacité du stockage, telles que les copies Snapshot.
 - Lorsque vous affichez le panneau de détails, vous voyez à la fois le ratio affiché sur le panneau de vue d'ensemble et le ratio global de tout l'espace utilisé logique par rapport à l'espace physique utilisé. Appelée **avec les copies Snapshot**, cette valeur inclut les avantages découlant de l'utilisation des copies Snapshot et d'autres fonctionnalités d'efficacité du stockage.
 - Dans la ONTAP 9.12.1 et les versions antérieures, les taux de réduction des données sont affichés

comme suit :

- La valeur de réduction des données affichée sur le panneau **capacité** correspond au rapport global de tout l'espace logique utilisé par rapport à l'espace physique utilisé, et elle inclut les avantages découlant de l'utilisation des copies Snapshot et d'autres fonctionnalités d'efficacité du stockage.
- Lorsque vous affichez le panneau de détails, vous voyez à la fois le ratio **global** qui était affiché sur le panneau de vue d'ensemble et le rapport de l'espace logique utilisé uniquement par les données client par rapport à l'espace physique utilisé uniquement par les données client, appelé **sans copies Snapshot et clones**.

- **Logique utilisée :**

- Depuis ONTAP 9.13.1, la capacité utilisée par les données client est appelée **logique utilisée** et la capacité utilisée par les copies Snapshot est affichée séparément.
- Dans ONTAP 9.12.1 et versions antérieures, la capacité utilisée par les données client ajoutées à la capacité utilisée par les copies Snapshot est appelée **logique utilisée**.

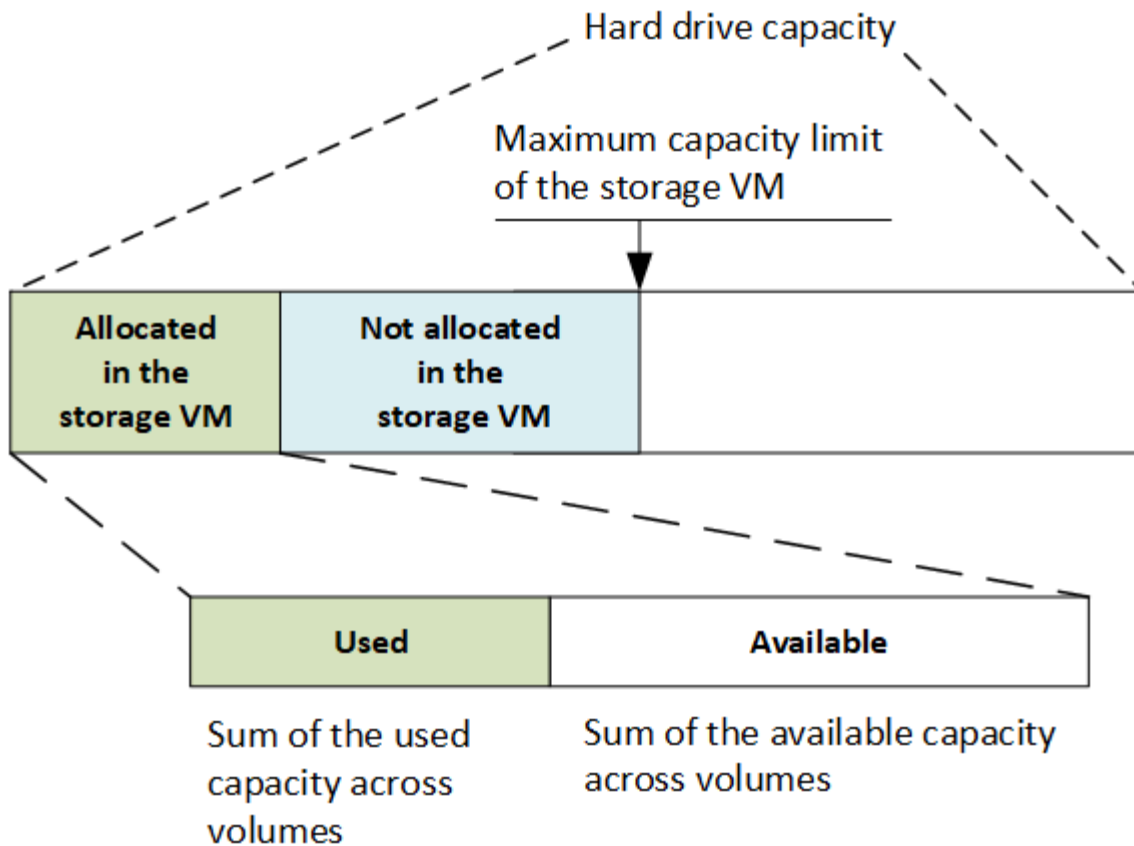
- **Logical Used %** : pourcentage de la capacité logique utilisée actuelle par rapport à la taille provisionnée, à l'exclusion des réserves snapshot. Cette valeur peut être supérieure à 100 %, grâce aux économies en termes d'efficacité réalisées dans le volume.
- **Capacité maximale** : quantité maximale d'espace allouée aux volumes sur une machine virtuelle de stockage.
- **Physical Used**: La capacité utilisée dans les blocs physiques d'un volume ou d'un niveau local.
- **Physical Used %** : pourcentage de capacité utilisée dans les blocs physiques d'un volume par rapport à la taille provisionnée.
- **Capacité provisionnée** : un système de fichiers (volume) qui a été alloué à partir d'un système Cloud Volumes ONTAP et est prêt à stocker les données des utilisateurs ou des applications.
- **Réservé** : espace réservé pour les volumes déjà provisionnés dans un niveau local.
- **Utilisé**: La quantité d'espace qui contient des données.
- **Utilisé et réservé** : somme de l'espace physique utilisé et réservé.

Capacité d'une VM de stockage

La capacité maximale d'une machine virtuelle de stockage est déterminée par l'espace total alloué aux volumes plus l'espace restant non alloué.

- L'espace alloué aux volumes correspond à la somme de la capacité utilisée et de la capacité disponible des volumes FlexVol, des volumes FlexGroup et des volumes FlexCache.
- La capacité des volumes est incluse dans les sommes, même lorsqu'elles sont restreintes, hors ligne ou dans la file d'attente de restauration après suppression.
- Si les volumes sont configurés avec l'extension automatique, la valeur de taille automatique maximale du volume est utilisée dans les sommes. Sans croissance automatique, la capacité réelle du volume est utilisée dans les sommes.

Le tableau suivant explique comment la mesure de la capacité sur l'ensemble des volumes est liée à la limite de capacité maximale.



À partir de ONTAP 9.13.1, les administrateurs du cluster peuvent "[Limiter la capacité maximale pour une VM de stockage](#)". Toutefois, il est impossible de définir des limites de stockage pour une VM de stockage qui contient des volumes destinés à la protection des données, dans une relation SnapMirror ou dans une configuration MetroCluster. De même, les quotas ne peuvent pas être configurés pour dépasser la capacité maximale d'une machine virtuelle de stockage.

Une fois la limite de capacité maximale définie, elle ne peut pas être modifiée pour obtenir une taille inférieure à la capacité actuellement allouée.

Lorsqu'une machine virtuelle de stockage atteint sa capacité maximale, certaines opérations ne peuvent pas être effectuées. System Manager fournit des suggestions pour les étapes suivantes de "[Aperçus](#)".

Unités de mesure de la capacité

System Manager calcule la capacité de stockage en fonction des unités binaires de 1024 (2^{10}) octets.

- À partir de la version ONTAP 9.10.1, les unités de capacité de stockage sont affichées dans System Manager sous la forme KiB, MiB, GiB, TiB et PiB.
- Dans ONTAP 9.10.0 et les versions antérieures, ces unités sont affichées dans System Manager sous la forme de Ko, Mo, Go, To et po.



Les unités utilisées dans System Manager pour le débit continuent à être les Ko/s, Mo/s, Go/s, To/s et po/s pour toutes les versions des systèmes ONTAP.

Unité de capacité affichée dans System Manager pour ONTAP 9.10.0 et versions antérieures	Unité de capacité affichée dans System Manager pour ONTAP 9.10.1 et versions ultérieures	Calcul	Valeur en octets
KO	Kio	1024	1024 octets
MO	Mio	1024 * 1024	1,048,576 octets
GO	Gio	1024 * 1024 * 1024	1,073,741,824 octets
TO	Tio	1024 * 1024 * 1024 * 1024	1,099,511,627,776 octets
PO	Pio	1024 * 1024 * 1024 * 1024 * 1024	1,125,899,906,842,624 octets

Informations associées

["Contrôle de la capacité dans System Manager"](#)

["Création de rapports sur l'espace logique et application des volumes"](#)

Présentation de l'efficacité du stockage sensible à la température

ONTAP offre des avantages en termes d'efficacité du stockage sensibles à la température en évaluant la fréquence d'accès aux données de votre volume et en mappant cette fréquence au niveau de compression appliqué à ces données. Pour les données inactives peu utilisées, les blocs de données plus volumineux sont compressés et pour les données actives, qui sont fréquemment utilisées et remplacées plus souvent, les blocs de données plus petits sont compressés, ce qui améliore l'efficacité du processus.

L'efficacité du stockage sensible à la température, introduite dans ONTAP 9.8, est automatiquement activée sur les volumes AFF nouvellement créés à provisionnement fin. Vous pouvez activer l'efficacité du stockage sensible à la température sur les volumes AFF existants et sur les volumes non-AFF DP à provisionnement fin.

Introduction des modes « par défaut » et « efficace »

À partir de ONTAP 9.10.1, les modes d'efficacité du stockage *default* et *Efficient* au niveau du volume sont introduits uniquement pour les systèmes AFF. Les deux modes permettent de choisir entre la compression de fichiers (par défaut), qui est le mode par défaut lors de la création de nouveaux volumes AFF, ou l'efficacité du stockage sensible à la température (efficace), ce qui permet d'obtenir une efficacité du stockage sensible à la température. Avec ONTAP 9.10.1, ["l'efficacité du stockage sensible à la température doit être définie de manière explicite"](#) pour activer la compression auto-adaptative. Cependant, d'autres fonctionnalités d'efficacité du stockage telles que la compaction des données, la déduplication automatique, la déduplication à la volée, la déduplication à la volée entre volumes et la déduplication en arrière-plan entre volumes sont activées par défaut sur les plateformes AFF pour les modes par défaut et efficaces.

Les deux modes d'efficacité du stockage (par défaut et efficace) sont pris en charge sur les agrégats compatibles avec FabricPool et avec tous les types de règles de Tiering.

Effacité du stockage sensible à la température activée sur les plateformes C-Series

L'efficacité du stockage sensible à la température est activée par défaut sur les plates-formes AFF série C et lors de la migration de volumes d'une plate-forme non TSSE vers une plate-forme C-Series compatible TSSE à l'aide de Volume Move ou de SnapMirror avec les versions suivantes installées sur la destination :

- ONTAP 9.12.1P4 et versions ultérieures
- ONTAP 9.13.1 et versions ultérieures

Pour plus d'informations, voir ["Efficacité du stockage avec déplacement de volumes et opérations SnapMirror"](#).

Pour les volumes existants, l'efficacité du stockage sensible à la température n'est pas activée automatiquement, mais elle le peut ["modifier le mode d'efficacité du stockage"](#) manuellement pour passer en mode efficace.



Une fois que vous avez défini le mode d'efficacité du stockage sur efficace, vous ne pouvez plus le redéfinir.

Amélioration de l'efficacité du stockage grâce à la compression séquentielle des blocs physiques contigus

Depuis la version ONTAP 9.13.1, l'efficacité du stockage sensible à la température ajoute la compaction séquentielle des blocs physiques contigus afin d'améliorer encore l'efficacité du stockage. Sur les volumes dont l'efficacité du stockage sensible à la température est activée automatiquement, la compression séquentielle est activée lorsque vous mettez à niveau des systèmes vers ONTAP 9.13.1. Une fois l'emballage séquentiel activé, vous devez le faire ["reconditionnement manuel des données existantes"](#).

Mise à niveau

Lors de la mise à niveau vers ONTAP 9.10.1 et versions ultérieures, un mode d'efficacité du stockage est attribué aux volumes existants, basé sur le type de compression actuellement activé sur les volumes. Au cours d'une mise à niveau, le mode par défaut est attribué aux volumes dont la compression est activée et le mode efficace est activé pour les volumes dont l'efficacité de stockage est sensible à la température. Si la compression n'est pas activée, le mode d'efficacité du stockage reste vide.

Effacité du stockage du processeur ou du processeur de déchargement dédié

À partir de ONTAP 9.15.1, ONTAP assure l'efficacité du stockage et la compaction des données sur les plateformes AFF A70, AFF A90 et AFF A1K. Selon la plate-forme, la compression s'effectue à l'aide du processeur principal ou d'un processeur de déchargement dédié. L'efficacité du stockage est activée automatiquement, sans configuration. L'efficacité du stockage est activée par défaut sur les volumes nouvellement créés à provisionnement fin. Elle est appliquée aux données existantes, y compris les volumes déplacés d'autres plateformes vers les plateformes AFF A70, AFF A90 ou AFF A1K.

L'efficacité du stockage sensible à la température n'est pas appliquée aux plateformes AFF A70, AFF A90 et AFF A1K. La compression n'est pas basée sur les données actives ou inactives de ces plateformes. La compression commence donc sans attendre que les données deviennent inactives.

Efficacité du stockage sur les plateformes AFF A70, AFF A90 et AFF A1K utilise la compaction séquentielle de blocs physiques contigus pour améliorer encore l'efficacité du stockage des données compressées.

Les données migrées vers des plateformes AFF A70, AFF A90 ou AFF A1K à l'aide de la migration de volumes ou de la technologie SnapMirror sont automatiquement converties en compression en ligne de 32 Ko.

L'efficacité du stockage des données migrées d'une plateforme AFF A70, A90 ou A1K vers une plateforme antérieure est transformée automatiquement en fonction des fonctionnalités d'efficacité de la plateforme cible.

Pour plus d'informations sur la mise à niveau d'un contrôleur vers un AFF A70, AFF A90 ou AFF A1K, reportez-vous au ["Documentation sur la mise à niveau du matériel ONTAP"](#).

Sécurité

Authentification et autorisation du client

ONTAP utilise des méthodes standard pour sécuriser l'accès client et administrateur au stockage et se protéger contre les virus. Des technologies avancées sont disponibles pour le chiffrement des données au repos et WORM.

ONTAP authentifie un ordinateur client et un utilisateur en vérifiant son identité avec une source de confiance. ONTAP autorise un utilisateur à accéder à un fichier ou à un répertoire en comparant les informations d'identification de l'utilisateur aux autorisations configurées sur le fichier ou le répertoire.

Authentification

Vous pouvez créer des comptes utilisateur locaux ou distants :

- Un compte local est un compte dans lequel les informations de compte résident sur le système de stockage.
- Un compte distant est un compte dans lequel les informations de compte sont stockées sur un contrôleur de domaine Active Directory, un serveur LDAP ou un serveur NIS.

ONTAP utilise des services de noms locaux ou externes pour rechercher les informations de nom d'hôte, d'utilisateur, de groupe, de groupe réseau et de mappage de noms. ONTAP prend en charge les noms suivants :

- Utilisateurs locaux
- DNS
- Domaines NIS externes
- Domaines LDAP externes

Une *name service switch table* spécifie les sources à rechercher des informations sur le réseau et l'ordre dans lequel les rechercher (fournissant la fonctionnalité équivalente du fichier `/etc/nsswitch.conf` sur les systèmes UNIX). Lorsqu'un client NAS se connecte au SVM, ONTAP vérifie les services de nom spécifiés pour obtenir les informations requises.

prise en charge de Kerberos Kerberos est un protocole d'authentification réseau qui fournit "l'authentification `tongs`" en cryptant les mots de passe utilisateur dans les implémentations client-serveur. ONTAP prend en charge l'authentification Kerberos 5 avec contrôle d'intégrité (krb5i) et l'authentification Kerberos 5 avec vérification de la confidentialité (krb5p).

Autorisation

ONTAP évalue trois niveaux de sécurité pour déterminer si une entité est autorisée à effectuer une action demandée sur les fichiers et répertoires résidant sur une SVM. L'accès est déterminé par les autorisations effectives après évaluation des niveaux de sécurité :

- Sécurité des exportations (NFS) et des partages (SMB)

La sécurité des exportations et des partages s'applique à l'accès client à une exportation NFS ou à un partage SMB donné. Les utilisateurs disposant de privilèges d'administration peuvent gérer la sécurité au niveau de l'exportation et du partage à partir des clients SMB et NFS.

- Sécurité des fichiers et répertoires Access Guard du niveau de stockage

La sécurité Access Guard du niveau de stockage s'applique aux accès des clients SMB et NFS pour les volumes SVM. Seules les autorisations d'accès NTFS sont prises en charge. Pour que ONTAP puisse effectuer des vérifications de sécurité sur les utilisateurs UNIX afin d'accéder aux données sur les volumes pour lesquels Storage-Level Access Guard a été appliqué, l'utilisateur UNIX doit mapper un utilisateur Windows sur le SVM propriétaire du volume.

- Sécurité native au niveau des fichiers NTFS, UNIX et NFSv4

La sécurité native au niveau du fichier existe sur le fichier ou le répertoire qui représente l'objet de stockage. Vous pouvez définir la sécurité au niveau des fichiers à partir d'un client. Les autorisations liées aux fichiers sont efficaces, que SMB ou NFS soit utilisé pour accéder aux données.

Authentification avec SAML

ONTAP prend en charge le langage SAML (Security assertion Markup Language) pour l'authentification des utilisateurs distants. Plusieurs fournisseurs d'identité (PDI) populaires sont pris en charge. Pour plus d'informations sur les PDI pris en charge et pour savoir comment activer l'authentification SAML, reportez-vous à la section "[Configurez l'authentification SAML](#)".

OAuth 2.0 avec clients API REST ONTAP

La prise en charge de l'infrastructure d'autorisation ouverte (OAuth 2.0) est disponible à partir de ONTAP 9.14. Vous ne pouvez utiliser OAuth 2.0 que pour prendre des décisions d'autorisation et de contrôle d'accès lorsque le client utilise l'API REST pour accéder à ONTAP. Toutefois, vous pouvez configurer et activer cette fonctionnalité avec n'importe quelle interface d'administration ONTAP, y compris l'interface de ligne de commandes, System Manager et l'API REST.

Les fonctionnalités standard d'OAuth 2.0 sont prises en charge avec plusieurs serveurs d'autorisation courants. Vous pouvez améliorer davantage la sécurité ONTAP en utilisant des jetons d'accès limités par l'expéditeur basés sur le protocole commun. De plus, de nombreuses options d'autorisation sont disponibles, notamment des étendues autonomes, ainsi que l'intégration avec les rôles REST ONTAP et les définitions d'utilisateur local. Voir "[Présentation de la mise en œuvre de ONTAP OAuth 2.0](#)" pour en savoir plus.

Authentification de l'administrateur et RBAC

Les administrateurs utilisent des comptes de connexion locaux ou distants pour s'authentifier auprès du cluster et du SVM. Le contrôle d'accès basé sur des rôles (RBAC) détermine les commandes à laquelle un administrateur a accès.

Authentification

Vous pouvez créer des comptes d'administrateur du cluster et des SVM locaux ou distants :

- Un compte local est un compte dans lequel les informations de compte, la clé publique ou le certificat de sécurité résident sur le système de stockage.

- Un compte distant est un compte dans lequel les informations de compte sont stockées sur un contrôleur de domaine Active Directory, un serveur LDAP ou un serveur NIS.

À l'exception du DNS, ONTAP utilise les mêmes services de noms pour authentifier les comptes d'administrateur qu'il utilise pour authentifier les clients.

RBAC

Le *role* attribué à un administrateur détermine les commandes auxquelles l'administrateur a accès. Vous attribuez le rôle lorsque vous créez le compte pour l'administrateur. Vous pouvez attribuer un autre rôle ou définir des rôles personnalisés selon vos besoins.

Analyse antivirus

Vous pouvez utiliser la fonctionnalité antivirus intégrée sur le système de stockage afin de protéger vos données contre les virus ou tout autre code malveillant. L'analyse antivirus ONTAP, appelée *Vscan*, associe le meilleur logiciel antivirus tiers à des fonctionnalités ONTAP, vous offrant ainsi la flexibilité nécessaire pour contrôler quels fichiers sont analysés et à quel moment.

Les systèmes de stockage délèguent des opérations d'analyse à des serveurs externes hébergeant le logiciel antivirus de fournisseurs tiers. Le *ONTAP antivirus Connector*, fourni par NetApp et installé sur le serveur externe, gère les communications entre le système de stockage et le logiciel antivirus.

- Vous pouvez utiliser *On-Access scan* pour rechercher des virus lorsque les clients ouvrent, lisent, renomment ou ferment des fichiers sur SMB. L'opération de fichier est suspendue jusqu'à ce que le serveur externe indique l'état de numérisation du fichier. Si le fichier a déjà été numérisé, ONTAP autorise l'opération de fichier. Dans le cas contraire, il demande un scan à partir du serveur.

L'analyse lors de l'accès n'est pas prise en charge par NFS.

- Vous pouvez utiliser *On-Demand scan* pour vérifier immédiatement ou selon un planning les fichiers à la recherche de virus. Il se peut que vous souhaitiez exécuter des analyses uniquement pendant les heures creuses, par exemple. Le serveur externe met à jour l'état d'analyse des fichiers vérifiés, de sorte que la latence d'accès aux fichiers pour ces fichiers (en supposant qu'ils n'ont pas été modifiés) est généralement réduite lorsqu'ils sont ensuite accédés par SMB.

Vous pouvez utiliser l'analyse à la demande pour n'importe quel chemin du namespace du SVM, même pour les volumes exportés uniquement via NFS.

Vous activez généralement les deux modes de scan sur un SVM. Dans les deux modes, le logiciel antivirus prend des mesures correctives sur les fichiers infectés en fonction de vos paramètres dans le logiciel.

analyse antivirus dans la reprise après sinistre et configurations MetroCluster

Pour la reprise sur incident et les configurations MetroCluster, il faut configurer des serveurs Vscan séparés pour les clusters locaux et partenaires.



The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.

Le cryptage

ONTAP propose des technologies de cryptage logicielles et matérielles qui permettent de garantir que les données au repos ne peuvent pas être lues si le support de stockage est requalifié, perdu ou volé.

ONTAP est conforme à la norme FIPS (Federal Information Processing Standards) 140-2 pour toutes les connexions SSL. Vous pouvez utiliser les solutions de cryptage suivantes :

- Solutions matérielles :

- NetApp Storage Encryption (NSE)

NSE est une solution matérielle qui utilise des lecteurs auto-cryptés (SED).

- Disques SED NVMe

ONTAP fournit le chiffrement de disque intégral pour les disques SED NVMe qui ne sont pas certifiés FIPS 140-2.

- Solutions logicielles :

- Chiffrement d'agrégat NetApp (NAE)

NAE est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque grâce à des clés uniques pour chaque agrégat.

- NVE (NetApp Volume Encryption)

NVE est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque où il est activé avec une clé unique pour chaque volume.

Utilisez les solutions de chiffrement logiciel (NAE ou NVE) et matériel (NSE ou NVMe SED) afin d'obtenir le double chiffrement au repos. L'efficacité du stockage n'est pas affectée par le chiffrement NAE ou NVE.

NetApp Storage Encryption

NetApp Storage Encryption (NSE) prend en charge les disques SED qui cryptent les données au fur et à mesure de leur écriture. Les données ne peuvent pas être lues sans une clé de chiffrement stockée sur le disque. La clé de chiffrement, à son tour, n'est accessible qu'à un nœud authentifié.

Lors d'une demande d'E/S, un nœud s'authentifie auprès d'un SED à l'aide d'une clé d'authentification extraite d'un serveur de gestion de clés externe ou d'un gestionnaire de clés intégré :

- Le serveur externe de gestion des clés est un système tiers de votre environnement de stockage qui transmet des clés d'authentification aux nœuds à l'aide du protocole KMIP (Key Management Interoperability Protocol).
- Le gestionnaire de clés intégré est un outil intégré qui sert des clés d'authentification aux nœuds du même système de stockage que vos données.

NSE prend en charge les disques durs et SSD à autocryptage. Vous pouvez utiliser NetApp Volume Encryption avec NSE pour doubler le chiffrement des données sur les disques NSE.



Si vous utilisez NSE sur un système doté d'un module Flash cache, vous devez également activer NVE ou NAE. NSE ne chiffre pas les données qui résident sur le module Flash cache.

Disques à autochiffrement NVMe

Les disques SED NVMe ne disposent pas de la certification FIPS 140-2-2. Cependant, ces disques utilisent le chiffrement de disque transparent AES 256 bits pour protéger les données au repos.

Les opérations de chiffrement des données, telles que la génération d'une clé d'authentification, sont effectuées en interne. La clé d'authentification est générée la première fois que le système de stockage accède au disque. Les disques protègent ensuite les données au repos en demandant une authentification du système de stockage à chaque fois que des opérations de données sont demandées.

Chiffrement d'agrégat NetApp

NetApp Aggregate Encryption (NAE) est une technologie logicielle de chiffrement de toutes les données dans un agrégat. NAE a pour avantage de regrouper les volumes dans la déduplication au niveau des agrégats, là où les volumes NVE sont exclus.

NAE permet de chiffrer les volumes au sein de l'agrégat à l'aide de clés d'agrégat.

Depuis la version ONTAP 9.7, les agrégats et volumes nouvellement créés sont chiffrés par défaut lorsque vous disposez de "[Licence NVE](#)" et de la gestion des clés intégrée ou externe.

NetApp Volume Encryption

NetApp Volume Encryption (NVE) est une technologie logicielle de chiffrement des données au repos d'un volume à la fois. Une clé de chiffrement accessible uniquement au système de stockage garantit que les données du volume ne peuvent pas être lues si le périphérique sous-jacent est séparé du système.

Les données, y compris les copies Snapshot, et les métadonnées sont chiffrées. L'accès aux données est donné par une clé XTS-AES-256 unique, une par volume. Un gestionnaire de clés intégré sécurise les clés du même système avec vos données.

Vous pouvez utiliser NVE sur n'importe quel type d'agrégat (HDD, SSD, hybride, LUN de baie), avec n'importe quel type RAID et dans n'importe quelle implémentation ONTAP prise en charge, y compris ONTAP Select. Vous pouvez également utiliser NVE avec NetApp Storage Encryption (NSE) pour doubler le chiffrement des données sur les disques NSE.

quand utiliser des serveurs KMIP bien qu'il soit moins onéreux et généralement plus pratique pour utiliser le gestionnaire de clés intégré, vous devez configurer des serveurs KMIP si l'un des cas suivants est vrai :

- Votre solution de gestion des clés de chiffrement doit être conforme à la norme FIPS 140-2 (Federal Information Processing Standards) ou OASIS KMIP.
- Vous avez besoin d'une solution à plusieurs clusters. Les serveurs KMIP prennent en charge plusieurs clusters avec une gestion centralisée des clés de chiffrement.

Les serveurs KMIP prennent en charge plusieurs clusters avec une gestion centralisée des clés de chiffrement.

- Votre entreprise exige que les clés d'authentification soient sécurisées sur un système ou à un emplacement différent de celui des données.

Les serveurs KMIP stockent les clés d'authentification séparément des données.

Informations associées

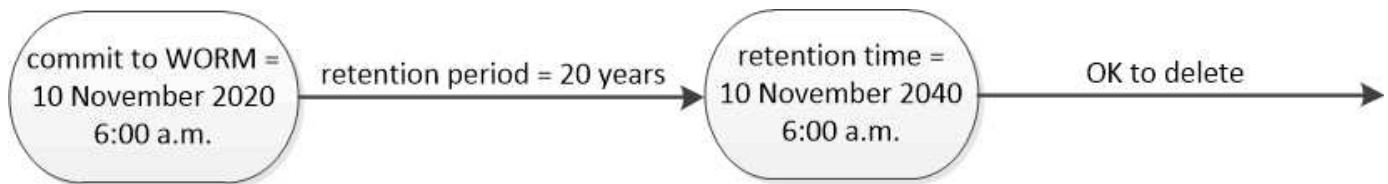
["FAQ : NetApp Volume Encryption et NetApp Aggregate Encryption"](#)

Stockage WORM

SnapLock est une solution de conformité hautes performances pour les entreprises qui utilisent le stockage WORM (Write Once, Read Many)_ pour conserver les fichiers stratégiques sous une forme non modifiée à des fins réglementaires et de gouvernance.

Une seule licence vous donne droit à l'utilisation de SnapLock en mode strict *Compliance*, afin de répondre aux obligations externes telles que la règle SEC 17a-4 et un mode plus lâche *Enterprise* afin de respecter les réglementations internes régissant la protection des ressources numériques. SnapLock utilise un *ComplianceClock* inviolable pour déterminer quand la période de conservation d'un fichier WORM est écoulée.

Vous pouvez utiliser *SnapLock for SnapVault* pour protéger les copies Snapshot sur un stockage secondaire. Vous pouvez utiliser SnapMirror pour répliquer des fichiers WORM dans un autre emplacement géographique à des fins autres que la reprise après incident.



SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.

ONTAP et VMware vSphere

Vous pouvez intégrer ONTAP et les produits NetApp associés à VMware vSphere. Plusieurs options sont disponibles en fonction de votre environnement technologique et des besoins de votre entreprise.

Concepts et terminologie sélectionnés

Lorsque vous commencez à utiliser ONTAP et les produits NetApp associés dans un environnement VMware, il est conseillé de vous familiariser avec certains concepts et termes clés.

LUN

Un LUN est un nombre utilisé pour identifier une unité *logique* au sein d'un réseau de stockage (SAN). Ces périphériques adressables sont généralement des disques logiques accessibles via le protocole SCSI (Small Computer System interface) ou l'un de ses dérivés encapsulés.

Volume virtuel VMware vSphere

Un volume virtuel (vVol) assure l'abstraction au niveau du volume pour le stockage utilisé par une machine virtuelle. Elle présente plusieurs avantages et offre une alternative à l'utilisation d'un LUN classique.

Réserves persistantes

Les réservations persistantes sont prises en charge par le SCSI-3 et une amélioration par rapport aux réservations SCSI-2 précédentes. Elles permettent à plusieurs initiateurs clients de communiquer avec une seule cible tout en verrouillant d'autres nœuds. Les réservations peuvent persister même si le bus est réinitialisé pour la récupération d'erreur.



Depuis ONTAP 9.15.1, vous pouvez créer une réservation permanente pour un volume virtuel à l'aide de SCSI-3. Cette fonctionnalité est uniquement prise en charge à l'aide des outils ONTAP pour VMware vSphere 9 avec un cluster de basculement Windows Server (WSFC).

Clustering avec basculement sur incident Windows Server

Microsoft WSFC est une fonctionnalité du système d'exploitation Windows Server qui fournit une tolérance aux pannes et une haute disponibilité. Un ensemble de nœuds de serveur (physiques ou virtuels) sont regroupés en tant que cluster afin d'assurer la résilience en cas de défaillance. WSFC est généralement utilisé pour déployer des services d'infrastructure, notamment des serveurs de bases de données, de fichiers et d'espaces de noms.

API de stockage VMware vSphere - sensibilisation au stockage

Vasa est un ensemble d'API permettant l'intégration des baies de stockage avec vCenter à des fins de gestion et d'administration. L'architecture repose sur plusieurs composants, notamment le *VASA Provider* qui gère la communication entre VMware vSphere et les systèmes de stockage. Avec ONTAP, le fournisseur est implémenté dans le cadre des outils ONTAP pour VMware vSphere.

API de stockage VMware vSphere - intégration de baies

VAAI est un ensemble d'API qui permet la communication entre les hôtes VMware vSphere ESXi et les périphériques de stockage. L'API inclut un ensemble d'opérations primitives utilisées par les hôtes pour décharger les opérations de stockage vers la baie. VAAI permet d'améliorer considérablement les performances des tâches consommatrices de stockage.

NetApp SnapCenter

SnapCenter est une plateforme centralisée et évolutive qui protège les données des applications, bases de données, systèmes de fichiers hôtes et machines virtuelles utilisant des systèmes de stockage ONTAP. Il exploite les technologies ONTAP natives, notamment Snapshot, SnapRestore, FlexClone, SnapMirror et SnapVault.

Plug-ins NetApp et technologies associées

NetApp offre une prise en charge robuste pour l'intégration de ONTAP et des produits associés aux technologies VMware vSphere.

Les outils ONTAP pour VMware vSphere

Les outils ONTAP pour VMware vSphere sont un ensemble d'outils permettant d'intégrer ONTAP et vSphere. Il implémente les fonctionnalités de fournisseur du framework d'API VASA. Les outils ONTAP incluent également le plug-in vCenter, un adaptateur de réplication du stockage (SRA) pour VMware Site Recovery Manager et un serveur d'API REST qui vous permet de créer des applications d'automatisation.

Plug-in NFS pour VMware VAAI

Le plug-in NetApp NFS pour VMware VAAI permet d'accéder aux fonctionnalités VAAI. Le plug-in peut être installé sur des hôtes ESXi et permet aux hôtes d'exploiter VAAI avec les datastores NFS sur ONTAP. Elle fournit plusieurs opérations, dont le clonage, les réservations d'espace et le déchargement de snapshots.

VMware Site Recovery Manager

VMware Site Recovery Manager (SRM) propose une fonctionnalité de reprise après incident. SRM s'intègre aux outils ONTAP pour VMware vSphere afin d'accéder aux fonctionnalités de gestion des données ONTAP et de les exploiter.

Cluster de stockage vSphere Metro

VSphere Metro Storage Cluster (vMSC) est une technologie qui active et prend en charge vSphere dans un déploiement de cluster étendu. Les solutions VMSC sont prises en charge avec NetApp MetroCluster et SnapMirror Active Sync (anciennement SMBC). Ces solutions assurent une meilleure continuité de l'activité en cas de défaillance de domaine. Le modèle de résilience est basé sur vos choix de configuration spécifiques.

Plug-in SnapCenter pour VMware vSphere

Le plug-in SnapCenter pour VMware vSphere (SCV) est une appliance virtuelle Linux que vous pouvez déployer avec le serveur SnapCenter ou en tant qu'application autonome. Dans les deux cas, SCV assure les opérations de sauvegarde et de restauration pour les machines virtuelles, les datastores et les VMDK. Les opérations sont rapides, compactes, cohérentes après panne et cohérentes avec les machines virtuelles.

En savoir plus

Plusieurs ressources supplémentaires sont disponibles pour vous aider à préparer le déploiement de ONTAP dans un environnement VMware vSphere.

- ["Documentation sur les outils ONTAP pour VMware vSphere"](#)
- ["Applications d'entreprise : VMware vSphere avec ONTAP"](#)
- ["Base de connaissances NetApp : que sont les réservations SCSI et les réservations persistantes SCSI ?"](#)
- ["Documentation du plug-in SnapCenter pour VMware vSphere"](#)

Gestion des données intégrant la cohérence applicative

La gestion des données intégrant la cohérence applicative vous permet de décrire l'application que vous souhaitez déployer sur ONTAP en termes d'application, et non en termes de stockage. L'application peut être configurée et prête à diffuser les données rapidement avec un minimum d'entrées grâce à System Manager et aux API REST.

La fonction de gestion des données intégrant la cohérence applicative offre un moyen de configurer, de gérer et de surveiller le stockage au niveau de chaque application. Cette fonctionnalité inclut les meilleures pratiques ONTAP qui permettent de provisionner des applications de manière optimale, avec un placement équilibré des objets de stockage en fonction des niveaux de service de performances souhaités et des ressources du système disponibles.

La fonction de gestion des données intégrant la cohérence applicative comprend un ensemble de modèles d'application, chaque modèle étant composé d'un ensemble de paramètres décrivant collectivement la configuration d'une application. Ces paramètres, qui sont souvent prédéfinis avec des valeurs par défaut, définissent les caractéristiques qu'un administrateur d'applications peut spécifier pour le provisionnement du stockage sur un système ONTAP, comme la taille des bases de données, les niveaux de service, les éléments d'accès par protocole tels que les LIF, ainsi que les critères de protection locale et les critères de protection à distance. En fonction des paramètres spécifiés, ONTAP configure des entités de stockage telles que les LUN et les volumes, avec des tailles et des niveaux de service appropriés pour l'application.

Vous pouvez effectuer les tâches suivantes pour vos applications :

- Créez des applications à l'aide des modèles d'application
- Gérez le stockage associé aux applications
- Modifiez ou supprimez les applications
- Afficher les applications
- Gérer les copies Snapshot des applications
- Création [groupes de cohérence](#) Pour fournir des fonctionnalités de protection des données, sélectionnez plusieurs LUN dans le même volume ou sur des volumes différents

FabricPool

De nombreux clients de NetApp disposent d'une quantité importante de données stockées rarement utilisées. On appelle les données *COLD*. Les clients disposent également de données fréquemment utilisées, que nous appelons les données *hot*. Dans l'idéal, vous souhaitez maintenir vos données actives dans votre système de stockage le plus rapide pour obtenir des performances optimales. Les données inactives peuvent être déplacées vers un stockage plus lent tant qu'elles sont immédiatement disponibles si nécessaire. Mais comment savoir quelles parties de vos données sont actives et lesquelles sont inactives ?

FabricPool est une fonctionnalité ONTAP qui déplace automatiquement les données entre un Tier local (agrégat) haute performance et un Tier cloud selon les modèles d'accès. Le Tiering libère du stockage local coûteux pour les données actives, tout en maintenant les données inactives disponibles immédiatement à partir d'un stockage objet à faible coût dans le cloud. FabricPool surveille en permanence l'accès aux données et les déplace entre les différents niveaux pour des performances optimales et des économies maximales.

L'utilisation de FabricPool pour déplacer les données inactives vers le cloud est l'un des moyens les plus simples d'obtenir des services efficaces dans le cloud et de créer une configuration de cloud hybride. FabricPool fonctionne au niveau du bloc de stockage et fonctionne donc aussi bien avec les données de fichiers que de LUN.

Toutefois, FabricPool n'est pas seulement pour le Tiering des données sur site vers le cloud. De nombreux clients utilisent FabricPool dans Cloud Volumes ONTAP pour transférer les données inactives d'un stockage cloud plus onéreux vers un stockage objet moins coûteux au sein du fournisseur cloud. À partir de ONTAP 9.8, vous pouvez capturer l'analytique sur les volumes compatibles avec FabricPool avec ["Analytique du système de fichiers"](#) ou ["efficacité du stockage sensible à la température"](#).

Les applications qui utilisent les données n'ont pas connaissance du Tier de stockage. Aucune modification n'est donc nécessaire. Le Tiering est entièrement automatique. Aucune administration n'est donc nécessaire.

Vous pouvez stocker les données inactives dans le stockage objet à partir de l'un des principaux fournisseurs cloud. Vous pouvez également choisir NetApp StorageGRID pour conserver vos données inactives dans votre propre cloud privé et bénéficier d'une performance optimale et d'un contrôle total sur vos données.

Informations associées

["Document FabricPool System Manager"](#)

["Tiering BlueXP"](#)

["Liste de lecture FabricPool sur NetApp TechComm TV"](#)

Intégration de System Manager à BlueXP

À partir de ONTAP 9.12.1, System Manager est entièrement intégré à BlueXP. BlueXP vous permet de gérer votre infrastructure multicloud hybride à partir d'un seul plan de contrôle tout en conservant le tableau de bord familier de System Manager.

BlueXP vous permet de créer et de gérer le stockage cloud (par exemple Cloud Volumes ONTAP), d'utiliser les services de données NetApp (par exemple, Cloud Backup) et de contrôler de nombreux périphériques de stockage sur site et périphériques.

Pour utiliser System Manager dans BlueXP, effectuez les opérations suivantes :

Étapes

1. Ouvrez un navigateur Web et entrez l'adresse IP de l'interface réseau de gestion du cluster.

Si le cluster est connecté à BlueXP, une invite de connexion s'affiche.

2. Cliquez sur **Continuer vers BlueXP** pour suivre le lien vers BlueXP.



Si vos paramètres système ont bloqué des réseaux externes, vous ne pourrez pas accéder à BlueXP. Pour accéder à System Manager à l'aide de BlueXP, vous devez vous assurer que l'adresse « cloudmanager.cloud.netapp.com`" est accessible par votre système. Sinon, à l'invite, vous pouvez choisir d'utiliser la version de System Manager installée avec votre système ONTAP.

3. Sur la page de connexion BlueXP, sélectionnez **Connectez-vous avec vos informations d'identification du site de support NetApp** et saisissez vos identifiants.

Si vous avez déjà utilisé BlueXP et que vous disposez d'une connexion à l'aide d'un e-mail et d'un mot de passe, vous devez continuer à utiliser cette option de connexion.

["En savoir plus sur la connexion à BlueXP"](#).

4. Si vous y êtes invité, entrez un nom pour votre nouveau compte BlueXP.

Dans la plupart des cas, BlueXP crée automatiquement un compte pour vous en fonction des données de votre cluster.

5. Saisissez les informations d'identification de l'administrateur du cluster pour le cluster.

Résultat

System Manager s'affiche et vous pouvez désormais gérer le cluster depuis BlueXP.

Découvrez vos clusters directement à partir de BlueXP

BlueXP offre deux façons de découvrir et de gérer vos clusters :

- Détection directe pour la gestion via System Manager

Il s'agit de la même option de découverte décrite dans la section précédente avec laquelle vous suivez la redirection.

- Découverte via un connecteur

Ce connecteur est un logiciel installé dans votre environnement qui vous permet d'accéder aux fonctions de gestion via System Manager. Il permet également d'accéder aux services cloud BlueXP qui offrent des fonctionnalités telles que la réplication, la sauvegarde et la restauration, le classement des données, le Tiering des données, etc.

Accédez au ["Documentation BlueXP"](#) pour en savoir plus sur ces options de découverte et de gestion.

En savoir plus sur BlueXP

- ["Présentation de BlueXP"](#)
- ["Gérez vos systèmes NetApp AFF et FAS à l'aide de BlueXP"](#)

Configuration, mise à niveau et restauration du logiciel et du firmware ONTAP

Configuration de ONTAP

Commencez avec la configuration de clusters ONTAP

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes ONTAP pour configurer de nouveaux clusters ONTAP. Avant de commencer, vous devez rassembler les informations nécessaires pour terminer la configuration du cluster, telles que le port et l'adresse IP de l'interface de gestion du cluster.

NetApp vous recommande de le faire ["Utilisez System Manager pour configurer de nouveaux clusters"](#). System Manager simplifie et simplifie l'installation et la configuration du cluster, notamment l'attribution d'une adresse IP de gestion de nœud, l'initialisation du cluster, la création d'un niveau local, la configuration des protocoles et le provisionnement du stockage initial.

Il n'est nécessaire que de ["Configurez votre cluster à l'aide de l'interface de ligne de commandes ONTAP"](#) Si vous exécutez ONTAP 9.7 ou une version antérieure sur une configuration MetroCluster. À partir de ONTAP 9.13.1, sur les plateformes AFF A800 et FAS8700, vous pouvez également utiliser l'interface de ligne de commande ONTAP pour créer et configurer de nouveaux clusters dans des environnements de mise en réseau IPv6 uniquement. Si vous devez utiliser IPv6 dans ONTAP 9.13.0 et versions antérieures, ou sur d'autres plateformes dans ONTAP 9.13.1 et versions ultérieures, vous pouvez utiliser System Manager pour créer de nouveaux clusters à l'aide d'IPv4, puis ["Convertir en IPv6"](#).

Ce dont vous aurez besoin pour la configuration de clusters

La configuration du cluster implique de rassembler les informations nécessaires pour configurer la configuration de chaque nœud, de créer le cluster sur le premier nœud et de joindre les nœuds restants au cluster.

Commencez par rassembler toutes les informations pertinentes dans les feuilles de calcul de configuration du cluster.

La fiche de configuration du cluster vous permet d'enregistrer les valeurs nécessaires au cours du processus de configuration du cluster. Si une valeur par défaut est fournie, vous pouvez utiliser cette valeur ou saisir votre propre valeur.

Paramètres par défaut du système

Les valeurs par défaut du système sont les valeurs par défaut pour le réseau de cluster privé. Il est préférable d'utiliser ces valeurs par défaut. Toutefois, s'ils ne répondent pas à vos exigences, vous pouvez utiliser le tableau pour enregistrer vos propres valeurs.



Pour les clusters configurés pour utiliser les switchs réseau, chaque switch de cluster doit utiliser une taille MTU de 9 9000.

Types d'information	Vos valeurs
Ports privés du réseau en cluster	

Types d'information	Vos valeurs
Masque de réseau du réseau de cluster	
Adresses IP de l'interface de cluster (pour chaque port réseau de cluster sur chaque nœud) Les adresses IP de chaque nœud doivent se trouver sur le même sous-réseau.	

Informations sur le cluster


Types d'information	Vos valeurs
Nom du cluster Le nom doit commencer par une lettre et doit comporter moins de 44 caractères. Le nom peut comprendre les caractères spéciaux suivants : · - _	

Clés de licence des fonctionnalités

Vous pouvez trouver les clés de licence pour vos commandes logicielles initiales ou d'extensions sur le site de support NetApp, sous **mon support > licences logicielles**.

Types d'information	Vos valeurs
Clés de licence des fonctionnalités	

Serveur virtuel de stockage d'administration (SVM)

Types d'information	Vos valeurs
<p>Mot de passe de l'administrateur du cluster</p> <p>Le mot de passe du compte admin dont le cluster requiert avant d'accorder l'accès de l'administrateur du cluster à la console ou via un protocole sécurisé.</p> <div>  <p>Pour des raisons de sécurité, il n'est pas recommandé d'enregistrer les mots de passe dans cette fiche.</p> </div> <p>Les règles par défaut pour les mots de passe sont les suivantes :</p> <ul style="list-style-type: none"> • Un mot de passe doit comporter au moins huit caractères. • Un mot de passe doit contenir au moins une lettre et un chiffre. 	

Types d'information	Vos valeurs
<p>Port d'interface de gestion du cluster</p> <p>Le port physique connecté au réseau de données et permet à l'administrateur du cluster de gérer le cluster.</p>	
<p>Adresse IP de l'interface de gestion du cluster</p> <p>Une adresse IPv4 ou IPv6 unique pour l'interface de gestion du cluster. L'administrateur du cluster utilise cette adresse pour accéder à la SVM admin et gérer le cluster. Généralement, cette adresse doit se trouver sur le réseau de données.</p> <p>Vous pouvez obtenir cette adresse IP auprès de l'administrateur responsable de l'attribution des adresses IP dans votre organisation.</p> <p>Exemple : 192.0.2.66</p>	
<p>Masque de réseau de l'interface de gestion du cluster (IPv4)</p> <p>Le masque de sous-réseau qui définit la plage d'adresses IPv4 valides sur le réseau de gestion du cluster.</p> <p>Exemple : 255.255.255.0</p>	
<p>Longueur du masque de réseau de l'interface de gestion du cluster (IPv6)</p> <p>Si l'interface de gestion du cluster utilise une adresse IPv6, cette valeur correspond à la longueur du préfixe qui définit la plage d'adresses IPv6 valides sur le réseau de gestion du cluster.</p> <p>Exemple : 64</p>	
<p>Passerelle par défaut de l'interface de gestion du cluster</p> <p>Adresse IP du routeur sur le réseau de gestion de cluster.</p>	

Types d'information	Vos valeurs
<p>Nom de domaine DNS</p> <p>Nom du domaine DNS de votre réseau.</p> <p>Le nom de domaine doit être composé de caractères alphanumériques. Pour entrer plusieurs noms de domaine DNS, séparez chaque nom par une virgule ou un espace.</p>	
<p>Adresses IP du serveur de noms</p> <p>Les adresses IP des serveurs de noms DNS. Séparez chaque adresse par une virgule ou un espace.</p>	

Informations de nœud (pour chaque nœud du cluster)

Types d'information	Vos valeurs
<p>Emplacement physique du contrôleur (en option)</p> <p>Description de l'emplacement physique du contrôleur. Utilisez une description qui indique où trouver ce nœud dans le cluster (par exemple, « Lab 5, rangée 7, rack B »).</p>	
<p>Port de l'interface de gestion des nœuds</p> <p>Port physique connecté au réseau de gestion de nœuds et permet à l'administrateur du cluster de gérer le nœud.</p>	
<p>Adresse IP de l'interface de gestion des nœuds</p> <p>Une adresse IPv4 ou IPv6 unique pour l'interface de gestion des nœuds sur le réseau de gestion. Si vous avez défini le port d'interface de gestion de nœuds comme port de données, cette adresse IP doit être une adresse IP unique sur le réseau de données.</p> <p>Vous pouvez obtenir cette adresse IP auprès de l'administrateur responsable de l'attribution des adresses IP dans votre organisation.</p> <p>Exemple : 192.0.2.66</p>	

Types d'information	Vos valeurs
<p>Masque de réseau de l'interface de gestion de nœud (IPv4)</p> <p>Masque de sous-réseau qui définit la plage d'adresses IP valides sur le réseau de gestion de nœud.</p> <p>Si vous avez défini le port de l'interface de gestion de nœud comme un port de données, le masque de réseau doit être le masque de sous-réseau du réseau de données.</p> <p>Exemple : 255.255.255.0</p>	
<p>Longueur du masque de réseau de l'interface de gestion des nœuds (IPv6)</p> <p>Si l'interface de gestion des nœuds utilise une adresse IPv6, cette valeur représente la longueur du préfixe qui définit la plage d'adresses IPv6 valides sur le réseau de gestion des nœuds.</p> <p>Exemple : 64</p>	
<p>Passerelle par défaut de l'interface de gestion du nœud</p> <p>Adresse IP du routeur sur le réseau de gestion des nœuds.</p>	

Informations sur le serveur NTP

Types d'information	Vos valeurs
<p>Adresses des serveurs NTP</p> <p>Les adresses IP des serveurs NTP (Network Time Protocol) de votre site. Ces serveurs sont utilisés pour synchroniser l'heure sur l'ensemble du cluster.</p>	

Configurez ONTAP sur un nouveau cluster avec System Manager

System Manager offre un workflow simple et facile pour l'installation d'un nouveau cluster et la configuration du stockage.

Dans certains cas, comme certains déploiements MetroCluster ou clusters qui nécessitent un adressage réseau IPv6, vous devrez peut-être utiliser l'interface de ligne de commandes de ONTAP pour configurer un nouveau cluster. Cliquez sur ["ici"](#) Pour plus d'informations sur ces exigences, ainsi que sur les étapes de configuration des clusters à l'aide de l'interface de ligne de commandes de ONTAP.

Avant de commencer

- Vous devez avoir installé, câblé et mis sous tension votre nouveau système de stockage conformément aux instructions d'installation et de configuration du modèle de votre plate-forme.
Voir la "[Documentation AFF et FAS](#)".
- Les interfaces réseau du cluster doivent être configurées sur chaque nœud du cluster pour les communications intra-cluster.
- Vous devez connaître les exigences de support suivantes de System Manager :
 - Lorsque vous configurez le logiciel de gestion des nœuds manuellement via l'interface de ligne de commandes, System Manager prend uniquement en charge IPv4 et ne prend pas en charge IPv6. Cependant, si vous lancez System Manager après avoir terminé la configuration matérielle à l'aide de DHCP avec une adresse IP auto-assignée et avec la découverte de Windows, System Manager peut configurer une adresse de gestion IPv6.

Dans ONTAP 9.6 et versions antérieures, System Manager ne prend pas en charge les déploiements nécessitant une mise en réseau IPv6.

- La prise en charge de l'installation MetroCluster est destinée aux configurations IP MetroCluster avec deux nœuds sur chaque site.

Dans ONTAP 9.7 et versions antérieures, System Manager ne prend pas en charge la nouvelle configuration du cluster pour les configurations MetroCluster.

- Vous devez recueillir les informations suivantes :
 - Adresse IP de gestion du cluster
 - Masque de sous-réseau réseau
 - Adresse IP de la passerelle réseau
 - Adresses IP du serveur DNS (Domain Name Services)
 - Adresses IP du serveur Network Time Protocol



Attribuez une adresse IP de gestion des nœuds

Système Windows

Vous devez connecter votre ordinateur Windows au même sous-réseau que les contrôleurs. L'adresse IP de gestion des nœuds sera automatiquement attribuée à votre système.

Étape

1. À partir du système Windows, ouvrez le lecteur **réseau** pour découvrir les nœuds.
2. Double-cliquez sur le nœud pour lancer l'assistant de configuration du cluster.

Autres systèmes

Vous devez configurer l'adresse IP node-management pour l'un des nœuds du cluster. Vous pouvez utiliser cette adresse IP node-management pour lancer l'assistant de configuration des clusters.

Voir ["Création du cluster sur le premier nœud"](#) Pour plus d'informations sur l'attribution d'une adresse IP de gestion des nœuds.

Initialiser le cluster

Vous initialisez le cluster en définissant un mot de passe administratif pour le cluster et en configurant les réseaux de gestion du cluster et de gestion des nœuds. Vous pouvez également configurer des services tels qu'un serveur DNS pour résoudre les noms d'hôtes et un serveur NTP pour synchroniser l'heure.

Étapes

1. Dans un navigateur Web, saisissez l'adresse IP de gestion des nœuds que vous avez configurée :
"<https://node-management-IP>"

System Manager détecte automatiquement les nœuds restants dans le cluster.

2. Sous **initialiser le système de stockage**, entrez le nom du cluster et le mot de passe admin.
3. Sous **réseau**, entrez l'adresse IP, le masque de sous-réseau et la passerelle de gestion du cluster.
4. Si vous souhaitez utiliser le service de nom de domaine pour résoudre les noms d'hôte, sélectionnez **utiliser le service de nom de domaine (DNS)**, puis entrez les informations sur le serveur DNS.
5. Si vous souhaitez utiliser le protocole NTP (Network Time Protocol) pour maintenir la synchronisation des heures dans votre cluster, sous **autres**, sélectionnez **utiliser les services de temps (NTP)**, puis entrez les informations du serveur NTP.
6. Cliquez sur **soumettre**.

Et la suite

Une fois que vous avez initialisé votre cluster, vous pouvez le faire ["Exécutez Active IQ Config Advisor pour valider votre configuration et vérifier les erreurs de configuration courantes"](#).

Créez votre niveau local

Créez des niveaux locaux à partir des disques ou disques SSD disponibles dans vos nœuds. System Manager calcule automatiquement la configuration de niveau la plus adaptée en fonction de votre matériel.

Étapes

1. Cliquez sur **Dashboard**, puis sur **Prepare Storage**.

Acceptez les recommandations de stockage pour votre niveau local.

Configurez des protocoles

En fonction des licences activées sur le cluster, vous pouvez activer les protocoles souhaités sur le cluster. Vous créez ensuite des interfaces réseau à l'aide desquelles vous pouvez accéder au stockage.

Étapes

1. Cliquez sur **Dashboard**, puis sur **configurer les protocoles**.
 - Activez iSCSI ou FC pour l'accès au SAN.
 - Activation de NFS ou SMB pour l'accès NAS.
 - Activez NVMe pour l'accès FC-NVMe.

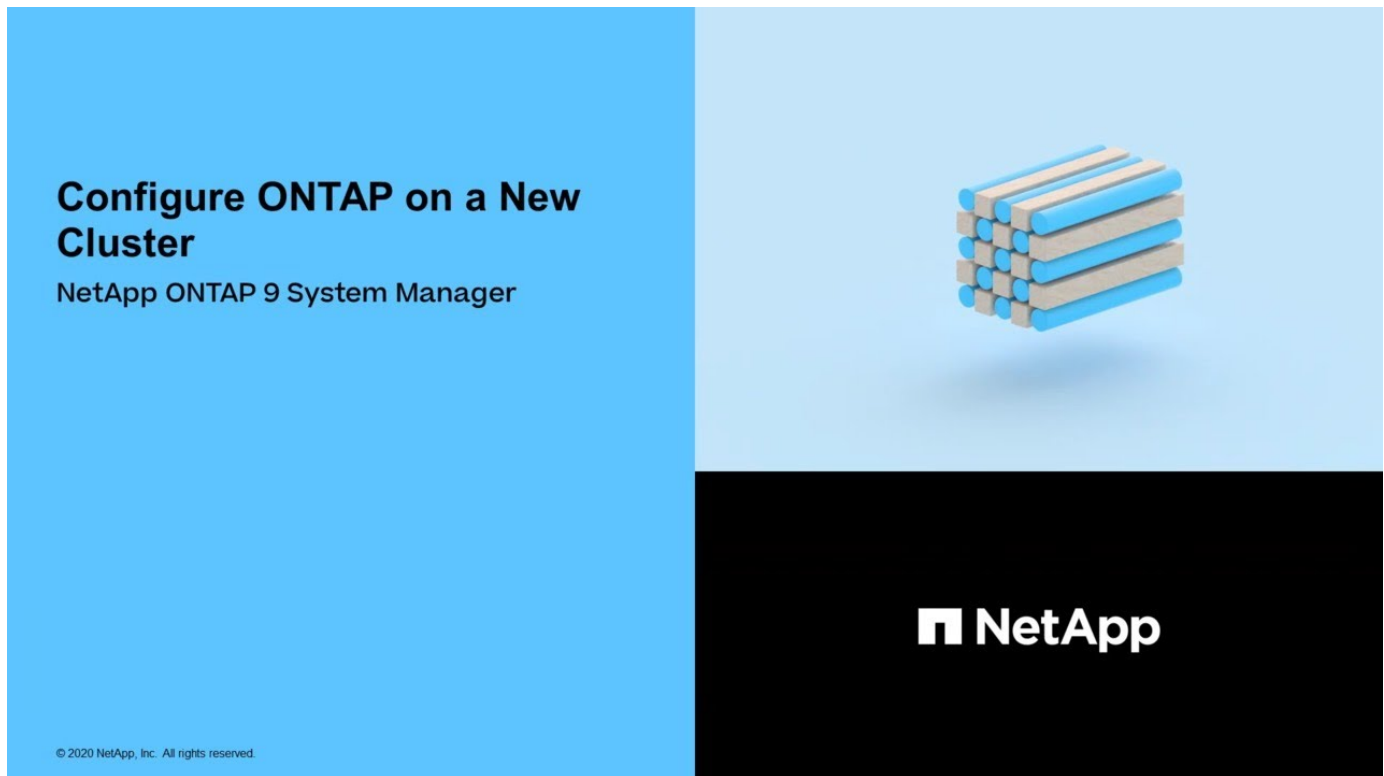
Provisionner le stockage

Une fois les protocoles configurés, vous pouvez provisionner le stockage. Les options que vous voyez dépendent des licences installées.

Étapes

1. Cliquez sur **Dashboard**, puis sur **Provision Storage**.
 - À "[Provisionnement de l'accès SAN](#)", Cliquez sur **Ajouter des LUN**.
 - À "[Provisionnez l'accès NAS](#)", Cliquez sur **Ajouter des volumes**.
 - À "[Provisionner le stockage NVMe](#)", Cliquez sur **Ajouter espaces de noms**.

Configurez ONTAP sur une nouvelle vidéo de cluster



Configuration d'un cluster via l'interface de ligne de commandes

Créer le cluster sur le premier nœud

Vous utilisez l'assistant de configuration du cluster pour créer le cluster sur le premier nœud. L'assistant vous aide à configurer le réseau de cluster qui connecte les nœuds, à créer le SVM (Cluster admin Storage Virtual machine), à ajouter des clés de licence de fonction et à créer l'interface de gestion des nœuds pour le premier nœud.

Avant de commencer

- Vous devez avoir installé, câblé et mis sous tension votre nouveau système de stockage conformément aux instructions d'installation et de configuration du modèle de votre plate-forme. Voir la "[Documentation AFF et FAS](#)".
- Les interfaces réseau du cluster doivent être configurées sur chaque nœud du cluster pour les communications intra-cluster.

- Si vous configurez IPv6 sur votre cluster, IPv6 doit être configuré sur le contrôleur BMC (base Management Controller) pour que vous puissiez accéder au système via SSH.

Étapes

1. Mettez tous les nœuds que vous ajoutez au cluster sous tension. Cela est nécessaire pour activer la détection pour la configuration de votre cluster.
2. Se connecter à la console du premier nœud.

Le nœud démarre, puis l'assistant de configuration du cluster démarre sur la console.

```
Welcome to the cluster setup wizard....
```

3. Acceptez la déclaration AutoSupport.

```
Type yes to confirm and continue {yes}: yes
```



AutoSupport est activé par défaut.

4. Suivez les instructions à l'écran pour attribuer une adresse IP au nœud.

À partir de la version ONTAP 9.13.1, vous pouvez attribuer des adresses IPv6 pour les LIF de gestion sur les plateformes A800 et FAS8700. Pour les versions ONTAP antérieures à 9.13.1, ou pour la version 9.13.1 et ultérieures sur d'autres plateformes, vous devez attribuer des adresses IPv4 pour les LIF de gestion, puis les convertir en IPv6 une fois que vous avez terminé la configuration du cluster.

5. Appuyez sur **entrée** pour continuer.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

6. Créez un nouveau cluster : `create`
7. Acceptez les valeurs par défaut du système ou entrez vos propres valeurs.
8. Une fois l'installation terminée, connectez-vous au cluster et vérifiez que le cluster est actif et que le premier nœud fonctionne correctement en entrant la commande CLI ONTAP : `cluster show`

L'exemple suivant montre un cluster dans lequel le premier nœud (cluster 1-01) est sain et peut participer :

```
cluster1::> cluster show
Node                      Health  Eligibility
-----
cluster1-01              true    true
```

Pour modifier les valeurs saisies pour le SVM admin ou le SVM node, il est possible d'accéder à l'assistant Cluster Setup en utilisant le `cluster setup` commande.

Une fois que vous avez terminé

Si besoin, ["Convertir d'IPv4 en IPv6"](#).

Associez les nœuds restants au cluster

Une fois le cluster créé, l'assistant de configuration du cluster vous permet de relier chaque nœud restant au cluster un par un. L'assistant vous aide à configurer l'interface de gestion de nœuds de chaque nœud.

Lorsque vous associez deux nœuds à un cluster, vous créez une paire haute disponibilité (HA). Si vous rejoignez 4 nœuds, vous créez deux paires haute disponibilité. Pour en savoir plus sur la haute disponibilité, voir ["En savoir plus sur la haute disponibilité"](#).

Vous ne pouvez relier qu'un seul nœud au cluster à la fois. Lorsque vous commencez à joindre un nœud au cluster, vous devez terminer l'opération de jointure pour ce nœud, et le nœud doit faire partie du cluster avant de pouvoir commencer à vous connecter au nœud suivant.

Meilleure pratique : si vous disposez d'un FAS2720 avec 24 disques NL-SAS ou moins, vous devez vérifier que la configuration de stockage par défaut est définie sur actif/passif pour optimiser les performances. Pour plus d'informations, reportez-vous à la documentation ["configuration d'une configuration actif-passif sur les nœuds à l'aide du partitionnement données-racines"](#) de .

1. Connectez-vous au nœud que vous prévoyez de joindre au cluster.

L'assistant de configuration du cluster démarre sur la console.

```
Welcome to the cluster setup wizard....
```

2. Acceptez la déclaration AutoSupport.



AutoSupport est activé par défaut.

```
Type yes to confirm and continue {yes}: yes
```

3. Suivez les instructions à l'écran pour attribuer une adresse IP au nœud.

À partir de la version ONTAP 9.13.1, vous pouvez attribuer des adresses IPv6 pour les LIF de gestion sur les plateformes A800 et FAS8700. Pour les versions ONTAP antérieures à 9.13.1, ou pour la version 9.13.1 et ultérieures sur d'autres plateformes, vous devez attribuer des adresses IPv4 pour les LIF de gestion, puis les convertir en IPv6 une fois que vous avez terminé la configuration du cluster.

4. Appuyez sur **entrée** pour continuer.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

5. Associez le nœud au cluster : `join`

6. Suivez les instructions à l'écran pour configurer le nœud et le joindre au cluster.
7. Une fois l'installation terminée, vérifiez que le nœud fonctionne correctement et qu'il peut participer au cluster : `cluster show`

L'exemple suivant montre un cluster après le rattachement du second nœud (cluster1-02) au cluster :

```
cluster1::> cluster show
Node                      Health  Eligibility
-----
cluster1-01              true    true
cluster1-02              true    true
```

Pour modifier les valeurs saisies pour le SVM admin ou le SVM node, il est possible d'accéder à l'assistant Cluster Setup en utilisant la commande `cluster setup`.

8. Répétez cette tâche pour chaque nœud restant.

Une fois que vous avez terminé

Si besoin, ["Convertir d'IPv4 en IPv6"](#).

Convertissez les LIF de gestion d'IPv4 en IPv6

À partir de la version ONTAP 9.13.1, vous pouvez attribuer des adresses IPv6 aux LIF de gestion sur les plateformes A800 et FAS8700 lors de la configuration initiale des clusters. Pour les versions ONTAP antérieures à 9.13.1, ou pour la version 9.13.1 et ultérieure sur d'autres plateformes, vous devez d'abord attribuer des adresses IPv4 aux LIF de gestion, puis les convertir en adresses IPv6 une fois que vous avez terminé la configuration du cluster.

Étapes

1. Activer IPv6 pour le cluster :

```
network options ipv6 modify -enable true
```

2. Définir le privilège sur avancé :

```
set priv advanced
```

3. Afficher la liste des préfixes RA appris sur différentes interfaces :

```
network ndp prefix show
```

4. Créer une LIF de gestion IPv6 :

Utiliser le format `prefix::id` Dans le paramètre d'adresse pour construire l'adresse IPv6 manuellement.

```
network interface create -vserver <svm_name> -lif <LIF> -home-node  
<home_node> -home-port <home_port> -address <IPv6prefix::id> -netmask  
-length <netmask_length> -failover-policy <policy> -service-policy  
<service_policy> -auto-revert true
```

5. Vérifier que le LIF a été créé :

```
network interface show
```

6. Vérifiez que l'adresse IP configurée est accessible :

```
network ping6
```

7. Marquer le LIF IPv4 comme administrative comme down :

```
network interface modify -vserver <svm_name> -lif <lif_name> -status  
-admin down
```

8. Supprimez la LIF de gestion IPv4 :

```
network interface delete -vserver <svm_name> -lif <lif_name>
```

9. Vérifier que la LIF de gestion IPv4 est supprimée :

```
network interface show
```

Vérifiez votre cluster avec Active IQ Config Advisor

Une fois que vous avez rejoint tous les nœuds sur le nouveau cluster, il est important d'exécuter Active IQ Config Advisor pour valider votre configuration et vérifier l'absence d'erreurs de configuration courantes.

Config Advisor est une application web que vous installez sur votre ordinateur portable, ordinateur virtuel ou serveur, et qui fonctionne sur les plates-formes Windows, Linux et Mac.

Config Advisor exécute une série de commandes permettant de valider votre installation et de vérifier l'état global de la configuration, notamment les commutateurs de cluster et de stockage.

1. Téléchargez et installez Active IQ Config Advisor.

"Active IQ Config Advisor"

2. Lancez Active IQ et configurez une phrase de passe lorsque vous y êtes invité.
3. Vérifiez vos paramètres et cliquez sur **Enregistrer**.
4. Sur la page **objectifs**, cliquez sur **ONTAP validation post-déploiement**.
5. Choisissez le mode guidé ou Expert.

Si vous choisissez le mode guidé, les commutateurs connectés sont détectés automatiquement.

6. Saisissez les identifiants du cluster.
7. (Facultatif) cliquez sur **Form Validate**.
8. Pour commencer la collecte de données, cliquez sur **Enregistrer et évaluer**.
9. Une fois la collecte de données terminée, sous **moniteur de tâche > actions**, affichez les données collectées en cliquant sur l'icône **Affichage des données** et affichez les résultats en cliquant sur l'icône **Résultats**.
10. Résoudre les problèmes identifiés par Config Advisor.

Synchronisation de l'heure du système sur le cluster

La synchronisation de l'heure garantit que chaque nœud du cluster est à la même heure et empêche les défaillances CIFS et Kerberos.

Un serveur NTP (Network Time Protocol) doit être configuré sur votre site. Depuis ONTAP 9.5, vous pouvez configurer votre serveur NTP avec une authentification symétrique. Pour plus d'informations, reportez-vous à la documentation "[gestion de l'heure du cluster \(administrateurs du cluster uniquement\)](#)" de .

Vous synchronisez l'heure sur le cluster en associant le cluster à un ou plusieurs serveurs NTP.

1. Vérifiez que le fuseau horaire et l'heure du système sont correctement définis pour chaque nœud.

Tous les nœuds du cluster doivent être définis sur le même fuseau horaire.

- a. Utilisez la commande `cluster date show` pour afficher la date, l'heure et le fuseau horaire actuels pour chaque nœud.

```
cluster1::> cluster date show
Node           Date           Time zone
-----
cluster1-01    01/06/2015 09:35:15 America/New_York
cluster1-02    01/06/2015 09:35:15 America/New_York
cluster1-03    01/06/2015 09:35:15 America/New_York
cluster1-04    01/06/2015 09:35:15 America/New_York
4 entries were displayed.
```

- b. Utiliser la commande `cluster date modify` pour modifier le fuseau horaire ou la date de tous les nœuds.

Cet exemple modifie le fuseau horaire du cluster en GMT :

```
cluster1::> cluster date modify -timezone GMT
```

2. Utilisez la commande `cluster time-service ntp server create` pour associer le cluster à votre serveur NTP.

- Pour configurer votre serveur NTP sans authentification symétrique, entrez la commande suivante :
`cluster time-service ntp server create -server server_name`
- Pour configurer votre serveur NTP avec une authentification symétrique, entrez la commande suivante :
`cluster time-service ntp server create -server server_ip_address -key-id key_id`



L'authentification symétrique est disponible à partir de ONTAP 9.5. Elle n'est pas disponible dans ONTAP 9.4 ou version antérieure.

Cet exemple suppose que le DNS a été configuré pour le cluster. Si vous n'avez pas configuré de DNS, vous devez spécifier l'adresse IP du serveur NTP :

```
cluster1::> cluster time-service ntp server create -server  
ntp1.example.com
```

3. Vérifiez que le cluster est associé à un serveur NTP : `cluster time-service ntp server show`

```
cluster1::> cluster time-service ntp server show  
Server                Version  
-----  
ntp1.example.com      auto
```

Informations associées

["Administration du système"](#)

Commandes de gestion de l'authentification symétrique sur les serveurs NTP

Depuis ONTAP 9.5, le protocole NTP (Network Time Protocol) version 3 est pris en charge. NTPv3 inclut une authentification symétrique à l'aide de clés SHA-1 qui augmente la sécurité du réseau.

Pour cela...	Utilisez cette commande...
Configurer un serveur NTP sans authentification symétrique	<code>cluster time-service ntp server create -server server_name</code>
Configurez un serveur NTP avec une authentification symétrique	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>

Pour cela...	Utilisez cette commande...
<p>Activez l'authentification symétrique pour un serveur NTP existant</p> <p>Un serveur NTP existant peut être modifié pour activer l'authentification en ajoutant l'ID de clé requis</p>	<pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre>
Configurez une clé NTP partagée	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <p>Remarque : les clés partagées sont désignées par un ID. L'ID, son type et la valeur doivent être identiques sur le nœud et le serveur NTP</p>
Configurez un serveur NTP avec un ID de clé inconnu	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre>
Configurez un serveur dont l'ID de clé n'est pas configuré sur le serveur NTP.	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <p>Remarque : l'ID, le type et la valeur de la clé doivent être identiques à l'ID, au type et à la valeur de clé configurés sur le serveur NTP.</p>
Désactiver l'authentification symétrique	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

Tâches de configuration système supplémentaires à réaliser

Une fois le cluster configuré, vous pouvez continuer à configurer le cluster à l'aide de System Manager ou de l'interface de ligne de commandes ONTAP.

Tâche de configuration du système	Ressource
<p>Configurer le réseau :</p> <ul style="list-style-type: none"> • Créer des domaines de diffusion • Créer des sous-réseaux • Créez des espaces IP 	"Configuration du réseau"
Configurez le processeur de service	"Administration du système"
Placez vos agrégats	"Gestion des disques et des agrégats"

Tâche de configuration du système	Ressource
Créez et configurez des machines virtuelles de stockage des données (SVM)	"Configuration NFS" "Configuration SMB" "Administration SAN"
Configurer les notifications d'événements	"Configuration EMS"

Configurez le logiciel des baies SAN 100 % Flash

Présentation de la configuration logicielle des baies SAN 100 % Flash

Les baies SAN 100 % Flash NetApp sont disponibles à partir de ONTAP 9.7. Les systèmes ASAS sont des solutions SAN 100 % Flash basées sur les plateformes NetApp éprouvées de AFF.

Les plateformes ASA utilisent une symétrie actif-actif pour les chemins d'accès multiples. Tous les chemins sont optimisés/en mode actif. Ainsi, en cas de basculement de stockage, l'hôte n'a pas besoin d'attendre la transition ALUA des chemins de basculement pour reprendre les E/S. Le délai de basculement est ainsi réduit.

Configurer un ASA

Les baies SAN 100 % Flash (ASA) suivent la même procédure de configuration que les systèmes non ASA.

System Manager vous guide tout au long des procédures nécessaires pour initialiser votre cluster, créer un niveau local, configurer les protocoles et provisionner le stockage de votre ASA.

[Commencez avec la configuration de clusters ONTAP.](#)

Utilitaires et paramètres d'hôte ASA

Les paramètres d'hôte pour la configuration des baies SAN 100 % Flash (ASA) sont les mêmes que pour tous les autres hôtes SAN.

Vous pouvez télécharger le ["Logiciel NetApp Host Utilities"](#) pour vos hôtes spécifiques sur le site de support.

Méthodes d'identification d'un système ASA

Vous pouvez identifier un système ASA via System Manager ou l'interface de ligne de commandes de ONTAP.

- **Dans le tableau de bord System Manager** : cliquez sur **Cluster > Présentation**, puis sélectionnez le nœud système.

La **PERSONNALITÉ** s'affiche sous la forme **Baie SAN 100 % Flash**.

- **À partir de l'interface CLI** : entrez le `san config show` commande.

La valeur « Baie SAN 100 % Flash » est renvoyée pour les systèmes ASA.

Informations associées

- ["Rapport technique 4968 : disponibilité et intégrité des données des baies SAN 100 % Flash de NetApp"](#)
- ["Rapport technique de NetApp 4080 : meilleures pratiques pour le SAN moderne"](#)

Limites de configuration et prise en charge des baies SAN 100 % Flash

Les limites de configuration et la prise en charge varient en fonction de la ONTAP version du système ASA.

Les détails les plus récents sur les limites de configuration prises en charge sont disponibles dans ["NetApp Hardware Universe"](#).

Protocoles SAN et nombre de nœuds pris en charge par cluster

Les protocoles SAN pris en charge et le nombre maximum de nœuds par cluster dépendent de votre configuration non MetroCluster ou MetroCluster :

Configurations non MetroCluster

Le tableau suivant présente la prise en charge des protocoles SAN par ASA et le nombre de nœuds pris en charge par cluster dans des configurations non MetroCluster :

Depuis ONTAP...	Protocoles pris en charge	Nombre maximal de nœuds par cluster
9.11.1	<ul style="list-style-type: none">• NVMe/TCP• NVMe/FC	12
9.10.1	<ul style="list-style-type: none">• NVMe/TCP	2
9.9.1	<ul style="list-style-type: none">• NVMe/FC	2
	<ul style="list-style-type: none">• FC• iSCSI	12
9.7	<ul style="list-style-type: none">• FC• iSCSI	2

Configurations MetroCluster IP

Le tableau ci-dessous présente la prise en charge des protocoles SAN par ASA et le nombre de nœuds pris en charge par cluster dans les configurations MetroCluster IP :

Depuis ONTAP...	Protocoles pris en charge	Nombre maximal de nœuds par cluster
9.15.1	<ul style="list-style-type: none">• NVMe/TCP	2 nœuds par cluster dans des configurations IP MetroCluster à quatre nœuds
9.12.1	<ul style="list-style-type: none">• NVMe/FC	2 nœuds par cluster dans des configurations IP MetroCluster à quatre nœuds
9.9.1	<ul style="list-style-type: none">• FC• iSCSI	4 nœuds par cluster dans des configurations IP MetroCluster à 8 nœuds
9.7	<ul style="list-style-type: none">• FC• iSCSI	2 nœuds par cluster dans des configurations IP MetroCluster à quatre nœuds

Prise en charge des ports persistants

Depuis la version ONTAP 9.8, les ports persistants sont activés par défaut sur les baies SAN 100 % Flash (ASA) configurées pour utiliser le protocole FC. Les ports persistants sont uniquement disponibles pour FC et

requièrent l'appartenance de zone identifiée par WWPN (World Wide Port Name).

Les ports persistants réduisent l'impact des basculements en créant une LIF « shadow » sur le port physique correspondant du partenaire haute disponibilité. Lorsqu'un nœud est repris, la LIF shadow sur le nœud partenaire assume l'identité du LIF d'origine, y compris le WWPNe. Avant que le chemin d'accès au nœud mis en service ne soit modifié en défectueux, le shadow LIF apparaît sous la forme d'un chemin actif-optimisé vers la pile MPIO hôte, ainsi que de transferts d'E/S. Cela réduit les perturbations d'E/S car l'hôte voit toujours le même nombre de chemins vers la cible, même lors des opérations de basculement de stockage.

Pour les ports persistants, les caractéristiques de port FCP suivantes doivent être identiques dans la paire haute disponibilité :

- Nombre de ports FCP
- Noms des ports FCP
- Vitesses du port FCP
- Segmentation basée sur le WWPN FCP LIF

Si l'une de ces caractéristiques n'est pas identique au sein de la paire HA, le message EMS suivant est généré :

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

Pour plus d'informations sur les ports persistants, voir ["Rapport technique de NetApp 4080 : meilleures pratiques pour le SAN moderne"](#).

Mettez à niveau ONTAP

Présentation de la mise à niveau ONTAP

La mise à niveau de votre logiciel ONTAP vous permet de bénéficier des nouvelles fonctionnalités améliorées de ONTAP qui contribuent à réduire les coûts, accélérer les workloads stratégiques, améliorer la sécurité et étendre la portée de la protection des données disponible pour votre entreprise.

Une mise à niveau majeure de ONTAP consiste à passer d'une version portant un numéro ONTAP inférieur à supérieur. Par exemple, une mise à niveau de votre cluster de ONTAP 9.8 vers ONTAP 9.12.1 est possible.

Une mise à niveau mineure (ou correctif) consiste à passer d'une version ONTAP inférieure à une version ONTAP supérieure dans la même version numérotée. Par exemple, une mise à niveau de votre cluster de ONTAP 9.12.1P1 à 9.12.1P4.

Pour commencer, vous devez ["préparer la mise à niveau"](#). Si vous avez un contrat SupportEdge actif pour le conseiller digital Active IQ, vous devriez ["Planifiez votre mise à niveau avec Upgrade Advisor"](#). Upgrade Advisor fournit des informations intelligentes qui vous aident à minimiser l'incertitude et les risques en évaluant votre cluster et en créant un plan de mise à niveau propre à votre configuration.

Une fois que vous avez préparé la mise à niveau, il est recommandé d'effectuer les mises à niveau à l'aide de ["Mise à niveau automatisée sans interruption \(ANDU\) depuis System Manager"](#). ANDU exploite la technologie de basculement haute disponibilité d'ONTAP pour assurer le service des données sans interruption lors de la mise à niveau.



À partir de ONTAP 9.12.1, System Manager est entièrement intégré à BlueXP. Si BlueXP est configuré sur votre système, vous pouvez effectuer une mise à niveau via l'environnement de travail BlueXP.

Si vous avez besoin d'aide pour mettre à niveau votre logiciel ONTAP, les services professionnels NetApp proposent une ["Service géré de mise à niveau"](#). Si vous souhaitez utiliser ce service, contactez votre ingénieur commercial NetApp ou ["Envoyez le formulaire de demande de renseignements NetApp"](#). Le service géré de mise à niveau ainsi que d'autres types d'assistance de mise à niveau sont disponibles pour les clients disposant de ["Services SupportEdge Expert"](#) sans frais supplémentaires.

Quand dois-je mettre à niveau ONTAP ?

Vous devez régulièrement mettre à niveau votre logiciel ONTAP. La mise à niveau de ONTAP vous permet de profiter des fonctionnalités nouvelles et améliorées et de mettre en œuvre les correctifs actuels pour les problèmes connus.

Mises à niveau majeures de ONTAP

Une mise à niveau ou une version majeure de ONTAP comprend généralement :

- Nouvelles fonctionnalités de ONTAP
- Modifications importantes de l'infrastructure, telles que les modifications fondamentales apportées au fonctionnement NetApp WAFL ou au fonctionnement RAID
- Prise en charge des nouveaux systèmes matériels NetApp
- Prise en charge des composants matériels de remplacement tels que les cartes d'interface réseau plus récentes ou les cartes de bus hôte

Les nouvelles versions de ONTAP bénéficient d'un support complet pendant 3 ans. NetApp vous recommande d'exécuter la dernière version pendant un an à compter de la disponibilité générale, puis d'utiliser le temps restant dans la fenêtre de support complet pour planifier votre transition vers une nouvelle version de ONTAP.

Mises à niveau de correctifs ONTAP

Les mises à niveau de correctifs apportent des correctifs rapides pour les bugs critiques qui ne peuvent pas attendre la prochaine version majeure de la fonctionnalité ONTAP. Les mises à niveau de correctifs non critiques doivent être appliquées tous les 3-6 mois. Les mises à niveau critiques des correctifs doivent être appliquées dès que possible.

En savoir plus sur ["niveaux de patch minimum recommandés"](#) Pour les versions ONTAP.

Dates de publication de ONTAP

À partir de la version ONTAP 9.8, NetApp publie deux fois par an les versions ONTAP. Bien que les plans soient susceptibles d'être modifiés, l'objectif est de fournir de nouvelles versions de ONTAP au cours des deuxième et quatrième trimestres de chaque année civile. Utilisez ces informations pour planifier la durée de votre mise à niveau et bénéficier de la dernière version de ONTAP.

Version	Date de sortie
9.15.1	Mai 2024

Version	Date de sortie
9.14.1	Janvier 2024
9.13.1	Juin 2023
9.12.1	Février 2023
9.11.1	Juillet 2022
9.10.1	Janvier 2022
9.9.1	Juin 2021

Niveaux de support ONTAP

Le niveau de support disponible pour une version spécifique de ONTAP varie en fonction du moment où le logiciel a été commercialisé.

Niveau de support	Support complet			Prise en charge limitée		Support en libre-service		
Année	1	2	3	4	5	6	7	8
Accès à la documentation en ligne	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.
Support technique	Oui.	Oui.	Oui.	Oui.	Oui.			
Analyse de la cause première	Oui.	Oui.	Oui.	Oui.	Oui.			
Téléchargements de logiciels	Oui.	Oui.	Oui.	Oui.	Oui.			
Mises à jour de service (correctifs [versions P])	Oui.	Oui.	Oui.					
Alertes concernant les vulnérabilités	Oui.	Oui.	Oui.					

Informations associées

- Apprendre ["Nouveautés des versions ONTAP actuellement prises en charge"](#).
- En savoir plus sur ["Versions minimales recommandées de ONTAP"](#).
- En savoir plus sur ["Prise en charge de la version du logiciel ONTAP"](#).

- En savoir plus sur le ["Modèle de version ONTAP"](#).

Exécutez des vérifications ONTAP automatisées avant la mise à niveau

Vous n'avez pas besoin de mettre à niveau votre logiciel ONTAP pour exécuter les pré-contrôles de mise à niveau automatisés ONTAP. En exécutant les vérifications avant mise à niveau indépendamment de la procédure de mise à niveau automatique ONTAP, vous pouvez voir quelles vérifications sont effectuées sur votre cluster et afficher la liste des erreurs ou avertissements à corriger avant de commencer la mise à niveau réelle. Supposons, par exemple, que vous prévoyez de mettre à niveau votre logiciel ONTAP pendant une fenêtre de maintenance qui doit avoir lieu dans deux semaines. Pendant que vous attendez la date programmée, vous pouvez exécuter les pré-contrôles de mise à niveau automatisés et effectuer les actions correctives nécessaires avant la fenêtre de maintenance. Cela permet de réduire les risques d'erreurs de configuration inattendues après le démarrage de la mise à niveau.

Si vous êtes prêt à commencer la mise à niveau du logiciel ONTAP, vous n'avez pas besoin d'effectuer cette procédure. Vous devez suivre le ["processus de mise à niveau automatisé"](#), qui inclut l'exécution des pré-contrôles de mise à niveau automatisés.



Pour les configurations MetroCluster, vous devez d'abord exécuter ces étapes sur le cluster A, puis effectuer les mêmes étapes sur le cluster B.

Avant de commencer

Vous devriez ["Téléchargez l'image du logiciel ONTAP cible"](#).

Pour exécuter les pré-contrôles de mise à niveau automatisés pour un ["mise à niveau directe à plusieurs sauts"](#), Il vous suffit de télécharger le progiciel pour votre version ONTAP cible. Vous n'aurez pas besoin de charger la version intermédiaire de ONTAP jusqu'à ce que vous commenciez la mise à niveau réelle. Par exemple, si vous exécutez des contrôles de pré-mise à niveau automatisés pour une mise à niveau de 9.8 à 9.13.1, vous devez télécharger le progiciel pour ONTAP 9.13.1. Vous n'avez pas besoin de télécharger le pack logiciel pour ONTAP 9.12.1.

Exemple 1. Étapes

System Manager

1. Valider l'image cible ONTAP :



Si vous mettez à niveau une configuration MetroCluster, vous devez valider le cluster A, puis répéter le processus de validation sur le cluster B.

a. Selon la version de ONTAP que vous utilisez, effectuez l'une des opérations suivantes :

Si vous exécutez...	Procédez comme ça...
ONTAP 9.8 ou version ultérieure	Cliquez sur Cluster > Présentation .
ONTAP 9.5, 9.6 et 9.7	Cliquez sur Configuration > Cluster > Update .
ONTAP 9.4 ou version antérieure	Cliquez sur Configuration > Cluster Update .

b. Dans le coin droit du volet **vue d'ensemble**, cliquez sur :

c. Cliquez sur **mise à jour ONTAP**.

d. Dans l'onglet **mise à jour du cluster**, ajoutez une nouvelle image ou sélectionnez une image disponible.

Les fonctions que vous recherchez...	Alors...
Ajoutez une nouvelle image logicielle à partir d'un dossier local Vous devriez déjà avoir "téléchargez l'image - effectué" au client local.	<ul style="list-style-type: none">i. Sous Images logicielles disponibles, cliquez sur Ajouter à partir de local.ii. Accédez à l'emplacement où vous avez enregistré l'image logicielle, sélectionnez l'image, puis cliquez sur Ouvrir.
Ajoutez une nouvelle image logicielle à partir d'un serveur HTTP ou FTP	<ul style="list-style-type: none">i. Cliquez sur Ajouter à partir du serveur.ii. Dans la boîte de dialogue Ajouter une nouvelle image logicielle, entrez l'URL du serveur HTTP ou FTP vers lequel vous avez téléchargé l'image du logiciel ONTAP à partir du site de support NetApp. Pour le FTP anonyme, vous devez spécifier l'URL dans le ftp://anonymous@ftpserver format.iii. Cliquez sur Ajouter.
Sélectionnez une image disponible	Choisissez l'une des images répertoriées.

e. Cliquez sur **Valider** pour exécuter les vérifications de validation de pré-mise à niveau.

Si des erreurs ou des avertissements sont détectés pendant la validation, ils s'affichent avec une liste d'actions correctives. Vous devez résoudre toutes les erreurs avant de poursuivre la mise à niveau. Il est recommandé de résoudre également les avertissements.

CLI

1. Charger l'image logicielle ONTAP cible dans le référentiel de packages de clusters :

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url  
http://www.example.com/software/9.13.1/image.tgz
```

```
Package download completed.  
Package processing completed.
```

2. Vérifiez que le pack logiciel est disponible dans le référentiel du package de cluster :

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository  
Package Version  Package Build Time  
-----  
9.13.1           MM/DD/YYYY 10:32:15
```

3. Exécuter les vérifications automatiques préalables à la mise à niveau :

```
cluster image validate -version <package_version_number> -show  
-validation-details true
```



Si vous exécutez un "[mise à niveau directe à plusieurs sauts](#)", utiliser le paquet ONTAP cible pour la vérification. Il n'est pas nécessaire de valider séparément l'image de mise à niveau intermédiaire. Par exemple, si vous effectuez une mise à niveau de 9.8 vers 9.13.1, vous devez utiliser le package 9.13.1 pour la vérification. Vous n'avez pas besoin de valider le package 9.12.1 séparément.

```
cluster1::> cluster image validate -version 9.14.1 -show-validation  
-details true
```

It can take several minutes to complete validation...
Validation checks started successfully. Run the "cluster image
show-update-progress" command to check validation status.

4. Vérifier l'état de validation :

```
cluster image show-update-progress
```



Si **Status** est "en cours", attendez et exécutez à nouveau la commande jusqu'à ce qu'elle soit terminée.

```
cluster1::*> cluster image show-update-progress
```

Update Phase	Status	Duration
Pre-update checks	completed	00:10:00

Details:

Pre-update Check	Status	Error-Action
AMPQ Router and Broker Config Cleanup	OK	N/A
Aggregate online status and parity check	OK	N/A
Aggregate plex resync status check	OK	N/A
Application Provisioning Cleanup	OK	N/A
Autoboot Bootargs Status	OK	N/A
Backend	OK	N/A
...		
Volume Conversion In Progress Check	OK	N/A
Volume move progress status check	OK	N/A
Volume online status check	OK	N/A
iSCSI target portal groups status check	OK	N/A
Overall Status	Warning	Warning

75 entries were displayed.

Une liste de pré-contrôles de mise à niveau automatisés complets s'affiche, ainsi que les erreurs ou avertissements qui doivent être résolus avant de commencer le processus de mise à niveau.

Exemple complet de résultats des pré-contrôles de mise à niveau

```
cluster1::*> cluster image validate -version 9.14.1 -show-validation
-details true
```

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks that must be performed after these automated validation checks have completed successfully.

Refer to the Upgrade Advisor Plan or the "What should I verify before I upgrade with or without Upgrade Advisor" section in the "Upgrade ONTAP" documentation for the remaining manual validation checks that need to be performed before update.

Upgrade ONTAP documentation available at: <https://docs.netapp.com/us-en/ontap/upgrade/index.html>

The list of checks are available at: https://docs.netapp.com/us-en/ontap/upgrade/task_what_to_check_before_upgrade.html

Failing to do so can result in an update failure or an I/O disruption. Please use Interoperability Matrix Tool (IMT <http://mysupport.netapp.com/matrix>) to verify host system supportability configuration information.

Validation checks started successfully. Run the "cluster image show-update-progress" command to check validation status.

```
fas2820-2n-wic-1::*> cluster image show-update-progress
```

Update Phase	Status	Estimated Duration	Elapsed Duration
Pre-update checks	in-progress	00:10:00	00:00:42

Details:

Pre-update Check	Status	Error-Action
-----	-----	-----
-----	-----	-----

```
fas2820-2n-wic-1::*> cluster image show-update-progress
```

Update Phase	Status	Estimated Duration	Elapsed Duration
Pre-update checks	completed	00:10:00	00:01:03

Details:

Pre-update Check	Status	Error-Action
-----	-----	-----
AMPQ Router and Broker Config Cleanup	OK	N/A
Aggregate online status and parity check	OK	N/A
Aggregate plex resync status check	OK	N/A
Application Provisioning Cleanup	OK	N/A
Autoboot Bootargs Status	OK	N/A
Backend Configuration Status	OK	N/A
Boot Menu Status	Warning	Warning: bootarg.init.bootmenu is enabled on nodes: fas2820-wic- 1a, fas2820-wic-1b. The boot process of the nodes will be delayed. Action: Set the bootarg.init.bootmenu bootarg to false before proceeding with the upgrade.
Broadcast Domain availability and uniqueness for HA pair status	OK	N/A
CIFS compatibility status check	OK	N/A
CLAM quorum online status check	OK	N/A
CPU Utilization Status	OK	N/A
Capacity licenses install status check	OK	N/A
Check For SP/BMC Connectivity To Nodes	OK	N/A

Check LDAP fastbind users using unsecure connection.	OK	N/A
Check for unsecure kex algorithm configurations.	OK	N/A
Check for unsecure mac configurations.	OK	N/A
Cloud keymanager connectivity check	OK	N/A
Cluster health and eligibility status	OK	N/A
Cluster quorum status check	OK	N/A
Cluster/management switch check	OK	N/A
Compatible New Image Check	OK	N/A
Current system version check if it is susceptible to possible outage during NDU	OK	N/A
Data ONTAP Version and Previous Upgrade Status	OK	N/A
Data aggregates HA policy check	OK	N/A
Disk status check for failed, broken or non-compatibility	OK	N/A
Duplicate Initiator Check	OK	N/A
Encryption key migration status check	OK	N/A
External key-manager with legacy KMIP client check	OK	N/A
External keymanager key server status check	OK	N/A
Fabricpool Object Store Availability	OK	N/A
High Availability	OK	N/A

configuration		
status check		
Infinite Volume	OK	N/A
availability check		
LIF failover	OK	N/A
capability status		
check		
LIF health check	OK	N/A
LIF load balancing	OK	N/A
status check		
LIFs is on home	OK	N/A
node status		
Logically over	OK	N/A
allocated DP		
volumes check		
MetroCluster	OK	N/A
configuration		
status check for		
compatibility		
Minimum number of	OK	N/A
aggregate disks		
check		
NAE Aggregate and	OK	N/A
NVE Volume		
Encryption Check		
NDMP sessions check	OK	N/A
NFS mounts status	Warning	Warning: This cluster is serving
NFS		
check		clients. If NFS soft mounts are
used,		there is a possibility of
frequent		NFS timeouts and race conditions
that		can lead to data corruption
during		the upgrade.
		Action: Use NFS hard mounts, if
		possible. To list Vservers
running		NFS, run the following command:
		vserver nfs show
Name Service	OK	N/A
Configuration DNS		
Check		
Name Service	OK	N/A

Configuration LDAP

Check

Node to SP/BMC	OK	N/A
----------------	----	-----

connectivity check

OKM/KMIP enabled	OK	N/A
------------------	----	-----

systems - Missing

keys check

ONTAP API to REST been transition warning data	Warning	Warning: NetApp ONTAP API has used on this cluster for ONTAP storage management within the
---	---------	--

last 30

approaching

automation

REST

days. NetApp ONTAP API is

end of availability.

Action: Transition your

tools from ONTAP API to ONTAP

API. For more details, refer to
CPC-00410 - End of availability:
ONTAPI

<https://mysupport.netapp.com/info/>

[communications/ECMLP2880232.html](https://mysupport.netapp.com/info/communications/ECMLP2880232.html)

ONTAP Image	OK	N/A
-------------	----	-----

Capability Status

OpenSSL 3.0.x	OK	N/A
---------------	----	-----

upgrade validation

check

Openssh 7.2 upgrade	OK	N/A
---------------------	----	-----

validation check

Platform Health	OK	N/A
-----------------	----	-----

Monitor check

Pre-Update	OK	N/A
------------	----	-----

Configuration

Verification

RDB Replica Health	OK	N/A
--------------------	----	-----

Check

Replicated database	OK	N/A
---------------------	----	-----

schema consistency

check

Running Jobs Status	OK	N/A
---------------------	----	-----

SAN LIF association	OK	N/A
---------------------	----	-----

status check

SAN compatibility for manual configurability check	OK	N/A
SAN kernel agent status check	OK	N/A
Secure Purge operation Check	OK	N/A
Shelves and Sensors check	OK	N/A
SnapLock Version Check	OK	N/A
SnapMirror Synchronous relationship status check	OK	N/A
SnapMirror compatibility status check	OK	N/A
Supported platform check	OK	N/A
Target ONTAP release support for FiberBridge 6500N check	OK	N/A
Upgrade Version Compatibility Status	OK	N/A
Verify all bgp peer-groups are in the up state	OK	N/A
Verify if a cluster management LIF exists	OK	N/A
Verify that e0M is home to no LIFs with high speed services.	OK	N/A
Volume Conversion In Progress Check	OK	N/A
Volume move progress status check	OK	N/A
Volume online status check	OK	N/A
iSCSI target portal groups status check	OK	N/A

Overall Status Warning Warning
75 entries were displayed.

Préparez la mise à niveau de ONTAP

Déterminez le temps nécessaire à une mise à niveau ONTAP

Prévoyez au moins 30 minutes pour effectuer les étapes préparatoires à une mise à niveau ONTAP, 60 minutes pour mettre à niveau chaque paire HA et au moins 30 minutes pour effectuer les étapes post-mise à niveau.



Si vous utilisez NetApp Encryption avec un serveur de gestion externe des clés et un protocole KMIP (Key Management Interoperability Protocol), attendez-vous que la mise à niveau de chaque paire haute disponibilité soit plus d'une heure.

Ces instructions relatives à la durée des mises à niveau sont basées sur des configurations et des charges de travail standard. Ces instructions vous aideront à estimer le temps nécessaire pour effectuer une mise à niveau sans interruption dans votre environnement. La durée réelle du processus de mise à niveau dépend de votre environnement et du nombre de nœuds.

Planifier votre mise à niveau avec Upgrade Advisor

Si vous avez un actif ["Services SupportEdge"](#) contrat pour ["Conseiller digital Active IQ"](#), il est recommandé d'utiliser Upgrade Advisor pour générer un plan de mise à niveau.

Le service Upgrade Advisor de Active IQ Digital Advisor vous aide à planifier votre mise à niveau et réduit les incertitudes et les risques.

Active IQ identifie les problèmes qui peuvent être résolus dans votre environnement en passant à une version plus récente de ONTAP. Ce service vous aide à planifier une mise à niveau réussie et génère un rapport sur les problèmes vers la version ONTAP vers laquelle vous effectuez la mise à niveau.



Upgrade Advisor nécessite un pack AutoSupport complet pour créer le rapport.

Si vous ne disposez pas d'un contrat support Edge Services actif pour Active IQ Digital Advisor, vous devez ["Préparez votre mise à niveau sans Upgrade Advisor"](#).

Étapes

1. ["Lancez Active IQ"](#)
2. Dans Active IQ ["affichez les risques associés à votre cluster et prenez manuellement des actions correctives"](#).

Les risques inclus dans les catégories **SW Config change**, **HW Config change** et **HW Replacement** doivent être résolus avant d'effectuer une mise à niveau ONTAP.

3. Vérifiez le chemin de mise à niveau recommandé et ["générez votre plan de mise à niveau"](#).

Et la suite

- Vous devez consulter le ["Notes de version de ONTAP"](#) Pour la version ONTAP cible recommandée pour

votre cluster par Upgrade Advisor, vous devez suivre le plan généré par Upgrade Advisor pour la mise à niveau du cluster.

- Vous devriez "[Redémarrez le processeur de service ou le contrôleur BMC](#)" avant le début de la mise à niveau.

Informations associées

- "[Comment télécharger manuellement des messages AutoSupport sur NetApp](#)"

Préparez la mise à niveau sans Upgrade Advisor

Préparez-vous à une mise à niveau du logiciel ONTAP sans Upgrade Advisor

En préparant correctement la mise à niveau du logiciel ONTAP, vous pourrez identifier et limiter les obstacles ou les risques de mise à niveau avant de commencer le processus. Lors de la préparation de la mise à niveau, vous pouvez également identifier les considérations particulières que vous devrez peut-être prendre en compte avant de procéder à la mise à niveau. Par exemple, si le mode SSL FIPS est activé sur votre cluster et que les comptes d'administrateur utilisent des clés publiques SSH pour l'authentification, vous devez vérifier que l'algorithme de clé hôte est pris en charge dans votre version ONTAP cible.

Si vous avez un contrat SupportEdge actif pour "[Conseiller digital Active IQ](#)", "[Planifiez votre mise à niveau avec Upgrade Advisor](#)". Si vous n'avez pas accès à Active IQ Digital Advisor, procédez comme suit pour préparer une mise à niveau ONTAP.

1. "[Choisissez votre version ONTAP cible](#)".
2. Vérifiez le "[Notes de version de ONTAP](#)" pour la version cible.

La section « mises en garde de mise à niveau » décrit les problèmes potentiels auxquels vous devez être conscient avant de passer à la nouvelle version. Les sections « Nouveautés » et « problèmes et limitations connus » décrivent le nouveau comportement du système après la mise à niveau vers la nouvelle version.

3. "[Confirmez le support ONTAP pour votre configuration matérielle](#)".

La plateforme matérielle, les commutateurs de gestion de cluster et les commutateurs MetroCluster IP doivent prendre en charge la version cible. Si votre cluster est configuré pour SAN, la configuration SAN doit être entièrement prise en charge.

4. "[Utilisez Active IQ Config Advisor pour vérifier que vous n'avez pas d'erreurs de configuration courantes](#)".
5. Consultez le ONTAP pris en charge "[chemins de mise à niveau](#)" pour déterminer si vous pouvez effectuer une mise à niveau directe ou si vous devez effectuer la mise à niveau par étapes.
6. "[Vérifier la configuration du basculement de LIF](#)".

Avant d'effectuer une mise à niveau, vous devez vérifier que les stratégies de basculement et les groupes de basculement du cluster sont correctement configurés.

7. "[Vérifier la configuration de routage du SVM](#)".
8. "[Vérifier les considérations spéciales](#)" de votre cluster.

Si certaines configurations existent sur le cluster, certaines actions spécifiques doivent être effectuées avant de procéder à une mise à niveau du logiciel ONTAP.

9. "Redémarrez le processeur de service ou le contrôleur BMC".

Choisissez votre version ONTAP cible pour une mise à niveau

Lorsque vous utilisez Upgrade Advisor pour générer un plan de mise à niveau pour votre cluster, le plan inclut une version ONTAP cible recommandée pour la mise à niveau. La recommandation fournie par Upgrade Advisor est basée sur votre configuration actuelle et votre version actuelle de ONTAP.

Si vous n'utilisez pas l'outil Upgrade Advisor pour planifier votre mise à niveau, vous devez choisir la version ONTAP cible pour la mise à niveau en fonction des recommandations de NetApp ou la version minimale requise pour répondre à vos besoins en termes de performances.

- Mise à niveau vers la dernière version disponible (recommandé)

NetApp vous recommande de mettre à niveau votre logiciel ONTAP vers la dernière version de correctif de la dernière version numérotée de ONTAP. Si cela n'est pas possible parce que la dernière version numérotée n'est pas prise en charge par les systèmes de stockage de votre cluster, vous devez effectuer une mise à niveau vers la dernière version numérotée prise en charge.

- Version minimale recommandée

Si vous souhaitez limiter votre mise à niveau à la version minimale recommandée pour votre cluster, reportez-vous à la section "[Versions minimales recommandées de ONTAP](#)". Pour déterminer la version de ONTAP, vous devez effectuer la mise à niveau vers.

Confirmez le support ONTAP pour votre configuration matérielle

Avant de mettre à niveau ONTAP, vérifiez que votre configuration matérielle peut prendre en charge la version cible de ONTAP.

Toutes les configurations

Utiliser "[NetApp Hardware Universe](#)". Pour vérifier que votre plateforme matérielle et vos commutateurs de cluster et de gestion sont pris en charge dans la version cible de ONTAP. Les commutateurs de cluster et de gestion incluent les commutateurs de réseau de cluster (NX-OS), les commutateurs de réseau de gestion (IOS) et le fichier de configuration de référence (RCF). Si votre cluster et vos switches de gestion sont pris en charge, mais n'exécutent pas les versions logicielles minimales requises pour la version cible de ONTAP, mettez à niveau vos switches vers les versions logicielles prises en charge.

- "[Téléchargements NetApp : commutateurs de cluster Broadcom](#)"
- "[Téléchargements NetApp : commutateurs Ethernet Cisco](#)"
- "[Téléchargements NetApp : commutateurs de cluster NetApp](#)"



Si vous avez besoin de mettre à niveau vos commutateurs, NetApp vous recommande d'effectuer d'abord la mise à niveau du logiciel ONTAP, puis d'effectuer la mise à niveau logicielle de vos commutateurs.

Configurations MetroCluster

Avant de mettre à niveau ONTAP, si vous disposez d'une configuration MetroCluster, utilisez "[Matrice d'interopérabilité NetApp](#)". Pour vérifier que vos commutateurs IP MetroCluster sont pris en charge dans la

version cible de ONTAP.

Configurations SAN

Avant de mettre à niveau ONTAP, si votre cluster est configuré pour SAN, utilisez "[Matrice d'interopérabilité NetApp](#)". Pour vérifier que la configuration SAN est entièrement prise en charge.

Tous les composants SAN, y compris la version du logiciel ONTAP cible, le système d'exploitation hôte et les correctifs, les logiciels d'utilitaires hôtes requis, les logiciels de chemins d'accès multiples, les pilotes d'adaptateur et les firmwares, doivent être pris en charge.

Identifier les erreurs de configuration avec Active IQ Config Advisor

Avant de mettre à niveau ONTAP, vous pouvez utiliser l'outil Active IQ Config Advisor pour vérifier les erreurs de configuration courantes.

Active IQ Config Advisor est un outil de validation de la configuration des systèmes NetApp. Il peut être déployé à la fois sur des sites sécurisés et non sécurisés à des fins de collecte de données et d'analyse du système.



Le support pour Active IQ Config Advisor est limité et n'est disponible qu'en ligne.

Étapes

1. Connectez-vous au "[Site de support NetApp](#)", Puis cliquez sur **TOOLS > Tools**.
2. Sous **Active IQ Config Advisor**, cliquez sur "[Télécharger l'application](#)".
3. Téléchargez, installez et exécutez Active IQ Config Advisor.
4. Après avoir exécuté Active IQ Config Advisor, vérifiez les résultats de l'outil et suivez les recommandations fournies pour résoudre les problèmes détectés par l'outil.

Chemins de mise à niveau ONTAP pris en charge

La version de ONTAP vers laquelle vous pouvez effectuer la mise à niveau dépend de votre plateforme matérielle et de la version de ONTAP actuellement exécutée sur les nœuds de votre cluster.

Pour vérifier que votre plate-forme matérielle est prise en charge pour la version de mise à niveau cible, reportez-vous à la section "[NetApp Hardware Universe](#)". Utilisez le "[Matrice d'interopérabilité NetApp](#)" à "[confirmez la prise en charge de votre configuration](#)".

Pour déterminer la version actuelle de ONTAP :

- Dans System Manager, cliquez sur **Cluster > Overview**.
- Dans l'interface de ligne de commande, utilisez le `cluster image show` commande.
Vous pouvez également utiliser le `system node image show` au niveau de privilège avancé pour afficher les détails.

Types de chemins de mise à niveau

Les mises à niveau automatisées sans interruption sont recommandées lorsque cela est possible. En fonction de vos versions actuelles et cibles, votre chemin de mise à niveau sera **direct**, **multi-hop** direct ou **multi-étape**.

- **Direct**

Vous pouvez toujours effectuer une mise à niveau directe vers la prochaine version de la gamme ONTAP à l'aide d'une seule image logicielle. Pour de nombreuses versions, vous pouvez également installer une image logicielle qui vous permet de mettre à niveau directement vers des versions jusqu'à quatre versions ultérieures à la version en cours d'exécution.

Par exemple, vous pouvez utiliser le chemin de mise à niveau directe de 9.11.1 à 9.12.1, ou de 9.11.1 à 9.15.1.

Tous les chemins de mise à niveau *direct* sont pris en charge pour "[clusters à versions mixtes](#)".

- **Multi-saut direct**

Pour certaines mises à niveau automatiques sans interruption (ANDU) vers des versions non adjacentes, vous devez installer l'image logicielle pour une version intermédiaire ainsi que la version cible. Le processus de mise à niveau automatique utilise l'image intermédiaire en arrière-plan pour terminer la mise à jour vers la version cible.

Par exemple, si le cluster exécute 9.3 et que vous souhaitez effectuer la mise à niveau vers 9.7, vous devez charger les packages d'installation ONTAP pour 9.5 et 9.7, puis lancer ANDU sur 9.7. ONTAP met automatiquement à niveau le cluster d'abord vers la version 9.5, puis vers la version 9.7. Vous devez attendre plusieurs opérations de basculement/rétablissement et redémarrages associés au cours du processus.

- **Multi-étape**

Si un chemin de multi-sauts direct ou direct n'est pas disponible pour votre version cible non adjacente, vous devez d'abord mettre à niveau vers une version intermédiaire prise en charge, puis mettre à niveau vers la version cible.

Par exemple, si vous exécutez actuellement 9.6 et que vous voulez passer à 9.11.1, vous devez effectuer une mise à niveau multi-étapes : d'abord de 9.6 à 9.8, puis de 9.8 à 9.11.1. Les mises à niveau à partir des versions antérieures peuvent nécessiter trois étapes ou plus, avec plusieurs mises à niveau intermédiaires.



Avant de commencer les mises à niveau en plusieurs étapes, assurez-vous que votre version cible est prise en charge sur votre plate-forme matérielle.

Avant de commencer une mise à niveau majeure, il est recommandé de commencer par la mise à niveau vers la dernière version de correctif de la version ONTAP exécutée sur votre cluster. Cela vous permettra de vous assurer que tout problème dans votre version actuelle de ONTAP sera résolu avant la mise à niveau.

Par exemple, si votre système exécute ONTAP 9.3P9 et que vous comptez mettre à niveau vers 9.11.1, vous devez d'abord effectuer une mise à niveau vers la dernière version de correctif 9.3, puis suivre le chemin de mise à niveau de 9.3 à 9.11.1.

Découvrez "[Versions minimales ONTAP recommandées sur le site de support NetApp](#)".

Chemins de mise à niveau pris en charge

Les chemins de mise à niveau suivants sont pris en charge dans le cadre des mises à niveau manuelles et automatisées de votre logiciel ONTAP. Ces mises à niveau s'appliquent aux systèmes ONTAP et ONTAP Select sur site. Il y en a différents "[Chemins de mise à niveau pris en charge pour Cloud Volumes ONTAP](#)".



Pour les clusters ONTAP de versions mixtes : tous les chemins de mise à niveau *directe* et *direct multi-hop* incluent des versions ONTAP compatibles avec les clusters de versions mixtes. Les versions ONTAP incluses dans les mises à niveau *multi-étapes* ne sont pas compatibles avec les clusters de versions mixtes. Par exemple, une mise à niveau de 9.8 à 9.12.1 est une mise à niveau *directe*. Un cluster avec des nœuds exécutant 9.8 et 9.12.1 est un cluster à version mixte pris en charge. Une mise à niveau de 9.8 à 9.13.1 est une mise à niveau *multi-étapes*. Un cluster avec des nœuds exécutant 9.8 et 9.13.1 n'est pas un cluster à version mixte pris en charge.

À partir de ONTAP 9.10.1 et versions ultérieures

Les mises à niveau automatisées et manuelles depuis ONTAP 9.10.1 et versions ultérieures suivent les mêmes chemins.

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau automatique ou manuel est...
9.14.1	9.15.1	directe
9.13.1	9.15.1	directe
	9.14.1	directe
9.12.1	9.15.1	directe
	9.14.1	directe
	9.13.1	directe
9.11.1	9.15.1	directe
	9.14.1	directe
	9.13.1	directe
	9.12.1	directe
9.10.1	9.15.1	multi-étages -9.10.1 → 9.14.1 -9.14.1 → 9.15.1
	9.14.1	directe
	9.13.1	directe
	9.12.1	directe
	9.11.1	directe

Depuis ONTAP 9.9.1

Les mises à niveau automatisées et manuelles depuis ONTAP 9.9.1 suivent les mêmes chemins.

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau automatique ou manuel est...
9.9.1	9.15.1	multi-étages -9.9.1 → 9.13.1 -9.13.1 → 9.15.1
	9.14.1	multi-étages -9.9.1 → 9.13.1 -9.13.1 → 9.14.1
	9.13.1	directe
	9.12.1	directe
	9.11.1	directe
	9.10.1	directe

Depuis ONTAP 9.8

Les mises à niveau automatisées et manuelles depuis ONTAP 9.8 suivent les mêmes chemins.



Si vous mettez à niveau l'un des modèles de plate-forme suivants dans une configuration MetroCluster IP de ONTAP 9.8 vers 9.10.1 ou une version ultérieure, vous devez d'abord effectuer une mise à niveau vers ONTAP 9.9 :

- FAS2750
- FAS500f
- AVEC AFF A220
- AFF A250

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau automatique ou manuel est...
9.8	9.15.1	multi-étages -9,8 → 9.12.1 -9.12.1 → 9.15.1
9.14.1	multi-étages -9,8 → 9.12.1 -9.12.1 → 9.14.1	9.13.1
multi-étages -9,8 → 9.12.1 -9.12.1 → 9.13.1	9.12.1	directe
9.11.1	directe	9.10.1
directe	9.9.1	directe

Depuis ONTAP 9.7

Les chemins de mise à niveau d'ONTAP 9.7 peuvent varier selon que vous effectuez une mise à niveau automatique ou manuelle.

Chemins automatisés

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau automatique est...
9.7	9.15.1	multi-étages -9,7 → 9.8 -9,8 → 9.12.1 -9.12.1 → 9.15.1
	9.14.1	multi-étages -9,7 → 9.8 -9,8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1	multi-étages -9,7 → 9.9.1 -9.9.1 → 9.13.1
	9.12.1	multi-étages -9,7 → 9.8 -9,8 → 9.12.1
	9.11.1	multi-sauts directs (nécessite des images pour 9.8 et 9.11.1)
	9.10.1	Multi-saut direct (nécessite des images pour la version P 9.8 et 9.10.1P1 ou ultérieure)
	9.9.1	directe
	9.8	directe

Chemins manuels

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau manuelle est...
9.7	9.15.1	multi-étages -9,7 → 9.8 -9,8 → 9.12.1 -9.12.1 → 9.15.1
	9.14.1	multi-étages -9,7 → 9.8 -9,8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1	multi-étages -9,7 → 9.9.1 -9.9.1 → 9.13.1
	9.12.1	multi-étages - 9.7 → 9.8 - 9.8 → 9.12.1
	9.11.1	multi-étages - 9.7 → 9.8 - 9.8 → 9.11.1
	9.10.1	multi-étages - 9.7 → 9.8 - 9.8 → 9.10.1
	9.9.1	directe
	9.8	directe

Depuis ONTAP 9.6

Les chemins de mise à niveau d'ONTAP 9.6 peuvent varier selon que vous effectuez une mise à niveau automatique ou manuelle.

Chemins automatisés

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau automatique est...
9.6	9.15.1	multi-étages -9,6 → 9.8 -9,8 → 9.12.1 -9.12.1 → 9.15.1
	9.14.1	multi-étages -9,6 → 9.8 -9,8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1	multi-étages -9,6 → 9.8 -9,8 → 9.12.1 -9.12.1 → 9.13.1
	9.12.1	multi-étages - 9.6 → 9.8 -9,8 → 9.12.1
	9.11.1	multi-étages - 9.6 → 9.8 - 9.8 → 9.11.1
	9.10.1	Multi-saut direct (nécessite des images pour la version P 9.8 et 9.10.1P1 ou ultérieure)
	9.9.1	multi-étages - 9.6 → 9.8 - 9.8 → 9.9.1
	9.8	directe
	9.7	directe

Chemins manuels

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau manuelle est...
9.6	9.15.1	multi-étages - 9.6 → 9.8 - 9.8 → 9.12.1 - 9.12.1 → 9.15.1
	9.14.1	multi-étages - 9.6 → 9.8 - 9.8 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multi-étages - 9.6 → 9.8 - 9.8 → 9.12.1 - 9.12.1 → 9.13.1
	9.12.1	multi-étages - 9.6 → 9.8 - 9.8 → 9.12.1
	9.11.1	multi-étages - 9.6 → 9.8 - 9.8 → 9.11.1
	9.10.1	multi-étages - 9.6 → 9.8 - 9.8 → 9.10.1
	9.9.1	multi-étages - 9.6 → 9.8 - 9.8 → 9.9.1
	9.8	directe
	9.7	directe

Depuis ONTAP 9.5

Les chemins de mise à niveau d'ONTAP 9.5 peuvent varier selon que vous effectuez une mise à niveau automatique ou manuelle.

Chemins automatisés

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau automatique est...
9.5	9.15.1	multi-étages - 9.5 → 9.9.1 (multi-saut direct, nécessite des images pour 9.7 et 9.9.1) - 9.9.1 → 9.13.1 - 9.13.1 → 9.15.1
	9.14.1	multi-étages - 9.5 → 9.9.1 (multi-saut direct, nécessite des images pour 9.7 et 9.9.1) - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multi-étages - 9.5 → 9.9.1 (multi-saut direct, nécessite des images pour 9.7 et 9.9.1) - 9.9.1 → 9.13.1
	9.12.1	multi-étages - 9.5 → 9.9.1 (multi-saut direct, nécessite des images pour 9.7 et 9.9.1) - 9.9.1 → 9.12.1
	9.11.1	multi-étages - 9.5 → 9.9.1 (multi-saut direct, nécessite des images pour 9.7 et 9.9.1) - 9.9.1 → 9.11.1
	9.10.1	multi-étages - 9.5 → 9.9.1 (multi-saut direct, nécessite des images pour 9.7 et 9.9.1) - 9.9.1 → 9.10.1
	9.9.1	multi-saut direct (nécessite des images pour 9.7 et 9.9.1)
	9.8	multi-étages - 9.5 → 9.7 - 9.7 → 9.8
	9.7	directe
	9.6	directe

Chemins de mise à niveau manuelle

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau manuelle est...
9.5	9.15.1	multi-étages - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.15.1
	9.14.1	multi-étages - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multi-étages - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.13.1
	9.12.1	multi-étages - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-étages - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-étages - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-étages - 9.5 → 9.7 - 9.7 → 9.9.1
	9.8	multi-étages - 9.5 → 9.7 - 9.7 → 9.8
	9.7	directe
	9.6	directe

De la ONTAP 9.4-9.0

Les chemins de mise à niveau de ONTAP 9.4, 9.3, 9.2, 9.1 et 9.0 peuvent varier selon que vous effectuez une mise à niveau automatique ou manuelle.



Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau automatique est...
9.4		

		9.7 → 9.8 - 9.5 → 9.8 (multi-saut direct, nécessite des images pour 9.7 et 9.8)
Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau automatique est...
	9.7	multi-étages - 9.4 → 9.5 - 9.5 → 9.7
	9.6	multi-étages - 9.4 → 9.5 - 9.5 → 9.6
	9.5	directe

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau automatique est...
9.3		

	9.8	multi-étages - 9.3 → 9.7 (multi-saut direct, nécessite des images pour 9.5 et 9.7) - 9.7 → 9.8
Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau automatique est...
	9.6	multi-étages - 9.3 → 9.5 - 9.5 → 9.6
	9.5	directe
	9.4	non disponible

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau automatique est...
9.2		

	9.9.1	multi-étages - 9.2 → 9.3 - 9.3 → 9.7 (multi-saut direct, nécessite des images pour 9.5 et 9.7) - 9.7 → 9.9.1
Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à jour est automatique
	9.8	multi-étages - 9.2 → 9.3 - 9.3 → 9.7 (multi-saut direct, nécessite des images pour 9.5 et 9.7) - 9.7 → 9.8
	9.7	multi-étages - 9.2 → 9.3 - 9.3 → 9.7 (multi-saut direct, nécessite des images pour 9.5 et 9.7)
	9.6	multi-étages - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-étages - 9.3 → 9.5 - 9.5 → 9.6
	9.4	non disponible
	9.3	directe

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau automatique est...
9.1		

	9.9.1	multi-étages - 9.1 → 9.3 - 9.3 → 9.7 (multi-saut direct, nécessite des images pour 9.5 et 9.7) - 9.7 → 9.9.1
Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à jour est automatique
	9.8	multi-étages - 9.1 → 9.3 - 9.3 → 9.7 (multi-saut direct, nécessite des images pour 9.5 et 9.7) - 9.7 → 9.8
	9.7	multi-étages - 9.1 → 9.3 - 9.3 → 9.7 (multi-saut direct, nécessite des images pour 9.5 et 9.7)
	9.6	multi-étages - 9.1 → 9.3 - 9.3 → 9.6 (multi-saut direct, nécessite des images pour 9.5 et 9.6)
	9.5	multi-étages - 9.1 → 9.3 - 9.3 → 9.5
	9.4	non disponible
	9.3	directe
	9.2	non disponible

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau automatique est...
9.0		

		- 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.7 (multi-saut direct, nécessite des images pour 9.5 et 9.7) Votre chemin de mise à niveau automatique est...
Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	
	9.9.1	multi-étages - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.7 (multi-saut direct, nécessite des images pour 9.5 et 9.7) - 9.7 → 9.9.1
	9.8	multi-étages - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.7 (multi-saut direct, nécessite des images pour 9.5 et 9.7) - 9.7 → 9.8
	9.7	multi-étages - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.7 (multi-saut direct, nécessite des images pour 9.5 et 9.7)
	9.6	multi-étages - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-étages - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5
	9.4	non disponible
	9.3	multi-étages - 9.0 → 9.1 - 9.1 → 9.3
	9.2	non disponible
	9.1	directe

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau ANDU est...
9.4		

		multi-étages - 9.4 → 9.5 - 9.5 → 9.7
Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau ANDU est... - 9.4 → 9.5 - 9.5 → 9.6
	9.5	directe

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau ANDU est...
9.3		

		multi-étages - 9.3 → 9.5 - 9.5 → 9.7
Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau ANDU est... - 9.3 → 9.5 - 9.5 → 9.6
	9.5	directe
	9.4	non disponible

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau ANDU est...
9.2		

	9.8	multi-étages - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.8
Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau ANDU est...
	9.7	multi-étages - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7
	9.6	multi-étages - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-étages - 9.2 → 9.3 - 9.3 → 9.5
	9.4	non disponible
	9.3	directe

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau ANDU est...
9.1		

	9.8	multi-étages - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.8
Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau ANDU est...
	9.7	multi-étages - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7
	9.6	multi-étages - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-étages - 9.1 → 9.3 - 9.3 → 9.5
	9.4	non disponible
	9.3	directe
	9.2	non disponible

Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau ANDU est...
9.0		

	9.9.1	multi-étages - 9.0 → 9.1 - 9.1 → 9.3
Si votre version actuelle de ONTAP est...	Et votre version ONTAP cible est...	Votre chemin de mise à niveau ANDU est...
		- 9.5 → 9.7 - 9.7 → 9.9.1
	9.8	multi-étages - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.8
	9.7	multi-étages - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7
	9.6	multi-étages - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-étages - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5
	9.4	non disponible
	9.3	multi-étages - 9.0 → 9.1 - 9.1 → 9.3
	9.2	non disponible
	9.1	directe

Data ONTAP 8

Assurez-vous que votre plateforme peut exécuter la version ONTAP cible à l'aide du ["NetApp Hardware Universe"](#).

Remarque : le Guide de mise à niveau Data ONTAP 8.3 indique par erreur que dans un cluster à quatre nœuds, vous devez mettre à niveau le nœud qui contient epsilon en dernier. Cette étape n'est plus obligatoire pour les mises à niveau à partir de la version Data ONTAP 8.2.3. Pour plus d'informations, voir ["Bogues en ligne NetApp ID 805277"](#).

À partir de Data ONTAP 8.3.x

Vous pouvez effectuer une mise à niveau directe vers ONTAP 9.1, puis effectuer une mise à niveau vers des versions ultérieures.

À partir Data ONTAP de versions antérieures à 8.3.x, dont 8.2.x

Vous devez d'abord effectuer une mise à niveau vers Data ONTAP 8.3.x, puis effectuer une mise à niveau vers ONTAP 9.1, puis effectuer une mise à niveau vers des versions ultérieures.

Vérifier la configuration du basculement LIF

Avant de mettre à niveau ONTAP, vous devez vérifier que les stratégies de basculement et les groupes de basculement du cluster sont correctement configurés.

Lors du processus de mise à niveau, les LIF sont migrées selon la méthode de mise à niveau. Selon la méthode de mise à niveau, la règle de basculement de LIF peut ou non être utilisée.

Si le cluster contient au moins 8 nœuds, la mise à niveau automatisée est effectuée à l'aide de la méthode par lot. La méthode de mise à niveau par lot consiste à diviser le cluster en plusieurs lots, à mettre à niveau les nœuds du premier lot, à mettre à niveau leurs partenaires haute disponibilité (HA), puis à répéter le processus pour les autres lots. Dans ONTAP 9.7 et version antérieure, si la méthode de traitement par lots est utilisée, les LIF sont migrées vers le partenaire de haute disponibilité du nœud mis à niveau. Dans ONTAP 9.8 et version ultérieure, si la méthode de traitement par lots est utilisée, les LIF sont migrées vers l'autre groupe de batches.

Si votre cluster compte moins de 8 nœuds, la mise à niveau automatisée est effectuée à l'aide de la méthode de déploiement. La méthode de mise à jour par déploiement implique d'initier une opération de basculement sur chaque nœud d'une paire HA, de mettre à jour le nœud ayant basculé, d'initier le rétablissement, puis de répéter le processus pour chaque paire HA dans le cluster. Si la méthode de reprise est utilisée, les LIF sont migrées vers le nœud cible du basculement, tel que défini par la politique de basculement de LIF.

Étapes

1. Afficher la politique de basculement pour chaque LIF de données :

Si votre version ONTAP est...	Utilisez cette commande
9.6 ou ultérieure	<code>network interface show -service-policy *data* -failover</code>
9.5 ou antérieure	<code>network interface show -role data -failover</code>

Cet exemple montre la configuration de basculement par défaut d'un cluster à deux nœuds avec deux LIF de données :

```
cluster1::> network interface show -role data -failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
vs0	lif0	node0:e0b	nextavail	system-
defined		Failover Targets: node0:e0b, node0:e0c, node0:e0d, node0:e0e, node0:e0f, node1:e0b, node1:e0c, node1:e0d, node1:e0e, node1:e0f		
vs1	lif1	node1:e0b	nextavail	system-
defined		Failover Targets: node1:e0b, node1:e0c, node1:e0d, node1:e0e, node1:e0f, node0:e0b, node0:e0c, node0:e0d, node0:e0e, node0:e0f		

Le champ **Failover Targets** affiche une liste hiérarchisée de cibles de basculement pour chaque LIF. Par exemple, si 'lif0' bascule depuis son port d'attache (e0b sur le nœud 0), elle tente d'abord de basculer vers le port e0c sur le nœud 0. Si lif0 ne peut pas basculer vers e0c, il tente ensuite de basculer vers le port e0d du nœud 0, etc.

2. Si la règle de basculement est définie sur **disabled** pour toute LIF autre que les LIFs SAN, utilisez le `network interface modify` commande permettant d'activer le basculement.
3. Pour chaque LIF, vérifiez que le champ **Failover target** inclut des ports de données d'un nœud différent qui resteront actifs pendant la mise à niveau du nœud de rattachement de la LIF.

Vous pouvez utiliser le `network interface failover-groups modify` commande permettant d'ajouter une cible de basculement au groupe de basculement.

Exemple

```
network interface failover-groups modify -vserver vs0 -failover-group
fg1 -targets sti8-vsim-ucs572q:e0d,sti8-vsim-ucs572r:e0d
```

Informations associées

["Gestion du réseau et des LIF"](#)

Vérifier la configuration du routage SVM

Pour éviter toute perturbation, avant de mettre à niveau votre logiciel ONTAP, veillez à ce

que la route par défaut du SVM puisse atteindre toute adresse réseau inaccessible par une route plus spécifique. Il est recommandé de configurer une route par défaut pour un SVM. Pour plus d'informations, voir ["SU134 : l'accès au réseau peut être interrompu par une configuration de routage incorrecte dans ONTAP"](#).

La table de routage d'un SVM détermine le chemin réseau utilisé par la SVM pour communiquer avec une destination. Il est important de comprendre comment fonctionnent les tables de routage afin d'éviter les problèmes de réseau avant qu'ils ne surviennent.

Les règles de routage sont les suivantes :

- ONTAP achemine le trafic sur l'itinéraire le plus spécifique disponible.
- ONTAP achemine le trafic sur une route de passerelle par défaut (ayant 0 bits de masque de réseau) comme dernier recours, lorsque des routes plus spécifiques ne sont pas disponibles.

Dans le cas de routes avec la même destination, le même masque de réseau et la même mesure, il n'est pas garanti que le système utilisera la même route après un redémarrage ou après une mise à niveau. Cela peut être particulièrement problématique si vous avez configuré plusieurs routes par défaut.

Considérations spéciales

Considérations spéciales avant une mise à niveau ONTAP

Certaines configurations de cluster nécessitent que vous entreprenne des actions spécifiques avant de commencer une mise à niveau logicielle de ONTAP. Par exemple, si vous avez une configuration SAN, vous devez vérifier que chaque hôte est configuré avec le nombre correct de chemins directs et indirects avant de commencer la mise à niveau.

Consultez le tableau suivant pour déterminer les étapes supplémentaires à suivre.

Avant de mettre à niveau ONTAP, demandez-vous...	Si votre réponse est oui, alors faites ceci...
Mon cluster est-il actuellement à l'état de version mixte ?	Vérifier la configuration requise pour les versions mixtes
Ai-je une configuration MetroCluster ?	Examinez les exigences de mise à niveau spécifiques pour les configurations MetroCluster
Disposez-vous d'une configuration SAN ?	Vérifiez la configuration de l'hôte SAN
Mon cluster dispose-t-il de relations SnapMirror ?	"Vérifier la compatibilité des versions ONTAP pour les relations SnapMirror"
Ai-je des relations SnapMirror de type DP définies et suis-je en train de passer à ONTAP 9.12.1 ou version ultérieure ?	"Convertir les relations de type DP existantes en relation XDP"
Suis-je en train d'utiliser SnapMirror S3 et puis-je effectuer une mise à niveau vers ONTAP 9.12.1 ou une version ultérieure ?	"Vérifiez les licences pour les configurations SnapMirror S3"

Avant de mettre à niveau ONTAP, demandez-vous...	Si votre réponse est oui, alors faites ceci...
Utilise-t-on une relation SnapMirror et effectue-t-on une mise à niveau de ONTAP 9.9.1 ou version antérieure vers la version 9.10.1 ou ultérieure ?	"Désactivez les snapshots de rétention à long terme dans les volumes centraux des topologies en cascade"
Dois-je utiliser NetApp Storage Encryption avec des serveurs de gestion des clés externes ?	Supprimez toute connexion existante au serveur de gestion des clés
Ai-je chargé des groupes réseau dans les SVM ?	Vérifiez que le fichier de groupe réseau est présent sur chaque nœud
Ai-je des clients LDAP utilisant SSLv3 ?	Configurez les clients LDAP pour qu'ils utilisent TLS
Dois-je utiliser des protocoles orientés session ?	Examiner les considérations relatives aux protocoles orientés session
Le mode SSL FIPS est-il activé sur un cluster où les comptes d'administrateur s'authentifient avec une clé publique SSH ?	Vérifiez la prise en charge de l'algorithme de clé hôte SSH

Clusters ONTAP à version mixte

Un cluster ONTAP à version mixte se compose de nœuds exécutant deux versions principales de ONTAP différentes pendant une durée limitée. Par exemple, si un cluster se compose actuellement de nœuds exécutant ONTAP 9.8 et 9.12.1, il s'agit d'un cluster à version mixte. De même, un cluster dans lequel les nœuds exécutent ONTAP 9.9.1 et 9.13.1 est un cluster à version mixte. NetApp prend en charge les clusters ONTAP à versions mixtes pendant une période limitée et dans des scénarios spécifiques.

Les scénarios suivants sont les plus courants dans lesquels un cluster ONTAP sera dans un état de version mixte :

- Mises à niveau logicielles ONTAP dans les clusters de grande taille
- Des mises à niveau logicielles ONTAP sont nécessaires lorsque vous prévoyez d'ajouter de nouveaux nœuds à un cluster

Ces informations s'appliquent aux versions ONTAP qui prennent en charge les systèmes de plateformes NetApp, tels que les systèmes AFF A-Series et C-Series, ASA, FAS et C-Series. Ces informations ne s'appliquent pas aux versions cloud de ONTAP (9.x.0) telles que 9.12.0.

Conditions requises pour les clusters ONTAP à versions mixtes

Si votre cluster doit avoir un état de version mixte de ONTAP, vous devez connaître les exigences et restrictions importantes.

- Un cluster ne peut pas contenir plus de deux versions principales de ONTAP différentes. Par exemple, ONTAP 9.9.1 et 9.13.1 sont pris en charge, mais pas ONTAP 9.9.1, 9.12.1 et 9.13.1. Les clusters dont les nœuds fonctionnent avec différents niveaux de patch P ou D de la même version ONTAP, tels que ONTAP 9.9.1P1 et 9.9.1P5, ne sont pas considérés comme des clusters ONTAP de version mixte.
- Le cluster étant à l'état de version mixte, vous ne devez pas saisir de commandes pour modifier le fonctionnement ou la configuration du cluster, à l'exception de celles requises pour le processus de mise à niveau ou de migration des données. Par exemple, les activités telles que la migration de LIF, les

opérations planifiées de basculement du stockage ou la création ou suppression d'objets à grande échelle ne doivent pas être effectuées avant la fin de la mise à niveau et de la migration des données.

- Pour un fonctionnement optimal du cluster, la durée pendant laquelle celui-ci se trouve dans un état à version mixte doit être aussi courte que possible. La durée maximale pendant laquelle un cluster peut rester dans un état de version mixte dépend de la version ONTAP la plus faible du cluster.

Si la version la plus basse de ONTAP s'exécutant dans le cluster de version mixte est :	Vous pouvez alors rester dans un état de version mixte pendant un maximum de
ONTAP 9.8 ou supérieur	90 jours
ONTAP 9.7 ou inférieur	7 jours

- À partir de ONTAP 9.8, la différence de version entre les nœuds d'origine et les nouveaux nœuds ne peut pas être supérieure à quatre. Par exemple, un cluster ONTAP à version mixte peut avoir des nœuds exécutant ONTAP 9.8 et 9.12.1, ou des nœuds exécutant ONTAP 9.9.1 et 9.13.1. Cependant, un cluster ONTAP à versions mixtes avec des nœuds exécutant ONTAP 9.8 et 9.13.1 ne serait pas pris en charge.

Pour obtenir la liste complète des clusters à versions mixtes pris en charge, reportez-vous à la section ["chemins de mise à niveau pris en charge"](#). Tous les chemins de mise à niveau *direct* sont pris en charge pour les clusters de versions mixtes.

Mise à jour de la version ONTAP d'un grand cluster

Pour la saisie d'un état de cluster à version mixte, vous devez notamment mettre à niveau la version ONTAP d'un cluster à plusieurs nœuds afin de bénéficier des fonctionnalités disponibles dans les versions ultérieures de ONTAP 9. Lorsque vous devez mettre à niveau la version ONTAP d'un cluster de plus grande taille, vous entrez une version mixte de l'état du cluster pendant un certain temps au fur et à mesure de la mise à niveau de chaque nœud du cluster.

Ajout de nouveaux nœuds à un cluster ONTAP

Un autre scénario de saisie d'un état de cluster de version mixte implique l'ajout de nouveaux nœuds à votre cluster. Vous pouvez ajouter de nouveaux nœuds à votre cluster pour augmenter sa capacité, ou vous pouvez ajouter de nouveaux nœuds lors du processus de remplacement complet de vos contrôleurs. Dans les deux cas, vous devez activer la migration de vos données à partir de contrôleurs existants vers les nouveaux nœuds de votre nouveau système.

Si vous prévoyez d'ajouter de nouveaux nœuds au cluster et que ces nœuds nécessitent une version minimale de ONTAP ultérieure à la version actuellement en cours d'exécution, vous devez effectuer toutes les mises à niveau logicielles prises en charge sur les nœuds existants du cluster avant d'ajouter de nouveaux nœuds.

Dans l'idéal, vous devez mettre à niveau tous les nœuds existants vers la version minimale de ONTAP requise par les nœuds que vous prévoyez d'ajouter au cluster. Toutefois, si cela n'est pas possible parce que certains de vos nœuds ne prennent pas en charge la version ultérieure de ONTAP, vous devrez entrer un état de version mixte pendant une durée limitée dans le cadre de votre processus de mise à niveau. Si certains nœuds ne prennent pas en charge la version ONTAP minimale requise par vos nouveaux contrôleurs, effectuez les opérations suivantes :

1. ["Mise à niveau"](#) Jusqu'à la version maximale de ONTAP prise en charge par les nœuds qui ne prennent pas en charge la version minimale de ONTAP requise par vos nouveaux contrôleurs.

Par exemple, si vous disposez d'un système FAS8080 exécutant ONTAP 9.5 et que vous ajoutez une

nouvelle plateforme C-Series exécutant ONTAP 9.12.1, vous devez mettre à niveau votre système FAS8080 vers ONTAP 9.8 (qui correspond à la version ONTAP maximale prise en charge).

2. ["Ajoutez les nouveaux nœuds à votre cluster"](#).
3. ["Migration des données"](#) des nœuds en cours de suppression du cluster vers les nouveaux nœuds ajoutés.
4. ["Supprimez les nœuds non pris en charge du cluster"](#).
5. ["Mise à niveau"](#) la version des nœuds restants de votre cluster est identique à celle des nouveaux nœuds.

Vous pouvez également mettre à niveau l'ensemble du cluster (y compris vos nouveaux nœuds) vers le ["dernière version de correctif recommandée"](#) De la version ONTAP exécutée sur les nouveaux nœuds.

Pour plus d'informations sur la migration des données, voir :

- ["Création d'un agrégat et déplacement des volumes vers les nouveaux nœuds"](#)
- ["Configuration de nouvelles connexions iSCSI pour les déplacements de volumes SAN"](#)
- ["Déplacement de volumes avec chiffrement"](#)

Conditions de mise à niveau de ONTAP pour les configurations MetroCluster

Avant de mettre à niveau le logiciel ONTAP sur une configuration MetroCluster, vos clusters doivent répondre à certaines exigences.

- La même version de ONTAP doit être exécutée sur les deux clusters.

Vous pouvez vérifier la version de ONTAP à l'aide de la commande `version`.

- Si vous effectuez une mise à niveau majeure de ONTAP, la configuration MetroCluster doit être en mode normal.
- Si vous effectuez une mise à niveau de patch ONTAP, la configuration MetroCluster peut être en mode normal ou en mode de basculement.
- Dans toutes les configurations, à l'exception des clusters à deux nœuds, vous pouvez mettre à niveau les deux clusters à la fois sans interruption.

Pour assurer la mise à niveau sans interruption dans des clusters à deux nœuds, les clusters doivent être mis à niveau à un nœud à la fois.

- L'état RAID ne doit pas être resynchronisés dans les deux clusters.

Au cours de la correction MetroCluster, les agrégats mis en miroir sont resynchronisés. Vous pouvez vérifier si la configuration MetroCluster est dans cet état en utilisant le `storage aggregate plex show -in-progress true` commande. Si des agrégats sont synchronisés, vous ne devez pas effectuer de mise à niveau tant que la resynchronisation n'est pas terminée.

- Les opérations de basculement négociées échouent alors que la mise à niveau est en cours.

Pour éviter tout problème de mise à niveau ou de restauration des opérations, évitez tout basculement non planifié lors d'une opération de mise à niveau ou de restauration, sauf si tous les nœuds des deux clusters exécutent la même version d'ONTAP.

Configuration requise pour le fonctionnement normal de MetroCluster

- Les LIFs du SVM source doivent être up et situées sur leurs home nœuds.

Les LIF de données du SVM de destination ne sont pas nécessairement stockées sur leurs nœuds de base.

- Tous les agrégats du site local doivent être en ligne.
- Tous les volumes root et de données possédés par les SVM du cluster local doivent être en ligne.

Configuration requise pour le basculement MetroCluster

- Toutes les LIFs doivent être up et situées sur leur home node.
- Tous les agrégats doivent être en ligne, à l'exception des agrégats root du site de DR.

Les agrégats racine du site de reprise après incident sont hors ligne pendant certaines phases de basculement.

- Tous les volumes doivent être en ligne.

Informations associées

["Vérification de l'état du réseau et du stockage pour les configurations MetroCluster"](#)

Vérifiez la configuration de l'hôte SAN avant de procéder à une mise à niveau de ONTAP

La mise à niveau de ONTAP dans un environnement SAN modifie les chemins directs. Avant de mettre à niveau un cluster SAN, vérifiez que chaque hôte est configuré avec le bon nombre de chemins directs et indirects, et que chaque hôte est connecté aux bonnes LIFs.

Étapes

1. Sur chaque hôte, vérifiez qu'un nombre suffisant de chemins directs et indirects sont configurés et que chaque chemin est actif.

Chaque hôte doit disposer d'un chemin d'accès à chaque nœud du cluster.

2. Vérifiez que chaque hôte est connecté à une LIF sur chaque nœud.

Vous devez enregistrer la liste des initiateurs à comparer après la mise à niveau. Si vous exécutez ONTAP 9.11.1 ou une version ultérieure, utilisez System Manager pour afficher l'état de la connexion, car l'affichage est plus clair que celui de l'interface de ligne de commande.

System Manager

- a. Dans System Manager, cliquez sur **hôtes > groupes initiateurs SAN**.

La page affiche la liste des groupes initiateurs. Si la liste est grande, vous pouvez afficher des pages supplémentaires de la liste en cliquant sur les numéros de page dans le coin inférieur droit de la page.

Les colonnes affichent diverses informations sur les igroups. Depuis 9.11.1, l'état de connexion du groupe initiateur est également affiché. Passez le curseur sur les alertes d'état pour afficher les détails.

CLI

- Lister les initiateurs iSCSI :

```
iscsi initiator show -fields igroup,initiator-name,tpgroup
```

- Lister les initiateurs FC :

```
fcip initiator show -fields igroup,wwpn,lif
```

SnapMirror

Compatibilité des versions ONTAP pour les relations SnapMirror

Les volumes source et destination doivent exécuter des versions ONTAP compatibles avant de créer une relation de protection des données SnapMirror. Avant de mettre à niveau ONTAP, vérifiez que votre version actuelle de ONTAP est compatible avec votre version cible de ONTAP pour les relations SnapMirror.

Relations de réplication unifiée

Pour les relations SnapMirror de type « XDP », utilisant des versions sur site ou Cloud Volumes ONTAP.

Depuis ONTAP 9.9 :



- Les versions ONTAP 9.x.0 sont des versions cloud uniquement et prennent en charge les systèmes Cloud Volumes ONTAP. L'astérisque (*) après la version de la version indique une version en nuage uniquement.
- Les versions ONTAP 9.x.1 sont des versions générales qui prennent en charge à la fois les systèmes sur site et les systèmes Cloud Volumes ONTAP.



L'interopérabilité est bidirectionnelle.

Interopérabilité pour ONTAP version 9.3 et ultérieure

Ver sion ON TA P...	Interopérabilité avec ces versions précédentes de ONTAP...																			
	9.1 5.1	9.1 5.0*	9.1 4.1	9.1 4.0*	9.1 3.1	9.1 3.0*	9.1 2.1	9.1 2.0*	9.1 1.1	9.1 1.0*	9.1 0.1	9.1 0.0*	9.9. 1	9.9. 0*	9.8	9.7	9.6	9.5	9.4	9.3
9.1 5.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non	Non
9.1 5.0*	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non	Non
9.1 4.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non
9.1 4.0*	Oui	Oui	Oui	Oui	Oui	Non	Oui	Non	Oui	Non	Oui	Non	Oui	Non	Non	Non	Non	Non	Non	Non
9.1 3.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non
9.1 3.0*	Oui	Oui	Oui	Non	Oui	Oui	Oui	Non	Oui	Non	Oui	Non	Oui	Non	Oui	Non	Non	Non	Non	Non
9.1 2.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non
9.1 2.0*	Oui	Oui	Oui	Non	Oui	Non	Oui	Oui	Oui	Non	Oui	Non	Oui	Non	Oui	Oui	Non	Non	Non	Non
9.1 1.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
9.1 1.0*	Oui	Oui	Oui	Non	Oui	Non	Oui	Non	Oui	Oui	Oui	Non	Oui	Non	Oui	Oui	Oui	Non	Non	Non
9.1 0.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
9.1 0.0*	Oui	Oui	Oui	Non	Oui	Non	Oui	Non	Oui	Non	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui	Non	Non
9.9. 1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
9.9. 0*	Non	Non	Oui	Non	Oui	Non	Oui	Non	Oui	Non	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
9.8	Non	Non	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui
9.7	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui
9.6	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui
9.5	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
9.4	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui
9.3	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui

Relations synchrones SnapMirror



SnapMirror synchrone n'est pas pris en charge par les instances de cloud ONTAP.

Version ONTAP ...	Interopérabilité avec ces versions précédentes de ONTAP...										
	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.15.1	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non
9.14.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
9.13.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
9.12.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
9.11.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non
9.10.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
9.9.1	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
9.8	Non	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui	Oui	Non
9.7	Non	Non	Oui	Oui	Non	Non	Oui	Oui	Oui	Oui	Oui
9.6	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui	Oui
9.5	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui

Relations de reprise d'activité SVM SnapMirror

Pour les données de reprise d'activité SVM et la protection des SVM :

La reprise d'activité SVM n'est prise en charge qu'entre les clusters exécutant la même version d'ONTAP.

L'indépendance de la version n'est pas prise en charge pour la réplication du SVM.

Pour la reprise d'activité de SVM pour la migration de SVM :

- La réplication est prise en charge dans une direction unique depuis une version antérieure de ONTAP sur la source vers la même version ou une version ultérieure de ONTAP sur la destination.
- La version ONTAP du cluster cible ne doit pas être plus récente que deux versions majeures sur site ou deux versions majeures de cloud plus récentes, comme illustré dans le tableau ci-dessous.
 - La réplication n'est pas prise en charge pour les cas d'usage de protection des données à long terme.

L'astérisque (*) après la version de la version indique une version en nuage uniquement.

Pour déterminer la prise en charge, recherchez la version source dans la colonne de gauche du tableau, puis recherchez la version de destination sur la ligne supérieure (DR/migration pour les versions similaires et migration uniquement pour les versions plus récentes).

Sou rce	Destination																			
	9.3	9.4	9.5	9.6	9.7	9.8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1	9.15.0*	9.15.1

9.3	Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on														
9.4		Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on													
9.5			Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on												
9.6				Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on											
9.7					Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on										
9.8						Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on									

9.9.0*							Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on								
9.9.1							Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on								
9.10.0*								Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on							
9.10.1									Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on						
9.11.0*										Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on					
9.11.1											Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on				

9.1 2.0*												Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on			
9.1 2.1												Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on			
9.1 3.0*												Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on			
9.1 3.1													Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on	Mig rati on		
9.1 4.0*														Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on	Mig rati on		
9.1 4.1															Rep rise sur inci den t/mi grat ion	Mig rati on	Mig rati on		

9.1 5.0*																			Reprise sur inci den t/mi grat ion	Migra tion
9.1 5.1																				Reprise sur inci den t/mi grat ion

Relations de reprise sur incident SnapMirror

Pour les relations SnapMirror de type « DP » et de type de règle « asynchrone-mirror » :



Les miroirs de type DP ne peuvent pas être initialisés depuis ONTAP 9.11.1 et sont complètement obsolètes dans ONTAP 9.12.1. Pour plus d'informations, voir "[Dérecation des relations SnapMirror de protection des données](#)".



Dans le tableau suivant, la colonne de gauche indique la version ONTAP sur le volume source, et la ligne supérieure indique les versions ONTAP que vous pouvez avoir sur le volume de destination.

Source	Destination											
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3	9.2	9.1	9
9.11.1	Oui.	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
9.10.1	Oui.	Oui.	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
9.9.1	Oui.	Oui.	Oui.	Non	Non	Non	Non	Non	Non	Non	Non	Non
9.8	Non	Oui.	Oui.	Oui.	Non	Non	Non	Non	Non	Non	Non	Non
9.7	Non	Non	Oui.	Oui.	Oui.	Non	Non	Non	Non	Non	Non	Non
9.6	Non	Non	Non	Oui.	Oui.	Oui.	Non	Non	Non	Non	Non	Non
9.5	Non	Non	Non	Non	Oui.	Oui.	Oui.	Non	Non	Non	Non	Non
9.4	Non	Non	Non	Non	Non	Oui.	Oui.	Oui.	Non	Non	Non	Non
9.3	Non	Non	Non	Non	Non	Non	Oui.	Oui.	Oui.	Non	Non	Non
9.2	Non	Non	Non	Non	Non	Non	Non	Oui.	Oui.	Oui.	Non	Non
9.1	Non	Non	Non	Non	Non	Non	Non	Non	Oui.	Oui.	Oui.	Non
9	Non	Non	Non	Non	Non	Non	Non	Non	Non	Oui.	Oui.	Oui.



L'interopérabilité n'est pas bidirectionnelle.

Convertir une relation de type DP existante en XDP

Si vous procédez à une mise à niveau vers ONTAP 9.12.1 ou version ultérieure, vous devez convertir les relations de type DP en relation XDP avant la mise à niveau. ONTAP 9.12.1 et versions ultérieures ne prennent pas en charge les relations de type DP. Vous pouvez facilement convertir une relation de type DP existante en XDP pour tirer parti de SnapMirror flexible à la version.

Description de la tâche

- SnapMirror ne convertit pas automatiquement les relations de type DP existantes en relation XDP. Pour convertir la relation, vous devez rompre et supprimer la relation existante, créer une nouvelle relation XDP et resynchroniser la relation. Pour plus d'informations, reportez-vous à la section "[XDP remplace DP par défaut SnapMirror](#)".
- Lors de la planification de votre conversion, notez que la préparation en arrière-plan et la phase d'entreposage des données d'une relation SnapMirror XDP peuvent prendre un certain temps. Il n'est pas rare de voir la relation SnapMirror indiquant l'état « préparation » pour une période prolongée.



Après avoir converti un type de relation SnapMirror de DP en XDP, les paramètres d'espace, tels que la taille automatique et la garantie d'espace ne sont plus répliqués vers la destination.

Étapes

1. Depuis le cluster de destination, s'assurer que la relation SnapMirror est de type DP, que l'état du miroir est SnapMirror, que l'état de la relation est inactif et que la relation fonctionne correctement :

```
snapmirror show -destination-path <SVM:volume>
```

L'exemple suivant montre la sortie du `snapmirror show` commande :


```
cluster_dst:>snapmirror show -destination-path svm_backup:volA_dst
```

```
Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```



Vous pouvez le trouver utile de conserver une copie du `snapmirror show` sortie de la commande pour garder le suivi existant des paramètres de relation.

2. Depuis les volumes source et de destination, assurez-vous que les deux volumes disposent d'une copie Snapshot commune :

```
volume snapshot show -vserver <SVM> -volume <volume>
```

L'exemple suivant montre le `volume snapshot show` sortie pour les volumes source et de destination :

```
cluster_src:> volume snapshot show -vserver svml -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-----
-----
svml volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.
```

```
cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-----
-----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. Pour vous assurer que les mises à jour planifiées ne s'exécutent pas pendant la conversion, mettez au repos la relation de type DP existante :

```
snapmirror quiesce -source-path <SVM:volume> -destination-path  
<SVM:volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["page de manuel"](#).



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

L'exemple suivant arrête la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

4. Casser la relation de type DP existante :

```
snapmirror break -destination-path <SVM:volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["page de manuel"](#).



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

L'exemple suivant rompt la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

5. Si la suppression automatique des copies Snapshot est activée sur le volume de destination, désactivez-la :

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_  
-enabled false
```

L'exemple suivant désactive la suppression automatique de la copie Snapshot sur le volume de destination `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup  
-volume volA_dst -enabled false
```

6. Supprimez la relation DP-type existante :

```
snapmirror delete -destination-path <SVM:volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["page de manuel"](#).



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

L'exemple suivant supprime la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Relâcher la relation de reprise d'activité SVM d'origine sur la source :

```
snapmirror release -destination-path <SVM:volume> -relationship-info  
-only true
```

L'exemple suivant permet de libérer la relation de SVM Disaster Recovery :

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst  
-relationship-info-only true
```

8. Vous pouvez utiliser la sortie que vous avez conservée de l' `snapmirror show` Commande pour créer la nouvelle relation de type XDP :

```
snapmirror create -source-path <SVM:volume> -destination-path  
<SVM:volume> -type XDP -schedule <schedule> -policy <policy>
```

La nouvelle relation doit utiliser le même volume source et destination. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

L'exemple suivant illustre la création d'une relation de reprise d'activité SnapMirror entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup` utilisation de la valeur par défaut `MirrorAllSnapshots` règle :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst  
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Resynchronisation des volumes source et de destination :

```
snapmirror resync -source-path <SVM:volume> -destination-path  
<SVM:volume>
```

Pour améliorer le temps de resynchronisation, vous pouvez utiliser le `-quick-resync` mais vous devez savoir que vous pouvez perdre des économies en matière d'efficacité du stockage. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man : "[Commande SnapMirror resync](#)".



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination. Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.

L'exemple suivant resynchronise la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

10. Si vous avez désactivé la suppression automatique de copies Snapshot, réactivez-la :

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>  
-enabled true
```

Une fois que vous avez terminé

1. Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée.
2. Une fois que le volume de destination SnapMirror XDP commence à mettre à jour les copies Snapshot, comme défini par la règle SnapMirror, utilisez les valeurs de sortie de `snapmirror list-destinations` Commande depuis le cluster source pour afficher la nouvelle relation SnapMirror XDP

Désactivez les snapshots de conservation à long terme avant la mise à niveau de ONTAP

Si vous effectuez une mise à niveau de ONTAP 9.9.1 ou d'une version antérieure vers ONTAP 9.10.1 ou une version ultérieure et que vous disposez d'une relation SnapMirror en cascade configurée sur votre cluster, vous devez désactiver les snapshots LTR (long-Term Retention) des volumes intermédiaires dans la cascade avant de procéder à la mise à niveau. La mise en cascade d'un volume avec les snapshots LTR activés n'est pas prise en charge dans ONTAP 9.10.1 ou version ultérieure. L'utilisation de cette configuration après la mise à niveau peut entraîner des sauvegardes et des instantanés manqués.

Vous devez prendre des mesures dans les scénarios suivants :

- Les snapshots de conservation à long terme (LTR) sont configurés sur le volume « B » dans une cascade SnapMirror « A > B > C » ou sur un autre volume de destination SnapMirror moyen dans votre cascade plus importante.

- Les snapshots LTR sont définis par un planning appliqué à une règle de règle SnapMirror. Cette règle ne réplique pas les snapshots depuis le volume source, mais les crée directement sur le volume de destination.



Pour plus d'informations sur les planifications et les règles SnapMirror, consultez l'article de la base de connaissance ["Comment fonctionne le paramètre « schedule » dans une règle de politique ONTAP 9 SnapMirror ?"](#).

Étapes

1. Supprimer la règle LTR de la règle SnapMirror sur le volume intermédiaire de la cascade :

```
Secondary::> snapmirror policy remove-rule -vserver <> -policy <>  
-snapmirror-label <>
```

2. Ajouter à nouveau la règle pour l'étiquette SnapMirror sans la planification LTR :

```
Secondary::> snapmirror policy add-rule -vserver <> -policy <>  
-snapmirror-label <> -keep <>
```



La suppression des snapshots LTR des règles de règles de SnapMirror permet à SnapMirror d'extraire les snapshots avec le libellé donné du volume source. Vous pouvez également avoir besoin d'ajouter ou de modifier une planification sur la règle de snapshot du volume source pour créer des snapshots correctement étiquetés.

3. Si nécessaire, modifier (ou créer) une planification sur la règle Snapshot du volume source pour permettre la création de snapshots avec une étiquette SnapMirror :

```
Primary::> volume snapshot policy modify-schedule -vserver <> -policy <>  
-schedule <> -snapmirror-label <>
```

```
Primary::> volume snapshot policy add-schedule -vserver <> -policy <>  
-schedule <> -snapmirror-label <> -count <>
```



Les snapshots LTR peuvent toujours être activés sur le volume de destination SnapMirror final dans une configuration en cascade SnapMirror.

Vérifiez les licences pour les configurations SnapMirror S3

Avant de mettre à niveau ONTAP, si vous utilisez SnapMirror S3 et que vous effectuez une mise à niveau vers ONTAP 9.12.1 ou une version ultérieure, vérifiez que vous disposez des licences SnapMirror appropriées.

Après la mise à niveau de ONTAP, les modifications de licence qui se sont produites entre ONTAP 9.11.1 et les

versions antérieures et ONTAP 9.12.1 et ultérieures peuvent entraîner l'échec des relations SnapMirror S3.

ONTAP 9.11.1 et versions antérieures

- Lors de la réplication dans un compartiment de destination hébergé par NetApp (ONTAP S3 ou StorageGRID), SnapMirror S3 vérifie la licence synchrone SnapMirror, incluse dans le bundle de protection des données avant l'introduction de la "ONTAP One" suite logicielle.
- Lors de la réplication dans un compartiment de destination non NetApp, SnapMirror S3 vérifie la licence cloud SnapMirror, incluse dans le bundle de cloud hybride qui était disponible avant le lancement de la "ONTAP One" suite logicielle.

ONTAP 9.12.1 et versions ultérieures

- Lors de la réplication sur un compartiment de destination hébergé par NetApp (ONTAP S3 ou StorageGRID), SnapMirror S3 vérifie la licence SnapMirror S3, incluse dans le bundle de protection des données qui était disponible avant l'introduction de la "ONTAP One" suite logicielle.
- Lors de la réplication dans un compartiment de destination non NetApp, SnapMirror S3 vérifie la licence externe SnapMirror S3, incluse dans le bundle de cloud hybride qui était disponible avant l'introduction de "ONTAP One" la suite logicielle et du "Pack de compatibilité ONTAP One".

Relations SnapMirror S3 existantes

Les relations SnapMirror S3 existantes doivent continuer à fonctionner après une mise à niveau de ONTAP 9.11.1 ou d'une version antérieure vers ONTAP 9.12.1 ou version ultérieure, même si le cluster ne dispose pas de la nouvelle licence.

La création de nouvelles relations SnapMirror S3 échoue si la licence appropriée n'est pas installée sur le cluster.

Supprimez les connexions existantes au serveur de gestion des clés externes avant de mettre ONTAP à niveau

Avant de mettre à niveau ONTAP, si vous exécutez ONTAP 9.2 ou une version antérieure avec NetApp Storage Encryption (NSE) et si vous effectuez une mise à niveau vers ONTAP 9.3 ou une version ultérieure, vous devez utiliser l'interface de ligne de commandes pour supprimer toutes les connexions de serveur KMIP (gestion externe des clés) existantes.

Étapes

1. Vérifiez que les disques NSE sont déverrouillés, ouverts et définis sur l'ID sécurisé de fabrication par défaut 0x0 :

```
storage encryption disk show -disk *
```

2. Saisissez le mode de privilège avancé :

```
set -privilege advanced
```

3. Utilisez l'ID sécurisé 0x0 de fabrication par défaut pour affecter la clé FIPS aux disques auto-cryptés (SED)

:

```
storage encryption disk modify -fips-key-id 0x0 -disk *
```

4. Vérifiez que l'assignation de la clé FIPS à tous les disques est terminée :

```
storage encryption disk show-status
```

5. Vérifiez que le **mode** pour tous les disques est défini sur données

```
storage encryption disk show
```

6. Consultez les serveurs KMIP configurés :

```
security key-manager show
```

7. Supprimez les serveurs KMIP configurés :

```
security key-manager delete -address <kmip_ip_address>
```

8. Supprimez la configuration externe du gestionnaire de clés :

```
security key-manager delete-kmip-config
```



Cette étape ne supprime pas les certificats NSE.

Et la suite

Une fois la mise à niveau terminée, vous devez [Reconfigurer les connexions du serveur KMIP](#).

Vérifiez que le fichier de groupe réseau est présent sur tous les nœuds avant une mise à niveau de ONTAP

Avant de mettre à niveau ONTAP, si vous avez chargé des groupes réseau sur des machines virtuelles de stockage (SVM), vous devez vérifier que le fichier netgroup est présent sur chaque nœud. Un fichier de groupe réseau manquant sur un nœud peut entraîner l'échec d'une mise à niveau.

Étapes

1. Définissez le niveau de privilège sur avancé :


```
set -privilege advanced
```

2. Afficher le statut netgroup pour chaque SVM :

```
vserver services netgroup status
```

3. Vérifier que pour chaque SVM, chaque nœud affiche la même valeur de hachage de fichier netgroup :

```
vserver services name-service netgroup status
```

Si c'est le cas, vous pouvez passer à l'étape suivante et poursuivre la mise à niveau ou la restauration. Sinon, passez à l'étape suivante.

4. Sur un nœud du cluster, chargez manuellement le fichier netgroup :

```
vserver services netgroup load -vserver vserver_name -source uri
```

Cette commande télécharge le fichier netgroup sur tous les nœuds. Si un fichier de groupe réseau existe déjà sur un nœud, il est écrasé.

Informations associées

["Utilisation des groupes réseau"](#)

Configurez les clients LDAP pour qu'ils utilisent TLS pour une sécurité optimale

Avant de mettre à niveau ONTAP, vous devez configurer des clients LDAP à l'aide de SSLv3 pour des communications sécurisées avec des serveurs LDAP afin qu'ils utilisent TLS. SSL ne sera pas disponible après la mise à niveau.

Par défaut, les communications LDAP entre les applications client et serveur ne sont pas chiffrées. Vous devez interdire l'utilisation de SSL et appliquer l'utilisation de TLS.

Étapes

1. Vérifiez que les serveurs LDAP de votre environnement prennent en charge TLS.

Si ce n'est pas le cas, ne pas continuer. Vous devez mettre à niveau vos serveurs LDAP vers une version prenant en charge TLS.

2. Vérifiez les configurations du client LDAP ONTAP pour lesquelles LDAP sur SSL/TLS est activé :

```
vserver services name-service ldap client show
```

S'il n'y en a pas, vous pouvez ignorer les étapes restantes. Cependant, il est recommandé d'envisager d'utiliser LDAP sur TLS pour une meilleure sécurité.

3. Pour chaque configuration de client LDAP, interdire à SSL d'appliquer l'utilisation de TLS :

```
vserver services name-service ldap client modify -vserver <vserver_name>  
-client-config <ldap_client_config_name> -allow-ssl false
```

4. Vérifiez que l'utilisation de SSL n'est plus autorisée pour les clients LDAP :

```
vserver services name-service ldap client show
```

Informations associées

["Gestion NFS"](#)

Considérations relatives aux protocoles orientés session

Les clusters et les protocoles orientés session peuvent avoir des effets néfastes sur les clients et les applications dans certains domaines, tels que le service d'E/S pendant les mises à niveau.

Si vous utilisez des protocoles orientés session, prenez en compte les points suivants :

- PME

Si vous utilisez des partages disponibles en continu (CA) avec SMBv3, vous pouvez utiliser le système automatisé

Méthode de mise à niveau sans interruption (avec System Manager ou l'interface de ligne de commandes), et sans interruption expérimenté par le client.

Si vous accédez à des partages avec SMBv1 ou SMBv2, ou des partages non-CA avec SMBv3, les sessions client sont interrompues lors des opérations de basculement et de redémarrage de mise à niveau. Invitez les utilisateurs à arrêter leurs sessions avant de procéder à la mise à niveau.

Hyper-V et SQL Server sur SMB prennent en charge la continuité de l'activité. Si vous avez configuré une solution Hyper-V ou SQL Server over SMB, les serveurs d'applications et les machines virtuelles ou bases de données qui y sont contenues restent en ligne et garantissent une disponibilité continue lors de la mise à niveau de ONTAP.

- NFSv4.x

Les clients NFSv4.x récupèrent automatiquement des pertes de connexion lors de la mise à niveau en suivant les procédures de restauration NFSv4.x standard. Les applications peuvent rencontrer un retard temporaire des E/S au cours de ce processus.

- NDMP

L'état est perdu et l'utilisateur client doit recommencer l'opération.

- Les sauvegardes et les restaurations

L'état est perdu et l'utilisateur client doit recommencer l'opération.



Ne lancez pas de sauvegarde ou de restauration pendant ou immédiatement avant une mise à niveau. Cela peut entraîner une perte de données.

- Applications (par exemple, Oracle ou Exchange)

Les effets dépendent des applications. Dans le cas des applications basées sur le délai d'expiration, il est possible que vous puissiez modifier le paramètre de délai d'expiration sur une durée supérieure au délai de redémarrage de ONTAP afin de minimiser les effets indésirables.

Vérifiez la prise en charge de l'algorithme de clé hôte SSH avant la mise à niveau de ONTAP

Avant de mettre à niveau ONTAP, si le mode SSL FIPS est activé sur un cluster où les comptes d'administrateur s'authentifient avec une clé publique SSH, vous devez vous assurer que l'algorithme de clé d'hôte est pris en charge sur la version cible de ONTAP.

Le tableau suivant indique les algorithmes de type de clé hôte pris en charge pour les connexions ONTAP SSH. Ces types de clés ne s'appliquent pas à la configuration de l'authentification publique SSH.

Version de ONTAP	Types de clés pris en charge en mode FIPS	Types de clés pris en charge en mode non FIPS
9.11.1 et versions ultérieures	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 et versions antérieures	ecdsa-sha2-nistp256 ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss ssh-rsa



La prise en charge de l'algorithme de clé hôte ssh-ed25519 a été supprimée à partir de ONTAP 9.11.1.

Pour plus d'informations, voir ["Configurez la sécurité réseau à l'aide de FIPS"](#).

Les comptes de clé publique SSH existants sans les algorithmes de clé pris en charge doivent être reconfigurés avec un type de clé pris en charge avant la mise à niveau ou l'authentification de l'administrateur échouera.

["En savoir plus sur l'activation des comptes de clé publique SSH."](#)

Redémarrez le processeur de service ou le contrôleur BMC pour préparer la mise à jour du firmware lors d'une mise à niveau de ONTAP

Vous n'avez pas besoin de mettre à jour manuellement votre micrologiciel avant d'effectuer une mise à niveau ONTAP. Le firmware de votre cluster est inclus dans le pack de mise à niveau ONTAP et copié sur le périphérique de démarrage de chaque

noëud. Le nouveau micrologiciel est ensuite installé dans le cadre du processus de mise à niveau.

Le firmware des composants suivants est mis à jour automatiquement si la version de votre cluster est antérieure au firmware inclus dans le pack de mise à niveau ONTAP :

- BIOS/CHARGEUR
- Processeur de service (SP) ou contrôleur BMC (Baseboard Management Controller)
- Tiroir de stockage
- Disque
- Flash cache

Pour préparer une mise à jour en douceur, redémarrez le SP ou le BMC avant le début de la mise à niveau.

Étape

1. Redémarrez le SP ou le BMC avant la mise à niveau :

```
system service-processor reboot-sp -node <node_name>
```

Redémarrez uniquement un SP ou un BMC à la fois. Attendez que le processeur de stockage ou le contrôleur BMC redémarré se recycle complètement avant de redémarrer le prochain.

Vous pouvez également "[mettre à jour le micrologiciel manuellement](#)" Entre les mises à niveau ONTAP. Si vous avez Active IQ, c'est possible "[Affichez la liste des versions de micrologiciel actuellement incluses dans votre image ONTAP](#)".

Les mises à jour du micrologiciel sont disponibles comme suit :

- "[Micrologiciel système \(BIOS, BMC, SP\)](#)"
- "[Micrologiciel du tiroir](#)"
- "[Firmwares des disques et de Flash cache](#)"

Téléchargez l'image du logiciel ONTAP

Avant de mettre à niveau ONTAP, vous devez d'abord télécharger l'image du logiciel ONTAP cible depuis le site du support NetApp. Selon la version de votre ONTAP, vous pouvez télécharger le logiciel ONTAP sur un serveur HTTPS, HTTP ou FTP de votre réseau, ou dans un dossier local.

Si vous exécutez...	Vous pouvez télécharger l'image à cet emplacement...
ONTAP 9.6 et versions ultérieures	<ul style="list-style-type: none"> • Un serveur HTTPS Le certificat CA du serveur doit être installé sur le système local. • Un dossier local • Un serveur HTTP ou FTP
ONTAP 9.4 et versions ultérieures	<ul style="list-style-type: none"> • Un dossier local • Un serveur HTTP ou FTP
ONTAP 9.0 et versions ultérieures	Un serveur HTTP ou FTP

Description de la tâche

- Si vous effectuez une mise à niveau automatisée sans interruption (ANDU) à l'aide d'un ["chemin de mise à niveau multi-sauts direct"](#), vous devez le faire ["télécharger"](#) Le progiciel pour la version intermédiaire de ONTAP et la version cible de ONTAP requise pour votre mise à niveau. Par exemple, si vous effectuez une mise à niveau de ONTAP 9.8 vers ONTAP 9.13.1, vous devez télécharger les progiciels pour ONTAP 9.12.1 et ONTAP 9.13.1. Voir ["chemins de mise à niveau pris en charge"](#) pour déterminer si votre chemin de mise à niveau nécessite le téléchargement d'un progiciel intermédiaire.
- Si vous mettez à niveau un système avec NetApp Volume Encryption vers ONTAP 9.5 ou une version ultérieure, vous devez télécharger l'image logicielle de ONTAP pour les pays non soumis à des restrictions, notamment NetApp Volume Encryption.

Si vous utilisez l'image logicielle ONTAP pour des pays limités pour mettre à niveau un système avec NetApp Volume Encryption, le système fonctionne de façon incohérente et l'accès aux volumes est perdu.

- Il n'est pas nécessaire de télécharger un pack logiciel distinct pour votre micrologiciel. La mise à jour de firmware de votre cluster est incluse dans le pack de mise à niveau logicielle ONTAP et est copiée sur le périphérique de démarrage de chaque nœud. Le nouveau micrologiciel est ensuite installé dans le cadre du processus de mise à niveau.

Étapes

1. Recherchez le logiciel ONTAP cible dans le ["Téléchargements de logiciels"](#) Domaine du site de support NetApp.

Pour une mise à niveau ONTAP Select, sélectionnez **mise à niveau de nœud ONTAP Select**.

2. Copiez l'image logicielle (par exemple, 97_q_image.tgz) à l'emplacement approprié.

En fonction de votre version ONTAP, l'emplacement sera un répertoire, un serveur HTTP, HTTPS ou FTP à partir duquel l'image sera desservie par le système local, ou un dossier local sur le système de stockage.

Méthodes de mise à niveau de ONTAP

Méthodes de mise à niveau du logiciel ONTAP

Vous pouvez effectuer une mise à niveau automatisée de votre logiciel ONTAP à l'aide de la fonction gestion du système. Vous pouvez également effectuer une mise à niveau

automatique ou manuelle à l'aide de l'interface de ligne de commande ONTAP. La méthode utilisée pour mettre à niveau ONTAP dépend de votre configuration, de votre version actuelle de ONTAP et du nombre de nœuds dans votre cluster. NetApp recommande d'utiliser System Manager pour effectuer des mises à niveau automatisées, sauf si la configuration requiert une approche différente. Par exemple, si vous disposez d'une configuration MetroCluster avec 4 nœuds exécutant ONTAP 9.3 ou version ultérieure, vous devez utiliser System Manager pour effectuer une mise à niveau automatisée (parfois appelée mise à niveau automatisée sans interruption ou ANDU). Si vous avez une configuration MetroCluster avec 8 nœuds exécutant ONTAP 9.2 ou une version antérieure, vous devez utiliser l'interface de ligne de commande pour effectuer une mise à niveau manuelle.



Si vous effectuez une mise à niveau vers ONTAP 9.15.1 ou une version ultérieure via BlueXP, suivez la ["Procédure de mise à niveau dans la documentation BlueXP"](#).

Une mise à niveau peut être exécutée à l'aide du processus de mise à niveau par déploiement ou par lots. Ces deux solutions ne perturbent pas l'activité.

Pour les mises à niveau automatisées, ONTAP installe automatiquement l'image ONTAP cible sur chaque nœud, valide les composants du cluster pour s'assurer qu'il peut être mis à niveau sans interruption, puis exécute une mise à niveau par lot ou par déploiement en arrière-plan en fonction du nombre de nœuds. Dans le cas des mises à niveau manuelles, l'administrateur vérifie que chaque nœud du cluster est prêt pour la mise à niveau, puis effectue la procédure d'exécution d'une mise à niveau par déploiement.

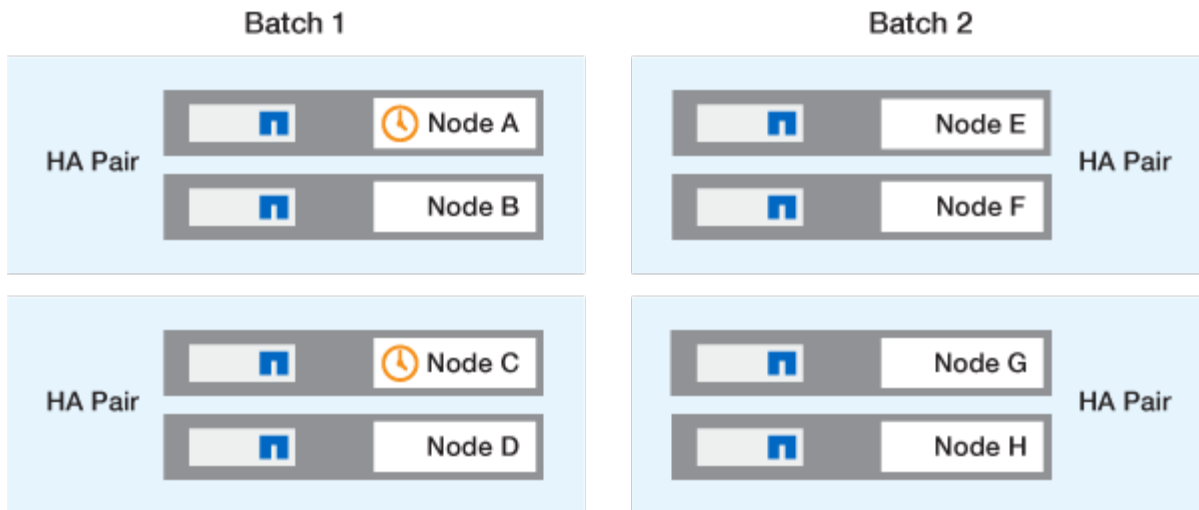
Mises à niveau du déploiement ONTAP

Le processus de mise à niveau par déploiement est le processus par défaut pour les clusters de moins de 8 nœuds. Lors du processus de mise à niveau par déploiement, un nœud est mis hors ligne et mis à niveau alors que son partenaire prend le relais. Une fois la mise à niveau du nœud terminée, le nœud partenaire contrôle à nouveau le nœud propriétaire d'origine et le processus est répété sur le nœud partenaire. Chaque paire haute disponibilité supplémentaire est mise à niveau séquentiellement jusqu'à ce que toutes les paires haute disponibilité exécutent la version cible.

Mises à niveau par lots ONTAP

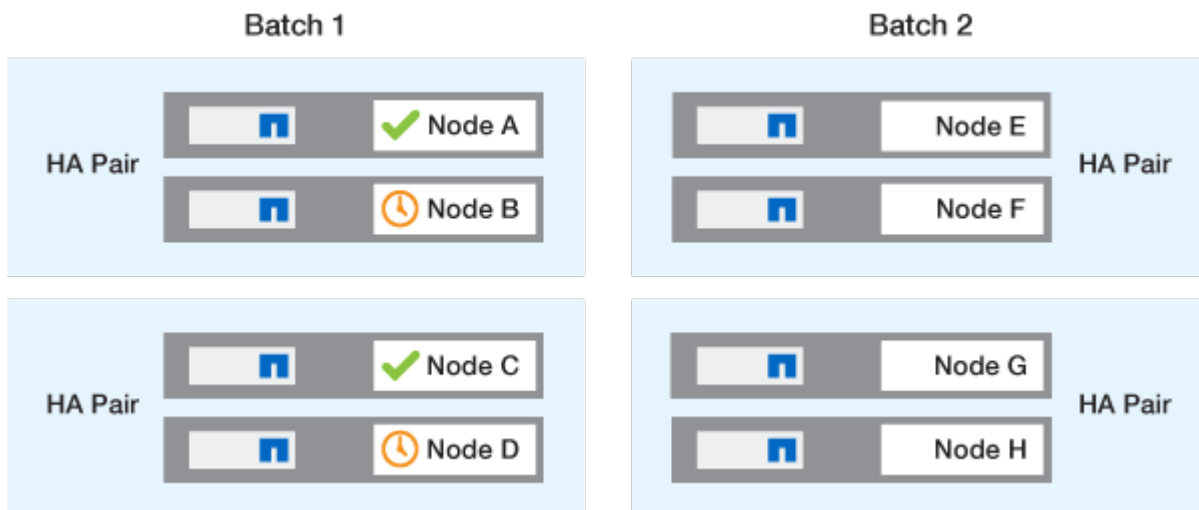
Le processus de mise à niveau par lot est le processus par défaut pour les clusters de 8 nœuds ou plus. Dans le processus de mise à niveau par lots, le cluster est divisé en deux lots. Chaque lot contient plusieurs paires HA. Dans le premier lot, le premier nœud de chaque paire haute disponibilité est mis à niveau simultanément avec le premier nœud de toutes les autres paires haute disponibilité du lot.

L'exemple ci-dessous illustre la présence de deux paires haute disponibilité par lot. Lorsque la mise à niveau par lots commence, les nœuds A et C sont mis à niveau simultanément.



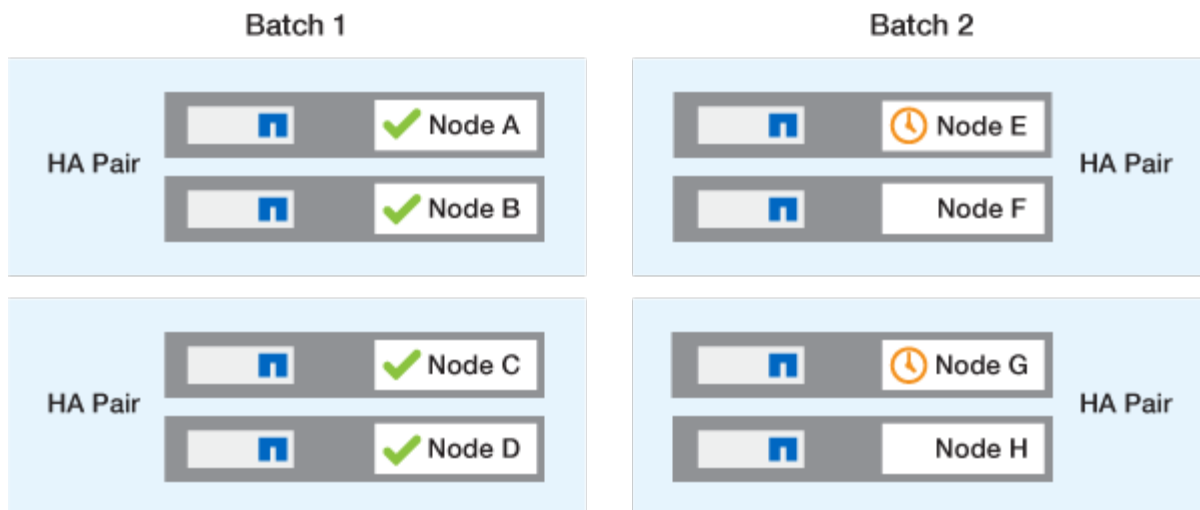
Une fois la mise à niveau des premiers nœuds de chaque paire haute disponibilité terminée, les nœuds partenaires du lot 1 sont mis à niveau simultanément.

Dans l'exemple suivant, une fois les nœuds A et C mis à niveau, les nœuds B et D sont mis à niveau simultanément.



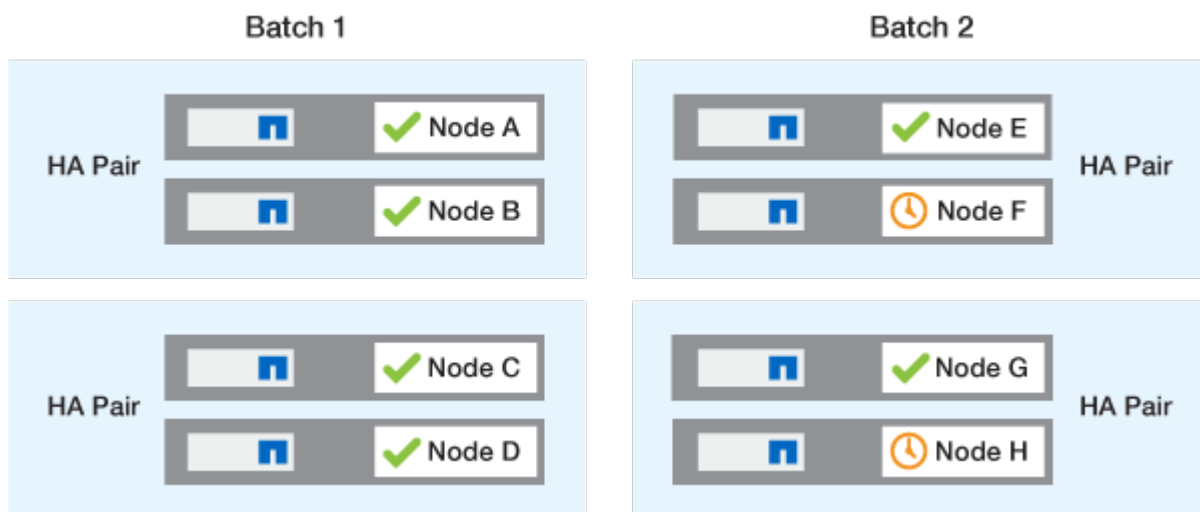
Le processus est ensuite répété pour les nœuds du batch 2. Le premier nœud de chaque paire HA est mis à niveau simultanément avec le premier nœud de toutes les autres paires HA du batch.

Dans l'exemple suivant, les nœuds E et G sont mis à niveau simultanément.



Une fois la mise à niveau des premiers nœuds de chaque paire haute disponibilité terminée, les nœuds partenaires du lot 2 sont mis à niveau simultanément.

Dans l'exemple suivant, les nœuds F et H sont mis à niveau simultanément pour terminer le processus de mise à niveau par lots.



Méthodes de mise à niveau recommandées pour ONTAP en fonction de la configuration

Les méthodes de mise à niveau prises en charge par votre configuration sont répertoriées par ordre d'utilisation recommandée.

Configuration	Version ONTAP	Nombre de nœuds	Méthode de mise à niveau recommandée
Standard	9.0 ou ultérieure	2 ou plus	<ul style="list-style-type: none"> Continuité de l'activité automatisée grâce à System Manager Automatisation de la continuité de l'activité à l'aide de l'interface
Standard	9.0 ou ultérieure	Unique	"Interruption automatisée"

Configuration	Version ONTAP	Nombre de nœuds	Méthode de mise à niveau recommandée
MetroCluster	9.3 ou ultérieure	8	<ul style="list-style-type: none"> Automatisation de la continuité de l'activité à l'aide de l'interface Continuité manuelle de l'activité pour les MetroCluster à 4 ou 8 nœuds via l'interface de ligne de commande
MetroCluster	9.3 ou ultérieure	2,4	<ul style="list-style-type: none"> Continuité de l'activité automatisée grâce à System Manager Automatisation de la continuité de l'activité à l'aide de l'interface
MetroCluster	9.2 ou antérieure	4, 8	Continuité manuelle de l'activité pour les MetroCluster à 4 ou 8 nœuds via l'interface de ligne de commande
MetroCluster	9.2 ou antérieure	2	Continuité manuelle de l'activité pour le MetroCluster à 2 nœuds via l'interface de ligne de commande

ANDU l'utilisation de System Manager est la méthode de mise à niveau recommandée pour toutes les mises à niveau de correctifs, quelle que soit la configuration.



A [mise à niveau manuelle sans interruption](#) peut être effectué sur n'importe quelle configuration. Cependant, vous ne devez pas effectuer une mise à niveau perturbation sauf si vous pouvez mettre le cluster hors ligne pendant la durée de la mise à niveau. Si vous travaillez dans un environnement SAN, vous devez être prêt à arrêter ou à suspendre tous les clients SAN avant d'effectuer une mise à niveau entraînant des perturbations. Les interruptions sont réalisées à l'aide de l'interface de ligne de commandes ONTAP.

Mise à niveau automatisée sans interruption du ONTAP

Lorsque vous effectuez une mise à niveau automatisée, ONTAP installe automatiquement l'image ONTAP cible sur chaque nœud, vérifie que le cluster peut être mis à niveau correctement, puis exécute un ou plusieurs [mise à niveau par lot ou déploiement](#) en arrière-plan basé sur le nombre de nœuds dans le cluster.

Si votre configuration le prend en charge, vous devez utiliser System Manager pour effectuer une mise à niveau automatisée. Si votre configuration ne prend pas en charge la mise à niveau automatisée à l'aide de System Manager, vous pouvez utiliser l'interface de ligne de commandes ONTAP pour effectuer une mise à

niveau automatisée.



Si vous effectuez une mise à niveau vers ONTAP 9.15.1 ou une version ultérieure via BlueXP , suivez la ["Procédure de mise à niveau dans la documentation BlueXP "](#).



Modification du paramètre de l' `storage failover modify-auto-giveback` L'option de commande avant le début d'une mise à niveau automatique sans interruption (ANDU) n'a aucun impact sur le processus de mise à niveau. Le processus ANDU ignore toute valeur prédéfinie à cette option lors du basculement/retour requis pour la mise à jour. Par exemple, paramètre `-autogiveback` À `false` avant de commencer ANDU n'interrompt pas la mise à jour automatique avant le retour.

Avant de commencer

- Vous devriez ["préparez votre mise à niveau"](#).
- Vous devriez ["Téléchargez l'image du logiciel ONTAP"](#) Pour votre version cible de ONTAP.

Si vous exécutez un ["mise à niveau directe à plusieurs sauts"](#), Vous devez télécharger les deux images ONTAP requises pour votre spécifique ["chemin de mise à niveau"](#).

- Pour chaque paire haute disponibilité, chaque nœud doit avoir un ou plusieurs ports sur le même broadcast domain.

Si votre cluster ONTAP comporte 8 nœuds ou plus, la méthode de mise à niveau par lot est utilisée dans la mise à niveau automatique sans interruption pour forcer de manière préventive la migration des LIF de données avant le basculement de SFO. Le mode de migration des LIF lors d'une mise à niveau par lot varie en fonction de votre version d'ONTAP.

Si vous utilisez ONTAP...	Migration des LIF...
<ul style="list-style-type: none">• 9.15.1 ou ultérieure• 9.14.1P5• 9.13.1P10• 9.12.1P13• 9.11.1P16, P17• 9.10.1P19	<p>À un nœud de l'autre groupe de lots.</p> <p>Si la migration vers l'autre groupe de batchs échoue, les LIFs sont migrées vers le partenaire HA du nœud dans le même groupe de batchs.</p>
9.8 à 9.14.1	<p>À un nœud de l'autre groupe de lots.</p> <p>Si le broadcast domain réseau n'autorise pas la migration de LIF vers l'autre groupe de batchs, la migration de LIF échoue et s'interrompt.</p>
9.7 ou antérieure	<p>Vers le partenaire de haute disponibilité du nœud en cours de mise à niveau.</p> <p>Si le partenaire ne dispose d'aucun port dans le même broadcast domain, la migration de LIF échoue et l'ANDU s'interrompt.</p>

- Si vous mettez à niveau ONTAP dans une configuration MetroCluster FC, le cluster doit être activé en vue

du basculement automatique non planifié.

- Si vous ne prévoyez pas de suivre la progression du processus de mise à niveau, vous devriez "[Demandez des notifications EMS d'erreurs susceptibles de nécessiter une intervention manuelle](#)".
- Si vous disposez d'un cluster à un seul nœud, suivez les instructions de la "[mise à niveau automatisée et disruptive](#)" processus.

Les mises à niveau des clusters à un seul nœud entraînent des perturbations.

Exemple 2. Étapes

System Manager

1. Valider l'image cible ONTAP :



Si vous mettez à niveau une configuration MetroCluster, vous devez valider le cluster A, puis répéter le processus de validation sur le cluster B.

a. Selon la version de ONTAP que vous utilisez, effectuez l'une des opérations suivantes :

Si vous exécutez...	Procédez comme ça...
ONTAP 9.8 ou version ultérieure	Cliquez sur Cluster > Présentation .
ONTAP 9.5, 9.6 et 9.7	Cliquez sur Configuration > Cluster > Update .
ONTAP 9.4 ou version antérieure	Cliquez sur Configuration > Cluster Update .

b. Dans le coin droit du volet **vue d'ensemble**, cliquez sur

c. Cliquez sur **mise à jour ONTAP**.

d. Dans l'onglet **mise à jour du cluster**, ajoutez une nouvelle image ou sélectionnez une image disponible.

Les fonctions que vous recherchez...	Alors...
Ajoutez une nouvelle image logicielle à partir d'un dossier local Vous devriez déjà avoir "téléchargez l'image - effectué" au client local.	<ul style="list-style-type: none">i. Sous Images logicielles disponibles, cliquez sur Ajouter à partir de local.ii. Accédez à l'emplacement où vous avez enregistré l'image logicielle, sélectionnez l'image, puis cliquez sur Ouvrir.
Ajoutez une nouvelle image logicielle à partir d'un serveur HTTP ou FTP	<ul style="list-style-type: none">i. Cliquez sur Ajouter à partir du serveur.ii. Dans la boîte de dialogue Ajouter une nouvelle image logicielle, entrez l'URL du serveur HTTP ou FTP vers lequel vous avez téléchargé l'image du logiciel ONTAP à partir du site de support NetApp. Pour le FTP anonyme, vous devez spécifier l'URL dans le ftp://anonymous@ftpserver format.iii. Cliquez sur Ajouter.
Sélectionnez une image disponible	Choisissez l'une des images répertoriées.

e. Cliquez sur **Valider** pour exécuter les vérifications de validation de pré-mise à niveau.

Si des erreurs ou des avertissements sont détectés pendant la validation, ils s'affichent avec une liste d'actions correctives. Vous devez résoudre toutes les erreurs avant de poursuivre la mise à niveau. Il est recommandé de résoudre également les avertissements.

2. Cliquez sur **Suivant**.

3. Cliquez sur **mettre à jour**.

La validation est à nouveau effectuée. Les erreurs ou avertissements restants s'affichent avec une liste d'actions correctives. Les erreurs doivent être corrigées avant de pouvoir procéder à la mise à niveau. Si la validation est terminée avec des avertissements, vous corrigez les avertissements ou choisissez **mettre à jour avec des avertissements**.



Par défaut, ONTAP utilise le "[processus de mise à niveau par lot](#)" pour mettre à niveau les clusters avec huit nœuds ou plus. À partir de ONTAP 9.10.1, si vous le souhaitez, vous pouvez sélectionner **mettre à jour une paire haute disponibilité à la fois** pour remplacer la valeur par défaut et demander à votre cluster de mettre à niveau une paire haute disponibilité à la fois à l'aide du processus de mise à niveau par déploiement.

Pour les configurations MetroCluster de plus de 2 nœuds, le processus de mise à niveau ONTAP démarre simultanément sur les paires haute disponibilité des deux sites. Dans le cas d'une configuration MetroCluster à 2 nœuds, la mise à niveau commence par être démarrée sur le site sur lequel la mise à niveau n'est pas lancée. La mise à niveau sur le site restant commence une fois la première mise à niveau terminée.

4. Si votre mise à niveau s'interrompt en raison d'une erreur, cliquez sur le message d'erreur pour afficher les détails, puis corrigez l'erreur et "[reprenez la mise à niveau](#)".

Une fois que vous avez terminé

Une fois la mise à niveau terminée, le nœud redémarre et vous êtes redirigé vers la page de connexion de System Manager. Si le redémarrage du nœud prend beaucoup de temps, vous devez actualiser votre navigateur.

CLI

1. Validez l'image logicielle cible ONTAP



Si vous mettez à niveau une configuration MetroCluster, vous devez d'abord exécuter les étapes suivantes sur le cluster A, puis exécuter les mêmes étapes sur le cluster B.

a. Supprimez le pack logiciel ONTAP précédent :

```
cluster image package delete -version <previous_ONTAP_Version>
```

b. Charger l'image logicielle ONTAP cible dans le référentiel de packages de clusters :

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.13.1/image.tgz

Package download completed.
Package processing completed.
```

Si vous exécutez un "[mise à niveau directe à plusieurs sauts](#)", Vous devez également charger le progiciel pour la version intermédiaire de ONTAP requise pour votre mise à niveau. Par exemple, si vous effectuez une mise à niveau de 9.8 vers 9.13.1, vous devez charger le progiciel pour ONTAP 9.12.1, puis utiliser la même commande pour charger le progiciel pour 9.13.1.

- c. Vérifiez que le pack logiciel est disponible dans le référentiel du package de cluster :

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
-----
9.13.1           MM/DD/YYYY 10:32:15
```

- d. Exécuter les vérifications automatiques préalables à la mise à niveau :

```
cluster image validate -version <package_version_number>
```

Si vous exécutez un "[mise à niveau directe à plusieurs sauts](#)", Vous n'avez besoin que d'utiliser le paquet ONTAP cible pour la vérification. Il n'est pas nécessaire de valider séparément l'image de mise à niveau intermédiaire. Par exemple, si vous effectuez une mise à niveau de 9.8 vers 9.13.1, utilisez le package 9.13.1 pour la vérification. Vous n'avez pas besoin de valider le package 9.12.1 séparément.

```
cluster1::> cluster image validate -version 9.13.1

WARNING: There are additional manual upgrade validation checks that
must be performed after these automated validation checks have
completed...
```

- a. Surveiller la progression de la validation :

```
cluster image show-update-progress
```

- b. Effectuez toutes les actions requises identifiées par la validation.

c. Si vous mettez à niveau une configuration MetroCluster, répétez les étapes ci-dessus sur le cluster B.

2. Générer une estimation de mise à niveau logicielle :

```
cluster image update -version <package_version_number> -estimate  
-only
```



Si vous mettez à niveau une configuration MetroCluster, vous pouvez exécuter cette commande sur le cluster A ou le cluster B. Vous n'avez pas besoin de l'exécuter sur les deux clusters.

L'estimation de la mise à niveau logicielle affiche des détails sur chaque composant à mettre à jour, ainsi que la durée estimée de la mise à niveau.

3. Effectuez la mise à niveau logicielle :

```
cluster image update -version <package_version_number>
```

- Si vous exécutez un "[mise à niveau directe à plusieurs sauts](#)", Utilisez la version ONTAP cible pour le numéro_version_paquet. Par exemple, si vous effectuez une mise à niveau de ONTAP 9.8 vers 9.13.1, utilisez 9.13.1 comme numéro_version_paquet.
- Par défaut, ONTAP utilise le "[processus de mise à niveau par lot](#)" pour mettre à niveau les clusters avec huit nœuds ou plus. Si vous le souhaitez, vous pouvez utiliser le `-force-rolling` paramètre permettant de remplacer le processus par défaut et de faire mettre votre cluster à niveau un nœud à la fois à l'aide du processus de mise à niveau par déploiement.
- À l'issue de chaque basculement et rétablissement, la mise à niveau attend 8 minutes pour que les applications client puissent restaurer les données après la pause des E/S qui a lieu lors du basculement et du rétablissement. Si votre environnement nécessite plus ou moins de temps pour la stabilisation du client, vous pouvez utiliser le `-stabilize-minutes` paramètre pour spécifier une durée de stabilisation différente.
- Pour les configurations MetroCluster avec 4 nœuds de plus, la mise à niveau automatisée démarre simultanément sur les paires haute disponibilité des deux sites. Dans le cas d'une configuration MetroCluster à 2 nœuds, la mise à niveau commence sur le site où elle n'est pas initiée. La mise à niveau sur le site restant commence une fois la première mise à niveau terminée.

```

cluster1::> cluster image update -version 9.13.1

Starting validation for this update. Please wait..

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks...

Pre-update Check      Status      Error-Action
-----
...
20 entries were displayed

Would you like to proceed with update ? {y|n}: y
Starting update...

cluster-1::>

```

4. Afficher la progression de la mise à jour du cluster :

```
cluster image show-update-progress
```

Si vous mettez à niveau une configuration MetroCluster à 4 ou 8 nœuds, le `cluster image show-update-progress` commande uniquement affiche la progression du nœud sur lequel vous exécutez la commande. Vous devez exécuter la commande sur chaque nœud pour voir la progression de chaque nœud.

5. Vérifiez que la mise à niveau a été effectuée correctement sur chaque nœud.

```
cluster image show-update-progress
```



```
cluster1::> cluster image show-update-progress
```

Elapsed Update Phase Duration	Status	Estimated Duration
-----	-----	-----

Pre-update checks 00:02:07	completed	00:10:00
Data ONTAP updates 01:39:00	completed	01:31:00
Post-update checks 00:02:00	completed	00:10:00

3 entries were displayed.

Updated nodes: node0, node1.

6. Déclencher une notification AutoSupport :

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

Si votre cluster n'est pas configuré pour envoyer des messages AutoSupport, une copie de la notification est enregistrée localement.

7. Si vous mettez à niveau une configuration MetroCluster FC à 2 nœuds, vérifiez que le cluster est activé pour le basculement automatique non planifié.



Si vous mettez à niveau une configuration standard, une configuration IP MetroCluster ou une configuration FC MetroCluster de plus de 2 nœuds, vous n'avez pas besoin d'effectuer cette étape.

a. Vérifier si le basculement automatique non planifié est activé :

```
metrocluster show
```

Si le basculement automatique non planifié est activé, l'instruction suivante apparaît dans la sortie de la commande :

```
AUSO Failure Domain      auso-on-cluster-disaster
```

a. Si l'instruction n'apparaît pas dans la sortie, activez le basculement automatique non planifié :

```
metrocluster modify -auto-switchover-failure-domain auto-on-  
cluster-disaster
```

b. Vérifier que le basculement automatique non planifié a été activé :

```
metrocluster show
```

Reprenez la mise à niveau du logiciel ONTAP après une erreur dans le processus de mise à niveau automatique

Si une mise à niveau automatique du logiciel ONTAP s'interrompt en raison d'une erreur, vous devez résoudre l'erreur et poursuivre la mise à niveau. Une fois l'erreur résolue, vous pouvez choisir de poursuivre le processus de mise à niveau automatique ou de terminer le processus de mise à niveau manuellement. Si vous choisissez de poursuivre la mise à niveau automatique, n'effectuez aucune des étapes de mise à niveau manuellement.

Exemple 3. Étapes

System Manager

1. Selon la version de ONTAP que vous utilisez, effectuez l'une des opérations suivantes :

Si vous exécutez...	Alors...
ONTAP 9.8 ou version ultérieure	Cliquez sur Cluster > Présentation
ONTAP 9.7, 9.6 ou 9.5	Cliquez sur Configuration > Cluster > Update.
ONTAP 9.4 ou version antérieure	<ul style="list-style-type: none">• Cliquez sur Configuration > Cluster Update.• Dans le coin droit du volet vue d'ensemble, cliquez sur les trois points verticaux bleus et sélectionnez mise à jour ONTAP.

2. Poursuivez la mise à niveau automatique ou annulez-la et continuez manuellement.

Les fonctions que vous recherchez...	Alors...
Reprenez la mise à niveau automatisée	Cliquez sur reprendre.
Annulez la mise à niveau automatique et continuez manuellement	Cliquez sur Annuler.

CLI

1. Afficher l'erreur de mise à niveau :

```
cluster image show-update-progress
```

2. Résolez l'erreur.
3. Reprendre la mise à niveau :

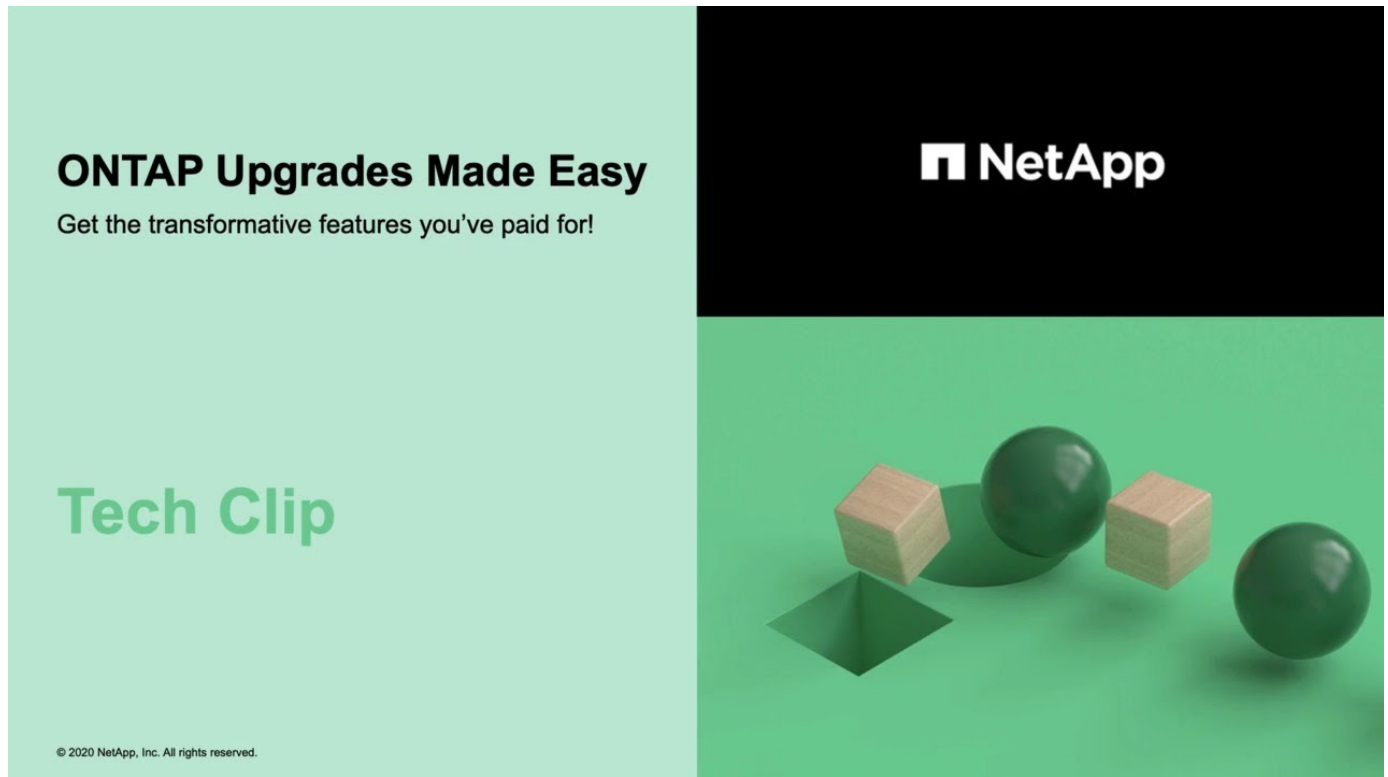
Les fonctions que vous recherchez...	Saisissez la commande suivante...
Reprenez la mise à niveau automatisée	<pre>cluster image resume-update</pre>
Annulez la mise à niveau automatique et continuez manuellement	<pre>cluster image cancel-update</pre>

Une fois que vous avez terminé

"Effectuez des vérifications post-mise à niveau".

Vidéo : des mises à niveau simplifiées

Découvrez les fonctionnalités simplifiées de mise à niveau de ONTAP de System Manager dans ONTAP 9.8.



Informations associées

- ["Lancez Active IQ"](#)
- ["Documentation Active IQ"](#)

Mises à niveau manuelles

Installez le progiciel ONTAP pour les mises à niveau manuelles

Après avoir téléchargé le pack logiciel ONTAP pour une mise à niveau manuelle, vous devez l'installer localement avant de commencer la mise à niveau.

Étapes

1. Définissez le niveau de privilège sur avancé, en entrant **y** lorsque vous êtes invité à continuer : `set -privilege advanced`

L'invite avancée (*>) s'affiche.

2. Installez l'image.

Si vous disposez de la configuration suivante...	Utilisez cette commande...
<ul style="list-style-type: none"> • Non MetroCluster • MetroCluster à 2 nœuds 	<pre>system node image update -node * -package <location> -replace -package true -setdefault true -background true</pre> <p><location> Il peut s'agir d'un serveur Web ou d'un dossier local, selon la version de ONTAP. Consultez la system node image update page man pour plus de détails.</p> <p>Cette commande installe l'image logicielle sur tous les nœuds simultanément. Pour installer l'image sur chaque nœud un par un, ne spécifiez pas le <code>-background</code> paramètre.</p>
<ul style="list-style-type: none"> • MetroCluster à 4 nœuds • Configuration MetroCluster à 8 nœuds 	<pre>system node image update -node * -package <location> -replace -package true -background true -setdefault false</pre> <p>Vous devez exécuter cette commande sur les deux clusters.</p> <p>Cette commande utilise une requête étendue pour modifier l'image du logiciel cible, qui est installée comme image alternative sur chaque nœud.</p>

3. Entrez `y` pour continuer lorsque vous y êtes invité.
4. Vérifiez que l'image logicielle est installée sur chaque nœud.

```
system node image show-update-progress -node *
```

Cette commande affiche l'état actuel de l'installation de l'image logicielle. Vous devez continuer à exécuter cette commande jusqu'à ce que tous les nœuds signalent un **Run Status** de **unch** et un **Exit Status** de **Success**.

La commande de mise à jour de l'image du nœud système peut échouer et afficher des messages d'erreur ou d'avertissement. Après avoir résolu les erreurs ou les avertissements, vous pouvez relancer la commande.

Cet exemple montre un cluster à deux nœuds dans lequel l'image logicielle est installée avec succès sur les deux nœuds :

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

Mise à niveau manuelle des ONTAP sans interruption via l'interface de ligne de commandes (configurations standard)

La mise à niveau automatisée à l'aide de System Manager est la méthode de mise à niveau préférée. Si System Manager ne prend pas en charge votre configuration, vous pouvez effectuer une mise à niveau manuelle sans interruption à l'aide de l'interface de ligne de commandes ONTAP. Pour mettre à niveau un cluster de deux nœuds ou plus à l'aide de la méthode manuelle sans interruption, vous devez lancer une opération de basculement sur chaque nœud d'une paire haute disponibilité, mettre à jour le nœud « en échec », lancer un rétablissement, puis répéter le processus pour chaque paire haute disponibilité du cluster.

Avant de commencer

Vous devez avoir satisfait la mise à niveau ["préparation"](#) conditions requises.

Mise à jour du premier nœud d'une paire HA

Vous pouvez mettre à jour le premier nœud d'une paire haute disponibilité en initiant un basculement par le partenaire du nœud. Le partenaire service des données du nœud pendant la mise à niveau du premier nœud.

Si vous effectuez une mise à niveau majeure, le premier nœud à mettre à niveau doit être le même nœud sur lequel vous avez configuré les LIFs de données pour la connectivité externe et installé la première image ONTAP.

Après la mise à niveau du premier nœud, il est conseillé de mettre à niveau le nœud partenaire aussi rapidement que possible. Ne laissez pas les deux nœuds dans un ["version mixte"](#) indiquer plus longtemps que nécessaire.

Étapes

1. Mettre à jour le premier nœud du cluster en invoquant un message AutoSupport :

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

Cette notification AutoSupport inclut un enregistrement de l'état du système juste avant la mise à jour. Il enregistre des informations de dépannage utiles en cas de problème avec le processus de mise à jour.

Si le cluster n'est pas configuré pour envoyer des messages AutoSupport, une copie de la notification est enregistrée localement.

2. Définissez le niveau de privilège sur avancé, en entrant **y** lorsque vous êtes invité à continuer :

```
set -privilege advanced
```

L'invite avancée (*>) s'affiche.

3. Définissez la nouvelle image du logiciel ONTAP comme image par défaut :

```
system image modify {-node nodenameA -iscurrent false} -isdefault true
```

La commande `system image modify` utilise une requête étendue pour remplacer la nouvelle image logicielle ONTAP (qui est installée comme image alternative) par l'image par défaut du nœud.

4. Surveiller la progression de la mise à jour :

```
system node upgrade-revert show
```

5. Vérifiez que la nouvelle image du logiciel ONTAP est définie comme image par défaut :

```
system image show
```

Dans l'exemple suivant, `image2` est la nouvelle version de ONTAP et est définie en tant qu'image par défaut sur le nœud 0 :

```
cluster1::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date

node0					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME
node1					
	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

6. Désactiver le rétablissement automatique sur le nœud partenaire s'il est activé :

```
storage failover modify -node nodenameB -auto-giveback false
```

Si le cluster est un cluster à deux nœuds, un message s'affiche vous informant que la désactivation du rétablissement automatique empêche la mise en ligne des services du cluster de gestion en cas de défaillance alternée. Entrez *y* pour continuer.

7. Vérifier que le rétablissement automatique est désactivé pour le partenaire du nœud :

```
storage failover show -node nodenameB -fields auto-giveback
```

```
cluster1::> storage failover show -node node1 -fields auto-giveback
```

node	auto-giveback

node1	false

1 entry was displayed.

8. Exécutez la commande suivante deux fois pour déterminer si le nœud à mettre à jour diffuse actuellement des clients

```
system node run -node nodenameA -command uptime
```

La commande UpTime affiche le nombre total d'opérations effectuées par le nœud pour les clients NFS, SMB, FC et iSCSI depuis le dernier démarrage du nœud. Pour chaque protocole, vous devez exécuter la commande deux fois afin de déterminer si le nombre d'opérations augmente. S'ils augmentent, le nœud diffuse actuellement des clients pour ce protocole. Si ce n'est pas le cas, le nœud ne diffuse actuellement pas les clients pour ce protocole.



Vous devez noter chaque protocole dont les opérations client augmentent, de sorte qu'après la mise à jour du nœud, vous pouvez vérifier que le trafic client a repris.

L'exemple suivant montre un nœud avec des opérations NFS, SMB, FC et iSCSI. Toutefois, le nœud dessert actuellement uniquement les clients NFS et iSCSI.

```
cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

9. Migrer tous les LIFs de données loin du nœud :

```
network interface migrate-all -node nodenameA
```

10. Vérifiez toutes les LIFs que vous avez migrées :

```
network interface show
```

Pour plus d'informations sur les paramètres que vous pouvez utiliser pour vérifier l'état des LIF, reportez-vous à la page man de l'interface réseau.

L'exemple suivant montre que les LIF de données du nœud 0 ont migré correctement. Pour chaque LIF, les champs inclus dans cet exemple vous permettent de vérifier le nœud et le port d'accueil de la LIF, le nœud et le port actuels vers lesquels la LIF a migré, ainsi que le statut opérationnel et administratif de la LIF.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node0 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif      home-node home-port curr-node curr-port status-oper
status-admin
-----
-----
vs0      data001 node0      e0a      node1      e0a      up      up
vs0      data002 node0      e0b      node1      e0b      up      up
vs0      data003 node0      e0b      node1      e0b      up      up
vs0      data004 node0      e0a      node1      e0a      up      up
4 entries were displayed.
```

11. Lancement d'un basculement :

```
storage failover takeover -ofnode nodenameA
```

Ne spécifiez pas le paramètre `-option` immédiate, car un basculement normal est nécessaire pour le nœud en cours de basculement pour démarrer sur la nouvelle image logicielle. Si vous n'avez pas migré manuellement les LIF en dehors du nœud, elles migrent automatiquement vers le partenaire de haute disponibilité du nœud afin d'assurer l'absence d'interruption du service.

Le premier nœud démarre jusqu'à l'état d'attente de rétablissement.



Si AutoSupport est activé, un message AutoSupport est envoyé, indiquant que le nœud n'a pas le quorum du cluster. Vous pouvez ignorer cette notification et poursuivre la mise à jour.

12. Vérifiez que le basculement est réussi :

```
storage failover show
```

Des messages d'erreur indiquant des problèmes de non-concordance de version et de format de boîte aux lettres peuvent s'afficher. Ce comportement est attendu, il s'agit d'un état temporaire lors d'une mise à niveau sans interruption majeure et ne présente aucun danger.

L'exemple suivant montre que le basculement a réussi. Le nœud `node0` est en attente de rétablissement et son partenaire est à l'état en attente.

```
cluster1::> storage failover show
```

Node	Partner	Takeover Possible	State Description
node0	node1	-	Waiting for giveback (HA mailboxes)
node1	node0	false	In takeover

2 entries were displayed.

13. Attendre au moins huit minutes pour que les conditions suivantes prennent effet :

- Les chemins d'accès multiples du client (si déployés) sont stabilisés.
- Les clients sont récupérés à partir de la pause lors d'une opération d'E/S qui se produit pendant le basculement.

Le temps de restauration est spécifique au client et peut prendre plus de huit minutes, selon les caractéristiques des applications client.

14. Renvoyer les agrégats vers le premier nœud :

```
storage failover giveback -ofnode nodenameA
```

Le rétablissement renvoie tout d'abord l'agrégat racine sur le nœud partenaire, puis, une fois le démarrage terminé, renvoie les agrégats non-root et toutes les LIF définies pour rétablir automatiquement ces agrégats. Le nœud qui vient d'être démarré commence à transmettre les données aux clients de chaque agrégat dès que l'agrégat est renvoyé.

15. Vérifier que tous les agrégats ont été renvoyés :

```
storage failover show-giveback
```

Si le champ État de rétablissement indique qu'il n'y a pas d'agrégats à renvoyer, tous les agrégats ont été renvoyés. Si le retour est vetoté, la commande affiche la progression du rétablissement et le sous-système qui a mis son veto au rétablissement.

16. Si un agrégat n'a pas été renvoyé, effectuez les opérations suivantes :

- Examinez la solution de contournement du veto pour déterminer si vous voulez répondre à la condition "veto" ou remplacer le veto.
- Si nécessaire, répondez à la condition "veto" décrite dans le message d'erreur, en veillant à ce que toutes les opérations identifiées soient arrêtées de manière normale.
- Exécutez à nouveau la commande Storage failover giveback.

Si vous décidez de remplacer la condition "veto", définissez le paramètre -override-vetos sur true.

17. Attendre au moins huit minutes pour que les conditions suivantes prennent effet :

- Les chemins d'accès multiples du client (si déployés) sont stabilisés.
- Les clients sont récupérés à partir de la pause dans une opération d'E/S qui se produit au cours du rétablissement.

Le temps de restauration est spécifique au client et peut prendre plus de huit minutes, selon les caractéristiques des applications client.

18. Vérifiez que la mise à jour a bien été effectuée pour le nœud :

- a. Accéder au niveau de privilège avancé :

```
set -privilege advanced
```

- b. Vérifiez que la mise à jour de l'état est terminée pour le nœud :

```
system node upgrade-revert show -node nodenameA
```

L'état doit être indiqué comme étant terminé.

Si le statut n'est pas terminé, contactez le support technique.

- a. Retour au niveau de privilège admin :

```
set -privilege admin
```

19. Vérifier que les ports du nœud sont bien :

```
network port show -node nodenameA
```

Vous devez exécuter cette commande sur un nœud mis à niveau vers la version supérieure de ONTAP 9.

L'exemple suivant indique que tous les ports du nœud sont up :

```
cluster1::> network port show -node node0
```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast	Domain	Link	MTU
						Admin/Oper
-----	-----	-----	-----	-----	-----	-----
node0						
	e0M	Default	-		up	1500 auto/100
	e0a	Default	-		up	1500 auto/1000
	e0b	Default	-		up	1500 auto/1000
	e1a	Cluster	Cluster		up	9000 auto/10000
	e1b	Cluster	Cluster		up	9000 auto/10000
5 entries were displayed.						

20. Rerestaurer les LIF sur le nœud :

```
network interface revert *
```

Cette commande renvoie les LIFs qui ont été migrées à l'écart du nœud.

```
cluster1::> network interface revert *  
8 entries were acted on.
```

21. Vérifiez que les LIF de données du nœud sont bien rétablies sur le nœud et qu'elles utilisent :

```
network interface show
```

L'exemple suivant montre que toutes les LIF de données hébergées par le nœud ont été rétablies au niveau du nœud et que leur état opérationnel est actif :

```
cluster1::> network interface show
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
vs0					
	data001	up/up	192.0.2.120/24	node0	e0a
true					
	data002	up/up	192.0.2.121/24	node0	e0b
true					
	data003	up/up	192.0.2.122/24	node0	e0b
true					
	data004	up/up	192.0.2.123/24	node0	e0a
true					

4 entries were displayed.

22. Si vous avez auparavant déterminé que ce nœud diffuse les clients, vérifiez que le nœud fournit un service à chaque protocole qu'il était auparavant en service :

```
system node run -node nodenameA -command uptime
```

L'opération compte à zéro pendant la mise à jour.

L'exemple suivant montre que le nœud mis à jour a repris le service de ses clients NFS et iSCSI :

```
cluster1::> system node run -node node0 -command uptime
3:15pm up 0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

23. Réactiver le rétablissement automatique sur le nœud partenaire s'il a été précédemment désactivé :

```
storage failover modify -node nodenameB -auto-giveback true
```

Vous devez continuer à mettre à jour le partenaire HA du nœud aussi rapidement que possible. Si vous devez interrompre le processus de mise à jour pour une raison quelconque, les deux nœuds de la paire HA doivent exécuter la même version de ONTAP.

Mise à jour du nœud partenaire dans une paire HA

Après la mise à jour du premier nœud d'une paire haute disponibilité, vous mettez à jour son partenaire en lançant un basculement sur incident. Le premier nœud transmet les données du partenaire pendant la mise à niveau du nœud partenaire.

1. Définissez le niveau de privilège sur avancé, en entrant **y** lorsque vous êtes invité à continuer :

```
set -privilege advanced
```

L'invite avancée (*>) s'affiche.

2. Définissez la nouvelle image du logiciel ONTAP comme image par défaut :

```
system image modify {-node nodenameB -iscurrent false} -isdefault true
```

La commande `system image modify` utilise une requête étendue pour modifier la nouvelle image logicielle ONTAP (qui est installée comme image alternative) comme image par défaut du nœud.

3. Surveiller la progression de la mise à jour :

```
system node upgrade-revert show
```

4. Vérifiez que la nouvelle image du logiciel ONTAP est définie comme image par défaut :

```
system image show
```

Dans l'exemple suivant : `image2` Est la nouvelle version d'ONTAP, définie en tant qu'image par défaut sur le nœud :

```
cluster1::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date

node0					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node1					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

5. Désactiver le rétablissement automatique sur le nœud partenaire s'il est activé :

```
storage failover modify -node nodenameA -auto-giveback false
```

Si le cluster est un cluster à deux nœuds, un message s'affiche vous informant que la désactivation du rétablissement automatique empêche la mise en ligne des services du cluster de gestion en cas de

défaillance alternée. Entrez y pour continuer.

6. Vérifier que le rétablissement automatique est désactivé pour le nœud partenaire :

```
storage failover show -node nodenameA -fields auto-giveback
```

```
cluster1::> storage failover show -node node0 -fields auto-giveback
node      auto-giveback
-----
node0     false
1 entry was displayed.
```

7. Exécutez la commande suivante deux fois pour déterminer si le nœud à mettre à jour diffuse actuellement des clients :

```
system node run -node nodenameB -command uptime
```

La commande UpTime affiche le nombre total d'opérations effectuées par le nœud pour les clients NFS, SMB, FC et iSCSI depuis le dernier démarrage du nœud. Pour chaque protocole, vous devez exécuter la commande deux fois afin de déterminer si le nombre d'opérations augmente. S'ils augmentent, le nœud diffuse actuellement des clients pour ce protocole. Si ce n'est pas le cas, le nœud ne diffuse actuellement pas les clients pour ce protocole.



Vous devez noter chaque protocole dont les opérations client augmentent, de sorte qu'après la mise à jour du nœud, vous pouvez vérifier que le trafic client a repris.

L'exemple suivant montre un nœud avec des opérations NFS, SMB, FC et iSCSI. Toutefois, le nœud dessert actuellement uniquement les clients NFS et iSCSI.

```
cluster1::> system node run -node node1 -command uptime
2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node1 -command uptime
2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

8. Migrer tous les LIFs de données loin du nœud :

```
network interface migrate-all -node nodenameB
```

9. Vérifiez l'état des LIFs que vous avez migrées :

```
network interface show
```

Pour plus d'informations sur les paramètres que vous pouvez utiliser pour vérifier l'état des LIF, reportez-vous à la page man de l'interface réseau.

L'exemple suivant montre que les LIF de données du nœud 1 ont migré correctement. Pour chaque LIF, les champs inclus dans cet exemple vous permettent de vérifier le nœud et le port d'accueil de la LIF, le nœud et le port actuels vers lesquels la LIF a migré, ainsi que le statut opérationnel et administratif de la LIF.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node1 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif      home-node home-port curr-node curr-port status-oper
status-admin
-----
vs0      data001 node1      e0a      node0      e0a      up      up
vs0      data002 node1      e0b      node0      e0b      up      up
vs0      data003 node1      e0b      node0      e0b      up      up
vs0      data004 node1      e0a      node0      e0a      up      up
4 entries were displayed.
```

10. Lancement d'un basculement :

```
storage failover takeover -ofnode nodenameB -option allow-version-
mismatch
```

Ne spécifiez pas le paramètre `-option` immédiate, car un basculement normal est nécessaire pour le nœud en cours de basculement pour démarrer sur la nouvelle image logicielle. Si vous n'avez pas migré manuellement les LIF en dehors du nœud, elles migrent automatiquement vers le partenaire de haute disponibilité du nœud, afin qu'il n'y ait aucune interruption de service.

Un avertissement s'affiche. Vous devez entrer `y` pour continuer.

Le nœud pris au relais est démarré jusqu'à l'état en attente de rétablissement.



Si AutoSupport est activé, un message AutoSupport est envoyé, indiquant que le nœud n'a pas le quorum du cluster. Vous pouvez ignorer cette notification et poursuivre la mise à jour.

11. Vérifier que le basculement a abouti :

```
storage failover show
```

L'exemple suivant montre que le basculement a réussi. Le nœud `node1` est en attente de rétablissement de l'état, et son partenaire est à l'état en basculement.


```
cluster1::> storage failover show
```

Node	Partner	Takeover Possible	State Description
node0	node1	-	In takeover
node1	node0	false	Waiting for giveback (HA mailboxes)

2 entries were displayed.

12. Attendre au moins huit minutes pour que les conditions suivantes prennent effet :

+

Les chemins d'accès multiples du client (si déployés) sont stabilisés.

Les clients sont récupérés à partir de la pause des E/S qui a lieu lors du basculement.

+

Le temps de restauration est spécifique au client et peut prendre plus de huit minutes, selon les caractéristiques des applications client.

13. Renvoyez les agrégats au nœud partenaire :

```
storage failover giveback -ofnode nodenameB
```

L'opération de rétablissement renvoie tout d'abord l'agrégat racine sur le nœud partenaire, puis, une fois le démarrage terminé, renvoie les agrégats non-root et les LIF définies pour rétablir automatiquement ces agrégats. Le nœud qui vient d'être démarré commence à transmettre les données aux clients de chaque agrégat dès que l'agrégat est renvoyé.

14. Vérifier que tous les agrégats sont renvoyés :

```
storage failover show-giveback
```

Si le champ État de rétablissement indique qu'il n'y a pas d'agrégats à renvoyer, tous les agrégats sont renvoyés. Si le retour est vetoté, la commande affiche la progression du rétablissement et le sous-système qui a opposé son veto à l'opération de rétablissement.

15. Si un agrégat n'est pas renvoyé, effectuez les opérations suivantes :

- Examinez la solution de contournement du veto pour déterminer si vous voulez répondre à la condition "verto" ou remplacer le veto.
- Si nécessaire, répondez à la condition "verto" décrite dans le message d'erreur, en veillant à ce que toutes les opérations identifiées soient arrêtées de manière normale.
- Exécutez à nouveau la commande `Storage failover giveback`.

Si vous décidez de remplacer la condition "verto", définissez le paramètre `-override-vetos` sur `true`.

16. Attendez au moins huit minutes pour que les conditions suivantes prennent effet :

- Les chemins d'accès multiples du client (si déployés) sont stabilisés.
- Les clients sont récupérés à partir de la pause dans une opération d'E/S qui se produit au cours du rétablissement.

Le temps de restauration est spécifique au client et peut prendre plus de huit minutes, selon les caractéristiques des applications client.

17. Vérifiez que la mise à jour a bien été effectuée pour le nœud :

a. Accéder au niveau de privilège avancé :

```
set -privilege advanced
```

b. Vérifiez que la mise à jour de l'état est terminée pour le nœud :

```
system node upgrade-revert show -node nodenameB
```

L'état doit être indiqué comme étant terminé.

Si l'état n'est pas complet, exécutez le dans le nœud `system node upgrade-revert upgrade` commande. Si la commande ne termine pas la mise à jour, contactez le support technique.

a. Retour au niveau de privilège admin :

```
set -privilege admin
```

18. Vérifier que les ports du nœud sont bien :

```
network port show -node nodenameB
```

Vous devez exécuter cette commande sur un nœud mis à niveau vers ONTAP 9.4.

L'exemple suivant montre que tous les ports de données du nœud up :

```
cluster1::> network port show -node node1
```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	

node1						
	e0M	Default	-	up	1500	auto/100
	e0a	Default	-	up	1500	auto/1000
	e0b	Default	-	up	1500	auto/1000
	e1a	Cluster	Cluster	up	9000	auto/10000
	e1b	Cluster	Cluster	up	9000	auto/10000
5 entries were displayed.						

19. Rerestaurer les LIF sur le nœud :

```
network interface revert *
```

Cette commande renvoie les LIFs qui ont été migrées à l'écart du nœud.

```
cluster1::> network interface revert *  
8 entries were acted on.
```

20. Vérifiez que les LIF de données du nœud sont bien rétablies sur le nœud et qu'elles utilisent :

```
network interface show
```

L'exemple suivant montre que toutes les LIFs de données hébergées par le nœud sont rétablies au niveau du nœud et que leur état opérationnel est actif :

```
cluster1::> network interface show
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
vs0					
	data001	up/up	192.0.2.120/24	node1	e0a
true					
	data002	up/up	192.0.2.121/24	node1	e0b
true					
	data003	up/up	192.0.2.122/24	node1	e0b
true					
	data004	up/up	192.0.2.123/24	node1	e0a
true					

4 entries were displayed.

21. Si vous avez auparavant déterminé que ce nœud diffuse les clients, vérifiez que le nœud fournit un service à chaque protocole qu'il était auparavant en service :

```
system node run -node nodenameB -command uptime
```

L'opération compte à zéro pendant la mise à jour.

L'exemple suivant montre que le nœud mis à jour a repris le service de ses clients NFS et iSCSI :

```
cluster1::> system node run -node node1 -command uptime
3:15pm up 0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

22. Si ce nœud était le dernier nœud du cluster à mettre à jour, déclenchez une notification AutoSupport :

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

Cette notification AutoSupport inclut un enregistrement de l'état du système juste avant la mise à jour. Il enregistre des informations de dépannage utiles en cas de problème avec le processus de mise à jour.

Si le cluster n'est pas configuré pour envoyer des messages AutoSupport, une copie de la notification est enregistrée localement.

23. Vérifiez que le nouveau logiciel ONTAP s'exécute sur les deux nœuds de la paire HA :

```
set -privilege advanced
```

```
system node image show
```

Dans l'exemple suivant, image2 est la version mise à jour de ONTAP et il s'agit de la version par défaut sur les deux nœuds :

```
cluster1::*> system node image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node1	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

24. Réactiver le rétablissement automatique sur le nœud partenaire s'il a été précédemment désactivé :

```
storage failover modify -node nodenameA -auto-giveback true
```

25. Vérifiez que le cluster est au quorum et que les services sont en cours d'exécution à l'aide du `cluster show` et `cluster ring show` commandes (niveau de privilège avancé).

Vous devez effectuer cette étape avant de mettre à niveau les paires haute disponibilité supplémentaires.

26. Retour au niveau de privilège admin :

```
set -privilege admin
```

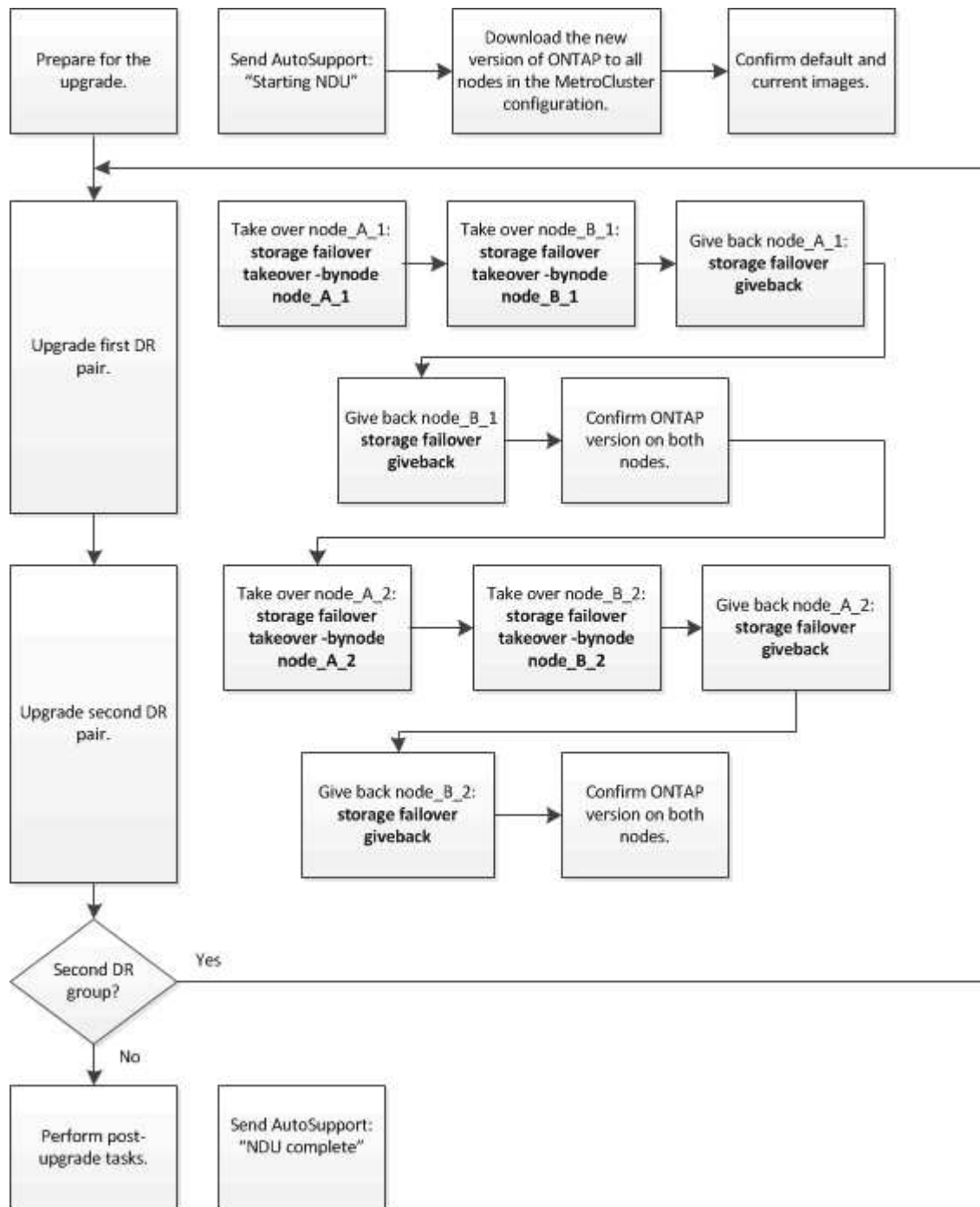
27. Mettez à niveau les paires haute disponibilité supplémentaires.

Mise à niveau manuelle sans interruption d'une configuration MetroCluster à quatre ou huit nœuds via l'interface de ligne de commande ONTAP

La mise à niveau manuelle d'une configuration MetroCluster à quatre ou huit nœuds implique de préparer la mise à jour, de mettre à jour les paires DR dans chacun des deux groupes DR simultanément et d'effectuer des tâches post-mise à niveau.

- Cette tâche s'applique aux configurations suivantes :
 - Configurations FC ou IP MetroCluster à quatre nœuds exécutant ONTAP 9.2 ou une version antérieure

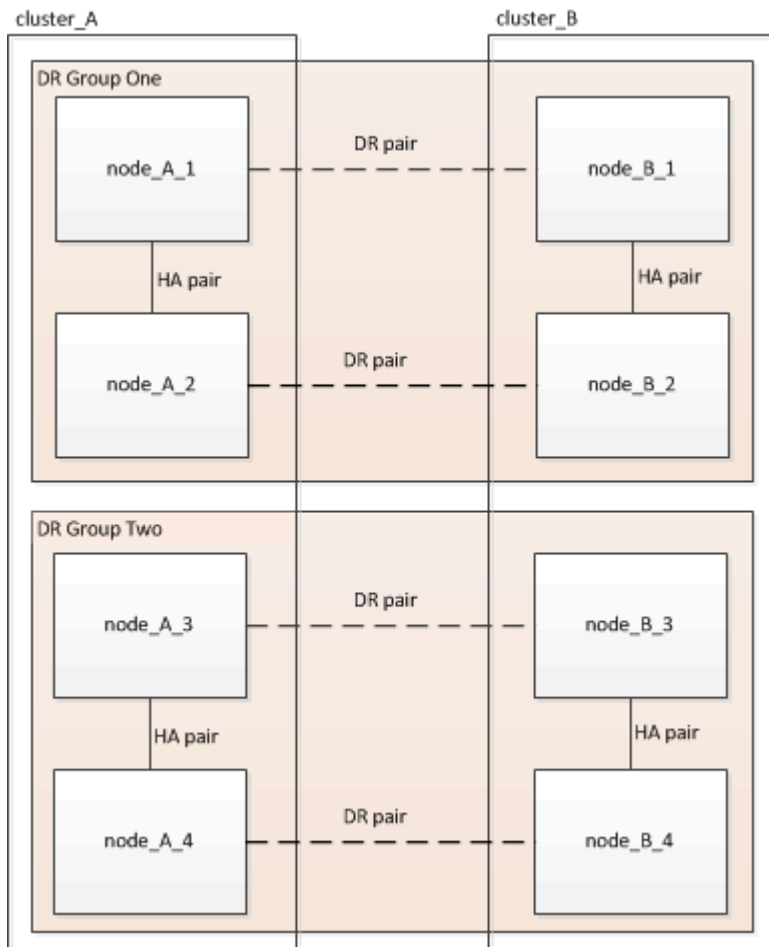
- Configurations FC à 8 nœuds MetroCluster, quelle que soit la version d'ONTAP utilisée
- Si vous disposez d'une configuration MetroCluster à deux nœuds, n'utilisez pas cette procédure.
- Les tâches suivantes font référence à l'ancienne et à la nouvelle version de ONTAP.
 - Lors de la mise à niveau, l'ancienne version est une version précédente de ONTAP, avec un numéro de version inférieur à celui de la nouvelle version de ONTAP.
 - Lors de la restauration, l'ancienne version est une version plus récente de ONTAP, avec un numéro de version plus élevé que la nouvelle version de ONTAP.
- Cette tâche utilise le flux de travail de haut niveau suivant :



Différences lors de la mise à jour du logiciel ONTAP sur une configuration MetroCluster à huit ou quatre nœuds

La procédure de mise à niveau du logiciel MetroCluster diffère selon qu'il y a huit ou quatre nœuds dans la configuration MetroCluster.

Une configuration MetroCluster se compose d'un ou deux groupes de reprise sur incident. Chaque groupe de reprise après incident est constitué de deux paires haute disponibilité, une paire haute disponibilité sur chaque cluster MetroCluster. Un MetroCluster à 8 nœuds inclut deux groupes de reprise après incident :



Vous mettez à niveau un groupe de reprise après incident à la fois.

Pour les configurations MetroCluster à quatre nœuds :

1. Mettre à niveau le groupe de reprise sur incident un :
 - a. Mettre à niveau les nœuds_A_1 et node_B_1.
 - b. Mettre à niveau node_A_2 et node_B_2.

Pour les configurations à 8 nœuds MetroCluster, vous effectuez deux fois la procédure de mise à niveau du groupe de reprise après incident :

1. Mettre à niveau le groupe de reprise sur incident un :
 - a. Mettre à niveau les nœuds_A_1 et node_B_1.
 - b. Mettre à niveau node_A_2 et node_B_2.
2. Mettre à niveau le DR Groupe deux :

- a. Mettre à niveau les nœuds_A_3 et node_B_3.
- b. Mettre à niveau les nœuds_A_4 et node_B_4.

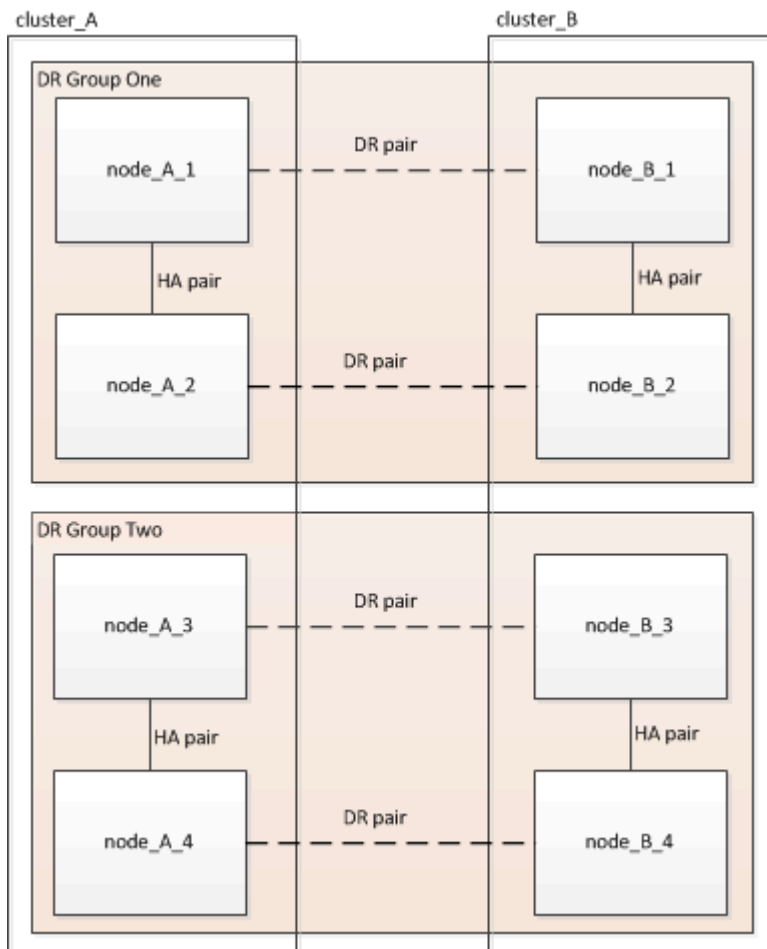
Préparation de la mise à niveau d'un groupe DR MetroCluster

Avant de mettre à niveau le logiciel ONTAP sur les nœuds, vous devez identifier les relations de DR entre les nœuds, envoyer un message AutoSupport indiquant que vous initiez une mise à niveau et confirmer la version de ONTAP exécutée sur chaque nœud.

Vous devez avoir "téléchargé" et "installé" les images du logiciel.

Cette tâche doit être répétée sur chaque groupe de reprise sur incident. Si la configuration MetroCluster comprend huit nœuds, il y a deux groupes de reprise sur incident. Cette tâche doit donc être répétée sur chaque groupe de reprise sur incident.

Les exemples fournis dans cette tâche utilisent les noms illustrés dans l'illustration suivante pour identifier les clusters et les nœuds :



1. Identifier les paires de reprise sur incident dans la configuration :

```
metrocluster node show -fields dr-partner
```



```
cluster_A::> metrocluster node show -fields dr-partner
(metrocluster node show)
dr-group-id cluster      node      dr-partner
-----
1           cluster_A    node_A_1  node_B_1
1           cluster_A    node_A_2  node_B_2
1           cluster_B    node_B_1  node_A_1
1           cluster_B    node_B_2  node_A_2
4 entries were displayed.

cluster_A::>
```

2. Définissez le niveau de privilège de admin sur avancé, en entrant **y** lorsque vous êtes invité à continuer :

```
set -privilege advanced
```

L'invite avancée (*>) s'affiche.

3. Confirmer la version de ONTAP sur cluster_A :

```
system image show
```

```
cluster_A::*> system image show
Node      Image      Is      Is      Version  Install
-----  -
node_A_1
  image1  true       true    X.X.X    MM/DD/YYYY TIME
  image2  false     false   Y.Y.Y    MM/DD/YYYY TIME
node_A_2
  image1  true       true    X.X.X    MM/DD/YYYY TIME
  image2  false     false   Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

4. Vérifier la version du cluster_B :

```
system image show
```

```
cluster_B::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date

node_B_1					
	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME
node_B_2					
	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_B::>
```

5. Déclencher une notification AutoSupport :

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

Cette notification AutoSupport inclut un enregistrement de l'état du système avant la mise à niveau. Il enregistre des informations de dépannage utiles en cas de problème avec le processus de mise à niveau.

Si votre cluster n'est pas configuré pour envoyer des messages AutoSupport, une copie de la notification est enregistrée localement.

6. Pour chaque nœud du premier jeu, définissez l'image logicielle ONTAP cible sur l'image par défaut :

```
system image modify {-node nodename -iscurrent false} -isdefault true
```

Cette commande utilise une requête étendue pour modifier l'image du logiciel cible, qui est installée comme image secondaire, comme image par défaut pour le nœud.

7. Vérifiez que l'image du logiciel ONTAP cible est définie comme image par défaut sur cluster_A :

```
system image show
```

Dans l'exemple suivant, image2 est la nouvelle version de ONTAP et est définie en tant qu'image par défaut sur chacun des nœuds du premier ensemble :

```
cluster_A::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date

node_A_1	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME
node_A_2	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

2 entries were displayed.

- a. Vérifiez que l'image du logiciel ONTAP cible est définie comme image par défaut sur cluster_B :

```
system image show
```

L'exemple suivant montre que la version cible est définie en tant qu'image par défaut sur chacun des nœuds du premier jeu :

```
cluster_B::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date

node_A_1	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/YY/YYYY TIME
node_A_2	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

2 entries were displayed.

8. Déterminer si les nœuds à mettre à niveau servent actuellement des clients deux fois pour chaque nœud :

```
system node run -node target-node -command uptime
```

La commande UpTime affiche le nombre total d'opérations que le nœud a effectuées pour les clients NFS, CIFS, FC et iSCSI depuis le dernier démarrage du nœud. Pour chaque protocole, vous devez exécuter la commande deux fois afin de déterminer si le nombre d'opérations augmente. S'ils augmentent, le nœud diffuse actuellement des clients pour ce protocole. Si ce n'est pas le cas, le nœud ne diffuse actuellement pas les clients pour ce protocole.



Vous devez noter chaque protocole dont les opérations client augmentent, de sorte qu'après la mise à niveau du nœud, vous pouvez vérifier que le trafic client a repris.

Cet exemple montre un nœud avec des opérations NFS, CIFS, FC et iSCSI. Toutefois, le nœud dessert actuellement uniquement les clients NFS et iSCSI.

```
cluster_x::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster_x::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

Mise à jour de la première paire DR dans un groupe MetroCluster DR

Vous devez effectuer un basculement et un retour des nœuds afin de faire de la nouvelle version d'ONTAP la version actuelle du nœud.

Tous les nœuds doivent exécuter l'ancienne version de ONTAP.

Dans cette tâche, les nœuds_A_1 et node_B_1 sont mis à niveau.

Si vous avez mis à niveau le logiciel ONTAP sur le premier groupe DR et que vous mettez à niveau le deuxième groupe DR dans une configuration MetroCluster à huit nœuds, dans cette tâche, vous mettez à jour node_A_3 et node_B_3.

1. Si le logiciel MetroCluster Tiebreaker est activé, désactivez-le.
2. Pour chaque nœud de la paire HA, désactiver le rétablissement automatique :

```
storage failover modify -node target-node -auto-giveback false
```

Cette commande doit être répétée pour chaque nœud de la paire HA.

3. Vérifier que le retour automatique est désactivé :

```
storage failover show -fields auto-giveback
```

Cet exemple montre que le rétablissement automatique a été désactivé sur les deux nœuds :

```
cluster_x::> storage failover show -fields auto-giveback
node      auto-giveback
-----
node_x_1  false
node_x_2  false
2 entries were displayed.
```

4. Assurez-vous que les E/S ne dépassent pas ~50 % pour chaque contrôleur et que l'utilisation du CPU ne dépasse pas ~50 % par contrôleur.

5. Initier un basculement du nœud cible sur cluster_A :

Ne spécifiez pas le paramètre -option immédiate, car un basculement normal est nécessaire pour les nœuds pris en charge afin de démarrer sur la nouvelle image logicielle.

a. Reprendre le partenaire de reprise après incident sur cluster_A (node_A_1) :

```
storage failover takeover -ofnode node_A_1
```

Le nœud démarre à l'état « waiting for giveback ».



Si AutoSupport est activé, un message AutoSupport est envoyé pour indiquer que les nœuds sont hors du quorum du cluster. Vous pouvez ignorer cette notification et poursuivre la mise à niveau.

b. Vérifiez que le basculement est réussi :

```
storage failover show
```

L'exemple suivant montre que le basculement a réussi. L'état « waiting for giveback » est défini sur node_A_1 et node_A_2 est à l'état « In Takeover ».

```
cluster1::> storage failover show
```

Node	Partner	Takeover Possible	State Description
node_A_1	node_A_2	-	Waiting for giveback (HA mailboxes)
node_A_2	node_A_1	false	In takeover

2 entries were displayed.

6. Reprendre le partenaire de reprise après incident sur le cluster_B (node_B_1) :

Ne spécifiez pas le paramètre -option immédiate, car un basculement normal est nécessaire pour les

nœuds pris en charge afin de démarrer sur la nouvelle image logicielle.

a. Reprendre le nœud_B_1 :

```
storage failover takeover -ofnode node_B_1
```

Le nœud démarre à l'état « waiting for giveback ».



Si AutoSupport est activé, un message AutoSupport est envoyé pour indiquer que les nœuds sont hors du quorum du cluster. Vous pouvez ignorer cette notification et poursuivre la mise à niveau.

b. Vérifiez que le basculement est réussi :

```
storage failover show
```

L'exemple suivant montre que le basculement a réussi. Le nœud_B_1 est dans l'état « waiting for giveback » et le nœud_B_2 est à l'état « In Takeover ».

```
cluster1::> storage failover show
```

Node	Partner	Takeover Possible	State Description
node_B_1	node_B_2	-	Waiting for giveback (HA mailboxes)
node_B_2	node_B_1	false	In takeover

2 entries were displayed.

7. Attendez au moins huit minutes pour vérifier les conditions suivantes :

- Les chemins d'accès multiples du client (si déployés) sont stabilisés.
- Les clients sont récupérés à partir de la pause des E/S qui a lieu lors du basculement.

Le temps de restauration est spécifique au client et peut prendre plus de huit minutes selon les caractéristiques des applications client.

8. Renvoyez les agrégats aux nœuds cibles :

Après la mise à niveau des configurations IP de MetroCluster vers ONTAP 9.5 ou une version ultérieure, les agrégats sont dégradés pendant une courte période avant de resynchroniser et de revenir à un état miroir.

a. Renvoyer les agrégats au partenaire de reprise après incident sur cluster_A :

```
storage failover giveback -ofnode node_A_1
```

b. Renvoyer les agrégats au partenaire de reprise après incident sur cluster_B :

```
storage failover giveback -ofnode node_B_1
```

L'opération de rétablissement renvoie tout d'abord l'agrégat racine sur le nœud, puis, une fois le démarrage du nœud terminé, renvoie les agrégats non-racine.

9. Vérifiez que tous les agrégats ont été renvoyés en exécutant la commande suivante sur les deux clusters :

```
storage failover show-giveback
```

Si le champ État de rétablissement indique qu'il n'y a pas d'agrégats à renvoyer, tous les agrégats ont été renvoyés. Si le retour est vetoté, la commande affiche la progression du rétablissement et le sous-système qui a mis son veto au rétablissement.

10. Si un agrégat n'a pas été renvoyé, procédez comme suit :

- a. Examinez la solution de contournement du veto pour déterminer si vous voulez répondre à la condition "veto" ou remplacer le veto.
- b. Si nécessaire, répondez à la condition "veto" décrite dans le message d'erreur, en veillant à ce que toutes les opérations identifiées soient arrêtées de manière normale.
- c. Saisissez de nouveau la commande Storage failover giveback.

Si vous décidez de remplacer la condition "veto", définissez le paramètre -override-vetos sur true.

11. Attendez au moins huit minutes pour vérifier les conditions suivantes :

- Les chemins d'accès multiples du client (si déployés) sont stabilisés.
- Les clients sont récupérés à partir de la pause des E/S qui a lieu au cours du rétablissement

Le temps de restauration est spécifique au client et peut prendre plus de huit minutes selon les caractéristiques des applications client.

12. Définissez le niveau de privilège de admin sur avancé, en entrant **y** lorsque vous êtes invité à continuer :

```
set -privilege advanced
```

L'invite avancée (*>) s'affiche.

13. Vérifier la version du cluster_A :

```
system image show
```

L'exemple suivant montre que System image2 doit être la version par défaut et la version en cours sur node_A_1 :

```
cluster_A::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date

node_A_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_A_2					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_A::>
```

14. Vérifier la version du cluster_B :

```
system image show
```

L'exemple suivant montre que System image2 (ONTAP 9.0.0) est la version par défaut et la version actuelle du noeud_A_1 :

```
cluster_A::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date

node_B_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_B_2					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_A::>
```

Mise à jour de la seconde paire DR dans un groupe MetroCluster DR

Vous devez effectuer un basculement et un retour du nœud afin de faire de la nouvelle version d'ONTAP la version actuelle du nœud.

Vous devez avoir mis à niveau la première paire DR (node_A_1 et node_B_1).

Dans cette tâche, les nœuds_A_2 et node_B_2 sont mis à niveau.

Si vous avez mis à niveau le logiciel ONTAP sur le premier groupe DR et que vous mettez à jour le deuxième

groupe DR dans une configuration MetroCluster à huit nœuds, dans cette tâche, vous mettez à jour node_A_4 et node_B_4.

1. Migrer tous les LIFs de données loin du nœud :

```
network interface migrate-all -node nodenameA
```

2. Initier un basculement du nœud cible sur cluster_A :

Ne spécifiez pas le paramètre -option immédiate, car un basculement normal est nécessaire pour les nœuds pris en charge afin de démarrer sur la nouvelle image logicielle.

- a. Reprendre le partenaire de reprise après incident sur cluster_A :

```
storage failover takeover -ofnode node_A_2 -option allow-version-  
mismatch
```



Le allow-version-mismatch Aucune option n'est requise pour les mises à niveau de ONTAP 9.0 vers ONTAP 9.1 ou pour les mises à niveau de correctifs.

Le nœud démarre à l'état « waiting for giveback ».

Si AutoSupport est activé, un message AutoSupport est envoyé pour indiquer que les nœuds sont hors du quorum du cluster. Vous pouvez ignorer cette notification et poursuivre la mise à niveau.

- b. Vérifiez que le basculement est réussi :

```
storage failover show
```

L'exemple suivant montre que le basculement a réussi. L'état « waiting for giveback » est défini sur node_A_2 et node_A_1 est à l'état « In Takeover ».

```
cluster1::> storage failover show
```


Node	Partner	Takeover Possible	State Description
node_A_1	node_A_2	false	In takeover
node_A_2	node_A_1	-	Waiting for giveback (HA mailboxes)

2 entries were displayed.

3. Initier un basculement du nœud cible sur cluster_B :

Ne spécifiez pas le paramètre -option immédiate, car un basculement normal est nécessaire pour les nœuds pris en charge afin de démarrer sur la nouvelle image logicielle.

a. Reprendre le partenaire de reprise sur incident sur cluster_B (node_B_2) :

Si vous effectuez une mise à niveau depuis...	Entrez cette commande...
ONTAP 9.2 ou ONTAP 9.1	<pre>storage failover takeover -ofnode node_B_2</pre>
ONTAP 9.0 ou Data ONTAP 8.3.x	<pre>storage failover takeover -ofnode node_B_2 -option allow- version-mismatch</pre> <div>  <p>Le allow-version-mismatch Aucune option n'est requise pour les mises à niveau de ONTAP 9.0 vers ONTAP 9.1 ou pour les mises à niveau de correctifs.</p> </div>

Le nœud démarre à l'état « waiting for giveback ».



Si AutoSupport est activé, un message AutoSupport est envoyé, indiquant que les nœuds ne disposent pas du quorum du cluster. Vous pouvez ignorer cette notification en toute sécurité et poursuivre la mise à niveau.

b. Vérifiez que le basculement est réussi :

```
storage failover show
```

L'exemple suivant montre que le basculement a réussi. L'état « waiting for giveback » est défini sur node_B_2 et le nœud_B_1 est à l'état « In Takeover ».

```
cluster1::> storage failover show

Node           Partner           Takeover
Possible State Description
-----
node_B_1       node_B_2           false      In takeover
node_B_2       node_B_1           -          Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

4. Attendez au moins huit minutes pour vérifier les conditions suivantes :

- Les chemins d'accès multiples du client (si déployés) sont stabilisés.

- Les clients sont récupérés à partir de la pause des E/S qui a lieu lors du basculement.

Le temps de restauration est spécifique au client et peut prendre plus de huit minutes selon les caractéristiques des applications client.

5. Renvoyez les agrégats aux nœuds cibles :

Après la mise à niveau des configurations IP de MetroCluster vers ONTAP 9.5, les agrégats seront sur une courte période avant de resynchroniser et de rétablir l'état miroir.

a. Renvoyer les agrégats au partenaire de reprise après incident sur cluster_A :

```
storage failover giveback -ofnode node_A_2
```

b. Renvoyer les agrégats au partenaire de reprise après incident sur cluster_B :

```
storage failover giveback -ofnode node_B_2
```

L'opération de rétablissement renvoie tout d'abord l'agrégat racine sur le nœud, puis, une fois le démarrage du nœud terminé, renvoie les agrégats non-racine.

6. Vérifiez que tous les agrégats ont été renvoyés en exécutant la commande suivante sur les deux clusters :

```
storage failover show-giveback
```

Si le champ État de rétablissement indique qu'il n'y a pas d'agrégats à renvoyer, tous les agrégats ont été renvoyés. Si le retour est vetoté, la commande affiche la progression du rétablissement et le sous-système qui a mis son veto au rétablissement.

7. Si un agrégat n'a pas été renvoyé, procédez comme suit :

- Examinez la solution de contournement du veto pour déterminer si vous voulez répondre à la condition "verto" ou remplacer le veto.
- Si nécessaire, répondez à la condition "verto" décrite dans le message d'erreur, en veillant à ce que toutes les opérations identifiées soient arrêtées de manière normale.
- Saisissez de nouveau la commande Storage failover giveback.

Si vous décidez de remplacer la condition "verto", définissez le paramètre -override-vetos sur true.

8. Attendez au moins huit minutes pour vérifier les conditions suivantes :

- Les chemins d'accès multiples du client (si déployés) sont stabilisés.
- Les clients sont récupérés à partir de la pause des E/S qui a lieu au cours du rétablissement

Le temps de restauration est spécifique au client et peut prendre plus de huit minutes selon les caractéristiques des applications client.

9. Définissez le niveau de privilège de admin sur avancé, en entrant **y** lorsque vous êtes invité à continuer :

```
set -privilege advanced
```

L'invite avancée (*>) s'affiche.

10. Vérifier la version du cluster_A :

```
system image show
```

L'exemple suivant montre que l'image système 2 (image ONTAP cible) est la version par défaut et la version actuelle du noeud_A_2 :

```
cluster_B::~*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date

node_A_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_A_2					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_A::~>
```

11. Vérifier la version du cluster_B :

```
system image show
```

L'exemple suivant montre que l'image système 2 (image ONTAP cible) est la version par défaut et la version actuelle du noeud_B_2 :

```
cluster_B::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date

node_B_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_B_2					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_A::>
```

12. Pour chaque nœud de la paire HA, activez le rétablissement automatique :

```
storage failover modify -node target-node -auto-giveback true
```

Cette commande doit être répétée pour chaque nœud de la paire HA.

13. Vérifier que le rétablissement automatique est activé :

```
storage failover show -fields auto-giveback
```

Cet exemple montre que le rétablissement automatique a été activé sur les deux nœuds :

```
cluster_x::> storage failover show -fields auto-giveback
```

node	auto-giveback

node_x_1	true
node_x_2	true

2 entries were displayed.

Mise à niveau non disruptive d'une configuration MetroCluster à deux nœuds sous ONTAP 9.2 ou version antérieure

La mise à niveau d'une configuration MetroCluster à deux nœuds varie en fonction de votre version de ONTAP. Si vous exécutez ONTAP 9.2 ou une version antérieure, utilisez cette procédure pour effectuer une mise à niveau manuelle sans interruption, notamment lancer un basculement négocié, mettre à jour le cluster sur le site en panne, initier le rétablissement, puis répéter le processus sur le cluster de l'autre site.

Si vous disposez d'une configuration MetroCluster à deux nœuds exécutant ONTAP 9.3 ou une version ultérieure, effectuez une [Mise à niveau automatisée avec System Manager](#).

Étapes

1. Définissez le niveau de privilège sur avancé, en entrant **y** lorsque vous êtes invité à continuer :

```
set -privilege advanced
```

L'invite avancée (*>) s'affiche.

2. Sur le cluster à mettre à niveau, installez la nouvelle image logicielle ONTAP comme image par défaut :

```
system node image update -package package_location -setdefault true  
-replace-package true
```

```
cluster_B::*> system node image update -package  
http://www.example.com/NewImage.tgz -setdefault true -replace-package  
true
```

3. Vérifiez que l'image du logiciel cible est définie comme image par défaut :

```
system node image show
```

L'exemple suivant montre cela NewImage est défini comme image par défaut :

```
cluster_B::*> system node image show
```

Node	Image	Is Default	Is Current	Version	Install Date

node_B_1					
	OldImage	false	true	X.X.X	MM/DD/YYYY TIME
	NewImage	true	false	Y.Y.Y	MM/DD/YYYY TIME

2 entries were displayed.

4. Si l'image du logiciel cible n'est pas définie comme image par défaut, modifiez-la :

```
system image modify {-node * -iscurrent false} -isdefault true
```

5. Vérifier que tous les SVM de cluster sont dans un état de santé :

```
metrocluster vserver show
```

6. Sur le cluster qui n'est pas mis à jour, initiez un basculement négocié :

```
metrocluster switchover
```

L'opération peut prendre plusieurs minutes. Vous pouvez utiliser la commande MetroCluster Operation show pour vérifier que le basculement est terminé.

Dans l'exemple suivant, un basculement négocié est effectué sur le cluster distant (« cluster_A »). Ceci entraîne l'arrêt du cluster local (« cluster_B ») pour que vous puissiez le mettre à jour.

```
cluster_A::> metrocluster switchover

Warning: negotiated switchover is about to start. It will stop all the
data
      Vservers on cluster "cluster_B" and
      automatically re-start them on cluster
      "cluster_A". It will finally gracefully shutdown
      cluster "cluster_B".
Do you want to continue? {y|n}: y
```

7. Vérifier que tous les SVM de cluster sont dans un état de santé :

```
metrocluster vservers show
```

8. Resynchroniser les agrégats de données sur le cluster « Surviving » :

```
metrocluster heal -phase aggregates
```

Après la mise à niveau des configurations IP de MetroCluster vers ONTAP 9.5 ou une version ultérieure, les agrégats sont dégradés pendant une courte période avant de resynchroniser et de revenir à un état miroir.

```
cluster_A::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

9. Vérifiez que l'opération de correction a bien été effectuée :

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

10. Resynchroniser les agrégats racine sur le cluster « Surviving » :

```
metrocluster heal -phase root-aggregates
```

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 131] Job succeeded: Heal Root Aggregates is successful.
```

11. Vérifiez que l'opération de correction a bien été effectuée :

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

12. Sur le cluster arrêté, démarrez le nœud à partir de l'invite DU CHARGEUR :

```
boot_ontap
```

13. Attendez la fin du processus de démarrage, puis vérifiez que tous les SVM du cluster sont bien en état de santé :

```
metrocluster vserver show
```

14. Effectuez un rétablissement à partir du cluster « Surviving » :

```
metrocluster switchback
```


15. Vérifiez que le rétablissement a été effectué correctement :

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

16. Vérifier que tous les SVM de cluster sont dans un état de santé :

```
metrocluster vserver show
```

17. Répétez toutes les étapes précédentes sur l'autre cluster.

18. Vérifier que la configuration MetroCluster est saine :

a. Vérifiez la configuration :

```
metrocluster check run
```

```
cluster_A::> metrocluster check run
Last Checked On: MM/DD/YYYY TIME
Component          Result
-----
nodes               ok
lifs                ok
config-replication ok
aggregates          ok
4 entries were displayed.
```

Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results.

To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.

b. Pour afficher des résultats plus détaillés, utilisez la commande MetroCluster check run :

```
metrocluster check aggregate show
```

```
metrocluster check config-replication show
```

```
metrocluster check lif show
```

```
metrocluster check node show
```

c. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

d. Simuler l'opération de basculement :

```
metrocluster switchover -simulate
```

e. Examinez les résultats de la simulation de basculement :

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
  Operation: switchover
    State: successful
  Start time: MM/DD/YYYY TIME
    End time: MM/DD/YYYY TIME
    Errors: -
```

f. Retour au niveau de privilège admin :

```
set -privilege admin
```

g. Répétez ces sous-étapes sur l'autre cluster.

Une fois que vous avez terminé

Effectuez toutes les opérations "[tâches post-mise à niveau](#)".

Informations associées

Mise à niveau manuelle des ONTAP perturbantes via l'interface de ligne de commande

Si vous pouvez mettre votre cluster hors ligne pour effectuer la mise à niveau vers une nouvelle version de ONTAP, vous pouvez utiliser la méthode de mise à niveau perturbation. Cette méthode se déroule en plusieurs étapes : désactivation du basculement du stockage pour chaque paire haute disponibilité, redémarrage de chaque nœud du cluster, puis réactivation du basculement du stockage.

- Vous devez **"télécharger"** et **"installer"** l'image du logiciel.
- Si vous travaillez dans un environnement SAN, tous les clients SAN doivent être arrêtés ou suspendus jusqu'à la fin de la mise à niveau.

Si les clients SAN ne sont pas arrêtés ou suspendus avant une mise à niveau perturbatrice, les systèmes de fichiers clients et les applications reçoivent des erreurs qui peuvent nécessiter une récupération manuelle après la fin de la mise à niveau.

Lors d'une mise à niveau sans interruption, un basculement du stockage est désactivé pour chaque paire haute disponibilité et chaque nœud est mis à jour. Lorsque le basculement de stockage est désactivé, chaque nœud se comporte comme un cluster à un seul nœud ; c'est-à-dire que les services système associés au nœud sont interrompus tant que le système doit redémarrer.

Étapes

1. Définissez le niveau de privilège de admin sur avancé, en entrant **y** lorsque vous êtes invité à continuer :

```
set -privilege advanced
```

L'invite avancée (*>) s'affiche.

2. Définissez la nouvelle image du logiciel ONTAP comme image par défaut :

```
system image modify {-node * -iscurrent false} -isdefault true
```

Cette commande utilise une requête étendue pour modifier l'image logicielle ONTAP cible (qui est installée comme image secondaire) en tant qu'image par défaut pour chaque nœud.

3. Vérifiez que la nouvelle image du logiciel ONTAP est définie comme image par défaut :

```
system image show
```

Dans l'exemple suivant, l'image 2 est la nouvelle version de ONTAP et est définie en tant qu'image par défaut sur les deux nœuds :

```
cluster1::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date

node0					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME
node1					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

4. Effectuez l'une des opérations suivantes :

Si le cluster est constitué de...	Procédez comme ça...
Un nœud	Passez à l'étape suivante.
Deux nœuds	<p>a. Désactiver la haute disponibilité du cluster :</p> <pre>cluster ha modify -configured false</pre> <p>Entrez y pour continuer lorsque vous y êtes invité.</p> <p>b. Désactivation du basculement du stockage pour la paire haute disponibilité :</p> <pre>storage failover modify -node * -enabled false</pre>
Plus de deux nœuds	<p>Désactiver le basculement du stockage pour chaque paire haute disponibilité du cluster :</p> <pre>storage failover modify -node * -enabled false</pre>

5. Reboot d'un noeud sur le cluster:

```
system node reboot -node nodename -ignore-quorum-warnings
```



Ne redémarrez pas plus d'un nœud à la fois.

Le nœud démarre la nouvelle image ONTAP. L'invite de connexion ONTAP apparaît, indiquant que le processus de redémarrage est terminé.

6. Après le redémarrage du nœud ou de l'ensemble de nœuds avec la nouvelle image ONTAP, définissez le niveau de privilège sur Advanced :

```
set -privilege advanced
```

Entrez **y** lorsque vous êtes invité à continuer

7. Vérifiez que le nouveau logiciel est en cours d'exécution :

```
system node image show
```

Dans l'exemple suivant, image1 est la nouvelle version de ONTAP et est définie comme la version actuelle sur le nœud 0 :

```
cluster1::*> system node image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME
node1	image1	true	false	X.X.X	MM/DD/YYYY TIME
	image2	false	true	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

8. Vérifiez que la mise à niveau est effectuée correctement :

- a. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

- b. Vérifiez que la mise à niveau est terminée pour chaque nœud :

```
system node upgrade-revert show -node nodename
```

L'état doit être indiqué comme étant terminé.

Si le statut n'est pas terminé, ["Contactez le support NetApp"](#) immédiatement.

a. Retour au niveau de privilège admin :

```
set -privilege admin
```

9. Répétez les étapes 2 à 8 pour chaque nœud supplémentaire.

10. Si le cluster comprend deux nœuds ou plus, activez le basculement du stockage pour chaque paire haute disponibilité du cluster :

```
storage failover modify -node * -enabled true
```

11. Si le cluster ne comprend que deux nœuds, activez la haute disponibilité du cluster :

```
cluster ha modify -configured true
```

Que faire après une mise à niveau de ONTAP

Que faire après une mise à niveau de ONTAP

Après la mise à niveau de ONTAP, vous devez effectuer plusieurs tâches pour vérifier que le cluster est prêt.

1. ["Vérifiez le cluster"](#).

Après la mise à niveau de ONTAP, vérifiez la version du cluster, l'état de santé du cluster et l'état du stockage. Si vous utilisez une configuration MetroCluster FC, vous devez également vérifier que le cluster est activé pour le basculement automatique non planifié.

2. ["Vérifier que toutes les LIFs se trouvent sur les ports home"](#).

Au cours d'un redémarrage, certaines LIFs ont peut-être été migrées vers leurs ports de basculement qui leur sont attribués. Une fois que vous avez mis à niveau un cluster, vous devez activer et restaurer toutes les LIF qui ne se trouvent pas sur leur port de base.

3. La vérification ["considérations spéciales"](#) spécifique à votre cluster.

Si certaines configurations existent sur le cluster, vous devrez peut-être effectuer des étapes supplémentaires après la mise à niveau.

4. ["Mettre à jour le package de qualification de disque \(DQP\)"](#).

Le DQP n'a pas été mis à jour dans le cadre d'une mise à niveau ONTAP.

Vérifiez votre cluster après la mise à niveau de ONTAP

Après la mise à niveau de ONTAP, vérifiez la version du cluster, l'état du cluster et l'état du stockage. Pour les configurations MetroCluster FC, vérifiez également que le cluster est activé en cas de basculement automatique non planifié.

Vérifiez la version du cluster

Une fois toutes les paires haute disponibilité mises à niveau, vous devez utiliser la commande `version` pour vérifier que tous les nœuds exécutent la version cible.

La version en cluster est la version la plus basse d'ONTAP s'exécutant sur n'importe quel nœud du cluster. Si la version du cluster n'est pas la version cible de ONTAP, vous pouvez mettre à niveau votre cluster.

1. Vérifiez que la version du cluster est la version ONTAP cible :

```
version
```

2. Si la version du cluster n'est pas la version cible de ONTAP, vous devez vérifier l'état de mise à niveau de tous les nœuds :

```
system node upgrade-revert show
```

Vérification de l'état du cluster

Une fois que vous avez mis à niveau un cluster, vous devez vérifier que les nœuds sont sains et peuvent participer au cluster, et que le cluster est dans le quorum.

1. Vérifiez que les nœuds du cluster sont en ligne et peuvent participer au cluster :

```
cluster show
```

```
cluster1::> cluster show
Node                               Health  Eligibility
-----
node0                             true    true
node1                             true    true
```

Si l'un des nœuds est défectueux ou non éligible, vérifiez la présence d'erreurs dans les journaux EMS et effectuez des actions correctives.

2. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

3. Vérifier les détails de configuration pour chaque processus RDB

- L'époque de la base de données relationnelle et les séries de tests de base de données doivent correspondre pour chaque nœud.
- Le maître de quorum par anneau doit être le même pour tous les nœuds.

Notez que chaque anneau peut avoir un maître de quorum différent.

Pour afficher ce processus RDB...	Entrez cette commande...
Application de gestion	<code>cluster ring show -unitname mgmt</code>
Base de données d'emplacement de volume	<code>cluster ring show -unitname vldb</code>
Gestionnaire d'interface virtuelle	<code>cluster ring show -unitname vifmgr</code>
Démon de gestion DU SAN	<code>cluster ring show -unitname bcomd</code>

Cet exemple représente le processus de la base de données d'emplacements de volumes :

```
cluster1::*> cluster ring show -unitname vldb
```

Node	UnitName	Epoch	DB Epoch	DB Trnxs	Master	Online
node0	vldb	154	154	14847	node0	master
node1	vldb	154	154	14847	node0	secondary
node2	vldb	154	154	14847	node0	secondary
node3	vldb	154	154	14847	node0	secondary

4 entries were displayed.

4. Si vous travaillez dans un environnement SAN, vérifiez que chaque nœud se trouve dans un quorum SAN :

```
cluster kernel-service show
```

```
cluster1::*> cluster kernel-service show
```

Master	Cluster	Quorum	Availability
Operational			
Node	Node	Status	Status
cluster1-01	cluster1-01	in-quorum	true
operational	cluster1-02	in-quorum	true
operational			

2 entries were displayed.

Informations associées

["Administration du système"](#)

Vérifier que le basculement automatique non planifié est activé (configurations MetroCluster FC uniquement)

Si votre cluster est dans une configuration FC MetroCluster, vérifiez que le basculement automatique non planifié est activé après la mise à niveau de ONTAP.

Si vous utilisez une configuration MetroCluster IP, ignorez cette procédure.

Étapes

1. Vérifier si le basculement automatique non planifié est activé :

```
metrocluster show
```

Si le basculement automatique non planifié est activé, l'instruction suivante apparaît dans la sortie de la commande :

```
AUSO Failure Domain  auso-on-cluster-disaster
```

2. Si l'instruction ne s'affiche pas, activez un basculement automatique non planifié :

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster
```

3. Vérifier qu'un basculement automatique non planifié a été activé :

```
metrocluster show
```

Informations associées

["Gestion des disques et des agrégats"](#)

Vérifiez que toutes les LIF se trouvent sur des ports de base après la mise à niveau de ONTAP

Au cours du redémarrage qui se produit dans le cadre du processus de mise à niveau de ONTAP, certaines LIF peuvent être migrées de leurs ports de base vers les ports de basculement qui leur sont attribués. Après une mise à niveau, vous devez activer et restaurer les LIF qui ne se trouvent pas sur leurs ports de base.

Étapes

1. Afficher le statut de toutes les LIFs :

```
network interface show -fields home-port,curr-port
```

Si **Status Admin** est "down" ou **is home** est "false" pour n'importe quelle LIF, passez à l'étape suivante.

2. Activation des LIFs de données :

```
network interface modify {-role data} -status-admin up
```

3. Rerestaurer les LIF sur leurs home ports :

```
network interface revert *
```

4. Vérifier que toutes les LIFs se trouvent sur leurs ports de type home :

```
network interface show
```

Cet exemple montre que toutes les LIFs pour SVM vs0 sont sur leurs ports de base.

```
cluster1::> network interface show -vserver vs0
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs0	data001	up/up	192.0.2.120/24	node0	e0e	true
	data002	up/up	192.0.2.121/24	node0	e0f	true
	data003	up/up	192.0.2.122/24	node0	e2a	true
	data004	up/up	192.0.2.123/24	node0	e2b	true
	data005	up/up	192.0.2.124/24	node1	e0e	true
	data006	up/up	192.0.2.125/24	node1	e0f	true
	data007	up/up	192.0.2.126/24	node1	e2a	true
	data008	up/up	192.0.2.127/24	node1	e2b	true

8 entries were displayed.

Configurations spéciales

Considérations spéciales après une mise à niveau de ONTAP

Si votre cluster est configuré avec l'une des fonctionnalités suivantes, vous devrez peut-être effectuer des étapes supplémentaires après la mise à niveau du logiciel ONTAP.

Demandez-vous...	Si votre réponse est oui, alors faites ceci...
Ai-je effectué une mise à niveau de ONTAP 9.7 ou version antérieure vers ONTAP 9.8 ou version ultérieure ?	Vérifiez la configuration de votre réseau Supprimez le service EMS LIF des stratégies de service réseau qui n'offrent pas de reachiité à la destination EMS
Mon cluster se trouve-t-il dans une configuration MetroCluster ?	Vérifiez l'état de votre réseau et de votre stockage

Demandez-vous...	Si votre réponse est oui, alors faites ceci...
Disposez-vous d'une configuration SAN ?	Vérifiez la configuration de votre SAN
Ai-je effectué une mise à niveau à partir de ONTAP 9.3 ou d'une version antérieure et utilise-t-il le chiffrement du stockage NetApp ?	Reconfigurer les connexions des serveurs KMIP
Ai-je des miroirs de partage de charge ?	Transférez les volumes source des miroirs de partage de charge déplacés
Existe-t-il des comptes utilisateur pour l'accès au processeur de service créés avant ONTAP 9.9 ?	Vérifiez la modification des comptes pouvant accéder au Service Processor

Vérifiez votre configuration réseau après une mise à niveau ONTAP à partir de ONTAP 9.7x ou version antérieure

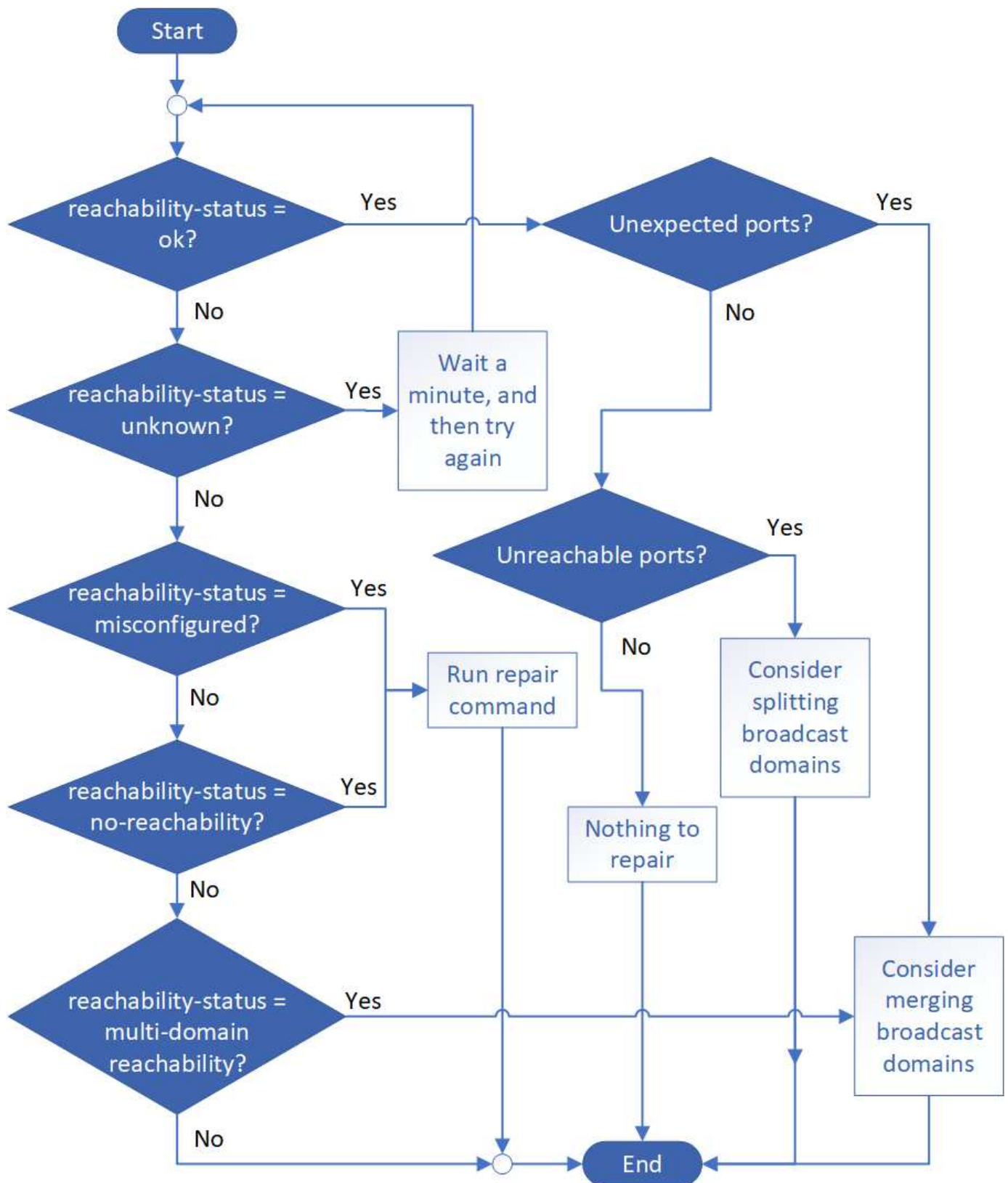
Après avoir effectué la mise à niveau de ONTAP 9.7x ou une version antérieure vers ONTAP 9.8 ou une version ultérieure, vous devez vérifier la configuration de votre réseau. Après la mise à niveau, ONTAP surveille automatiquement l'accessibilité de la couche 2.

Étape

1. Vérifiez que chaque port est joignable par rapport au domaine de diffusion attendu :

```
network port reachability show -detail
```

La sortie de la commande contient les résultats de l'accessibilité. Utilisez l'arbre décisionnel et le tableau ci-dessous pour comprendre les résultats de l'accessibilité (état-accessibilité) et déterminer ce que, le cas échéant, faire ensuite.



état-accessibilité	Description
--------------------	-------------

ok	<p>Le port a une capacité de réachabilité de couche 2 à son domaine de diffusion attribué.</p> <p>Si l'état de la capacité d'accessibilité est « ok », mais qu'il y a des « ports inattendus », envisagez de fusionner un ou plusieurs domaines de diffusion. Pour plus d'informations, voir "Fusionner les domaines de diffusion".</p> <p>Si le statut de la capacité d'accessibilité est « ok », mais qu'il y a des « ports inaccessibles », envisagez de diviser un ou plusieurs domaines de diffusion. Pour plus d'informations, voir "Séparer les domaines de diffusion".</p> <p>Si l'état de la capacité de reprise est « ok » et qu'il n'y a pas de ports inattendus ou inaccessibles, votre configuration est correcte.</p>
mauvaise configuration de la capacité de réachabilité	<p>Le port n'a pas la capacité de reachcapacité de couche 2 à son domaine de diffusion affecté ; cependant, le port a une capacité de reachcapacité de couche 2 à un domaine de diffusion différent.</p> <p>Vous pouvez réparer l'accessibilité du port. Lorsque vous exécutez la commande suivante, le système affecte le port au broadcast domain auquel il a la capacité de reachcapacité :</p> <pre>network port reachability repair -node -port</pre> <p>Pour plus d'informations, voir "Réparation de l'accessibilité de l'orifice".</p>
sans trabilité	<p>Le port n'a pas la possibilité de reachcapacité de couche 2 à un domaine de diffusion existant.</p> <p>Vous pouvez réparer l'accessibilité du port. Lorsque vous exécutez la commande suivante, le système affecte le port à un nouveau domaine de diffusion créé automatiquement dans l'IPspace par défaut :</p> <pre>network port reachability repair -node -port</pre> <p>Pour plus d'informations, voir "Réparation de l'accessibilité de l'orifice".</p>
accessibilité multi-domaines	<p>Le port a une capacité de réachabilité de couche 2 à son domaine de diffusion attribué ; cependant, il a également la possibilité de reachcapacité de couche 2 à au moins un autre domaine de broadcast.</p> <p>Examinez la connectivité physique et la configuration du commutateur pour déterminer si elle est incorrecte ou si le domaine de diffusion attribué au port doit être fusionné avec un ou plusieurs domaines de diffusion.</p> <p>Pour plus d'informations, voir "Fusionner les domaines de diffusion" ou "Réparation de l'accessibilité de l'orifice".</p>
inconnu	<p>Si l'état de la capacité d'accessibilité est « inconnu », attendez quelques minutes et essayez à nouveau la commande.</p>

Une fois que vous avez réparé un port, vous devez vérifier et résoudre les LIFs et les VLAN déplacés. Si le port faisait partie d'un groupe d'interfaces, vous devez également connaître ce qui s'est passé pour ce groupe.

Pour plus d'informations, voir ["Réparation de l'accessibilité de l'orifice"](#).

Supprimez le service LIF EMS des stratégies de service réseau

Si vous disposez de messages EMS (Event Management System) configurés avant la mise à niveau de ONTAP 9.7 ou version antérieure à ONTAP 9.8 ou version ultérieure, après la mise à niveau, il se peut que les messages EMS ne soient pas envoyés.

Au cours de la mise à niveau, management-ems, qui est le service EMS LIF, est ajouté à toutes les stratégies de service existantes. Cela permet d'envoyer des messages EMS depuis n'importe laquelle des LIFs associées à l'une des stratégies de service. Si la LIF sélectionnée n'a pas l'accessibilité à la destination de notification d'événement, le message n'est pas transmis.

Pour éviter cela, après la mise à niveau, vous devez supprimer le service EMS LIF des stratégies de service réseau qui ne permettent pas de reachabilité à la destination.

Étapes

1. Identifier les LIFs et les stratégies de service réseau associées via lesquelles les messages EMS peuvent être envoyés :

```
network interface show -fields service-policy -services management-ems
```

vserver	lif	service-policy
cluster-1	cluster_mgmt	
		default-management
cluster-1	node1-mgmt	
		default-management
cluster-1	node2-mgmt	
		default-management
cluster-1	inter_cluster	
		default-intercluster

4 entries were displayed.

2. Vérifier la connectivité de chaque LIF à la destination EMS :

```
network ping -lif <lif_name> -vserver <svm_name> -destination  
<destination_address>
```

Effectuez cette opération sur chaque nœud.

Exemples

```
cluster-1::> network ping -lif node1-mgmt -vserver cluster-1
-destination 10.10.10.10
10.10.10.10 is alive

cluster-1::> network ping -lif inter_cluster -vserver cluster-1
-destination 10.10.10.10
no answer from 10.10.10.10
```

3. Entrer le niveau de privilège avancé :

```
set advanced
```

4. Pour les LIF qui n'ont pas de accessibilité, supprimer le service LIF management-ems des politiques de service correspondantes :

```
network interface service-policy remove-service -vserver <svm_name>
-policy <service_policy_name> -service management-ems
```

5. Vérifier que la LIF management-ems est désormais uniquement associée aux LIFs qui fournissent une accessibilité à la destination EMS :

```
network interface show -fields service-policy -services management-ems
```

Liens connexes

["LIF et politiques de service dans ONTAP 9.6 et versions ultérieures"](#)

Vérifiez l'état du réseau et du stockage des configurations MetroCluster après une mise à niveau de ONTAP

Après la mise à niveau d'un cluster ONTAP dans une configuration MetroCluster, vérifiez le statut des LIF, des agrégats et des volumes de chaque cluster.

1. Vérifier le statut LIF :

```
network interface show
```

En fonctionnement normal, les LIF des SVM source doivent avoir un statut admin de up et être situées sur leurs home nœuds. Les LIF pour les SVM de destination ne sont pas nécessaires au démarrage ou à l'emplacement de leurs nœuds de base. En cas de basculement, l'état d'administration de toutes les LIF est up, mais il n'est pas nécessaire de les trouver sur les nœuds de base.

```

cluster1::> network interface show

```

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
Cluster					
	cluster1-a1_clus1	up/up	192.0.2.1/24	cluster1-01	e2a
true					
	cluster1-a1_clus2	up/up	192.0.2.2/24	cluster1-01	e2b
true					
cluster1-01					
	clus_mgmt	up/up	198.51.100.1/24	cluster1-01	e3a
true					
	cluster1-a1_inet4_intercluster1	up/up	198.51.100.2/24	cluster1-01	e3c
true					
	...				

27 entries were displayed.

2. Vérifiez l'état des agrégats :

```
storage aggregate show -state !online
```

Cette commande affiche tous les agrégats qui sont *not* online. En fonctionnement normal, tous les agrégats situés sur le site local doivent être en ligne. Cependant, si la configuration MetroCluster est en basculement, les agrégats root du site de reprise sur incident sont autorisés à être hors ligne.

Cet exemple montre un cluster en fonctionnement normal :

```

cluster1::> storage aggregate show -state !online
There are no entries matching your query.

```

Cet exemple montre un cluster en basculement, dans lequel les agrégats racine du site de reprise après

incident sont hors ligne :

```
cluster1::> storage aggregate show -state !online
Aggregate      Size Available Used% State   #Vols  Nodes      RAID
Status
-----
aggr0_b1
      0B      0B    0% offline    0 cluster2-01
raid_dp,
mirror
degraded
aggr0_b2
      0B      0B    0% offline    0 cluster2-02
raid_dp,
mirror
degraded
2 entries were displayed.
```

3. Vérifier l'état des volumes :

```
volume show -state !online
```

Cette commande affiche tous les volumes qui sont *not* online.

Si la configuration MetroCluster fonctionne normalement (sans basculement), le résultat doit afficher tous les volumes appartenant aux SVM secondaires du cluster (ceux portant le nom de SVM ajouté à « -mc »).

Ces volumes sont uniquement en ligne en cas de basculement.

Cet exemple montre un cluster en fonctionnement normal, dans lequel les volumes du site de reprise ne sont pas en ligne.

```
cluster1::> volume show -state !online
(volume show)
Vserver   Volume      Aggregate    State    Type    Size
Available Used%
-----
vs2-mc    vol1         aggr1_b1     -        RW      -
-         -
vs2-mc    root_vs2     aggr0_b1     -        RW      -
-         -
vs2-mc    vol2         aggr1_b1     -        RW      -
-         -
vs2-mc    vol3         aggr1_b1     -        RW      -
-         -
vs2-mc    vol4         aggr1_b1     -        RW      -
-         -
5 entries were displayed.
```

4. Vérifiez qu'il n'y a pas de volumes incohérents :

```
volume show -is-inconsistent true
```

Consultez l'article de la base de connaissances ["Volume affichant des WAFL incohérentes"](#) sur la manière de traiter les volumes incohérents.

Vérifiez la configuration SAN après une mise à niveau

Après une mise à niveau de ONTAP, dans un environnement SAN, vérifiez que chaque initiateur ayant été connecté à une LIF avant que la mise à niveau ne se reconnecte à la LIF.

1. Vérifiez que chaque initiateur est connecté au LIF correct.

Vous devez comparer la liste des initiateurs à la liste que vous avez faite lors de la préparation de la mise à niveau. Si vous exécutez ONTAP 9.11.1 ou une version ultérieure, utilisez System Manager pour afficher l'état de la connexion, car l'affichage est plus clair que celui de l'interface de ligne de commande.

System Manager

- a. Dans System Manager, cliquez sur **hôtes > groupes initiateurs SAN**.

La page affiche la liste des groupes initiateurs. Si la liste est grande, vous pouvez afficher des pages supplémentaires de la liste en cliquant sur les numéros de page dans le coin inférieur droit de la page.

Les colonnes affichent diverses informations sur les igroups. Depuis 9.11.1, l'état de connexion du groupe initiateur est également affiché. Passez le curseur sur les alertes d'état pour afficher les détails.

CLI

- Lister les initiateurs iSCSI :

```
iscsi initiator show -fields igroup,initiator-name,tpgroup
```

- Lister les initiateurs FC :

```
fcip initiator show -fields igroup,wwpn,lif
```

Reconfigurez les connexions de serveur KMIP après une mise à niveau à partir de ONTAP 9.2 ou d'une version antérieure

Après la mise à niveau de ONTAP 9.2 ou d'une version antérieure vers ONTAP 9.3 ou version ultérieure, vous devez reconfigurer les connexions au serveur de gestion externe des clés (KMIP).

Étapes

1. Configurez la connectivité du gestionnaire de clés :

```
security key-manager setup
```

2. Ajoutez vos serveurs KMIP :

```
security key-manager add -address <key_management_server_ip_address>
```

3. Vérifiez que les serveurs KMIP sont connectés :

```
security key-manager show -status
```

4. Interroger les serveurs de clés :

```
security key-manager query
```

5. Créez une nouvelle clé d'authentification et une nouvelle phrase secrète :

```
security key-manager create-key -prompt-for-key true
```

La phrase de passe doit comporter au moins 32 caractères.

6. Interroger la nouvelle clé d'authentification :

```
security key-manager query
```

7. Attribuez la nouvelle clé d'authentification à vos disques à autochiffrement (SED) :

```
storage encryption disk modify -disk <disk_ID> -data-key-id <key_ID>
```



Assurez-vous d'utiliser la nouvelle clé d'authentification de votre requête.

8. Si nécessaire, attribuez une clé FIPS aux disques SED :

```
storage encryption disk modify -disk <disk_id> -fips-key-id  
<fips_authentication_key_id>
```

Si votre configuration de sécurité exige que vous utilisiez des clés différentes pour l'authentification des données et l'authentification FIPS 140-2, vous devez créer une clé distincte pour chacune d'elles. Si ce n'est pas le cas, vous pouvez utiliser la même clé d'authentification pour la conformité FIPS que celle utilisée pour l'accès aux données.

Transfert des volumes source miroir de partage de charge déplacés après une mise à niveau de ONTAP

Après la mise à niveau de ONTAP, vous devez déplacer de nouveau les volumes source miroir de partage de charge vers leurs emplacements de pré-mise à niveau.

Étapes

1. Identifiez l'emplacement vers lequel vous déplacez le volume source du miroir de partage de charge en utilisant l'enregistrement que vous avez créé avant de déplacer le volume source du miroir de partage de charge.
2. Déplacez le volume source miroir de partage de charge à son emplacement d'origine :

```
volume move start
```

Modifier les comptes utilisateur pouvant accéder au Service Processor

Si vous avez créé des comptes utilisateur dans ONTAP 9.8 ou une version antérieure pouvant accéder au processeur de service avec un rôle non administrateur et que vous effectuez une mise à niveau vers ONTAP 9.9.1 ou une version ultérieure, toute valeur non administrateur dans `-role` le paramètre est modifié en `admin`.

Pour plus d'informations, voir ["Comptes pouvant accéder au processeur de service"](#).

Mettez à jour le package de qualification de disque

Après la mise à niveau du logiciel ONTAP, téléchargez et installez le DQP (ONTAP Disk qualification Package). Le DQP n'a pas été mis à jour dans le cadre d'une mise à niveau ONTAP.

Le DQP contient les paramètres appropriés pour l'interaction ONTAP avec tous les nouveaux lecteurs qualifiés. Si votre version du DQP ne contient pas d'informations sur un lecteur nouvellement qualifié, ONTAP ne dispose pas des informations nécessaires pour configurer correctement le lecteur.

Il est recommandé de mettre à jour le DQP tous les trimestres. Vous devez également mettre à jour le DQP pour les raisons suivantes :

- Chaque fois que vous ajoutez un nouveau type ou une nouvelle taille de disque à un nœud de votre cluster

Par exemple, si vous avez déjà des disques de 1 To et que vous ajoutez des disques de 2 To, vous devez vérifier la dernière mise à jour du DQP.

- Chaque fois que vous mettez à jour le micrologiciel du disque
- Chaque fois que les fichiers de firmware ou de DQP sont plus récents

Informations associées

- ["Téléchargements NetApp : pack de qualification des disques"](#)
- ["Téléchargements NetApp : firmware de disque"](#)

Des mises à jour du firmware et du système

Présentation des mises à jour du firmware et du système

Selon votre version de ONTAP, vous pouvez activer les mises à jour automatiques du micrologiciel et du système.

Version ONTAP	Ce qui est inclus dans les mises à jour automatiques
9.13.1 et versions ultérieures	<ul style="list-style-type: none">• Base de données fuseau horaire ONTAP• Micrologiciel de stockage pour les périphériques de stockage, les disques et les tiroirs disques• Micrologiciel SP/BMC pour les processeurs de service et les modules BMC

Version ONTAP	Ce qui est inclus dans les mises à jour automatiques
9.10.1 et versions ultérieures	<ul style="list-style-type: none"> • Micrologiciel de stockage pour les périphériques de stockage, les disques et les tiroirs disques • Micrologiciel SP/BMC pour les processeurs de service et les modules BMC
9.9.1 et versions antérieures	Non pris en charge

Si vous utilisez ONTAP 9.9.1 ou une version antérieure, ou si vous ne l'avez pas ["mises à jour automatiques du système"](#) activé, c'est possible ["effectuez les mises à jour de micrologiciel manuellement"](#).

Si vous utilisez ONTAP 9.12.1 ou une version antérieure, ou si vous ne l'avez pas ["mises à jour automatiques du système"](#) Activé, vous pouvez mettre à jour manuellement la base de données des fuseaux horaires. Consultez l'article de la base de connaissances, ["Comment mettre à jour les informations de fuseau horaire dans ONTAP 9"](#), pour plus de détails.

Vidéo : fonction de mise à jour automatique du micrologiciel

Jetez un coup d'œil à la fonction de mise à jour automatique du micrologiciel disponible à partir de ONTAP 9.10.1.



La planification des mises à jour automatiques pour l'installation

Tous les nœuds éligibles au sein d'un même cluster sont regroupés pour des mises à jour automatiques. La période pendant laquelle les nœuds éligibles sont programmés pour une mise à jour automatique varie en fonction du niveau de priorité de la mise à jour et du pourcentage de systèmes dans votre environnement qui nécessitent cette mise à jour.

Par exemple, si 10 % ou moins de vos systèmes sont admissibles à une mise à jour non prioritaire, la mise à jour est prévue pour tous les systèmes admissibles dans un délai d'une semaine. Toutefois, si 76 % ou plus de vos systèmes sont admissibles à une mise à jour non prioritaire, la mise à jour est échelonnée sur les systèmes admissibles au cours des 8 semaines. Cette installation échelonnée permet de réduire les risques pour l'ensemble de votre environnement en cas de problème avec une mise à jour qui doit être résolue.

Le pourcentage de vos systèmes totaux prévus pour les mises à jour automatiques par semaine est le suivant :

Pour les mises à jour critiques

% de systèmes nécessitant une mise à jour	% de mises à jour effectuées la semaine 1	% de mises à jour effectuées la semaine 2
50 % ou moins	100 %	
50 à 100 %	30 %	70 %

Pour les mises à jour prioritaires

% de systèmes nécessitant une mise à jour	% de mises à jour effectuées par semaine			
	semaine 1	semaine 2	semaine 3	semaine 4
25 % ou moins	100 %			
26-50%	30 %	70 %		
50-100%	10 %	20 %	30 %	40 %

Pour les mises à jour de priorité normales

% de systèmes nécessitant une mise à jour	% de mises à jour effectuées par semaine							
	semaine 1	semaine 2	semaine 3	semaine 4	semaine 5	semaine 6	semaine 7	semaine 8
10 % ou moins	100 %							
11-20%	30 %	70 %						
21-50%	10 %	20 %	30 %	40 %				
51-75%	5 %	10 %	15 %	20 %	20 %	30 %		
76-100%	5 %	5 %	10 %	10 %	15 %	15 %	20 %	20 %

Activer les mises à jour automatiques

Depuis ONTAP 9.10.1, vous pouvez activer les mises à jour automatiques pour permettre

à ONTAP de télécharger et d'installer des mises à jour de micrologiciel sans votre intervention.

Depuis ONTAP 9.13.1, ces mises à jour automatiques incluent également des mises à jour automatiques de la base de données de fuseaux horaires.

Avant de commencer

Vous devez disposer d'un support en cours. Ceci peut être validé sur le ["Site de support NetApp"](#) Dans la page **Détails du système**.

Description de la tâche

Pour activer les mises à jour automatiques, vous devez d'abord activer AutoSupport avec HTTPS. Si AutoSupport n'est pas activé sur votre cluster ou si AutoSupport est activé sur votre cluster avec un autre protocole de transport, vous aurez la possibilité de l'activer avec HTTPS au cours de cette procédure.

Étapes

1. Dans System Manager, cliquez sur **Events**.
2. Dans la section **Présentation**, en regard de **Activer la mise à jour automatique**, cliquez sur **actions>Activer**.
3. Si AutoSupport avec HTTPS n'est pas activé, sélectionnez pour l'activer.
4. Acceptez les conditions générales et sélectionnez **Enregistrer**.


Informations associées

["Dépanner la distribution des messages AutoSupport via HTTP ou HTTPS"](#)

Modifier les mises à jour automatiques

Lorsque les mises à jour automatiques sont activées, par défaut, ONTAP détecte, télécharge et installe automatiquement toutes les mises à jour de micrologiciel recommandées et, à partir de ONTAP 9.13.1, les mises à jour de la base de données de fuseau horaire ONTAP. Si vous souhaitez afficher les mises à jour recommandées avant qu'elles ne soient installées, ou si vous souhaitez que les recommandations soient automatiquement rejetées, vous pouvez modifier le comportement par défaut selon vos préférences.

Étapes

1. Dans System Manager, cliquez sur **Cluster > Paramètres**.
2. Dans la section **mise à jour automatique**, cliquez sur  pour afficher la liste des actions.
3. Cliquez sur **Modifier les paramètres de mise à jour automatique**.
4. Spécifiez les actions par défaut à effectuer pour chaque type d'événement.

Vous pouvez choisir de mettre à jour, d'afficher les notifications ou de rejeter automatiquement les mises à jour pour chaque type d'événement.






La base de données ONTAP Time zone est contrôlée par le type d'événement FICHIERS SYSTÈME.

Gérer les mises à jour automatiques recommandées

Le journal de mise à jour automatique affiche une liste de recommandations de mise à jour et des détails sur chacune d'elles, y compris une description, une catégorie, l'heure planifiée à installer, l'état et les erreurs éventuelles. Vous pouvez afficher le journal, puis décider de l'action que vous souhaitez effectuer pour chaque recommandation.

Étapes

1. Afficher la liste des recommandations :

Afficher à partir des paramètres du cluster	Afficher dans l'onglet mise à jour du micrologiciel
<ol style="list-style-type: none">a. Cliquez sur Cluster > Paramètres.b. Dans la section mise à jour automatique, cliquez sur , puis sur Afficher toutes les mises à jour automatiques.	<ol style="list-style-type: none">a. Cliquez sur Cluster > Présentation.b. Dans la section Présentation, cliquez sur plus , puis sur mise à jour ONTAP.c. Sélectionnez l'onglet Firmware Update.d. Dans l'onglet mise à jour du micrologiciel, cliquez sur plus , puis sur Afficher toutes les mises à jour automatiques.

2. Cliquez sur  en regard de la description pour afficher la liste des actions que vous pouvez effectuer sur la recommandation.

Vous pouvez effectuer l'une des actions suivantes, selon l'état de la recommandation :

Si la mise à jour est à cet état...	Vous pouvez...
N'a pas été planifié	Mise à jour : démarre le processus de mise à jour. Programme : permet de définir une date pour le début du processus de mise à jour. Rejeter : supprime la recommandation de la liste.
A été programmé	Mise à jour : démarre le processus de mise à jour. Modifier le calendrier : permet de modifier la date planifiée pour le début du processus de mise à jour. Annuler l'horaire : annule la date programmée.
A été rejeté	Unlicense : renvoie la recommandation à la liste.
Est en cours d'application ou est en cours de téléchargement	Annuler : annule la mise à jour.

Mettre à jour le micrologiciel manuellement

À partir de ONTAP 9.9.1, si vous êtes enregistré auprès de ["Active IQ Unified Manager"](#), Vous pouvez recevoir des alertes dans System Manager qui vous informent lorsque des mises à jour de micrologiciel pour les périphériques pris en charge, tels que les disques, les tiroirs disques, le processeur de service (SP) ou le contrôleur BMC (Baseboard Management Controller) sont en attente sur le cluster.

Si vous exécutez ONTAP 9.8 ou si vous n'êtes pas enregistré auprès de Active IQ Unified Manager, vous pouvez accéder au site du support NetApp pour télécharger les mises à jour du firmware.

Avant de commencer

Pour préparer une mise à jour du micrologiciel en douceur, redémarrez le SP ou le BMC avant le début de la mise à jour. Vous pouvez utiliser le `system service-processor reboot-sp -node node_name` commande de redémarrage.

Étapes

Suivez la procédure appropriée en fonction de votre version de ONTAP et si vous êtes enregistré auprès de Active IQ Unified Manager.

ONTAP 9.9.1 et versions ultérieures avec Active IQ

1. Dans System Manager, accédez à **Dashboard**.


Dans la section **Santé**, un message s'affiche si des mises à jour de micrologiciel sont recommandées pour le cluster.

2. Cliquez sur le message d'alerte.

L'onglet **Firmware Update** s'affiche dans la page **Update**.


3. Cliquez sur **Télécharger depuis le site de support NetApp** pour obtenir la mise à jour du firmware que vous souhaitez effectuer.

Le site de support NetApp s'affiche.

4. Connectez-vous au site du support NetApp et téléchargez le pack d'images du firmware nécessaire à la mise à jour.
5. Copiez les fichiers sur un serveur HTTP ou FTP de votre réseau ou dans un dossier local.
6. Dans System Manager, cliquez sur **Cluster > Overview**.
7. Dans le coin droit du volet **vue d'ensemble**, cliquez sur **plus**  et sélectionnez **mise à jour ONTAP**.
8. Cliquez sur **mise à jour du micrologiciel**.
9. Selon votre version de ONTAP, procédez comme suit :

ONTAP 9.9.1 et 9.10.0	ONTAP 9.10.1 et versions ultérieures
<ol style="list-style-type: none">a. Sélectionnez dans serveur ou client localb. Indiquez l'URL du serveur ou l'emplacement du fichier.	<ol style="list-style-type: none">a. Dans la liste des mises à jour recommandées, sélectionnez actions.b. Cliquez sur mettre à jour pour installer la mise à jour immédiatement ou sur planifier pour la programmer ultérieurement. Si la mise à jour est déjà programmée, vous pouvez la modifier ou la Annuler.c. Sélectionnez le bouton mettre à jour le micrologiciel.

ONTAP 9.8 et versions ultérieures sans Active IQ

1. Accédez au "[Site de support NetApp](#)" et connectez-vous.
2. Sélectionnez le pack firmware à utiliser pour la mise à jour du firmware du cluster.
3. Copiez les fichiers sur un serveur HTTP ou FTP de votre réseau ou dans un dossier local.
4. Dans System Manager, cliquez sur **Cluster > Overview**.
5. Dans le coin droit du volet **vue d'ensemble**, cliquez sur **plus**  et sélectionnez **mise à jour ONTAP**.
6. Cliquez sur **mise à jour du micrologiciel**.
7. Selon votre version de ONTAP, procédez comme suit :

ONTAP 9.8, 9.9.1 et 9.10.0	ONTAP 9.10.1 et versions ultérieures
<ol style="list-style-type: none"> 1. Sélectionnez dans serveur ou client local 2. Indiquez l'URL du serveur ou l'emplacement du fichier. 	<ol style="list-style-type: none"> 1. Dans la liste des mises à jour recommandées, sélectionnez actions. 2. Cliquez sur mettre à jour pour installer la mise à jour immédiatement ou sur planifier pour la programmer ultérieurement. Si la mise à jour est déjà programmée, vous pouvez la modifier ou la Annuler. 3. Sélectionnez le bouton mettre à jour le micrologiciel.

Une fois que vous avez terminé

Vous pouvez surveiller ou vérifier les mises à jour sous **Résumé des mises à jour du micrologiciel**. Pour afficher les mises à jour qui ont été rejetées ou qui n'ont pas pu être installées, cliquez sur **Cluster > Paramètres > mise à jour automatique > Afficher toutes les mises à jour automatiques**.

Restaurez la ONTAP

Rétablir la vue d'ensemble de la ONTAP

Pour effectuer la transition d'un cluster vers une version antérieure de ONTAP, vous devez effectuer une nouvelle version.

Les informations de cette section vous guideront dans les étapes à suivre avant et après votre retour, y compris les ressources que vous devez lire et les vérifications préalables et postérieures à la restauration que vous devez effectuer.



Si vous devez migrer un cluster d'ONTAP 9.1 vers ONTAP 9.0, vous devez suivre la procédure de restauration décrite ["ici"](#).

Ai-je besoin d'une assistance technique pour rétablir le service ?

Vous pouvez revenir aux clusters de test ou aux nouveaux clusters sans assistance. Contactez le support technique pour rétablir les clusters de production. Si vous rencontrez l'un des problèmes suivants, appelez le support technique :

- Vous êtes dans un environnement de production et la restauration échoue, ou vous rencontrez des problèmes avant ou après la restauration :
 - Le processus de restauration a échoué et ne peut pas se terminer.
 - Le processus de restauration est terminé, mais le cluster est inutilisable dans un environnement de production.
 - Le processus de restauration se termine et le cluster passe en production, mais vous n'êtes pas satisfait de son comportement.
- Vous avez créé des volumes dans ONTAP 9.5 ou version ultérieure et vous devez restaurer une version

antérieure. Les volumes qui utilisent la compression adaptative doivent être décompressés avant le rétablissement.

Rétablir les chemins

La version du ONTAP que vous pouvez restaurer varie en fonction de la version du ONTAP actuellement exécutée sur vos nœuds. Vous pouvez utiliser le `system image show` Commande permettant de déterminer la version de ONTAP exécutée sur chaque nœud.

Ces directives ne concernent que les versions ONTAP sur site. Pour plus d'informations sur le rétablissement d'ONTAP dans le cloud, consultez ["Restauration ou rétrogradation de Cloud Volumes ONTAP"](#).

Vous pouvez revenir à...	Pour...
ONTAP 9.15.1	ONTAP 9.14.1
ONTAP 9.14.1	ONTAP 9.13.1
ONTAP 9.13.1	ONTAP 9.12.1
ONTAP 9.12.1	ONTAP 9.11.1
ONTAP 9.11.1	ONTAP 9.10.1
ONTAP 9.10.1	ONTAP 9.9.1
ONTAP 9.9.1	ONTAP 9.8
ONTAP 9.8	ONTAP 9.7
ONTAP 9.7	ONTAP 9.6
ONTAP 9.6	ONTAP 9.5
ONTAP 9.5	ONTAP 9.4
ONTAP 9.4	ONTAP 9.3
ONTAP 9.3	ONTAP 9.2
ONTAP 9.2	ONTAP 9.1
ONTAP 9.1 ou ONTAP 9	Data ONTAP 8.3.x



Si vous devez passer de ONTAP 9.1 à 9.0, vous devez suivre la ["processus de rétrogradation"](#) documentation ici.

Que dois-je lire avant de revenir à la version précédente ?

Ressources à consulter avant de revenir en arrière

Avant de rétablir ONTAP, il est conseillé de confirmer le support matériel et de vérifier les ressources pour identifier les problèmes susceptibles de se produire ou doivent être résolus.

1. Vérifiez le ["Notes de mise à jour de ONTAP 9"](#) pour la version cible.

La section « mises en garde importantes » décrit les problèmes potentiels que vous devez connaître avant la rétrogradation ou le rétablissement.

2. Vérifiez que la plateforme matérielle est prise en charge dans la version cible.

["NetApp Hardware Universe"](#)

3. Vérifier que votre cluster et les commutateurs de gestion sont pris en charge dans la version cible.

Vous devez vérifier que les versions du logiciel NX-OS (commutateurs réseau en cluster), IOS (commutateurs de réseau de gestion) et RCF (fichier de configuration de référence) sont compatibles avec la version de ONTAP vers laquelle vous procédez à un rétablissement.

["Téléchargements NetApp : commutateur Ethernet Cisco"](#)

4. Si votre cluster est configuré pour SAN, vérifiez que la configuration SAN est entièrement prise en charge.

Tous les composants SAN, y compris la version du logiciel ONTAP cible, le système d'exploitation hôte et les correctifs, les logiciels utilitaires hôtes requis et les pilotes d'adaptateur et les firmwares, doivent être pris en charge.

["Matrice d'interopérabilité NetApp"](#)

Ne tenez pas compte des considérations

Vous devez tenir compte des problèmes et des limites de restauration avant de commencer une nouvelle version de ONTAP.

- La nouvelle version est perturbatrice.

Aucun accès client ne peut se produire lors de la nouvelle version. Si vous restaurez d'un cluster de production, veillez à inclure cette interruption dans votre planification.

- La nouvelle version affecte tous les nœuds du cluster.

La nouvelle version affecte tous les nœuds du cluster. Cependant, la nouvelle version doit être effectuée sur chaque paire HA avant que les autres paires HA ne soient rétablies.

- La nouvelle version est terminée lorsque tous les nœuds exécutent la nouvelle version cible.

Lorsque le cluster est à l'état de versions mixtes, vous ne devez entrer aucune commande susceptible de modifier l'opération ou la configuration du cluster, sauf si nécessaire pour satisfaire aux exigences de réversion ; les opérations de surveillance sont autorisées.



Si vous avez rétabli une partie des nœuds, mais pas tous, n'essayez pas de mettre à niveau le cluster vers la version source.

- Lorsque vous restaurez un nœud, il efface les données en cache dans un module Flash cache.

Comme aucune donnée en cache n'est disponible dans le module Flash cache, le nœud transmet les demandes de lecture initiales du disque, ce qui réduit les performances de lecture au cours de cette période. Le nœud retransfère le cache au fur et à mesure qu'il transmet les demandes de lecture.

- Un LUN sauvegardé sur bande s'exécutant sur ONTAP 9.x ne peut être restauré qu'avec les versions 9.x et ultérieures, et non vers une version antérieure.
- Si votre version actuelle de ONTAP prend en charge la fonctionnalité ACP intrabande (IBACP), et que vous restaurez à une version de ONTAP qui ne prend pas en charge IBACP, le chemin d'accès alternatif à votre tiroir disque est désactivé.
- Si le protocole LDAP est utilisé par l'un de vos SVM, la référence LDAP doit être désactivée avant de procéder à une nouvelle version.
- Dans les systèmes MetroCluster IP utilisant des commutateurs conformes à la norme MetroCluster, mais non validés par MetroCluster, la nouvelle version de ONTAP 9.7 à 9.6 est perturbatrice car les systèmes utilisant ONTAP 9.6 et versions antérieures ne prennent pas en charge.
- Avant de restaurer un nœud en ONTAP 9.13.1 ou version antérieure, vous devez d'abord convertir un volume racine SVM chiffré en volume non chiffré

Si vous tentez de revenir à une version qui ne prend pas en charge le chiffrement du volume root SVM, le système répondra avec un avertissement et bloquera la retour.

Éléments à vérifier avant de revenir en arrière

Avant de revenir à une version antérieure, vous devez vérifier l'état du cluster, l'état de stockage et l'heure du système. Vous devez également supprimer tous les travaux de cluster en cours d'exécution et mettre fin à toutes les sessions SMB qui ne sont pas disponibles en continu.

Vérification de l'état du cluster

Avant de revenir au cluster, vérifiez que les nœuds sont sains et peuvent participer au cluster, et que le cluster se trouve au quorum.

1. Vérifiez que les nœuds du cluster sont en ligne et peuvent participer au cluster : `cluster show`

```
cluster1::> cluster show
Node                               Health  Eligibility
-----
node0                             true    true
node1                             true    true
```

Si l'un des nœuds est défectueux ou non éligible, vérifiez la présence d'erreurs dans les journaux EMS et effectuez des actions correctives.

2. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

Entrez `y` pour continuer.

3. Vérifier les détails de configuration pour chaque processus RDB

- L'époque de la base de données relationnelle et les séries de tests de base de données doivent correspondre pour chaque nœud.
- Le maître de quorum par anneau doit être le même pour tous les nœuds.

Notez que chaque anneau peut avoir un maître de quorum différent.

Pour afficher ce processus RDB...	Entrez cette commande...
Application de gestion	<code>cluster ring show -unitname mgmt</code>
Base de données d'emplacement de volume	<code>cluster ring show -unitname vldb</code>
Gestionnaire d'interface virtuelle	<code>cluster ring show -unitname vifmgr</code>
Démon de gestion DU SAN	<code>cluster ring show -unitname bcomd</code>

Cet exemple représente le processus de la base de données d'emplacements de volumes :

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch      DB Epoch DB Trnxs Master      Online
-----
node0     vldb      154      154      14847  node0      master
node1     vldb      154      154      14847  node0      secondary
node2     vldb      154      154      14847  node0      secondary
node3     vldb      154      154      14847  node0      secondary
4 entries were displayed.
```

4. Revenir au niveau de privilège admin :

```
set -privilege admin
```

5. Si vous travaillez dans un environnement SAN, vérifiez que chaque nœud se trouve dans un quorum SAN

```
:event log show -severity informational -message-name scsiblade.*
```

Le message d'événement `scsiBlade` le plus récent pour chaque nœud doit indiquer que le SCSI-Blade est quorum.


```
cluster1::*> event log show -severity informational -message-name
scsiblade.*
```

Time	Node	Severity	Event
MM/DD/YYYY TIME	node0	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...
MM/DD/YYYY TIME	node1	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...

Informations associées

["Administration du système"](#)

Vérification de l'état du stockage

Avant de restaurer un cluster, vérifiez l'état de vos disques, agrégats et volumes.

1. Vérification de l'état du disque :

Pour vérifier...	Procédez comme ça...
Disques cassés	a. Afficher les éventuels disques défectueux : <code>storage disk show -state broken</code> b. Retirez ou remplacez tout disque endommagé.
Disques soumis à des opérations de maintenance ou de reconstruction	a. Afficher tous les disques en état de maintenance, en attente ou reconstruction : <code>`storage disk show -state maintenance</code>
pending	<code>reconstructing`</code> .. Attendez la fin de l'opération de maintenance ou de reconstruction avant de poursuivre.

2. Vérifiez que tous les agrégats sont en ligne en affichant l'état du stockage physique et logique, y compris les agrégats de stockage : `storage aggregate show -state !online`

Cette commande affiche les agrégats qui sont *not* online. Tous les agrégats doivent être en ligne avant et après avoir effectué une mise à niveau ou une nouvelle version majeure.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. Vérifiez que tous les volumes sont en ligne en affichant les volumes *NOT* online : `volume show -state !online`

Tous les volumes doivent être en ligne avant et après avoir effectué une mise à niveau ou une nouvelle version majeure.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. Vérifiez qu'il n'y a pas de volumes incohérents : `volume show -is-inconsistent true`

Consultez l'article de la base de connaissances "[Volume affichant des WAFL incohérentes](#)" sur la manière de traiter les volumes incohérents.

Informations associées

["Gestion des disques et des agrégats"](#)

Vérification de l'heure du système

Avant de revenir à une version antérieure, vérifiez que le protocole NTP est configuré et que son heure est synchronisée sur l'ensemble du cluster.

1. Vérifiez que le cluster est associé à un serveur NTP : `cluster time-service ntp server show`
2. Vérifiez que chaque nœud a la même date et l'heure : `cluster date show`

```
cluster1::> cluster date show
Node      Date              Timezone
-----
node0     4/6/2013 20:54:38 GMT
node1     4/6/2013 20:54:38 GMT
node2     4/6/2013 20:54:38 GMT
node3     4/6/2013 20:54:38 GMT
4 entries were displayed.
```

Vérifiez qu'aucune tâche n'est en cours d'exécution

Avant de restaurer le logiciel ONTAP, vous devez vérifier l'état des tâches du cluster. Si des tâches d'agrégat, de volume, NDMP (dump ou restore) ou Snapshot (telles que la création, la suppression, le déplacement, la modification, la réplication, et les travaux de montage) sont en cours d'exécution ou mis en file d'attente, vous devez permettre aux travaux de terminer correctement ou arrêter les entrées en file d'attente.

1. Examinez la liste de toutes les tâches en cours d'exécution ou en file d'attente d'agrégats, de volumes ou de copies Snapshot : `job show`

```
cluster1::> job show
```

Job ID	Name	Owning Vserver	Node	State
8629	Vol Reaper	cluster1	-	Queued
	Description: Vol Reaper Job			
8630	Certificate Expiry Check	cluster1	-	Queued
	Description: Certificate Expiry Check			
.				
.				
.				

2. Supprimez toute tâche en cours d'exécution ou en attente d'agrégats, de volumes ou de copies Snapshot :
- ```
job delete -id job_id
```

```
cluster1::> job delete -id 8629
```

3. Vérifiez qu'aucun travail d'agrégat, de volume ou de Snapshot n'est en cours d'exécution ou mis en file d'attente : `job show`

Dans cet exemple, tous les travaux en cours d'exécution et en file d'attente ont été supprimés :

```
cluster1::> job show
```

| Job ID | Name                                            | Owning Vserver | Node  | State   |
|--------|-------------------------------------------------|----------------|-------|---------|
| 9944   | SnapMirrorDaemon_7_2147484678                   | cluster1       | node1 | Dormant |
|        | Description: Snapmirror Daemon for 7_2147484678 |                |       |         |
| 18377  | SnapMirror Service Job                          | cluster1       | node0 | Dormant |
|        | Description: SnapMirror Service Job             |                |       |         |

2 entries were displayed

## Sessions SMB devant être arrêtées

Avant de procéder à une restauration, vous devez identifier et mettre fin à toutes les sessions SMB qui ne sont pas disponibles en continu.

Les partages SMB disponibles en permanence, auxquels les clients Hyper-V ou Microsoft SQL Server accèdent via le protocole SMB 3.0, n'ont pas à être résiliés avant de procéder à une mise à niveau ou à une rétrogradation.

1. Identifiez toutes les sessions SMB établies qui ne sont pas disponibles en continu : `vserver cifs session show -continuously-available No -instance`

Cette commande affiche des informations détaillées sur les sessions SMB qui ne sont pas disponibles en continu. Vous devez les mettre fin avant de procéder à la mise à niveau vers une version antérieure de ONTAP.

```
cluster1::> vserver cifs session show -continuously-available No
-instance
```

```

 Node: node1
 Vserver: vs1
 Session ID: 1
 Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
 Workstation IP address: 203.0.113.20
 Authentication Mechanism: NTLMv2
 Windows User: CIFS\user1
 UNIX User: nobody
 Open Shares: 1
 Open Files: 2
 Open Other: 0
 Connected Time: 8m 39s
 Idle Time: 7m 45s
 Protocol Version: SMB2_1
 Continuously Available: No
1 entry was displayed.
```

2. Si nécessaire, identifiez les fichiers ouverts pour chaque session SMB que vous avez identifié : `vserver cifs session file show -session-id session_ID`

```
cluster1::> vserver cifs session file show -session-id 1

Node: node1
Vserver: vs1
Connection: 4160072788
Session: 1
File File Open Hosting
Continuously
ID Type Mode Volume Share Available

1 Regular rw vol10 homedirshare No
Path: \TestDocument.docx
2 Regular rw vol10 homedirshare No
Path: \file1.txt
2 entries were displayed.
```

## Authentification intrabande NVMe

Si vous revenez de ONTAP 9.12.1 ou version ultérieure à ONTAP 9.12.0 ou version antérieure, vous devez ["désactivez l'authentification intrabande"](#) avant de revenir. Si l'authentification intrabande à l'aide de DH-HMAC-CHAP n'est pas désactivée, le retour échoue.

## Que dois-je vérifier d'autre avant de revenir ?

### Vérifications préalables

Selon votre environnement, vous devez tenir compte de certains facteurs avant de revenir à la version précédente. Commencez par consulter le tableau ci-dessous pour connaître les considérations particulières à prendre en compte.

| Demandez-vous...                                    | Si votre réponse est oui, alors faites ceci...                                                                                                                                                                                                                               |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mon cluster exécute-t-il SnapMirror ?               | <ul style="list-style-type: none"> <li>• <a href="#">Considérations relatives à l'inversion de systèmes avec relations synchrones SnapMirror</a></li> <li>• <a href="#">Examinez les exigences de nouvelle version pour les relations SnapMirror et SnapVault</a></li> </ul> |
| Mon cluster exécute-t-il SnapLock ?                 | <a href="#">Définir des périodes de validation automatique</a>                                                                                                                                                                                                               |
| Est-ce que je possède des volumes Split FlexClone ? | <a href="#">Inverser le partage de bloc physique</a>                                                                                                                                                                                                                         |
| Est-ce que je possède des volumes FlexGroup ?       | <a href="#">Désactiver la fonctionnalité qtree</a>                                                                                                                                                                                                                           |
| Ai-je des serveurs CIFS en mode Workgroups ?        | <a href="#">Déplacer ou supprimer des serveurs CIFS en mode groupe de travail</a>                                                                                                                                                                                            |
| Possède-je des volumes dédupliqués ?                | <a href="#">Vérifiez que le volume contient suffisamment d'espace libre</a>                                                                                                                                                                                                  |

| Demandez-vous...                                                                                    | Si votre réponse est oui, alors faites ceci...                                                |
|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Ai-je des copies Snapshot ?                                                                         | <a href="#">Préparer des copies Snapshot</a>                                                  |
| Est-ce que je suis en train de revenir à ONTAP 8.3.x ?                                              | <a href="#">Identifiez les comptes utilisateur qui utilisent la fonction de hachage SHA-2</a> |
| La protection contre les ransomwares est-elle configurée pour ONTAP 9.11.1 ou version ultérieure ?  | <a href="#">Vérifiez les licences anti-ransomwares</a>                                        |
| L'accès multiprotocole S3 est-il configuré pour ONTAP 9.12.1 ou version ultérieure ?                | <a href="#">Supprimez la configuration des compartiments NAS S3</a>                           |
| La mise en circuit de session NFSv4.1 est-elle configurée pour ONTAP 9.14.1 ou version ultérieure ? | <a href="#">Supprimer la configuration de partage de session NFSv4.1</a>                      |

### Vérifications préliminaires de MetroCluster

En fonction de la configuration de MetroCluster, vous devez tenir compte de certains facteurs avant de procéder à une restauration. Commencez par consulter le tableau ci-dessous pour connaître les considérations particulières à prendre en compte.

| Demandez-vous...                                                                                                                       | Si votre réponse est oui, alors faites ceci...                        |
|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| Dois-je disposer d'une configuration MetroCluster à deux ou quatre nœuds ?                                                             | <a href="#">Désactivation du basculement automatique non planifié</a> |
| Ai-je une configuration MetroCluster IP ou Fabric-Attached à quatre ou huit nœuds qui exécute ONTAP 9.12.1 ou une version ultérieure ? | <a href="#">Désactiver IPsec</a>                                      |

### SnapMirror

#### Considérations relatives à l'inversion de systèmes avec relations synchrones SnapMirror

Vous devez connaître les considérations relatives aux relations synchrones SnapMirror avant de revenir de ONTAP 9.6 à ONTAP 9.5.

Avant d'effectuer le rétablissement, vous devez effectuer les étapes suivantes si vous avez des relations SnapMirror synchrones :

- Vous devez supprimer toute relation synchrone SnapMirror dans laquelle le volume source diffuse des données via NFSv4 ou SMB.

ONTAP 9.5 ne prend pas en charge NFSv4 et SMB.

- Vous devez supprimer toutes les relations SnapMirror synchrones dans un déploiement en cascade miroir-miroir.

Un déploiement en cascade miroir-miroir n'est pas pris en charge pour les relations SnapMirror synchrones dans ONTAP 9.5.

- Si les copies Snapshot communes dans ONTAP 9.5 ne sont pas disponibles pendant la restauration, vous devez initialiser la relation synchrone SnapMirror après le rétablissement.

Après deux heures de mise à niveau vers ONTAP 9.6, les copies Snapshot courantes de ONTAP 9.5 sont

automatiquement remplacées par les copies Snapshot communes de ONTAP 9.6. Par conséquent, vous ne pouvez pas resynchroniser la relation synchrone SnapMirror après le rétablissement si les copies Snapshot communes de ONTAP 9.5 ne sont pas disponibles.

### Configuration requise pour la nouvelle version des relations SnapMirror et SnapVault

La commande `System node revert-to` vous informe de toutes les relations SnapMirror et SnapVault qui doivent être supprimées ou reconfigurées pour le processus de nouvelle version. Cependant, vous devez connaître ces exigences avant de commencer la nouvelle version.

- Toutes les relations de SnapVault et de miroir de protection des données doivent être suspendues, puis cassées.

Une fois la nouvelle version terminée, vous pouvez resynchroniser et reprendre ces relations si une copie Snapshot commune existe.

- Les relations SnapVault ne doivent pas contenir les types de règles SnapMirror suivants :
  - mise en miroir asynchrone

Vous devez supprimer toute relation utilisant ce type de stratégie.

- MirrorAndVault

Si l'une de ces relations existe, vous devez modifier la règle SnapMirror en miroir-vault.

- Tous les clones de charge et volumes de destination doivent être supprimés.
- Les relations SnapMirror avec des volumes de destination FlexClone doivent être supprimées.
- La compression réseau doit être désactivée pour chaque règle SnapMirror.
- La règle `All_source_snapshot` doit être supprimée de toute règle SnapMirror de type `async-mirror`.



Les opérations SFSR (Single File Snapshot Restore) et PFSR (Partial File Snapshot Restore) sont obsolètes au niveau du volume racine.

- Toutes les opérations de restauration d'un fichier unique et d'un Snapshot doivent être effectuées avant la réversion.

Vous pouvez soit attendre la fin de l'opération de restauration, soit l'abandonner.

- Toute opération de restauration de fichier unique et de snapshot incomplète doit être supprimée à l'aide de la commande `snapmirror restore`.

### Définissez des périodes d'autovalidation pour les volumes SnapLock avant le rétablissement

Pour restaurer une version antérieure à ONTAP 9, la valeur de la période de validation automatique des volumes SnapLock doit être définie en heures, et non en jours. Avant de tenter de restaurer la restauration, vous devez vérifier la valeur d'autovalidation de vos volumes SnapLock et la modifier de plusieurs jours à quelques heures, si nécessaire.

1. Vérifiez que le cluster contient des volumes SnapLock dont les périodes de validation automatique ne sont pas prises en charge :  
`:volume snaplock show -autocommit-period *days`

2. Modifier les périodes de validation automatique non prises en charge en heures : `volume snaplock modify -vserver vs1 -volume vol1 -autocommit-period value hours`

### Partage de blocs physiques inverse dans les volumes FlexClone fractionnés

Si vous avez séparé un volume FlexClone de son volume parent, vous devez annuler le partage d'un bloc physique entre le clone et son volume parent avant de restaurer ONTAP 9.4 ou version ultérieure vers une version antérieure de ONTAP.

Cette tâche n'est applicable que sur les systèmes AFF lorsque le fractionnement a été exécuté sur l'un des volumes FlexClone.

1. Connectez-vous au niveau de privilège avancé : `set -privilege advanced`
2. Identifiez les volumes FlexClone fractionnés avec des blocs physiques partagés : `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
Node Vserver Volume Aggregate

node1 vs1 vol_clone1 aggr1
node2 vs2 vol_clone2 aggr2
2 entries were displayed.
```

3. Annulez le partage de bloc physique dans tous les volumes FlexClone fractionnés sur le cluster : `volume clone sharing-by-split undo start-all`
4. Vérifier qu'il n'y a pas de volumes FlexClone fractionnés avec des blocs physiques partagés : `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
This table is currently empty.
```

### Désactivez la fonctionnalité qtree dans les volumes FlexGroup avant de procéder au rétablissement

Les qtrees pour volumes FlexGroup ne sont pas pris en charge avant ONTAP 9.3. Vous devez désactiver la fonctionnalité qtree sur les volumes FlexGroup avant de restaurer du ONTAP 9.3 vers une version antérieure de ONTAP.

La fonctionnalité qtree est activée lorsque vous créez un qtree ou si vous modifiez les attributs Security-style et oplock-mode du qtree par défaut.

1. Identifier et supprimer tous les qtrees non par défaut dans chaque volume FlexGroup activé pour la fonctionnalité qtree :
  - a. Connectez-vous au niveau de privilège avancé : `set -privilege advanced`



- b. Vérifiez si un volume FlexGroup est activé avec la fonctionnalité qtree.

Pour ONTAP 9.6 ou version ultérieure, utiliser : `volume show -is-qtree-caching-enabled true`

Pour ONTAP 9.5 ou version antérieure, utiliser : `volume show -is-flexgroup-qtree-enabled true`

```
cluster1::*> volume show -is-flexgroup-qtree-enabled true
Vserver Volume Aggregate State Type Size
Available Used%

vs0 fg - online RW 320MB
220.4MB 31%
```

- c. Supprimez tous les qtrees non par défaut de chaque volume FlexGroup activés via la fonctionnalité qtree : `volume qtree delete -vserver svm_name -volume volume_name -qtree qtree_name`

Si la fonctionnalité qtree est activée car vous avez modifié les attributs de la qtree par défaut et si vous n'avez pas de qtrees, vous pouvez ignorer cette étape.

```
cluster1::*> volume qtree delete -vserver vs0 -volume fg -qtree qtree4
WARNING: Are you sure you want to delete qtree qtree4 in volume fg
vserver vs0? {y|n}: y
[Job 38] Job is queued: Delete qtree qtree4 in volume fg vserver vs0.
```

2. Désactiver la fonctionnalité qtree sur chaque volume FlexGroup : `volume flexgroup qtree-disable -vserver svm_name -volume volume_name`

```
cluster1::*> volume flexgroup qtree-disable -vserver vs0 -volume fg
```

3. Identifier et supprimer toutes les copies Snapshot activées avec la fonctionnalité qtree.

- a. Vérifiez si des copies Snapshot sont activées avec la fonctionnalité qtree : `volume snapshot show -vserver vserver_name -volume volume_name -fields is-flexgroup-qtree-enabled`

```
cluster1::*> volume snapshot show -vserver vs0 -volume fg -fields is-
flexgroup-qtrees-enabled
vserver volume snapshot is-flexgroup-qtrees-enabled

vs0 fg fg_snap1 true
vs0 fg daily.2017-09-27_0010 true
vs0 fg daily.2017-09-28_0010 true
vs0 fg snapmirror.0241f354-a865-11e7-a1c0-
00a098a71764_2147867740.2017-10-04_124524 true
```

- b. Supprimer toutes les copies Snapshot activées avec la fonctionnalité qtrees : `volume snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot_name -force true -ignore-owners true`

Les copies Snapshot qui doivent être supprimées incluent des copies Snapshot régulières et les copies Snapshot prises pour les relations SnapMirror. Si vous avez créé une relation SnapMirror pour les volumes FlexGroup avec un cluster de destination qui exécute ONTAP 9.2 ou une version antérieure, vous devez supprimer toutes les copies Snapshot qui ont été effectuées lorsque le volume FlexGroup source a été activé pour la fonctionnalité qtrees.

```
cluster1::*> volume snapshot delete -vserver vs0 -volume fg -snapshot
daily.2017-09-27_0010 -force true -ignore-owners true
```

## Informations associées

["Gestion des volumes FlexGroup"](#)

## Identifier et déplacer les serveurs SMB en mode groupe de travail

Avant d'effectuer une restauration, vous devez supprimer les serveurs SMB en mode groupe de travail ou les déplacer vers un domaine. Le mode Groupe de travail n'est pas pris en charge sur les versions ONTAP antérieures à ONTAP 9.

1. Identifiez tous les serveurs SMB utilisant un style d'authentification de groupe de travail : `vserver cifs show`
2. Déplacez ou supprimez les serveurs que vous avez identifiés :

| Si vous allez à...                                                              | Utilisez ensuite cette commande                                            |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Déplacer le serveur SMB du groupe de travail vers un domaine Active Directory : | <code>vserver cifs modify -vserver vserver_name -domain domain_name</code> |
| Supprimez le serveur SMB                                                        | <code>vserver cifs delete -vserver vserver_name</code>                     |

3. Si vous avez supprimé le serveur SMB, entrez le nom d'utilisateur du domaine, puis entrez le mot de passe

utilisateur.

## Informations associées

### "Gestion SMB"

#### Vérifiez que l'espace disponible des volumes dédupliqués est suffisant avant de procéder au rétablissement

Avant de procéder à un rétablissement depuis une version de ONTAP 9, vous devez vérifier que les volumes contiennent suffisamment d'espace libre pour l'opération de restauration.

L'espace requis pour le volume doit être suffisant pour prendre en charge les économies réalisées grâce à la détection à la volée de blocs de zéro. Consultez l'article de la base de connaissances ["Découvrez les économies d'espace obtenues grâce à la déduplication, à la compression et à la compaction dans ONTAP 9"](#).

Si vous avez activé à la fois la déduplication et la compression des données sur un volume que vous souhaitez restaurer, vous devez revenir à la compression des données avant de restaurer la déduplication.

1. Utilisez la commande volume Efficiency show avec l'option -fields pour afficher la progression des opérations d'efficacité exécutées sur les volumes.

La commande suivante affiche la progression des opérations d'efficacité : `volume efficiency show -fields vserver,volume,progress`

2. Utilisez la commande volume Efficiency stop avec l'option -all pour arrêter toutes les opérations de déduplication actives et mises en attente.

La commande suivante arrête toutes les opérations de déduplication actives et mises en attente sur le volume Vola : `volume efficiency stop -vserver vs1 -volume VolA -all`

3. Utilisez la commande set -Privilege Advanced pour vous connecter au niveau de privilège avancé.
4. Utilisez la commande de restauration de l'efficacité des volumes avec l'option -version pour revenir à une version spécifique de ONTAP des métadonnées d'efficacité d'un volume.

La commande suivante restaure les métadonnées d'efficacité sur le volume Vola vers ONTAP 9.x : `volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x`



La commande de restauration de l'efficacité du volume restaure les volumes présents sur le nœud sur lequel cette commande est exécutée. Cette commande ne rétablit pas les volumes répartis sur les nœuds.

5. Utilisez la commande volume Efficiency show avec l'option -op-status pour surveiller la progression de la restauration.

La commande suivante contrôle et affiche l'état de la version antérieure : `volume efficiency show -vserver vs1 -op-status Downgrading`

6. Si la restauration n'a pas abouti, utilisez la commande volume Efficiency show avec l'option -instance pour voir pourquoi la restauration a échoué.

La commande suivante affiche des informations détaillées sur tous les champs : `volume efficiency show -vserver vs1 -volume voll - instance`

7. Une fois l'opération de restauration terminée, revenez au niveau de privilège admin : `set -privilege admin`

### "Gestion du stockage logique"

#### Préparez les copies Snapshot avant de procéder aux restaurations

Avant de restaurer vers une version antérieure d'ONTAP, vous devez désactiver toutes les règles de copie Snapshot et supprimer toutes les copies Snapshot créées après la mise à niveau vers la version actuelle.

Si vous procédez à une restauration dans un environnement SnapMirror, vous devez d'abord avoir supprimé les relations de miroir suivantes :

- Toutes les relations miroir de partage de charge
- Toutes les relations de miroir de protection des données créées dans ONTAP 8.3.x
- Toutes les relations de miroir de protection des données si le cluster a été recréé dans ONTAP 8.3.x.

a. Désactiver les règles de copies Snapshot pour tous les SVM de données : `volume snapshot policy modify -vserver * -enabled false`

b. Désactiver les règles de copie Snapshot pour les agrégats de chaque nœud :

- i. Identifiez les agrégats du nœud à l'aide de la commande `run-nodenodenodenameaggr status`.
- ii. Désactiver la règle de copie Snapshot pour chaque agrégat : `run -node nodename aggr options aggr_name nosnap on`
- iii. Répétez cette étape pour chaque nœud restant.

c. Désactiver les règles de copie Snapshot pour le volume racine de chaque nœud :

- i. Identifiez le volume racine du nœud à l'aide de la commande `run-nodenodaémaux status`.

Vous identifiez le volume racine par le mot `root` dans la colonne Options de la sortie de la commande `vol status`.

```
vs1::> run -node node1 vol status
```

| Volume | State  | Status                  | Options         |
|--------|--------|-------------------------|-----------------|
| vol0   | online | raid_dp, flex<br>64-bit | root, nvfail=on |

- i. Désactiver la policy de copie Snapshot sur le volume root : `run -node nodename vol options root_volume_name nosnap on`

- ii. Répétez cette étape pour chaque nœud restant.

d. Supprimez toutes les copies Snapshot créées après la mise à niveau vers la version actuelle :

- i. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
- ii. Désactiver les instantanés : `snapshot policy modify -vserver * -enabled false`

- iii. Supprimez les copies Snapshot les plus récentes du nœud : `volume snapshot prepare-for-revert -node nodename`

Cette commande supprime les copies Snapshot de version les plus récentes sur chaque volume de données, agrégat racine et volume racine.

Si aucune copie Snapshot ne peut être supprimée, la commande échoue et vous informe des actions requises que vous devez effectuer pour pouvoir supprimer les copies. Vous devez effectuer les actions requises, puis exécuter à nouveau la commande de préparation du snapshot du volume pour la restauration avant de passer à l'étape suivante.

```
cluster1::*> volume snapshot prepare-for-revert -node node1
```

```
Warning: This command will delete all Snapshot copies that have the
format used by the current version of ONTAP. It will fail if any
Snapshot copy polices are enabled, or
 if any Snapshot copies have an owner. Continue? {y|n}: y
```

- i. Vérifiez que les copies Snapshot ont été supprimées : `volume snapshot show -node nodename`

Si des copies Snapshot les plus récentes sont conservées, force-les à être supprimées : `volume snapshot delete {-fs-version 9.0 -node nodename -is-constituent true} -ignore-owners -force`

- ii. Répétez cette étape c pour chaque nœud restant.
- iii. Retour au niveau de privilège admin : `set -privilege admin`



Ces étapes doivent être réalisées sur les deux clusters en configuration MetroCluster.

## Identifiez les comptes utilisateur qui utilisent la fonction de hachage SHA-2

Si vous êtes en train de revenir de ONTAP 9.1 ou ONTAP 9.0 à ONTAP 8.3.x, les utilisateurs de comptes SHA-2 ne peuvent plus être authentifiés avec leurs mots de passe. Avant de revenir à la version précédente, vous devez identifier les comptes utilisateur qui utilisent la fonction de hachage SHA-2, de sorte qu'après le rétablissement, vous pouvez les faire réinitialiser pour utiliser le type de cryptage (MD5) pris en charge par la version à laquelle vous restaurez.

1. Passez au paramètre de privilège sur avancé : `set -privilege advanced`
2. Identifiez les comptes d'utilisateur qui utilisent le SHA-2 ont une fonction : `security login show -vserver * -username * -application * -authentication-method password -hash -function !md5`
3. Conservez le résultat de la commande à utiliser après la restauration.



Pendant la restauration, vous êtes invité à exécuter la commande avancée `security login password-prepare-to-downgrade` Pour réinitialiser votre propre mot de passe pour utiliser la fonction de hachage MD5. Si votre mot de passe n'est pas chiffré avec MD5, la commande vous invite à saisir un nouveau mot de passe et le crypte avec MD5, ce qui permet à vos informations d'identification d'être authentifiées après la restauration.

### **Vérifiez les licences autonomes de protection contre les ransomwares avant de restaurer depuis ONTAP 9.11.1 ou version ultérieure**

Si vous avez configuré la protection autonome contre les attaques par ransomware (ARP) et que vous restaurez de ONTAP 9.11.1 ou version ultérieure à ONTAP 9.10.1 ou version antérieure, vous risquez de rencontrer des messages d'avertissement et une fonctionnalité ARP limitée.

Dans ONTAP 9.11.1, la licence anti-ransomware a remplacé la licence MTKM (Multi-tenant Key Management). Si votre système dispose de la licence anti-ransomware mais qu'aucune licence MT\_EK\_MGMT n'est disponible, un avertissement s'affiche lors de la restauration indiquant que ARP ne peut pas être activé sur les nouveaux volumes lors de la restauration.

Les volumes bénéficiant d'une protection existante continuent de fonctionner normalement après restauration, et le statut ARP peut être affiché à l'aide de l'interface de ligne de commande de ONTAP. System Manager ne peut pas afficher l'état ARP sans la licence MTKM.

Par conséquent, si vous souhaitez que ARP continue après le retour à ONTAP 9.10.1, assurez-vous que la licence MTKM est installée avant le rétablissement. ["En savoir plus sur les licences ARP."](#)

### **Supprimez la configuration des compartiments NAS S3 avant la restauration de ONTAP 9.12.1 ou version ultérieure**

Si vous avez configuré l'accès client S3 pour les données NAS, avant de revenir de ONTAP 9.12.1 ou version ultérieure à ONTAP 9.11.1 ou version antérieure, vous devez utiliser l'interface de ligne de commande ONTAP pour supprimer la configuration du compartiment NAS et supprimer tout mappage de nom (utilisateurs S3 pour les utilisateurs Windows ou Unix).

#### **Description de la tâche**

Les tâches suivantes sont effectuées en arrière-plan pendant le processus de restauration.

- Supprimez toutes les créations d'objets singleton partiellement terminées (c'est-à-dire toutes les entrées des répertoires masqués).
- Supprimez tous les répertoires masqués : il peut y en avoir un pour chaque volume accessible à partir de la racine de l'exportation mappée depuis le compartiment NAS S3.
- Supprimez la table de chargement.
- Supprimez toutes les valeurs par défaut utilisateur-unix et utilisateur-Windows-par défaut de tous les serveurs S3 configurés.

#### **Étapes**

1. Supprimer la configuration de compartiment NAS S3 :

```
vserver object-store-server bucket delete -vserver <svm_name> -bucket <s3_nas_bucket_name>
```

2. Supprimer les mappages de noms pour UNIX :

```
vserver name-mapping delete -vserver <svm_name> -direction s3-unix
```

3. Supprimer les mappages de noms pour Windows :

```
vserver name-mapping delete -vserver <svm_name> -direction s3-win
```

4. Retirer les protocoles S3 du SVM :

```
vserver remove-protocols -vserver <svm_name> -protocols s3
```

**Supprimez la configuration d'agrégation de session NFSv4.1 avant de revenir à ONTAP 9.14.1 ou version ultérieure**

Si vous avez activé l'agrégation pour les connexions client et que vous revenez à une version antérieure à ONTAP 9.14.1, vous devez désactiver l'agrégation sur tous les serveurs NFSv4.1 avant le rétablissement.

Lorsque vous saisissez le `revert-to` un message d'avertissement s'affiche pour vous conseiller de désactiver l'agrégation avant de continuer.

Après le retour à une version antérieure de ONTAP, les clients utilisant des connexions à ressources partagées reviennent à utiliser une connexion unique. Leur débit de données sera affecté, mais aucune interruption ne sera constatée. Le comportement de `revert` est identique à la modification de l'option de mise en circuit NFSv4.1 pour le SVM de Enabled à Disabled.

### Étapes

1. Désactivez la mise en circuit sur le serveur NFSv4.1 :

```
vserver nfs modify -vserver svm_name -v4.1-trunking disabled
```

2. Vérifier que NFS est configuré comme souhaité :

```
vserver nfs show -vserver svm_name
```

**Désactivez le basculement automatique non planifié avant de restaurer les configurations MetroCluster à deux et quatre nœuds**

Avant de restaurer une configuration MetroCluster à deux ou quatre nœuds, vous devez désactiver le basculement automatique non planifié (AUSO).

1. Sur les deux clusters dans MetroCluster, désactiver le basculement automatique non planifié :

```
metrocluster modify -auto-switchover-failure-domain auso-disabled
```

## Informations associées

["Gestion et reprise après incident MetroCluster"](#)

### Désactivez IPSec avant d'annuler les configurations MetroCluster

Avant de restaurer une configuration MetroCluster, vous devez désactiver IPSec.

Vous ne pouvez pas restaurer ONTAP dans une configuration MetroCluster exécutant ONTAP 9.12.1 avec IPSec activé. Une vérification est effectuée avant la restauration pour s'assurer qu'il n'y a pas de configuration IPSec dans la configuration MetroCluster. Vous devez supprimer toutes les configurations IPSec présentes et désactiver IPSec avant de poursuivre la restauration. Le rétablissement de ONTAP est bloqué si IPSec est activé, même si vous n'avez configuré aucune stratégie utilisateur.

### Téléchargez et installez l'image du logiciel ONTAP

Vous devez d'abord télécharger le logiciel ONTAP sur le site de support NetApp, puis l'installer.

#### Téléchargez l'image du logiciel

Pour revenir à une version antérieure (ou version ultérieure) de ONTAP 9.4 ou ultérieure, vous pouvez copier l'image du logiciel ONTAP depuis le site de support NetApp vers un dossier local. Pour une restauration vers une version antérieure ou antérieure à ONTAP 9.3, vous devez copier l'image du logiciel ONTAP sur un serveur HTTP ou FTP de votre réseau.

Notez les informations importantes suivantes :

- Les images logicielles sont spécifiques aux modèles de plate-forme.

Vous devez obtenir l'image correcte pour votre cluster. Le site de support NetApp propose les images logicielles, les informations de version du firmware et la dernière version du firmware pour votre modèle de plateforme.

- Les images logicielles incluent la dernière version du micrologiciel système disponible lorsqu'une version donnée de ONTAP a été publiée.
- Si vous déclassez un système avec NetApp Volume Encryption depuis ONTAP 9.5 ou une version ultérieure, vous devez télécharger l'image logicielle ONTAP pour les pays non soumis à des restrictions, notamment NetApp Volume Encryption.

Si vous utilisez l'image logicielle ONTAP pour les pays où vous avez des restrictions, vous pouvez revenir à une version antérieure ou annuler un système avec NetApp Volume Encryption, le système fonctionne de façon incohérente et l'accès à vos volumes est perdu.

- a. Recherchez le logiciel ONTAP cible dans ["Téléchargements de logiciels"](#) la zone du site de support NetApp.
- b. Copiez l'image logicielle.
  - Pour ONTAP 9.3 ou version antérieure, copiez l'image logicielle (par exemple, 93\_q\_image.tgz) du site de support NetApp dans le répertoire du serveur HTTP ou du serveur FTP à partir duquel l'image sera traitée.
  - Pour ONTAP 9.4 ou version ultérieure, copiez l'image logicielle (par exemple, 97\_q\_image.tgz) du site de support NetApp vers le répertoire du serveur HTTP ou FTP à partir duquel l'image sera traitée ou dans un dossier local.



## Installez l'image logicielle

Vous devez installer l'image logicielle cible sur les nœuds du cluster.

- Si vous déclassez ou que vous restaurez un système avec NetApp Volume Encryption depuis ONTAP 9.5 ou une version ultérieure, vous devez avoir téléchargé l'image logicielle ONTAP pour les pays non soumis à des restrictions, notamment NetApp Volume Encryption.

Si vous utilisez l'image logicielle ONTAP pour les pays où vous avez des restrictions, vous pouvez revenir à une version antérieure ou annuler un système avec NetApp Volume Encryption, le système fonctionne de façon incohérente et l'accès à vos volumes est perdu.

- a. Définissez le niveau de privilège sur avancé, en entrant **y** lorsque vous êtes invité à continuer : `set -privilege advanced`

L'invite avancée (\*>) s'affiche.

- b. Installez l'image logicielle sur les nœuds.

Cette commande télécharge et installe l'image logicielle sur tous les nœuds simultanément. Pour télécharger et installer l'image un par un sur chaque nœud, ne spécifiez pas le paramètre `-background`.

- Si vous restaurez une configuration non MetroCluster ou une configuration MetroCluster à deux nœuds : `system node image update -node * -package location -replace-package true -setdefault true -background true`

Cette commande utilise une requête étendue pour modifier l'image du logiciel cible, qui est installée comme image secondaire, comme image par défaut pour le nœud.

- Si vous restaurez une configuration MetroCluster à quatre ou huit nœuds, vous devez lancer la commande suivante sur les deux clusters : `system node image update -node * -package location -replace-package true true -background true -setdefault false`

Cette commande utilise une requête étendue pour modifier l'image du logiciel cible, qui est installée comme image alternative sur chaque nœud.

- c. Entrez **y** pour continuer lorsque vous y êtes invité.
- d. Vérifiez que l'image logicielle est téléchargée et installée sur chaque nœud : `system node image show-update-progress -node *`

Cette commande affiche l'état actuel du téléchargement et de l'installation de l'image logicielle. Vous devez continuer à exécuter cette commande jusqu'à ce que tous les nœuds signalent un état d'exécution de fermeture et un état de sortie réussi.

La commande de mise à jour de l'image du nœud système peut échouer et afficher des messages d'erreur ou d'avertissement. Après avoir résolu les erreurs ou les avertissements, vous pouvez relancer la commande.

Cet exemple montre un cluster à deux nœuds dans lequel l'image logicielle est téléchargée et installée correctement sur les deux nœuds :

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
 Run Status: Exited
 Exit Status: Success
 Phase: Run Script
 Exit Message: After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
 Run Status: Exited
 Exit Status: Success
 Phase: Run Script
 Exit Message: After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

## Ne restaurez pas un cluster ONTAP

Pour mettre le cluster hors ligne afin de revenir à une version antérieure de ONTAP, vous devez désactiver le basculement du stockage et les LIF de données, mettre en place des conditions préalables à la reversion, rétablir les configurations du cluster et du système de fichiers sur un nœud, puis répéter le processus pour chaque nœud supplémentaire du cluster.

Vous devez avoir terminé la restauration "[vérifications](#)" et "[pré-contrôles](#)".

Pour restaurer un cluster, vous devez mettre le cluster hors ligne pendant la durée de la nouvelle version.

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`

Entrez **y** lorsque vous êtes invité à continuer.

2. Vérifier que le logiciel ONTAP cible est installé : `system image show`

L'exemple suivant montre que la version 9.1 est installée comme image alternative sur les deux nœuds :

```
cluster1::*> system image show
```

| Node  | Image  | Is<br>Default | Is<br>Current | Version | Install<br>Date |
|-------|--------|---------------|---------------|---------|-----------------|
| node0 | image1 | true          | true          | 9.2     | MM/DD/YYYY TIME |
|       | image2 | false         | false         | 9.1     | MM/DD/YYYY TIME |
| node1 | image1 | true          | true          | 9.2     | MM/DD/YYYY TIME |
|       | image2 | false         | false         | 9.1     | MM/DD/YYYY TIME |

4 entries were displayed.

3. Désactiver toutes les LIFs de données du cluster : `network interface modify {-role data} -status-admin down`
4. Déterminez si vous avez des relations FlexCache entre clusters : `flexcache origin show-caches -relationship-type inter-cluster`
5. Si des flexcar inter-cluster sont présents, désactiver les lifs de données sur le cluster de cache : `network interface modify -vserver vservice_name -lif lif_name -status-admin down`
6. Si le cluster ne comprend que deux nœuds, désactiver cluster HA : `cluster ha modify -configured false`
7. désactivez le basculement du stockage pour les nœuds de la paire haute disponibilité à partir de l'un des deux nœuds : `storage failover modify -node nodename -enabled false`

Il n'est nécessaire de désactiver qu'une seule fois le basculement du stockage pour la paire haute disponibilité. Lorsque vous désactivez le basculement du stockage pour un nœud, le basculement du stockage est également désactivé sur le partenaire du nœud.

8. Connectez-vous au nœud que vous souhaitez restaurer.

Pour restaurer un nœud, vous devez être connecté au cluster par l'intermédiaire du LIF de node management.

9. Définissez l'image du logiciel ONTAP cible du nœud sur l'image par défaut : `system image modify -node nodename -image target_image -isdefault true`
10. Vérifiez que l'image logicielle ONTAP cible est définie en tant qu'image par défaut du nœud que vous rétablissement : `system image show`

L'exemple suivant montre que la version 9.1 est définie comme image par défaut sur le noeud 0 :

```
cluster1::*> system image show
```

| Node  | Image  | Is Default | Is Current | Version | Install Date    |
|-------|--------|------------|------------|---------|-----------------|
| node0 | image1 | false      | true       | 9.2     | MM/DD/YYYY TIME |
|       | image2 | true       | false      | 9.1     | MM/DD/YYYY TIME |
| node1 | image1 | true       | true       | 9.2     | MM/DD/YYYY TIME |
|       | image2 | false      | false      | 9.1     | MM/DD/YYYY TIME |

4 entries were displayed.

11. Si le cluster ne comprend que deux nœuds, vérifier que le nœud ne contient pas epsilon :

a. Vérifier si le nœud contient actuellement epsilon : `cluster show -node nodename`

L'exemple suivant montre que le nœud contient epsilon :

```
cluster1::*> cluster show -node node1
```

```
Node: node1
UUID: 026efc12-ac1a-11e0-80ed-0f7eba8fc313
Epsilon: true
Eligibility: true
Health: true
```

a. Si le nœud contient epsilon, marquer l'epsilon comme false sur le nœud afin que l'epsilon peut être transféré au partenaire du nœud : `cluster modify -node nodenameA -epsilon false`

b. Transfert d'epsilon vers le partenaire du nœud par le marquage epsilon true sur le nœud partenaire : `cluster modify -node nodenameB -epsilon true`

12. Vérifiez que le nœud est prêt pour la nouvelle version : `system node revert-to -node nodename -check-only true -version 9.x`

Le paramètre de vérification seule identifie les conditions préalables qui doivent être abordées avant le rétablissement, comme les exemples suivants :

- Désactivation du basculement du stockage
- Désactivation de la règle Snapshot
- Suppression des copies Snapshot qui ont été créées après la mise à niveau vers la version ultérieure d'ONTAP

13. Vérifiez que toutes les conditions préalables ont été traitées : `system node revert-to -node nodename -check-only true -version 9.x`

14. Ne rétablit pas la configuration de cluster du nœud : `system node revert-to -node nodename -version 9.x`

L'option `-version` fait référence à la version cible. Par exemple, si le logiciel que vous avez installé et vérifié est ONTAP 9.1, la valeur correcte de l'option `-version` est 9.1.

La configuration du cluster est rétablie, puis vous êtes déconnecté du clustershell.

15. Reconnectez-vous au clustershell, puis basculez vers le nodeshell : `run -node nodename`

Après une nouvelle connexion au clustershell, quelques minutes suffisent avant qu'il soit prêt à accepter la commande nodeshell. Si la commande échoue, attendez quelques minutes et réessayez.

16. Ne rétablit pas la configuration du système de fichiers du nœud: `revert_to 9.x`

Cette commande vérifie que la configuration du système de fichiers du nœud est prête à être rétablie, puis la restaure. Si des conditions préalables sont identifiées, vous devez les résoudre et exécuter à nouveau la commande `revert_to`.



L'utilisation d'une console système pour surveiller le processus de restauration affiche des détails supérieurs à ceux affichés dans le nodeshell.

Si AUTOBOOT est vrai, lorsque la commande est terminée, le nœud redémarre en ONTAP.

Si AUTOBOOT est faux, lorsque la commande termine l'invite DU CHARGEUR s'affiche. Entrez `yes` pour revenir en arrière, utilisez ensuite `boot_ontap` pour redémarrer manuellement le nœud.

17. Une fois le nœud redémarré, vérifiez que le nouveau logiciel exécute : `system node image show`

Dans l'exemple suivant, `image1` est la nouvelle version de ONTAP et est définie comme la version actuelle sur le nœud 0 :

```
cluster1::*> system node image show
```

| Node  | Image  | Is Default | Is Current | Version | Install Date    |
|-------|--------|------------|------------|---------|-----------------|
| ----- |        |            |            |         |                 |
| node0 |        |            |            |         |                 |
|       | image1 | true       | true       | X.X.X   | MM/DD/YYYY TIME |
|       | image2 | false      | false      | Y.Y.Y   | MM/DD/YYYY TIME |
| node1 |        |            |            |         |                 |
|       | image1 | true       | false      | X.X.X   | MM/DD/YYYY TIME |
|       | image2 | false      | true       | Y.Y.Y   | MM/DD/YYYY TIME |

4 entries were displayed.

18. Vérifiez que l'état de restauration est complet pour chaque nœud : `system node upgrade-revert show -node nodename`

L'état doit être indiqué comme « complet », « non requis » ou « aucune entrée de table n'est renvoyée ».

19. Recommencez [\[step-6\]](#) à [\[step-16\]](#) Sur l'autre nœud de la paire HA.
20. Si le cluster ne comprend que deux nœuds, réactivez le cluster HA : `cluster ha modify -configured true`

21. réactivez le basculement du stockage sur les deux nœuds s'il était auparavant désactivé : `storage failover modify -node nodename -enabled true`
22. Recommencez [step-5] à [step-19] Pour chaque paire haute disponibilité supplémentaire et les deux clusters dans la configuration MetroCluster.

## Que dois-je faire après l’restauration de mon cluster ?

### Vérification de l’état du cluster et du stockage après une restauration antérieure

Une fois que vous avez déclassés ou repassé un cluster, vérifiez que les nœuds sont en bon état et peuvent participer au cluster, et que le cluster est au quorum. Vous devez également vérifier l’état de vos disques, agrégats et volumes.

#### Vérification de l’état du cluster

1. Vérifiez que les nœuds du cluster sont en ligne et peuvent participer au cluster : `cluster show`

```
cluster1::> cluster show
Node Health Eligibility

node0 true true
node1 true true
```

Si l’un des nœuds est défectueux ou non éligible, vérifiez la présence d’erreurs dans les journaux EMS et effectuez des actions correctives.

2. Définissez le niveau de privilège sur avancé :
- `set -privilege advanced`

Entrez `y` pour continuer.

3. Vérifier les détails de configuration pour chaque processus RDB
- L’époque de la base de données relationnelle et les séries de tests de base de données doivent correspondre pour chaque nœud.
  - Le maître de quorum par anneau doit être le même pour tous les nœuds.

Notez que chaque anneau peut avoir un maître de quorum différent.

| Pour afficher ce processus RDB...       | Entrez cette commande...                        |
|-----------------------------------------|-------------------------------------------------|
| Application de gestion                  | <code>cluster ring show -unitname mgmt</code>   |
| Base de données d’emplacement de volume | <code>cluster ring show -unitname vlddb</code>  |
| Gestionnaire d’interface virtuelle      | <code>cluster ring show -unitname vifmgr</code> |

| Pour afficher ce processus RDB... | Entrez cette commande...                       |
|-----------------------------------|------------------------------------------------|
| Démon de gestion DU SAN           | <code>cluster ring show -unitname bcomd</code> |

Cet exemple représente le processus de la base de données d'emplacements de volumes :

```
cluster1::*> cluster ring show -unitname vldb
```

| Node  | UnitName | Epoch | DB Epoch | DB Trnxs | Master | Online    |
|-------|----------|-------|----------|----------|--------|-----------|
| node0 | vldb     | 154   | 154      | 14847    | node0  | master    |
| node1 | vldb     | 154   | 154      | 14847    | node0  | secondary |
| node2 | vldb     | 154   | 154      | 14847    | node0  | secondary |
| node3 | vldb     | 154   | 154      | 14847    | node0  | secondary |

4 entries were displayed.

- Retour au niveau de privilège admin : `set -privilege admin`
- Si vous travaillez dans un environnement SAN, vérifiez que chaque nœud se trouve dans un quorum SAN : `event log show -severity informational -message-name scsiblade.*`

Le message d'événement scsiBlade le plus récent pour chaque nœud doit indiquer que le SCSI-Blade est quorum.

```
cluster1::*> event log show -severity informational -message-name
scsiblade.*
```

| Time            | Node  | Severity      | Event                                      |
|-----------------|-------|---------------|--------------------------------------------|
| MM/DD/YYYY TIME | node0 | INFORMATIONAL | scsiblade.in.quorum: The<br>scsi-blade ... |
| MM/DD/YYYY TIME | node1 | INFORMATIONAL | scsiblade.in.quorum: The<br>scsi-blade ... |

## Informations associées

["Administration du système"](#)

## Vérification de l'état du stockage

Lorsque vous restaurez ou déclassés un cluster, vous devez vérifier l'état de vos disques, agrégats et volumes.

- Vérification de l'état du disque :

| Pour vérifier...                                                    | Procédez comme ça...                                                                                                                             |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Disques cassés                                                      | a. Afficher les éventuels disques défectueux :<br><code>storage disk show -state broken</code><br>b. Retirez ou remplacez tout disque endommagé. |
| Disques soumis à des opérations de maintenance ou de reconstruction | a. Afficher tous les disques en état de maintenance, en attente ou reconstruction :<br><code>`storage disk show -state maintenance</code>        |
| pending                                                             | <code>reconstructing`</code><br>.. Attendez la fin de l'opération de maintenance ou de reconstruction avant de poursuivre.                       |

- Vérifiez que tous les agrégats sont en ligne en affichant l'état du stockage physique et logique, y compris les agrégats de stockage : `storage aggregate show -state !online`

Cette commande affiche les agrégats qui sont *not* online. Tous les agrégats doivent être en ligne avant et après avoir effectué une mise à niveau ou une nouvelle version majeure.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

- Vérifiez que tous les volumes sont en ligne en affichant les volumes *NOT* online : `volume show -state !online`

Tous les volumes doivent être en ligne avant et après avoir effectué une mise à niveau ou une nouvelle version majeure.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

- Vérifiez qu'il n'y a pas de volumes incohérents : `volume show -is-inconsistent true`

Consultez l'article de la base de connaissances "[Volume affichant des WAFL incohérentes](#)" sur la manière de traiter les volumes incohérents.

## Informations associées

["Gestion des disques et des agrégats"](#)

## Basculement automatique pour les configurations MetroCluster

Cette rubrique fournit des informations sur les tâches supplémentaires que vous devez effectuer après la reversion des configurations MetroCluster.

- Basculement automatique non planifié : `metrocluster modify -auto-switchover-failure -domain auto-on-cluster-disaster`



2. Valider la configuration MetroCluster : `metrocluster check run`

### Activez ou restaurez les LIF sur les ports de base après une restauration

Au cours d'un redémarrage, certaines LIFs ont peut-être été migrées vers leurs ports de basculement qui leur sont attribués. Une fois que vous restaurez un cluster, vous devez activer et restaurer toutes les LIF qui ne se trouvent pas sur leur port de base.

La commande `network interface revert` restaure une LIF qui n'est pas actuellement sur son port home port vers son port home port, à condition que le port home port soit opérationnel. Le port de base d'une LIF est spécifié lors de sa création ; vous pouvez déterminer le port d'origine d'une LIF à l'aide de la commande `network interface show`.

1. Afficher le statut de toutes les LIFs : `network interface show`

Cet exemple affiche l'état de toutes les LIFs d'un Storage Virtual machine (SVM).

```
cluster1::> network interface show -vserver vs0
```

|            | Logical   | Status     | Network        | Current |       |
|------------|-----------|------------|----------------|---------|-------|
| Current Is |           |            |                |         |       |
| Vserver    | Interface | Admin/Oper | Address/Mask   | Node    | Port  |
| Home       |           |            |                |         |       |
| -----      | -----     | -----      | -----          | -----   | ----- |
| -----      | -----     | -----      | -----          | -----   | ----- |
| vs0        |           |            |                |         |       |
|            | data001   | down/down  | 192.0.2.120/24 | node0   | e0e   |
| true       |           |            |                |         |       |
|            | data002   | down/down  | 192.0.2.121/24 | node0   | e0f   |
| true       |           |            |                |         |       |
|            | data003   | down/down  | 192.0.2.122/24 | node0   | e2a   |
| true       |           |            |                |         |       |
|            | data004   | down/down  | 192.0.2.123/24 | node0   | e2b   |
| true       |           |            |                |         |       |
|            | data005   | down/down  | 192.0.2.124/24 | node0   | e0e   |
| false      |           |            |                |         |       |
|            | data006   | down/down  | 192.0.2.125/24 | node0   | e0f   |
| false      |           |            |                |         |       |
|            | data007   | down/down  | 192.0.2.126/24 | node0   | e2a   |
| false      |           |            |                |         |       |
|            | data008   | down/down  | 192.0.2.127/24 | node0   | e2b   |
| false      |           |            |                |         |       |

8 entries were displayed.

Si des LIF dont le statut Status Admin est down ou avec un état is home est false, passez à l'étape suivante.

2. Activation des LIFs de données : `network interface modify {-role data} -status-admin up`

```
cluster1::> network interface modify {-role data} -status-admin up
8 entries were modified.
```

### 3. Rerestaurer les LIF sur leurs home ports : `network interface revert *`

Cette commande restaure toutes les LIF vers leur port de base.

```
cluster1::> network interface revert *
8 entries were acted on.
```

### 4. Vérifier que toutes les LIFs se trouvent sur leurs ports de type home : `network interface show`

Cet exemple montre que toutes les LIFs pour SVM vs0 sont sur leurs ports de base.

```
cluster1::> network interface show -vserver vs0
```

| Current Is | Logical   | Status     | Network        | Current |      |
|------------|-----------|------------|----------------|---------|------|
| Vserver    | Interface | Admin/Oper | Address/Mask   | Node    | Port |
| Home       |           |            |                |         |      |
| vs0        |           |            |                |         |      |
| true       | data001   | up/up      | 192.0.2.120/24 | node0   | e0e  |
| true       | data002   | up/up      | 192.0.2.121/24 | node0   | e0f  |
| true       | data003   | up/up      | 192.0.2.122/24 | node0   | e2a  |
| true       | data004   | up/up      | 192.0.2.123/24 | node0   | e2b  |
| true       | data005   | up/up      | 192.0.2.124/24 | node1   | e0e  |
| true       | data006   | up/up      | 192.0.2.125/24 | node1   | e0f  |
| true       | data007   | up/up      | 192.0.2.126/24 | node1   | e2a  |
| true       | data008   | up/up      | 192.0.2.127/24 | node1   | e2b  |

```
8 entries were displayed.
```

## Activez les règles de copie Snapshot après le rétablissement

Après avoir restauré vers une version antérieure de ONTAP, vous devez activer les

## règles de copie Snapshot pour recommencer la création de copies Snapshot.

Vous réactivez les planifications Snapshot que vous avez désactivées avant de revenir à une version antérieure de ONTAP.

1. Activez les règles de copie Snapshot pour tous les SVM de données :

```
volume snapshot policy modify -vserver * -enabled true
```

```
snapshot policy modify pg-rpo-hourly -enable true
```

2. Pour chaque nœud, activez la règle de copie Snapshot du volume racine à l'aide de la commande `run-nodenodenodaémaux optionsroot_vol_namenossip off`.

```
cluster1::> run -node node1 vol options vol0 nosnap off
```

### Vérification de l'accès client (SMB et NFS)

Pour les protocoles configurés, testez l'accès des clients SMB et NFS afin de vérifier que le cluster est accessible.

### Vérifiez les entrées du pare-feu IPv6

Une nouvelle version à partir de n'importe quelle version de ONTAP 9 peut entraîner l'absence d'entrées de pare-feu IPv6 par défaut pour certains services dans les politiques de pare-feu. Vous devez vérifier que les entrées de pare-feu requises ont été restaurées sur votre système.

1. Vérifiez que toutes les politiques de pare-feu sont correctes en les comparant aux politiques par défaut :

```
system services firewall policy show
```

L'exemple suivant montre les règles par défaut :

```
cluster1::*> system services firewall policy show
```

| Policy  | Service | Action | IP-List         |
|---------|---------|--------|-----------------|
| -----   |         |        |                 |
| cluster |         |        |                 |
|         | dns     | allow  | 0.0.0.0/0       |
|         | http    | allow  | 0.0.0.0/0       |
|         | https   | allow  | 0.0.0.0/0       |
|         | ndmp    | allow  | 0.0.0.0/0       |
|         | ntp     | allow  | 0.0.0.0/0       |
|         | rsh     | allow  | 0.0.0.0/0       |
|         | snmp    | allow  | 0.0.0.0/0       |
|         | ssh     | allow  | 0.0.0.0/0       |
|         | telnet  | allow  | 0.0.0.0/0       |
| data    |         |        |                 |
|         | dns     | allow  | 0.0.0.0/0, ::/0 |
|         | http    | deny   | 0.0.0.0/0, ::/0 |
|         | https   | deny   | 0.0.0.0/0, ::/0 |
|         | ndmp    | allow  | 0.0.0.0/0, ::/0 |
|         | ntp     | deny   | 0.0.0.0/0, ::/0 |
|         | rsh     | deny   | 0.0.0.0/0, ::/0 |
| .       |         |        |                 |
| .       |         |        |                 |
| .       |         |        |                 |

2. Ajoutez manuellement toutes les entrées de pare-feu IPv6 par défaut manquantes en créant une nouvelle politique de pare-feu : `system services firewall policy create`

```
cluster1::*> system services firewall policy create -policy newIPv6
-service ssh -action allow -ip-list ::/0
```

3. Appliquer la nouvelle policy à la LIF pour autoriser l'accès à un service réseau : `network interface modify`

```
cluster1::*> network interface modify -vserver VS1 -lif LIF1
-firewall-policy newIPv6
```

## Rétablit la fonction de hachage du mot de passe au type de cryptage pris en charge

Si vous êtes ramené de ONTAP 9.1 ou ONTAP 9.0 à ONTAP 8.3.x, les utilisateurs de compte SHA-2 ne peuvent plus être authentifiés avec leurs mots de passe. Les mots de passe doivent être réinitialisés pour utiliser le type de cryptage MDS.

1. Définissez un mot de passe temporaire pour chaque compte utilisateur SHA-2 que vous [identifié avant le](#)

[rétablissement](#): `security login password -username user_name -vserver vserver_name`

2. Communiquez le mot de passe temporaire aux utilisateurs concernés et demandez-leur de se connecter par le biais d'une console ou d'une session SSH pour modifier leur mot de passe comme le système l'invite.

### **Facteurs à prendre en compte pour la mise à jour manuelle du firmware du processeur de service**

Si la fonctionnalité de mise à jour automatique du processeur de service est activée (par défaut), la rétrogradation ou le rétablissement de ONTAP 8.3.x ne nécessite pas de mise à jour manuelle du micrologiciel du processeur de service. Le micrologiciel du processeur de service est automatiquement mis à jour vers la dernière version compatible prise en charge par la version ONTAP que vous avez rétablie ou rétrogradée.

Si la fonctionnalité de mise à jour automatique du processeur de service est désactivée (non recommandée), après ONTAP la fin du processus de restauration ou de mise à niveau vers une version antérieure du micrologiciel du processeur de service, vous devez mettre à jour manuellement la version prise en charge pour la version de ONTAP à laquelle vous avez rétabli ou déclassé.

["Matrice de prise en charge NetApp BIOS/ONTAP"](#)

["Téléchargements NetApp : firmware système et diagnostics"](#)

### **Modifier les comptes utilisateur pouvant accéder au Service Processor**

Si vous avez créé des comptes utilisateur sur ONTAP 9.8 ou une version antérieure, passez à ONTAP 9.9.1 ou une version ultérieure (lorsque l' `-role` paramètre est remplacé par `admin`), puis revient à ONTAP 9.8 ou antérieur, le `-role` le paramètre est restauré à sa valeur d'origine. Vous devez néanmoins vérifier que les valeurs modifiées sont acceptables.

Lors de la restauration, si le rôle d'un utilisateur SP a été supprimé, le message « `rbac.spuser.role.notfound` » EMS sera enregistré.

Pour plus d'informations, voir ["Comptes pouvant accéder au processeur de service"](#).

# Administration du cluster

## Gestion du cluster avec System Manager

### Présentation de l'administration avec System Manager

System Manager est une interface graphique de gestion basée sur HTML5 qui vous permet d'utiliser un navigateur Web pour gérer les systèmes et objets de stockage (tels que les disques, les volumes et les niveaux de stockage) et d'effectuer des tâches de gestion courantes liées aux systèmes de stockage.

Les procédures de cette section vous aident à gérer votre cluster avec System Manager dans ONTAP 9.7 et versions ultérieures.



- System Manager est inclus dans le logiciel ONTAP en tant que service Web, activé par défaut et accessible via un navigateur.
- Le nom de System Manager a été modifié depuis ONTAP 9.6. Dans ONTAP 9.5 et versions antérieures, il s'appelait OnCommand System Manager. Depuis ONTAP 9.6 et versions ultérieures, il s'appelle System Manager.
- Si vous utilisez le Gestionnaire système classique (disponible uniquement dans ONTAP 9.7 et versions antérieures), reportez-vous à la section "[System Manager Classic \(ONTAP 9.0 à 9.7\)](#)".

Grâce au tableau de bord de System Manager, vous pouvez afficher des informations d'un coup d'œil sur les alertes et notifications importantes, sur l'efficacité et la capacité des tiers et volumes de stockage, sur les nœuds disponibles dans un cluster, sur l'état des nœuds d'une paire haute disponibilité, sur les applications et objets les plus actifs, et les metrics de performance d'un cluster ou d'un nœud.

System Manager vous permet d'effectuer plusieurs tâches courantes, telles que :

- Création d'un cluster, configuration d'un réseau et configuration des détails de support du cluster.
- Configurer et gérer les objets de stockage, tels que les disques, les niveaux locaux, les volumes, les qtrees et quotas.
- Configurez des protocoles, tels que SMB et NFS, et provisionnez le partage de fichiers.
- Configurez les protocoles, tels que FC, FCoE, NVMe et iSCSI, pour l'accès au bloc.
- Créez et configurez des composants réseau, tels que des sous-réseaux, des domaines de diffusion, des interfaces de données et de gestion, et des groupes d'interfaces.
- Configuration et gestion de la mise en miroir et des relations à l'archivage.
- Exécutez les opérations de gestion des clusters, de gestion des nœuds de stockage et des machines virtuelles de stockage (VM).
- Créez et configurez des VM de stockage, gérez les objets de stockage associés aux VM de stockage et gérez les services de VM de stockage.
- Contrôle et gestion des configurations haute disponibilité (HA) dans un cluster.
- Configurez les processeurs de service pour connecter, gérer, surveiller et administrer le nœud à distance, quel que soit l'état du nœud.

## Terminologie de System Manager

System Manager utilise une terminologie différente de celle de l'interface de ligne de commandes pour certaines fonctionnalités de clés ONTAP.

- **Local Tier** – ensemble de disques SSD physiques ou de disques durs sur lequel vous stockez vos données. On peut les connaître comme des agrégats. En fait, si vous utilisez l'interface de ligne de commande ONTAP, vous verrez toujours le terme *aggrer* utilisé pour représenter un niveau local.
- **Tier cloud** – stockage dans le cloud utilisé par ONTAP lorsque vous souhaitez placer certaines données hors site pour l'une des raisons suivantes. Si vous pensez à la partie Cloud d'un FabricPool, vous l'avez déjà défigurée. Et si vous utilisez un système StorageGRID, il est possible que votre cloud ne soit pas hors site du tout. (Une expérience sur site similaire à celle du cloud est appelée « cloud privé ».)
- **Storage VM** – machine virtuelle fonctionnant sous ONTAP qui fournit des services de stockage et de données à vos clients. Vous pouvez le connaître comme *SVM* ou *vserver*.
- **Interface réseau** - adresse et propriétés affectées à un port réseau physique. Vous pouvez le connaître comme une *interface logique (LIF)*.
- **Pause** - une action qui interrompt les opérations. Avant ONTAP 9.8, vous avez peut-être fait référence à *quiesce* dans d'autres versions de System Manager.

## Utilisez System Manager pour accéder à un cluster

Si vous préférez utiliser une interface graphique plutôt que l'interface de ligne de commandes pour l'accès et la gestion d'un cluster, vous pouvez utiliser System Manager, inclus avec ONTAP en tant que service Web, activé par défaut et accessible via un navigateur.



À partir de ONTAP 9.12.1, System Manager est entièrement intégré à BlueXP.

BlueXP vous permet de gérer votre infrastructure multicloud hybride à partir d'un seul plan de contrôle tout en conservant le tableau de bord familier de System Manager.

Voir "[Intégration de System Manager à BlueXP](#)".

### Description de la tâche

Vous pouvez accéder à System Manager à l'aide d'une interface réseau de gestion de cluster (LIF) ou d'une interface de réseau de gestion de nœuds. Pour un accès ininterrompu à System Manager, vous devez utiliser une interface de réseau de gestion du cluster (LIF).

### Avant de commencer

- Vous devez disposer d'un compte d'utilisateur de cluster configuré avec le rôle « admin » et les types d'application « http » et « console ».
- Les cookies et les données du site doivent être activés dans le navigateur.

### Étapes

1. Indiquez l'adresse IP de l'interface réseau de gestion du cluster dans le navigateur Web :

- Si vous utilisez IPv4 : **`https://cluster-mgmt-LIF`**
- Si vous utilisez IPv6 : **`https://[cluster-mgmt-LIF]`**



Seul le protocole HTTPS est pris en charge pour l'accès au navigateur de System Manager.

Si le cluster utilise un certificat numérique auto-signé, il est possible que le navigateur affiche un avertissement indiquant que le certificat n'est pas approuvé. Vous pouvez accepter le risque de continuer l'accès ou installer un certificat numérique signé par l'autorité de certification sur le cluster pour l'authentification du serveur.

2. **Facultatif**: si vous avez configuré une bannière d'accès à l'aide de l'interface de ligne de commande, lisez le message affiché dans la boîte de dialogue **Avertissement** et choisissez l'option requise pour continuer.

Cette option n'est pas prise en charge sur les systèmes sur lesquels l'authentification SAML (Security assertion Markup Language) est activée.


- Si vous ne souhaitez pas continuer, cliquez sur **Annuler**, puis fermez le navigateur.
- Si vous souhaitez continuer, cliquez sur **OK** pour accéder à la page de connexion de System Manager.



3. Connectez-vous à System Manager à l'aide des identifiants de l'administrateur du cluster.



Depuis ONTAP 9.11.1, lorsque vous vous connectez à System Manager, vous pouvez spécifier les paramètres régionaux. Les paramètres régionaux indiquent certains paramètres de localisation, tels que la langue, la devise, le format de date et d'heure, ainsi que des paramètres similaires. Pour ONTAP 9.10.1 et versions antérieures, les paramètres régionaux de System Manager sont détectés à partir du navigateur. Pour modifier les paramètres régionaux de System Manager, vous devez modifier les paramètres régionaux du navigateur.

4. **Facultatif** : à partir de ONTAP 9.12.1, vous pouvez spécifier votre préférence pour l'apparence de System Manager :

- a. Dans le coin supérieur droit de System Manager, cliquez sur  pour gérer les options utilisateur.
- b. Placez le commutateur **thème système** sur votre préférence :

| Basculer la position                                                                         | Réglage de l'apparence                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  (gauche) | Thème lumineux (fond clair avec texte foncé)                                                                                                                                                  |
| OS (centre)                                                                                  | Valeur par défaut de la préférence de thème définie pour les applications du système d'exploitation (généralement le paramètre de thème du navigateur utilisé pour accéder à System Manager). |
|  (droite) | Thème foncé (fond sombre avec texte clair)                                                                                                                                                    |

## Informations associées

["Gestion de l'accès aux services Web"](#)

["Accès aux fichiers log d'un nœud, core dump, et MIB à l'aide d'un navigateur web"](#)



## Activation de nouvelles fonctionnalités en ajoutant des clés de licence

Dans les versions antérieures à ONTAP 9.10.1, les fonctionnalités ONTAP sont activées avec des clés de licence, et les fonctionnalités de ONTAP 9.10.1 et versions ultérieures sont activées avec un fichier de licence NetApp. Vous pouvez ajouter des clés de licence et des fichiers de licence NetApp à l'aide de System Manager.

Depuis ONTAP 9.10.1, System Manager vous permet d'installer un fichier de licence NetApp afin d'activer plusieurs fonctionnalités sous licence à la fois. L'utilisation d'un fichier de licence NetApp simplifie l'installation de la licence, car vous n'avez plus besoin d'ajouter des clés de licence distinctes. Vous téléchargez le fichier de licence NetApp depuis le site de support NetApp.

Si vous disposez déjà de clés de licence pour certaines fonctionnalités et que vous effectuez une mise à niveau vers ONTAP 9.10.1, vous pouvez continuer à utiliser ces clés de licence.

### Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Sous **licences**, sélectionnez ➔.
3. Sélectionnez **Parcourir**. Choisissez le fichier de licence NetApp que vous avez téléchargé.
4. Si vous souhaitez ajouter des clés de licence, sélectionnez **utiliser des clés de licence à 28 caractères** et entrez les clés.


## Télécharger une configuration de cluster

Depuis la version ONTAP 9.11.1, vous pouvez utiliser System Manager pour télécharger des informations de configuration sur le cluster et ses nœuds. Ces informations peuvent être utilisées pour la gestion des stocks, le remplacement du matériel et les activités de cycle de vie. Ces informations sont particulièrement utiles pour les sites qui n'envoient pas de données AutoSupport (ASUP).

Les détails de la configuration du cluster incluent le nom du cluster, la version du cluster ONTAP, la LIF de cluster management, le volume et le nombre de LIF.

Les informations détaillées sur la configuration des nœuds comprennent le nom du nœud, le numéro de série du système, l'ID système, le modèle du système, la version du ONTAP, les informations relatives au MetroCluster, les informations relatives au réseau SP/BMC et la configuration du cryptage.

### Étapes

1. Cliquez sur **Cluster > Présentation**.
2. Cliquez sur  **More** pour afficher le menu déroulant.
3. Sélectionnez **Télécharger la configuration**.
4. Sélectionnez les paires HA, puis cliquez sur **Download**.

La configuration est téléchargée sous forme de feuille de calcul Excel.

- La première feuille contient des détails sur le cluster.
- Les autres feuilles contiennent des détails de nœud.

## Attribuez des balises à un cluster

Depuis la version ONTAP 9.14.1, System Manager permet d'attribuer des balises à un cluster pour identifier les objets appartenant à une catégorie, tels que des projets ou des centres de coûts.

### Description de la tâche

Vous pouvez attribuer une balise à un cluster. Tout d'abord, vous devez définir et ajouter la balise. Vous pouvez ensuite modifier ou supprimer la balise.

Les balises peuvent être ajoutées lors de la création d'un cluster ou ultérieurement.

Vous définissez une balise en spécifiant une clé et en lui associant une valeur au format « `key:value' ». Par exemple : « `dept:engineering` » ou « location:san-jose ».

Les éléments suivants doivent être pris en compte lors de la création de balises :

- Les clés ont une longueur minimale d'un caractère et ne peuvent pas être nulles. Les valeurs peuvent être nulles.
- Une clé peut être associée à plusieurs valeurs en séparant les valeurs par une virgule, par exemple, « emplacement:san-jose,toronto ».
- Les balises peuvent être utilisées pour plusieurs ressources.
- Les touches doivent commencer par une lettre minuscule.

### Étapes


Pour gérer les balises, procédez comme suit :

1. Dans System Manager, cliquez sur **Cluster** pour afficher la page de présentation.

Les balises sont répertoriées dans la section **Tags**.

2. Cliquez sur **gérer les balises** pour modifier les balises existantes ou en ajouter de nouvelles.

Vous pouvez ajouter, modifier ou supprimer les balises.

| Pour effectuer cette action... | Procédez comme suit...                                                                                                                                                                                                         |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ajouter une balise             | <ol style="list-style-type: none"><li>a. Cliquez sur <b>Ajouter une balise</b>.</li><li>b. Spécifiez une clé et sa ou ses valeurs (séparez les valeurs par des virgules).</li><li>c. Cliquez sur <b>Enregistrer</b>.</li></ol> |
| Modifier une balise            | <ol style="list-style-type: none"><li>a. Modifiez le contenu dans les champs <b>Key</b> et <b>Values (facultatif)</b>.</li><li>b. Cliquez sur <b>Enregistrer</b>.</li></ol>                                                    |
| Supprimer une balise           | <ol style="list-style-type: none"><li>a. Cliquez sur  en regard de l'étiquette que vous souhaitez supprimer.</li></ol>                      |

## Consultation et envoi des dossiers de demande de support

Depuis la version ONTAP 9.9.1, vous pouvez consulter les dossiers de support Active IQ associés au cluster. Vous pouvez également copier les informations relatives au cluster dont vous avez besoin pour créer un nouveau dossier de demande de support sur le site de support NetApp.

Depuis ONTAP 9.10.1, vous pouvez activer la journalisation de télémétrie et aider le personnel de support à résoudre les problèmes.



Pour recevoir des alertes relatives aux mises à jour de firmwares, vous devez être enregistré auprès de Active IQ Unified Manager. Reportez-vous à la section "[Ressources de documentation Active IQ Unified Manager](#)".

### Étapes

1. Dans System Manager, sélectionnez **support**.

La liste des dossiers de demande de support ouverts associés à ce cluster s'affiche.

2. Cliquez sur les liens suivants pour effectuer les procédures :

- **Numéro de cas**: Voir détails sur le cas.
- **Accédez au site de support NetApp** : accédez à la page **My AutoSupport** du site de support NetApp pour consulter les articles de la base de connaissances ou ouvrir un nouveau dossier de support.
- **Afficher mes dossiers de demande de support** : accédez à la page **Mes dossiers de demande de support** sur le site de support NetApp.
- **Afficher les détails du cluster** : affichez et copiez les informations nécessaires lorsque vous soumettez un nouveau dossier.

### Activez la journalisation de télémétrie

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour activer la journalisation de télémétrie. Lorsque la journalisation de télémétrie est autorisée, un identificateur de télémétrie spécifique indique le processus exact qui a déclenché le message dans les messages consignés par System Manager. Tous les messages émis relatifs à ce processus ont le même identifiant, qui se compose du nom du workflow opérationnel et d'un nombre (par exemple « add-volume-1941290 »).

Si vous rencontrez des problèmes de performances, vous pouvez activer la journalisation de télémétrie, ce qui permet au personnel de support d'identifier plus facilement le processus spécifique pour lequel un message a été émis. Lorsque des identifiants de télémétrie sont ajoutés aux messages, le fichier journal n'est que légèrement agrandi.

### Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Dans la section **Paramètres d'interface utilisateur**, cochez la case **Autoriser la journalisation de télémétrie**.

## Gérez la limite de capacité maximale d'une machine virtuelle de stockage dans System Manager



À partir de ONTAP 9.13.1, vous pouvez utiliser System Manager pour activer une limite

de capacité maximale pour une machine virtuelle de stockage et définir un seuil pour déclencher des alertes lorsque le stockage utilisé atteint un certain pourcentage de la capacité maximale.

**Limite de capacité maximale pour une VM de stockage**

À partir de ONTAP 9.13.1, vous pouvez spécifier la capacité maximale pouvant être allouée à tous les volumes d’une machine virtuelle de stockage. Vous pouvez activer la capacité maximale lorsque vous ajoutez une machine virtuelle de stockage ou lorsque vous modifiez une machine virtuelle de stockage existante.


**Étapes**

- 1. Sélectionnez **stockage > machines virtuelles de stockage**.
- 2. Effectuez l’une des opérations suivantes :
  - Pour ajouter une machine virtuelle de stockage, cliquez sur  .
  - Pour modifier une machine virtuelle de stockage, cliquez sur  en regard du nom de la machine virtuelle de stockage, puis cliquez sur **Modifier**.
- 3. Entrez ou modifiez les paramètres de la machine virtuelle de stockage, puis cochez la case Activer la limite de capacité maximale.
- 4. Spécifiez la taille de capacité maximale.
- 5. Spécifiez le pourcentage de la capacité maximale que vous souhaitez utiliser comme seuil pour déclencher des alertes.
- 6. Cliquez sur **Enregistrer**.

**Modifiez la limite de capacité maximale d’une machine virtuelle de stockage**

À partir de ONTAP 9.13.1, vous pouvez modifier la limite de capacité maximale d’une machine virtuelle de stockage existante, si l’ [la limite de capacité maximale a été activée](#) déjà.

**Étapes**

- 1. Sélectionnez **stockage > machines virtuelles de stockage**.
- 2. Cliquez sur  en regard du nom de la machine virtuelle de stockage, puis cliquez sur **Modifier**.

La case à cocher intitulée « Activer la limite de capacité maximale » est déjà cochée.

- 3. Effectuez l’une des opérations suivantes :

| Action                                    | Étapes                                                                                                          |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Désactivez la limite de capacité maximale | <ul style="list-style-type: none"><li>1. Décochez la case.</li><li>2. Cliquez sur <b>Enregistrer</b>.</li></ul> |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modifier la limite de capacité maximale | <ol style="list-style-type: none"> <li>1. Spécifiez la nouvelle taille de capacité maximale. (Vous ne pouvez pas spécifier une taille inférieure à l'espace déjà alloué dans la machine virtuelle de stockage.)</li> <li>2. Spécifiez le nouveau pourcentage de la capacité maximale que vous souhaitez utiliser comme seuil pour déclencher des alertes.</li> <li>3. Cliquez sur <b>Enregistrer</b>.</li> </ol> |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Informations associées

- ["Afficher la limite de capacité maximale d'une machine virtuelle de stockage"](#)
- ["Mesures de la capacité dans System Manager"](#)
- ["Gérez les limites de capacité des SVM"](#)

## Contrôle de la capacité dans System Manager

System Manager vous permet de surveiller la capacité de stockage utilisée et la quantité disponible pour un cluster, un niveau local ou une machine virtuelle de stockage.

À chaque version d'ONTAP, System Manager fournit des informations plus fiables sur le contrôle de la capacité :

- Depuis ONTAP 9.10.1, System Manager vous permet de consulter l'historique des données sur la capacité du cluster, ainsi que des prévisions sur la capacité qui sera utilisée ou disponible à l'avenir. Vous pouvez également surveiller la capacité des niveaux et volumes locaux.
- À partir de ONTAP 9.12.1, System Manager affiche la quantité de capacité allouée pour un niveau local.
- À partir de ONTAP 9.13.1, vous pouvez activer une limite de capacité maximale pour une machine virtuelle de stockage et définir un seuil pour déclencher des alertes lorsque le stockage utilisé atteint un certain pourcentage de la capacité maximale.



Les mesures de la capacité utilisée s'affichent différemment en fonction de la version de ONTAP utilisée. Pour en savoir plus, consultez ["Mesures de la capacité dans System Manager"](#).

### Afficher la capacité d'un cluster

Vous pouvez afficher les mesures de capacité d'un cluster sur le tableau de bord dans System Manager.

#### Avant de commencer

Pour afficher les données relatives à la capacité dans le cloud, vous devez disposer d'un compte Active IQ Digital Advisor et être connecté.

#### Étapes

1. Dans System Manager, cliquez sur **Dashboard**.
2. Dans la section **capacité**, vous pouvez afficher les éléments suivants :
  - Capacité totale utilisée du cluster
  - Capacité totale disponible du cluster
  - Pourcentages de capacité utilisée et disponible.

- Ratio de réduction des données.
- Capacité utilisée dans le cloud.
- Historique de l'utilisation de la capacité.
- Projection de l'utilisation de la capacité



Dans System Manager, les représentations de capacité ne prennent pas en compte les capacités du niveau de stockage racine (agrégat).

3. Cliquez sur le graphique pour afficher plus de détails sur la capacité du cluster.

Les mesures de capacité sont indiquées dans deux graphiques à barres :

- Le graphique supérieur affiche la capacité physique : la taille de l'espace physique utilisé, réservé et disponible.
- Le graphique inférieur affiche la capacité logique : la taille des données client, les copies Snapshot et les clones, ainsi que l'espace logique total utilisé.

Les mesures de réduction des données se trouvent sous les graphiques à barres :

- Taux de réduction des données pour les données clients uniquement (les copies Snapshot et les clones ne sont pas inclus).
- Ratio global de réduction des données.

Pour plus d'informations, voir ["Mesures de la capacité dans System Manager"](#).

### Afficher la capacité d'un niveau local

Vous pouvez afficher des informations détaillées sur la capacité des niveaux locaux. À partir de ONTAP 9.12.1, la vue **capacité** inclut également la quantité de capacité allouée pour un niveau local, ce qui vous permet de déterminer si vous devez ajouter de la capacité au niveau local pour prendre en charge la capacité allouée et éviter de manquer d'espace libre.

#### Étapes

1. Cliquez sur **stockage > niveaux**.
2. Sélectionnez le nom du niveau local.
3. Sur la page **Présentation**, dans la section **capacité**, la capacité est indiquée dans un graphique à barres avec trois mesures :
  - Capacité utilisée et réservée
  - Capacité disponible
  - Capacité dédiée (à partir de ONTAP 9.12.1)
4. Cliquez sur le tableau pour afficher des détails sur la capacité du niveau local.

Les mesures de capacité sont indiquées dans deux graphiques à barres :

- Le graphique à barres du haut affiche la capacité physique : la taille de l'espace physique utilisé, réservé et disponible.
- La barre du bas affiche la capacité logique : la taille des données client, des copies Snapshot et des clones, ainsi que l'espace total logique utilisé.

Les graphiques à barres ci-dessous sont des rapports de mesure pour la réduction des données :

- Taux de réduction des données pour les données clients uniquement (les copies Snapshot et les clones ne sont pas inclus).
- Ratio global de réduction des données.

Pour plus d'informations, voir ["Mesures de la capacité dans System Manager"](#).

### Actions facultatives

- Si la capacité engagée est supérieure à la capacité du niveau local, vous pouvez envisager d'ajouter de la capacité au niveau local avant qu'il ne manque d'espace libre. Voir ["Ajout de capacité à un niveau local \(ajout de disques à un agrégat\)"](#).
- Vous pouvez également afficher le stockage utilisé par des volumes spécifiques dans le niveau local en sélectionnant l'onglet **volumes**.

### Affichez la capacité des volumes d'une VM de stockage

Vous pouvez afficher la quantité de stockage utilisée par les volumes d'une VM de stockage et la capacité disponible. La mesure totale du stockage utilisé et disponible est appelée « capacité sur tous les volumes ».

#### Étapes

1. Sélectionnez **stockage > machines virtuelles de stockage**.
2. Cliquez sur le nom de la machine virtuelle de stockage.
3. Accédez à la section **capacité**, qui affiche un graphique à barres avec les mesures suivantes :
  - **Physique utilisée** : somme du stockage physique utilisé sur tous les volumes de cette VM de stockage.
  - **Disponible** : somme de la capacité disponible sur tous les volumes de cette VM de stockage.
  - **Logique utilisée** : somme du stockage logique utilisé sur tous les volumes de cette machine virtuelle de stockage.

Pour plus de détails sur les mesures, voir ["Mesures de la capacité dans System Manager"](#).

### Afficher la limite de capacité maximale d'une machine virtuelle de stockage

À partir de ONTAP 9.13.1, vous pouvez afficher la limite de capacité maximale d'une machine virtuelle de stockage.

#### Avant de commencer

Vous devez ["Limite de capacité maximale d'une machine virtuelle de stockage"](#) avant de pouvoir l'afficher.

#### Étapes

1. Sélectionnez **stockage > machines virtuelles de stockage**.

Vous pouvez afficher les mesures de capacité maximale de deux manières :

- Dans la ligne de la machine virtuelle de stockage, affichez la colonne **capacité maximale** qui contient un graphique à barres indiquant la capacité utilisée, la capacité disponible et la capacité maximale.
- Cliquez sur le nom de la VM de stockage. Dans l'onglet **vue d'ensemble**, faites défiler pour afficher les valeurs de seuil de capacité maximale, de capacité allouée et d'alerte de capacité dans la colonne de

gauche.

#### Informations associées

- ["Modifiez la limite de capacité maximale d'une machine virtuelle de stockage"](#)
- ["Mesures de la capacité dans System Manager"](#)

## Consultez les configurations matérielles pour déterminer les problèmes

Depuis ONTAP 9.8, vous pouvez utiliser System Manager pour afficher la configuration matérielle de votre réseau et déterminer l'état de santé de vos systèmes matériels et des configurations de câblage.

### Étapes

Pour afficher les configurations matérielles, procédez comme suit :

1. Dans System Manager, sélectionnez **Cluster > Hardware**.
2. Placez le curseur de la souris sur les composants pour afficher l'état et d'autres détails.

Vous pouvez afficher différents types d'informations :

- [Informations sur les contrôleurs](#)
  - [Informations sur les tiroirs disques](#)
  - [Informations sur les commutateurs de stockage](#)
3. Depuis ONTAP 9.12.1, vous pouvez consulter les informations relatives au câblage dans System Manager. Cliquez sur la case à cocher **Afficher les câbles** pour afficher le câblage, puis passez le curseur sur un câble pour afficher ses informations de connectivité.
    - [Informations sur le câblage](#)

### Informations sur les contrôleurs

Vous pouvez afficher les éléments suivants :



## Nœuds

- Vous pouvez afficher les vues avant et arrière.
- Sur les modèles avec tiroir disque interne, vous pouvez également afficher la disposition des disques dans la vue avant.
- Vous pouvez afficher les plates-formes suivantes :

| Plateforme  | Pris en charge dans System Manager dans la version ONTAP... |        |        |        |        |        |       |                              |
|-------------|-------------------------------------------------------------|--------|--------|--------|--------|--------|-------|------------------------------|
|             | 9.15.1                                                      | 9.14.1 | 9.13.1 | 9.12.1 | 9.11.1 | 9.10.1 | 9.9.1 | 9.8 (mode aperçu uniquement) |
| AFF A70     | Oui.                                                        |        |        |        |        |        |       |                              |
| AFF A90     | Oui.                                                        |        |        |        |        |        |       |                              |
| AFF A1K     | Oui.                                                        |        |        |        |        |        |       |                              |
| AFF A150    | Oui.                                                        | Oui.   | Oui.   |        |        |        |       |                              |
| AFF A220    | Oui.                                                        | Oui.   | Oui.   | Oui.   | Oui.   | Oui.   | Oui.  | Oui.                         |
| AFF A250    | Oui.                                                        | Oui.   | Oui.   | Oui.   | Oui.   | Oui.   | Oui.  |                              |
| AFF A300    | Oui.                                                        | Oui.   | Oui.   | Oui.   | Oui.   | Oui.   | Oui.  | Oui.                         |
| A320 de AFF | Oui.                                                        | Oui.   | Oui.   | Oui.   | Oui.   | Oui.   | Oui.  |                              |
| AFF A400    | Oui.                                                        | Oui.   | Oui.   | Oui.   | Oui.   | Oui.   | Oui.  | Oui.                         |
| AFF A700    | Oui.                                                        | Oui.   | Oui.   | Oui.   | Oui.   | Oui.   | Oui.  | Oui.                         |
| AFF A700s   | Oui.                                                        | Oui.   | Oui.   | Oui.   | Oui.   | Oui.   | Oui.  |                              |
| AFF A800    | Oui.                                                        | Oui.   | Oui.   | Oui.   | Oui.   | Oui.   | Oui.  |                              |

|               |      |      |      |             |             |             |      |      |
|---------------|------|------|------|-------------|-------------|-------------|------|------|
| Baie AFF C190 | Oui. | Oui. | Oui. | Oui.        | Oui.        | Oui.        | Oui. | Oui. |
| AFF C250      | Oui. | Oui. | Oui. | Oui et 42 ; | Oui et 42 ; | Oui et 42 ; |      |      |
| AFF C400      | Oui. | Oui. | Oui. | Oui et 42 ; | Oui et 42 ; | Oui et 42 ; |      |      |
| AFF C800      | Oui. | Oui. | Oui. | Oui et 42 ; | Oui et 42 ; | Oui et 42 ; |      |      |
| ASA A150      | Oui. | Oui. | Oui. |             |             |             |      |      |
| ASA A250      | Oui. | Oui. | Oui. |             |             |             |      |      |
| ASA A400      | Oui. | Oui. | Oui. |             |             |             |      |      |
| ASA A800      | Oui. | Oui. | Oui. |             |             |             |      |      |
| ASA A900      | Oui. | Oui. | Oui. |             |             |             |      |      |
| ASA C250      | Oui. | Oui. | Oui. |             |             |             |      |      |
| ASA C400      | Oui. | Oui. | Oui. |             |             |             |      |      |
| ASA C800      | Oui. | Oui. | Oui. |             |             |             |      |      |
| FAS500f       | Oui. | Oui. | Oui. | Oui.        | Oui.        | Oui.        | Oui. |      |
| FAS2720       | Oui. | Oui. | Oui. | Oui.        | Oui.        |             |      |      |
| FAS2750       | Oui. | Oui. | Oui. | Oui.        | Oui.        |             |      |      |
| FAS8300       | Oui. | Oui. | Oui. | Oui.        | Oui.        |             |      |      |
| FAS8700       | Oui. | Oui. | Oui. | Oui.        | Oui.        |             |      |      |

|         |      |      |      |      |      |  |  |  |
|---------|------|------|------|------|------|--|--|--|
| FAS9000 | Oui. | Oui. | Oui. | Oui. | Oui. |  |  |  |
| FAS9500 | Oui. | Oui. | Oui. | Oui. | Oui. |  |  |  |

### Ports

- Un port s'affiche en rouge s'il est arrêté.
- Lorsque vous positionnez le curseur de votre souris sur le port, vous pouvez afficher l'état d'un port et d'autres informations.
- Vous ne pouvez pas afficher les ports console.

### Notes :

- Pour ONTAP 9.10.1 et les versions antérieures, les ports SAS s'affichent en rouge lorsqu'ils sont désactivés.
- À partir de ONTAP 9.11.1, les ports SAS sont mis en surbrillance en rouge uniquement s'ils sont en état d'erreur ou si un port câblé utilisé est mis hors ligne. Les ports apparaissent en blanc s'ils sont hors ligne et non accessibles.

### Unités remplaçables sur site

Les informations relatives aux FRU ne s'affichent que lorsque l'état d'une unité remplaçable sur site est non optimal.

- Défaillance des blocs d'alimentation dans les nœuds ou le châssis.
- Températures élevées détectées dans les nœuds.
- Défaillance des ventilateurs sur les nœuds ou le châssis.

### Cartes d'adaptateur

- Les cartes avec des champs de numéro de pièce définis s'affichent dans les logements si des cartes externes ont été insérées.
- Les ports s'affichent sur les cartes.
- Pour une carte prise en charge, vous pouvez afficher les images de cette carte. Si la carte ne figure pas dans la liste des références prises en charge, un graphique générique apparaît.

### Informations sur les tiroirs disques

Vous pouvez afficher les éléments suivants :

### Tiroirs disques

- Vous pouvez afficher les vues avant et arrière.
- Vous pouvez afficher les modèles de tiroirs disques suivants :

|                                              |                                                                                            |
|----------------------------------------------|--------------------------------------------------------------------------------------------|
| Si votre système est en cours d'exécution... | Vous pouvez ensuite utiliser System Manager pour afficher...                               |
| ONTAP 9.9.1 et versions ultérieures          | Tous les tiroirs qui ont été désignés comme « fin de service » ou « fin de disponibilité » |
| ONTAP 9.8                                    | DS4243, DS4486, DS212C, DS2246, DS224C, Et NS224                                           |

### Ports de tiroir

- Vous pouvez afficher l'état des ports.
- Vous pouvez afficher des informations sur les ports distants si le port est connecté.

### Unités remplaçables sur site

- Les informations de panne de bloc d'alimentation s'affichent.

## Informations sur les commutateurs de stockage

Vous pouvez afficher les éléments suivants :

### Commutateurs de stockage

- L'écran affiche les commutateurs qui font office de commutateurs de stockage utilisés pour connecter les tiroirs aux nœuds.
- Depuis la version ONTAP 9.9.1, System Manager affiche des informations sur un commutateur qui agit à la fois comme un commutateur de stockage et un cluster, qui peut également être partagé entre les nœuds d'une paire haute disponibilité.
- Les informations suivantes s'affichent :
  - Nom du commutateur
  - Adresse IP
  - Numéro de série
  - Version SNMP
  - Version du système
- Vous pouvez afficher les modèles de commutateurs de stockage suivants :

| Si votre système est en cours d'exécution... | Vous pouvez ensuite utiliser System Manager pour afficher...  |
|----------------------------------------------|---------------------------------------------------------------|
| ONTAP 9.11.1 ou version ultérieure           | Cisco Nexus 3232C<br>Cisco Nexus 9336C-FX2<br>Mellanox SN2100 |
| ONTAP 9.9.1 et 9.10.1                        | Cisco Nexus 3232C<br>Cisco Nexus 9336C-FX2                    |
| ONTAP 9.8                                    | Cisco Nexus 3232C                                             |

### Ports de commutateur de stockage

- Les informations suivantes s'affichent :
  - Nom d'identité
  - Index d'identité
  - État
  - Connexion à distance
  - Autres détails

### Informations sur le câblage

Depuis ONTAP 9.12.1, vous pouvez consulter les informations de câblage suivantes :

- **Câblage** entre contrôleurs, commutateurs et tiroirs lorsqu'aucun pont de stockage n'est utilisé
- **Connectivité** qui affiche les ID et les adresses MAC des ports de chaque extrémité du câble

### Gérez les nœuds avec System Manager

System Manager vous permet d'ajouter des nœuds à un cluster et de les renommer. Vous pouvez également redémarrer, prendre le contrôle et renvoyer les nœuds.

## Ajout de nœuds à un cluster

Vous pouvez augmenter la taille et les fonctionnalités de votre cluster en ajoutant de nouveaux nœuds.

### Avant de commencer

Vous devriez déjà avoir câblé les nouveaux nœuds au cluster.

### Description de la tâche

Il existe des processus distincts pour travailler avec System Manager dans ONTAP 9.7 ou ONTAP 9.8 et versions ultérieures.

#### Procédure ONTAP 9.8 et ultérieure

##### Ajout de nœuds à un cluster avec System Manager (ONTAP 9.8 et versions ultérieures)

#### Étapes

1. Sélectionnez **Cluster > Présentation**.

Les nouveaux contrôleurs s'affichent sous forme de nœuds connectés au réseau du cluster, mais ils ne se trouvent pas dans le cluster.

2. Sélectionnez **Ajouter**.

- Les nœuds sont ajoutés au cluster.
- Le stockage est alloué implicitement.

#### Procédure ONTAP 9.7

##### Ajout de nœuds à un cluster avec System Manager (ONTAP 9.7)

#### Étapes

1. Sélectionnez **(Retour à la version classique)**.
2. Sélectionnez **configurations > extension de cluster**.

System Manager détecte automatiquement les nouveaux nœuds.

3. Sélectionnez **passer à la nouvelle expérience**.
4. Sélectionnez **Cluster > Présentation** pour afficher les nouveaux nœuds.

## Arrêtez, redémarrez ou modifiez le processeur de service

Lorsque vous redémarrez ou arrêtez un nœud, son partenaire haute disponibilité exécute automatiquement un basculement.

### Étapes

1. Sélectionnez **Cluster > Présentation**.
2. Sous **nœuds**, sélectionnez .
3. Sélectionnez le nœud, puis sélectionnez **Arrêter**, **redémarrer** ou **Modifier le processeur de service**.

Si un nœud a été redémarré et attend le rétablissement, l'option **Giveback** est également disponible.


Si vous sélectionnez **Modifier le processeur de service**, vous pouvez choisir **Manuel** pour saisir

l'adresse IP, le masque de sous-réseau et la passerelle, ou choisir **DHCP** pour la configuration dynamique de l'hôte.

### Renommer les nœuds

Depuis la version ONTAP 9.14.1, vous pouvez renommer un nœud depuis la page de présentation du cluster.

#### Étapes

1. Sélectionnez **Cluster**. La page de présentation du cluster s'affiche.
2. Faites défiler jusqu'à la section **nœuds**.
3. En regard du nœud que vous souhaitez renommer, sélectionnez , puis sélectionnez **Renommer**.
4. Modifiez le nom du nœud, puis sélectionnez **Renommer**.

## Gestion des licences

### Présentation des licences ONTAP

Une licence est un enregistrement d'un ou plusieurs droits logiciels. À partir de ONTAP 9.10.1, toutes les licences sont livrées sous forme de fichier de licence NetApp (NLF), qui est un fichier unique qui active plusieurs fonctionnalités. À partir de mai 2023, tous les systèmes AFF (A-Series et C-Series) et FAS sont vendus avec la suite logicielle ONTAP One ou la suite logicielle de base ONTAP. À partir de juin 2023, tous les systèmes ASA sont vendus avec ONTAP One pour SAN. Chaque suite logicielle est fournie en tant que NLF unique, en remplacement des bundles NLF distincts introduits en premier dans ONTAP 9.10.1.

#### Licences incluses avec ONTAP One

ONTAP One contient toutes les fonctionnalités sous licence disponibles. Le tableau ci-dessous répertorie les contenus des anciens bundles de base, de protection des données, de sécurité et de conformité, de cloud hybride et de chiffrement. Le chiffrement n'est pas disponible dans les pays soumis à des restrictions.

| Ancien nom de bundle                | Clés ONTAP incluses                        |
|-------------------------------------|--------------------------------------------|
| Bundle principal                    | FlexClone                                  |
|                                     | SnapRestore                                |
|                                     | NFS, SMB, S3                               |
|                                     | FC et iSCSI                                |
|                                     | NVME-of                                    |
| Bundle de sécurité et de conformité | Protection autonome contre les ransomwares |
|                                     | MTKM                                       |
|                                     | SnapLock                                   |

|                                  |                                                                          |
|----------------------------------|--------------------------------------------------------------------------|
| Bundle de protection des données | SnapMirror (réplication asynchrone, synchrone, continuité de l'activité) |
|                                  | SnapCenter                                                               |
|                                  | SnapMirror S3 pour les cibles NetApp                                     |
| Bundle de cloud hybride          | Cloud SnapMirror                                                         |
|                                  | SnapMirror S3 pour les cibles non-NetApp                                 |
| Pack de chiffrement              | NetApp Volume Encryption                                                 |
|                                  | Module de plate-forme sécurisée                                          |

### Licences non incluses avec ONTAP One

ONTAP One n'inclut pas les services fournis dans le cloud de NetApp, notamment :

- Tiering BlueXP
- Cloud Insights
- Sauvegarde BlueXP
- Gouvernance

### ONTAP One pour les systèmes existants

Si vos systèmes existants sont actuellement pris en charge par NetApp, mais n'ont pas été mis à niveau vers ONTAP One, les licences existantes sur ces systèmes sont toujours valides et continuent de fonctionner comme prévu. Par exemple, si la licence SnapMirror est déjà installée sur les systèmes existants, il n'est pas nécessaire de passer à ONTAP One pour obtenir une nouvelle licence SnapMirror. Toutefois, si aucune licence SnapMirror n'est installée sur un système existant, la seule façon d'obtenir cette licence est de passer à ONTAP One moyennant des frais supplémentaires.

À partir de juin 2023, les systèmes ONTAP utilisant des clés de licence de 28 caractères peuvent également être utilisés "[Passez au pack de compatibilité ONTAP One ou ONTAP base](#)".

### Licences incluses avec ONTAP base

ONTAP base est une suite logicielle en option qui constitue une alternative à ONTAP One pour les systèmes ONTAP. C'est pour des utilisations spécifiques où les technologies de protection des données telles que SnapMirror et SnapCenter, ainsi que les fonctionnalités de sécurité telles que les ransomwares autonomes, ne sont pas requises, comme les systèmes non-production pour des environnements de test ou de développement dédiés. Des licences supplémentaires ne peuvent pas être ajoutées à ONTAP base. Si vous souhaitez disposer de licences supplémentaires, telles que SnapMirror, vous devez effectuer une mise à niveau vers ONTAP One.

| Ancien nom de bundle | Clés ONTAP incluses |
|----------------------|---------------------|
|----------------------|---------------------|



|                     |                                 |
|---------------------|---------------------------------|
| Bundle principal    | FlexClone                       |
|                     | SnapRestore                     |
|                     | NFS, SMB, S3                    |
|                     | FC et iSCSI                     |
|                     | NVME-of                         |
| Pack de chiffrement | NetApp Volume Encryption        |
|                     | Module de plate-forme sécurisée |

## Licences incluses avec ONTAP One pour SAN

ONTAP One pour SAN est disponible pour les systèmes ASA A-Series et C-Series. Il s'agit de la seule suite logicielle disponible pour SAN. ONTAP One pour SAN contient les licences suivantes :

|                                                                          |
|--------------------------------------------------------------------------|
| Clés ONTAP incluses                                                      |
| FlexClone                                                                |
| SnapRestore                                                              |
| FC et iSCSI                                                              |
| NVME-of                                                                  |
| MTKM                                                                     |
| SnapLock                                                                 |
| SnapMirror (réplication asynchrone, synchrone, continuité de l'activité) |
| SnapCenter                                                               |
| Cloud SnapMirror                                                         |
| NetApp Volume Encryption                                                 |
| Module de plate-forme sécurisée                                          |

## Autres méthodes de livraison de licence

Dans ONTAP 8.2 à ONTAP 9.9.1, les clés de licence sont livrées sous forme de chaînes de 28 caractères, et une clé par fonctionnalité ONTAP est disponible. Vous utilisez l'interface de ligne de commande ONTAP pour installer les clés de licence si vous utilisez ONTAP 8.2 à ONTAP 9.9.1.



ONTAP 9.10.1 prend en charge l'installation de clés de licence à 28 caractères à l'aide de System Manager ou de l'interface de ligne de commandes. Toutefois, si une licence NLF est installée pour une fonction, vous ne pouvez pas installer une clé de licence de 28 caractères sur le fichier de licence NetApp pour la même fonction. Pour plus d'informations sur l'installation de NLF ou de clés de licence à l'aide de System Manager, reportez-vous à la section "[Installez les licences ONTAP](#)".

## Informations associées

["Comment obtenir une licence ONTAP One lorsque le système possède déjà des NLF"](#)

["Vérification des droits du logiciel ONTAP et des clés de licence associées à l'aide du site de support"](#)

## Téléchargez les fichiers de licence NetApp (NLF) sur le site du support NetApp

Si votre système exécute ONTAP 9.10.1 ou une version ultérieure, vous pouvez mettre à niveau les fichiers de licence de l'offre groupée sur des systèmes existants en téléchargeant le fichier NLF pour ONTAP One ou ONTAP Core sur le site de support NetApp.



Les licences SnapMirror cloud et SnapMirror S3 ne sont pas incluses avec ONTAP One. Ils font partie de l'offre de compatibilité ONTAP One, que vous pouvez obtenir gratuitement si vous avez ONTAP One et ["à demander séparément"](#).

### Étapes

Vous pouvez télécharger les fichiers de licence ONTAP One pour les systèmes dotés de packs de fichiers de licence NetApp existants et pour les systèmes dotés de clés de licence de 28 caractères qui ont été converties en fichiers de licence NetApp sur les systèmes exécutant ONTAP 9.10.1 et versions ultérieures. Moyennant un supplément, vous pouvez également mettre à niveau les systèmes de ONTAP base vers ONTAP One.

### Mettre à niveau NLF existant

1. Contactez votre équipe commerciale NetApp et demandez le pack de fichiers de licence que vous souhaitez mettre à niveau ou convertir (par exemple, ONTAP base vers ONTAP One ou bundle de base et de protection des données vers ONTAP One).

Une fois votre demande traitée, vous recevrez un e-mail de [netappsw@netapp.com](mailto:netappsw@netapp.com) contenant l'objet « notification de licence logicielle NetApp pour la COMMANDE n° [numéro de COMMANDE] » et l'e-mail inclura une pièce jointe au format PDF qui inclut votre numéro de série de licence.

2. Connectez-vous au "[Site de support NetApp](#)".
3. Sélectionnez **systèmes > licences logicielles**.
4. Dans le menu, choisissez **Numéro de série**, entrez le numéro de série que vous avez reçu, puis cliquez sur **Nouvelle recherche**.
5. Recherchez le pack de licences que vous souhaitez convertir.
6. Cliquez sur **obtenir le fichier de licence NetApp** pour chaque ensemble de licences et téléchargez les fichiers NLF lorsqu'ils sont disponibles.
7. "[Installer](#)" Le fichier ONTAP One.

### Mise à niveau NLF convertie à partir de la clé de licence

1. Connectez-vous au "[Site de support NetApp](#)".
2. Sélectionnez **systèmes > licences logicielles**.
3. Dans le menu, choisissez **Numéro de série**, entrez le numéro de série du système et cliquez sur **Nouvelle recherche**.
4. Recherchez la licence que vous souhaitez convertir et, dans la colonne **admissibilité**, cliquez sur **vérifier**.
5. Dans le formulaire **vérifier l'admissibilité**, cliquez sur **générer des licences pour 9.10.x et versions ultérieures**.
6. Fermez le formulaire **vérifier admissibilité**.

Vous devez attendre au moins 2 heures pour que les licences soient générées.

7. Répétez les étapes 1 à 3.
8. Recherchez la licence ONTAP One, cliquez sur **obtenir le fichier de licence NetApp** et choisissez la méthode de livraison.
9. "[Installer](#)" Le fichier ONTAP One.

## Installez les licences ONTAP

Vous pouvez installer les fichiers de licence NetApp (NLF) et les clés de licence à l'aide du Gestionnaire système, qui est la méthode préférée pour installer les NLF, ou vous pouvez utiliser l'interface de ligne de commande ONTAP pour installer les clés de licence. Dans ONTAP 9.10.1 et versions ultérieures, les fonctionnalités sont activées avec un fichier de licence NetApp et dans les versions antérieures à ONTAP 9.10.1, les fonctionnalités ONTAP sont activées avec des clés de licence.

## Étapes

Si vous l'avez déjà "[Fichiers de licence NetApp téléchargés](#)" Ou des clés de licence, vous pouvez utiliser System Manager ou l'interface de ligne de commandes ONTAP pour installer des NLF et des clés de licence à 28 caractères.

### System Manager - ONTAP 9.8 et versions ultérieures

1. Sélectionnez **Cluster > Paramètres**.
2. Sous **licences**, sélectionnez ➔.
3. Sélectionnez **Parcourir**. Choisissez le fichier de licence NetApp que vous avez téléchargé.
4. Si vous souhaitez ajouter des clés de licence, sélectionnez **utiliser des clés de licence à 28 caractères** et entrez les clés.

### System Manager - ONTAP 9.7 et versions antérieures

1. Sélectionnez **Configuration > Cluster > licences**.
2. Sous **licences**, sélectionnez ➔.
3. Dans la fenêtre **Forfaits**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Add License Packages**, cliquez sur **Choose files** pour sélectionner le fichier de licence NetApp que vous avez téléchargé, puis cliquez sur **Add** pour télécharger le fichier sur le cluster.

## CLI

1. Ajoutez une ou plusieurs clés de licence :

```
system license add
```

L'exemple suivant installe les licences à partir du nœud local "/mroot/etc/lic\_file" si le fichier existe à cet emplacement :

```
cluster1::> system license add -use-license-file true
```

L'exemple suivant ajoute une liste de licences avec les clés  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA et  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB au cluster :

```
cluster1::> system license add -license-code
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA, BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
```

## Informations associées

- .

## Gérer les licences ONTAP

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour afficher et gérer les licences installées sur votre système, notamment l'affichage du numéro de série de licence, la vérification du statut d'une licence et la suppression d'une licence.

### Afficher les détails d'une licence

#### Étapes

La façon dont vous affichez les détails sur une licence dépend de la version de ONTAP que vous utilisez et si vous utilisez System Manager ou l'interface de ligne de commande de ONTAP.

#### System Manager - ONTAP 9.8 et versions ultérieures

1. Pour afficher des détails sur une licence de fonction spécifique, sélectionnez **Cluster > Paramètres**.
2. Sous **licences**, sélectionnez ➔.
3. Sélectionnez **caractéristiques**.
4. Recherchez la fonction sous licence que vous souhaitez afficher et sélectionnez ▼ pour afficher les détails de la licence.

#### System Manager - ONTAP 9.7 et versions antérieures

1. Sélectionnez **Configuration > Cluster > licences**.
2. Dans la fenêtre **Licenses**, effectuez l'action appropriée :
3. Cliquez sur l'onglet **Détails**.

#### CLI

1. Afficher les détails d'une licence installée :

```
system license show
```

### Supprimer une licence

### System Manager - ONTAP 9.8 et versions ultérieures

1. Pour supprimer une licence, sélectionnez **Cluster > Paramètres**.
2. Sous **licences**, sélectionnez ➔.
3. Sélectionnez **caractéristiques**.
4. Sélectionnez la fonction sous licence que vous souhaitez supprimer et **Supprimer la clé héritée**.

### System Manager - ONTAP 9.7 et versions antérieures

1. Sélectionnez **Configuration > Cluster > licences**.
2. Dans la fenêtre **Licenses**, effectuez l'action appropriée :

| Les fonctions que vous recherchez...                                          | Procédez comme ça...                   |
|-------------------------------------------------------------------------------|----------------------------------------|
| Supprimer un package de licences spécifique sur un nœud ou une licence maître | Cliquez sur l'onglet <b>Détails</b> .  |
| Supprime un pack de licences spécifique sur tous les nœuds du cluster         | Cliquez sur l'onglet <b>Packages</b> . |

3. Sélectionnez le package de licences logicielles que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

Vous ne pouvez supprimer qu'un seul package de licences à la fois.

4. Cochez la case de confirmation, puis cliquez sur **Supprimer**.

### CLI

1. Supprimer une licence :

```
system license delete
```

L'exemple suivant illustre la suppression d'une licence nommée CIFS et du numéro de série 1-81-00000000000000000000123456 du cluster :

```
cluster1::> system license delete -serial-number 1-81-00000000000000000000123456 -package CIFS
```

L'exemple suivant supprime du cluster toutes les licences du pack de licences installées pour le numéro de série 123456789 :

```
cluster1::> system license delete { -serial-number 123456789 -installed-license "Core Bundle" }
```

### Informations associées

## Types de licence et méthode sous licence

La compréhension des types de licence et la méthode sous licence vous aident à gérer les licences dans un cluster.

### Types de licence

Un pack peut disposer d'un ou plusieurs des types de licence suivants installés dans le cluster. Le `system license show` commande affiche le ou les types de licence installés pour un package.

- Licence standard (`license`)

Une licence standard est une licence verrouillée par un nœud. Il est émis pour un nœud avec un numéro de série système spécifique (également appelé *numéro de série du contrôleur*). Une licence standard n'est valide que pour le nœud qui possède le numéro de série correspondant.

L'installation d'une licence standard verrouillée par un nœud donne droit à la fonctionnalité sous licence d'un nœud. Pour que le cluster utilise la fonctionnalité sous licence, au moins un nœud doit être sous licence pour cette fonctionnalité. Il se peut qu'il soit hors conformité pour utiliser la fonctionnalité sous licence sur un nœud qui ne dispose pas d'un droit pour la fonctionnalité.

- Licence de site (`site`)

Une licence de site n'est pas liée à un numéro de série de système spécifique. Lorsque vous installez une licence de site, tous les nœuds du cluster ont droit à la fonctionnalité sous licence. Le `system license show` la commande affiche les licences du site sous le numéro de série du cluster.

Si votre cluster dispose d'une licence de site et que vous supprimez un nœud du cluster, le nœud ne dispose pas de la licence de site et il n'est plus autorisé à utiliser la fonctionnalité sous licence. Si vous ajoutez un nœud à un cluster qui possède une licence de site, le nœud a automatiquement droit à la fonctionnalité accordée par la licence de site.

- Licence d'évaluation (`demo`)

Une licence d'évaluation est une licence temporaire qui expire après une certaine période (indiquée par le `system license show` commande). Il vous permet d'essayer certaines fonctionnalités logicielles sans avoir à acheter un droit. Il s'agit d'une licence à l'échelle du cluster, qui n'est pas liée à un numéro de série spécifique d'un nœud.

Si votre cluster dispose d'une licence d'évaluation pour un package et que vous supprimez un nœud du cluster, celui-ci ne supporte pas la licence d'évaluation.

### Méthode sous licence

Il est possible d'installer une licence au niveau du cluster ( `site` ou `demo` type) et une licence verrouillée par nœud ( `license` type) pour un package. Par conséquent, un package installé peut avoir plusieurs types de licence au sein du cluster. Cependant, pour le cluster, il n'y a qu'une seule méthode *licensed* pour un package. Le `licensed method` champ du `system license status show` commande affiche le droit utilisé pour le pack. La commande détermine la méthode sous licence comme suit :

- Si un pack ne comporte qu'un seul type de licence installé dans le cluster, le type de licence installé est la méthode sous licence.
- Si aucune licence n'est installée dans le pack, la méthode sous licence est `none`.
- Si plusieurs types de licence sont installés sur un package, la méthode sous licence est déterminée dans l'ordre de priorité suivant du type de licence `:-site, license, et demo`.

Par exemple :

- Si vous disposez d'une licence de site, d'une licence standard et d'une licence d'évaluation pour un package, la méthode sous licence pour le package du cluster est `site`.
- Si vous disposez d'une licence standard et d'une licence d'évaluation pour un package, la méthode sous licence pour le package du cluster est `license`.
- Si vous ne disposez que d'une licence d'évaluation pour un package, la méthode sous licence pour le package du cluster est `demo`.

## Commandes de gestion des licences

Vous pouvez utiliser l'interface de ligne de commandes de ONTAP `system license` commandes permettant de gérer les licences des fonctions pour le cluster. Vous utilisez le `system feature-usage` commandes permettant de contrôler l'utilisation des fonctions.

Le tableau suivant répertorie certaines des commandes CLI courantes pour la gestion des licences et des liens vers les pages man de commandes pour plus d'informations.

| Les fonctions que vous recherchez...                                                                                                                                                                                                                                           | Utilisez cette commande...                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Afficher tous les packages qui requièrent des licences et leur état actuel de licence, y compris les éléments suivants : <ul style="list-style-type: none"> <li>• Nom du package</li> <li>• La méthode sous licence</li> <li>• La date d'expiration, le cas échéant</li> </ul> | " <a href="#">licence système show-status</a> "                                      |
| Afficher ou supprimer les licences expirées ou inutilisées                                                                                                                                                                                                                     | " <a href="#">nettoyage de la licence système</a> "                                  |
| Affiche un récapitulatif de l'utilisation des fonctionnalités dans le cluster par nœud                                                                                                                                                                                         | " <a href="#">récapitulatif de l'utilisation des fonctionnalités du système</a> "    |
| Affiche l'état d'utilisation de la fonction dans le cluster par nœud et par semaine                                                                                                                                                                                            | " <a href="#">historique d'affichage de l'utilisation des fonctions du système</a> " |



| Les fonctions que vous recherchez...                                         | Utilisez cette commande...                               |
|------------------------------------------------------------------------------|----------------------------------------------------------|
| Affiche l'état du risque de droit de licence pour chaque package de licences | " <a href="#">licence système - risque-droits show</a> " |

#### Informations associées

- ["Référence de commande ONTAP"](#)
- ["Article de la base de connaissances : présentation des licences ONTAP 9.10.1 et versions ultérieures"](#)
- ["Utilisez System Manager pour installer un fichier de licence NetApp"](#)

## Gestion du cluster via l'interface de ligne de commandes

### Présentation de l'administration avec l'interface de ligne de commande

Vous pouvez administrer les systèmes ONTAP via l'interface de ligne de commandes. Vous pouvez utiliser les interfaces de gestion ONTAP, accéder au cluster, gérer les nœuds et bien plus encore.

Vous devez utiliser ces procédures dans les circonstances suivantes :

- Vous voulez connaître la gamme de fonctionnalités d'administration ONTAP.
- Vous souhaitez utiliser l'interface de ligne de commandes, et non System Manager ou un outil de script automatisé.

#### Informations associées

Pour plus d'informations sur la syntaxe et l'utilisation de l'interface de ligne de commande, reportez-vous à la ["Référence de commande ONTAP"](#) documentation.

## Administrateurs Cluster et SVM

### Administrateurs Cluster et SVM

Les administrateurs du cluster administrent le cluster entier et les machines virtuelles de stockage (SVM, anciennement appelées vServers) qu'ils contiennent. Les administrateurs SVM n'administrent que leurs propres SVM de données.

Les administrateurs du cluster peuvent administrer l'ensemble du cluster et ses ressources. Ils peuvent également configurer des SVM de données et déléguer l'administration des SVM aux administrateurs des SVM. Les fonctionnalités spécifiques des administrateurs du cluster dépendent de leurs rôles de contrôle d'accès. Par défaut, un administrateur de cluster avec le nom de compte ou de rôle « admin » dispose de toutes les fonctionnalités de gestion du cluster et des SVM.

Les administrateurs du SVM ne peuvent gérer que leurs propres ressources de stockage et réseau SVM, telles que les volumes, les protocoles, les LIF et les services. Les fonctionnalités spécifiques des administrateurs SVM dépendent des rôles de contrôle d'accès qui sont attribués par les administrateurs du cluster.



L'interface de ligne de commande (CLI) ONTAP continue d'utiliser le terme *Vserver* dans la sortie, et `vserver` comme une commande ou un nom de paramètre n'a pas changé.

## Gérez l'accès à System Manager

Vous pouvez activer ou désactiver l'accès d'un navigateur Web à System Manager. Vous pouvez également afficher le journal de System Manager.

Vous pouvez contrôler l'accès d'un navigateur Web à System Manager à l'aide de `vserver services web modify -name sysmgr -vserver cluster_name -enabled[true|false]`.

La journalisation de System Manager est enregistrée dans le `/mroot/etc/log/mlog/sysmgr.log` Fichiers du nœud qui héberge la LIF de gestion du cluster au moment où System Manager est accessible. Vous pouvez afficher les fichiers journaux à l'aide d'un navigateur. Le journal de System Manager est également inclus dans les messages AutoSupport.

## Qu'est-ce que le serveur de gestion du cluster

Le serveur de gestion de cluster, également appelé *adminSVM*, est une implémentation SVM spécialisée qui présente le cluster comme une seule entité gérable. Outre les services faisant office de domaine d'administration de niveau le plus élevé, le serveur de gestion du cluster possède des ressources qui n'appartiennent pas de façon logique à un SVM de données.

Le serveur de gestion du cluster est toujours disponible sur le cluster. Vous pouvez accéder au serveur de gestion du cluster par le biais de la console ou du LIF de gestion du cluster.

En cas de défaillance de son port réseau local, la LIF de gestion du cluster bascule automatiquement vers un autre nœud du cluster. En fonction des caractéristiques de connectivité du protocole de gestion que vous utilisez, vous risquez de remarquer ou non le basculement. Si vous utilisez un protocole sans connexion (par exemple, SNMP) ou que vous disposez d'une connexion limitée (par exemple, HTTP), il est peu probable que vous remarquiez le basculement. Cependant, si vous utilisez une connexion à long terme (par exemple, SSH), vous devrez vous reconnecter au serveur de gestion du cluster après le basculement.

Lorsque vous créez un cluster, toutes les caractéristiques de la LIF de gestion du cluster sont configurées, y compris son adresse IP, son masque de réseau, sa passerelle et son port.

Contrairement à un SVM de données ou à un SVM de nœuds, un serveur de gestion du cluster ne possède pas de volume root ni de volumes utilisateur hôte (bien qu'il puisse héberger les volumes du système). En outre, un serveur de gestion du cluster ne peut avoir que des LIFs du type cluster management.

Si vous exécutez le `vserver show` commande, le serveur de gestion du cluster apparaît dans la liste de sortie de cette commande.

## Types de SVM

Un cluster se compose de quatre types de SVM, ce qui facilite la gestion du cluster, ainsi que de ses ressources et de l'accès aux données aux clients et aux applications.

Un cluster contient les types suivants de SVM :

- SVM d'administration

Le processus d'installation du cluster crée automatiquement le SVM d'admin pour le cluster. Le SVM admin représente le cluster.

- SVM de nœuds

Un SVM de nœud est créé lorsque le nœud rejoint le cluster, et le SVM de nœud représente les différents nœuds du cluster.

- System SVM (avancé)

Un SVM système est automatiquement créé pour les communications au niveau du cluster dans un IPspace.

- SVM de données

Un SVM de données représente le service des SVM de données. Une fois le cluster setup, un administrateur de cluster doit créer des SVM de données et ajouter des volumes à ces SVM afin de faciliter l'accès aux données depuis le cluster.

Un cluster doit disposer d'au moins un SVM de données pour transmettre des données à ses clients.



Sauf indication contraire, le terme SVM désigne un SVM de données (service de données).

Dans l'interface de ligne de commandes, les SVM sont affichés comme vServers.

## Accès au cluster via l'interface de ligne de commandes (administrateurs de cluster uniquement)

### Accéder au cluster via le port série

Vous pouvez accéder directement au cluster depuis une console connectée au port série d'un nœud.

#### Étapes

1. Sur la console, appuyez sur entrée.

Le système répond avec l'invite de connexion.

2. À l'invite de connexion, effectuez l'une des opérations suivantes :

| Pour accéder au cluster avec...             | Entrez le nom de compte suivant... |
|---------------------------------------------|------------------------------------|
| Compte de cluster par défaut                | <b>admin</b>                       |
| Un autre compte d'utilisateur administratif | <i>username</i>                    |

Le système répond avec l'invite de mot de passe.

3. Entrez le mot de passe du compte administrateur ou administrateur, puis appuyez sur entrée.

## Accédez au cluster via SSH

Vous pouvez envoyer des requêtes SSH à un cluster ONTAP pour effectuer des tâches d'administration. SSH est activé par défaut.

### Avant de commencer

- Vous devez disposer d'un compte utilisateur configuré pour l'utilisation `ssh` comme méthode d'accès.

Le `-application` paramètre du `security login` les commandes spécifie la méthode d'accès pour un compte utilisateur. Le `security login` "[pages de manuel](#)" contiennent des informations supplémentaires.

- Si vous utilisez un compte d'utilisateur de domaine Active Directory (AD) pour accéder au cluster, un tunnel d'authentification pour le cluster doit avoir été configuré via une VM de stockage compatible CIFS et votre compte d'utilisateur de domaine AD doit également avoir été ajouté au cluster avec `ssh` comme méthode d'accès et `domain` comme méthode d'authentification.

### Description de la tâche

- Vous devez utiliser un client OpenSSH 5.7 ou version ultérieure.
- Seul le protocole SSH v2 est pris en charge ; SSH v1 n'est pas pris en charge.
- ONTAP prend en charge un maximum de 64 sessions SSH simultanées par nœud.

Si la LIF de cluster management réside sur le nœud, il partage cette limite avec la LIF de node management.

Si le taux de connexions entrantes est supérieur à 10 par seconde, le service est temporairement désactivé pendant 60 secondes.

- ONTAP ne prend en charge que les algorithmes de cryptage AES et 3DES (également appelés *chiffrements*) pour SSH.

AES est pris en charge avec des clés de 128, 192 et 256 bits. 3DES a une longueur clé de 56 bits comme dans les DES d'origine, mais elle est répétée trois fois.

- Lorsque le mode FIPS est activé, les clients SSH doivent négocier avec les algorithmes de clé publique ECDSA (Elliptic Curve Digital Signature Algorithm) pour que la connexion soit réussie.
- Pour accéder à l'interface de ligne de commandes de ONTAP à partir d'un hôte Windows, vous pouvez faire appel à un utilitaire tiers tel que PuTTY.
- Si vous utilisez un nom d'utilisateur Windows AD pour vous connecter à ONTAP, vous devez utiliser les mêmes lettres majuscules ou minuscules que celles qui ont été utilisées lorsque le nom d'utilisateur AD et le nom de domaine ont été créés dans ONTAP.

Les noms d'utilisateur ET de domaine AD ne sont pas sensibles à la casse. Toutefois, les noms d'utilisateur ONTAP sont sensibles à la casse. La non-concordance de cas entre le nom d'utilisateur créé dans ONTAP et le nom d'utilisateur créé dans AD entraîne un échec de connexion.

### Options d'authentification SSH

- À partir de ONTAP 9.3, vous pouvez "[Activez l'authentification multifacteur SSH](#)" pour les comptes d'administrateur local.

Lorsque l'authentification multifacteur SSH est activée, les utilisateurs sont authentifiés à l'aide d'une clé

publique et d'un mot de passe.

- À partir de ONTAP 9.4, vous pouvez "[Activez l'authentification multifacteur SSH](#)" Pour les utilisateurs distants LDAP et NIS.
- À partir de ONTAP 9.13.1, vous pouvez éventuellement ajouter la validation du certificat au processus d'authentification SSH afin d'améliorer la sécurité de la connexion. Pour ce faire, "[Associer un certificat X.509 à la clé publique](#)" qu'un compte utilise. Si vous vous connectez à l'aide de SSH avec une clé publique SSH et un certificat X.509, ONTAP vérifie la validité du certificat X.509 avant de vous authentifier à l'aide de la clé publique SSH. La connexion SSH est refusée si le certificat a expiré ou a été révoqué et si la clé publique SSH est automatiquement désactivée.
- À partir de ONTAP 9.14.1, les administrateurs ONTAP peuvent "[Ajoutez l'authentification à deux facteurs Cisco Duo au processus d'authentification SSH](#)" pour améliorer la sécurité de connexion. Lors de la première connexion après avoir activé l'authentification Cisco Duo, les utilisateurs doivent inscrire un périphérique pour qu'il serve d'authentificateur pour les sessions SSH.
- À partir de ONTAP 9.15.1, les administrateurs peuvent "[Configurer l'autorisation dynamique](#)" Fournir une authentification adaptative supplémentaire aux utilisateurs SSH en fonction du score de confiance de l'utilisateur.

## Étapes

1. Depuis un hôte disposant d'un accès au réseau du cluster ONTAP, entrez dans le champ `ssh` commande dans l'un des formats suivants :

- `ssh username@hostname_or_IP [command]`
- `ssh -l username hostname_or_IP [command]`

Si vous utilisez un compte utilisateur de domaine AD, vous devez le préciser *username* au format de *domainname\AD\_accountname* (avec doubles barres obliques inverses après le nom de domaine) ou "*domainname\AD\_accountname*" (entre guillemets doubles et avec une barre oblique inverse unique après le nom de domaine).

*hostname\_or\_IP* Est le nom d'hôte ou l'adresse IP de la LIF de cluster management ou une LIF de node management. Il est recommandé d'utiliser la LIF de cluster management. Vous pouvez utiliser une adresse IPv4 ou IPv6.

*command* N'est pas requis pour les sessions interactives SSH.

## Exemples de requêtes SSH

Les exemples suivants montrent comment le compte utilisateur nommé « joe » peut émettre une demande SSH pour accéder à un cluster dont la LIF de gestion du cluster est 10.72.137.28 :

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node Health Eligibility

node1 true true
node2 true true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node Health Eligibility

node1 true true
node2 true true
2 entries were displayed.
```

Les exemples suivants montrent comment le compte utilisateur nommé « john » du domaine nommé « 'DOMAIN1' » peut émettre une requête SSH pour accéder à un cluster dont la LIF de gestion de cluster est 10.72.137.28 :

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node Health Eligibility

node1 true true
node2 true true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node Health Eligibility

node1 true true
node2 true true
2 entries were displayed.
```

L'exemple suivant montre comment le compte utilisateur nommé « joe » peut émettre une demande SSH MFA pour accéder à un cluster dont la LIF de gestion du cluster est de 10.72.137.32 :

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node Health Eligibility

node1 true true
node2 true true
2 entries were displayed.
```

## Informations associées

### "Authentification de l'administrateur et RBAC"

## Sécurité de connexion SSH

À partir de ONTAP 9.5, vous pouvez afficher des informations sur les connexions précédentes, les tentatives infructueuses de connexion et les modifications apportées à vos privilèges depuis votre dernière connexion réussie.

Les informations relatives à la sécurité s'affichent lorsque vous vous connectez en tant qu'utilisateur administrateur SSH. Vous êtes averti des conditions suivantes :

- La dernière fois que votre nom de compte a été connecté.
- Nombre de tentatives de connexion infructueuses depuis la dernière connexion réussie.
- Si le rôle a changé depuis la dernière connexion (par exemple, si le rôle du compte admin est passé de « admin » à « backup »).
- Les fonctionnalités d'ajout, de modification ou de suppression du rôle ont été modifiées depuis la dernière connexion.



Si l'une des informations affichées est suspecte, contactez immédiatement votre service de sécurité.

Pour obtenir ces informations lors de votre connexion, les conditions préalables suivantes doivent être remplies :

- Votre compte utilisateur SSH doit être provisionné dans ONTAP.
- Votre identifiant de sécurité SSH doit être créé.
- Votre tentative de connexion doit réussir.

## Restrictions et autres considérations relatives à la sécurité de la connexion SSH

Les restrictions et considérations suivantes s'appliquent aux informations de sécurité de connexion SSH :

- Les informations sont disponibles uniquement pour les connexions SSH.
- Pour les comptes admin basés sur un groupe, tels que LDAP/NIS et comptes AD, les utilisateurs peuvent afficher les informations de connexion SSH si le groupe dont ils sont membres est provisionné en tant que compte d'administrateur dans ONTAP.

Cependant, les alertes relatives aux modifications du rôle du compte utilisateur ne peuvent pas être affichées pour ces utilisateurs. En outre, les utilisateurs appartenant à un groupe AD qui a été provisionné en tant que compte d'administrateur dans ONTAP ne peuvent pas afficher le nombre de tentatives de connexion ayant échoué qui se sont produites depuis la dernière connexion.

- Les informations conservées pour un utilisateur sont supprimées lorsque le compte utilisateur est supprimé de ONTAP.
- Les informations ne s'affichent pas pour les connexions à d'autres applications que SSH.

## Exemples d'informations de sécurité de la connexion SSH

Les exemples suivants illustrent le type d'informations affichées après votre connexion.

- Ce message s'affiche après chaque connexion réussie :

```
Last Login : 7/19/2018 06:11:32
```

- Ces messages s'affichent si des tentatives de connexion ont échoué depuis la dernière connexion réussie :

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- Ces messages s'affichent si des tentatives de connexion ont échoué et que vos privilèges ont été modifiés depuis la dernière connexion réussie :

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

### Activer l'accès Telnet ou RSH au cluster

En tant que pratique de sécurité, Telnet et RSH sont désactivés par défaut. Pour permettre au cluster d'accepter les demandes Telnet ou RSH, vous devez activer le service dans la stratégie de service de gestion par défaut.

Au fil du temps, la façon dont ONTAP gère le type de trafic pris en charge sur les LIF a changé.

- ONTAP 9.5 et les versions antérieures utilisent des rôles LIF et des services de pare-feu
- Les versions ONTAP 9.6 et ultérieures utilisent les stratégies de service LIF
  - La version ONTAP 9.5 a introduit les stratégies de service LIF
  - ONTAP 9.6 a remplacé les rôles LIF par des stratégies de service LIF
  - ONTAP 9.10.1 a remplacé les services de pare-feu par des politiques de service LIF

La méthode que vous configurez dépend de la version de ONTAP que vous utilisez.

Pour en savoir plus sur :

- Politiques de pare-feu, voir ["Commande : firewall-policy-show"](#)
- Rôles LIF, voir ["Rôles LIF \(ONTAP 9.5 et versions antérieures\)"](#)
- Politiques de service LIF, voir ["LIF et règles de service \(ONTAP 9.6 et versions ultérieures\)"](#)

Telnet et RSH ne sont pas des protocoles sécurisés, vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive. Pour plus d'informations, reportez-vous à la section ["Accédez au cluster via SSH"](#)



## ONTAP 9.6 ou version ultérieure

### Description de la tâche

- RSH n'est pas un protocole sécurisé.

Vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive.

- ONTAP prend en charge un maximum de 50 sessions RSH simultanées par nœud.

Si la LIF de cluster management réside sur le nœud, il partage cette limite avec la LIF de node management.

Si le taux de connexions entrantes est supérieur à 10 par seconde, le service est temporairement désactivé pendant 60 secondes.

- Les commandes RSH nécessitent des privilèges avancés.

### Étapes

1. Vérifiez que le protocole de sécurité RSH ou Telnet est activé :

```
security protocol show
```

- a. Si le protocole de sécurité RSH ou Telnet est activé, passez à l'étape suivante.
- b. Si le protocole de sécurité RSH ou Telnet n'est pas activé, utilisez la commande suivante pour l'activer :

```
security protocol modify -application <rsh/telnet> -enabled true
```

2. Vérifier que le `management-rsh-server service` ou `management-telnet-server` existe sur les LIFs de management :

```
network interface show -services management-rsh-server
```

ou

```
network interface show -services management-telnet-server
```

- a. Si le `management-rsh-server service` ou `management-telnet-server` existe, passez à l'étape suivante.
- b. Si le `management-rsh-server service` ou `management-telnet-server` n'existe pas, utilisez la commande suivante pour l'ajouter :

```
network interface service-policy add-service -vserver cluster1 -policy
default-management -service management-rsh-server
```

```
network interface service-policy add-service -vserver cluster1 -policy
default-management -service management-telnet-server
```

## ONTAP 9.5 ou version antérieure

### Description de la tâche

ONTAP vous empêche de modifier des règles de pare-feu prédéfinies, mais vous pouvez créer une

nouvelle règle en clonant la `mgmt` stratégie de pare-feu de gestion prédéfinie, puis en activant Telnet ou RSH dans le cadre de la nouvelle règle.

### Étapes

1. Saisissez le mode de privilège avancé :

```
set advanced
```

2. Activer un protocole de sécurité (RSH ou Telnet) :

```
security protocol modify -application security_protocol -enabled true
```

3. Créez une nouvelle politique de pare-feu de gestion basée sur `mgmt` la politique de pare-feu de gestion :

```
system services firewall policy clone -policy mgmt -destination-policy
policy-name
```

4. Activer Telnet ou RSH dans la nouvelle politique de pare-feu de gestion :

```
system services firewall policy create -policy policy-name -service
security_protocol -action allow -ip-list ip_address/netmask
```

Pour autoriser toutes les adresses IP, vous devez spécifier `-ip-list 0.0.0.0/0`

5. Associer la nouvelle politique au LIF de gestion du cluster :

```
network interface modify -vserver cluster_management_LIF -lif cluster_mgmt
-firewall-policy policy-name
```

### Accéder au cluster à l'aide de Telnet

Vous pouvez envoyer des requêtes Telnet au cluster pour effectuer des tâches administratives. Telnet est désactivé par défaut.

Au fil du temps, la façon dont ONTAP gère le type de trafic pris en charge sur les LIF a changé.

- ONTAP 9.5 et les versions antérieures utilisent des rôles LIF et des services de pare-feu
- Les versions ONTAP 9.6 et ultérieures utilisent les stratégies de service LIF
  - La version ONTAP 9.5 a introduit les stratégies de service LIF
  - ONTAP 9.6 a remplacé les rôles LIF par des stratégies de service LIF
  - ONTAP 9.10.1 a remplacé les services de pare-feu par des politiques de service LIF

La méthode que vous configurez dépend de la version de ONTAP que vous utilisez.

Pour en savoir plus sur :

- Politiques de pare-feu, voir ["Commande : firewall-policy-show"](#)
- Rôles LIF, voir ["Rôles LIF \(ONTAP 9.5 et versions antérieures\)"](#)

- Politiques de service LIF, voir ["LIF et règles de service \(ONTAP 9.6 et versions ultérieures\)"](#)

Telnet et RSH ne sont pas des protocoles sécurisés, vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive. Pour plus d'informations, reportez-vous à la section ["Accédez au cluster via SSH"](#)

## ONTAP 9.6 ou version ultérieure

### Avant de commencer

Les conditions suivantes doivent être remplies pour que vous puissiez utiliser Telnet pour accéder au cluster :

- Vous devez disposer d'un compte utilisateur local de cluster configuré pour utiliser Telnet.

Le `-application` paramètre du `security login` les commandes spécifie la méthode d'accès pour un compte utilisateur. Pour plus d'informations, reportez-vous à la section `security login` pages de manuel.

### Description de la tâche

- Telnet n'est pas un protocole sécurisé.

Vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive.

- ONTAP prend en charge un maximum de 50 sessions Telnet simultanées par nœud.

Si la LIF de cluster management réside sur le nœud, il partage cette limite avec la LIF de node management.

Si le taux de connexions en cours est supérieur à 10 par seconde, le service est temporairement désactivé pendant 60 secondes.

- Pour accéder à l'interface de ligne de commandes de ONTAP à partir d'un hôte Windows, vous pouvez faire appel à un utilitaire tiers tel que PuTTY.
- Les commandes RSH nécessitent des privilèges avancés.

### Étapes

1. Vérifiez que le protocole de sécurité Telnet est activé :

```
security protocol show
```

- a. Si le protocole de sécurité Telnet est activé, passez à l'étape suivante.
- b. Si le protocole de sécurité Telnet n'est pas activé, utilisez la commande suivante pour l'activer :

```
security protocol modify -application telnet -enabled true
```

2. Vérifier que le `management-telnet-server` service existe sur les LIFs de management :

```
network interface show -services management-telnet-server
```

- a. Si le `management-telnet-server` service existe, passez à l'étape suivante.
- b. Si le `management-telnet-server` service n'existe pas, utilisez la commande suivante pour l'ajouter :

```
network interface service-policy add-service -vserver cluster1 -policy
default-management -service management-telnet-server
```

### Exemple de requête Telnet

L'exemple suivant montre comment l'utilisateur nommé « joe », qui a été configuré avec un accès Telnet, peut émettre une demande Telnet pour accéder à un cluster dont la LIF de gestion du cluster est 10.72.137.28 :

```
admin_host$ telnet 10.72.137.28
Data ONTAP
login: joe
Password:
cluster1::>
```

### ONTAP 9.5 ou version antérieure

#### Avant de commencer

Les conditions suivantes doivent être remplies pour que vous puissiez utiliser Telnet pour accéder au cluster :

- Vous devez disposer d'un compte utilisateur local de cluster configuré pour utiliser Telnet.

Le `-application` paramètre des commandes de connexion de sécurité spécifie la méthode d'accès pour un compte utilisateur. Pour plus d'informations, consultez les pages de manuel de connexion de sécurité.

- Telnet doit déjà être activé dans la politique de pare-feu de gestion utilisée par les LIF de cluster ou de node management afin que les requêtes Telnet puissent passer par le pare-feu.

Par défaut, Telnet est désactivé. La commande de stratégie de pare-feu `show` des services système avec le paramètre ``-service telnet`` indique si Telnet a été activé dans une politique de pare-feu. Pour plus d'informations, consultez les pages de manuel de la politique de pare-feu des services système.

- Si vous utilisez des connexions IPv6, vous devez déjà configurer et activer IPv6 sur le cluster, et les politiques de pare-feu doivent déjà être configurées avec des adresses IPv6.

La commande `ipv6 show` des options réseau indique si IPv6 est activé ou non. La commande `system services firewall policy show` affiche les politiques de pare-feu.

#### Description de la tâche

- Telnet n'est pas un protocole sécurisé.

Vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive.

- ONTAP prend en charge un maximum de 50 sessions Telnet simultanées par nœud.

Si la LIF de cluster management réside sur le nœud, il partage cette limite avec la LIF de node management.

Si le taux de connexions en cours est supérieur à 10 par seconde, le service est temporairement désactivé pendant 60 secondes.

- Pour accéder à l'interface de ligne de commandes de ONTAP à partir d'un hôte Windows, vous pouvez faire appel à un utilitaire tiers tel que PuTTY.

## Étapes

1. Depuis un hôte d'administration, entrez la commande suivante :

```
telnet hostname_or_IP
```

hostname\_or\_IP Est le nom d'hôte ou l'adresse IP de la LIF de cluster management ou d'une LIF de node management. Il est recommandé d'utiliser la LIF de cluster management. Vous pouvez utiliser une adresse IPv4 ou IPv6.

## Exemple de requête Telnet

L'exemple suivant montre comment l'utilisateur nommé « joe », qui a été configuré avec un accès Telnet, peut émettre une demande Telnet pour accéder à un cluster dont la LIF de cluster management est 10.72.137.28 :

```
admin_host$ telnet 10.72.137.28

Data ONTAP
login: joe
Password:

cluster1::>
```

## Accéder au cluster à l'aide de RSH

Vous pouvez émettre des requêtes RSH au cluster pour effectuer des tâches administratives. RSH n'est pas un protocole sécurisé et est désactivé par défaut.

Au fil du temps, la façon dont ONTAP gère le type de trafic pris en charge sur les LIF a changé.

- ONTAP 9.5 et les versions antérieures utilisent des rôles LIF et des services de pare-feu
- Les versions ONTAP 9.6 et ultérieures utilisent les stratégies de service LIF
  - La version ONTAP 9.5 a introduit les stratégies de service LIF
  - ONTAP 9.6 a remplacé les rôles LIF par des stratégies de service LIF
  - ONTAP 9.10.1 a remplacé les services de pare-feu par des politiques de service LIF

La méthode que vous configurez dépend de la version de ONTAP que vous utilisez.

Pour en savoir plus sur :

- Politiques de pare-feu, voir ["Commande : firewall-policy-show"](#)
- Rôles LIF, voir ["Rôles LIF \(ONTAP 9.5 et versions antérieures\)"](#)
- Politiques de service LIF, voir ["LIF et règles de service \(ONTAP 9.6 et versions ultérieures\)"](#)

Telnet et RSH ne sont pas des protocoles sécurisés, vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive. Pour plus d'informations, reportez-vous à la section ["Accédez au cluster via SSH"](#)

## ONTAP 9.6 ou version ultérieure

### Avant de commencer

Les conditions suivantes doivent être remplies pour que vous puissiez utiliser RSH pour accéder au cluster :

- Vous devez disposer d'un compte utilisateur local de cluster configuré pour utiliser la fonction RSH comme méthode d'accès.

Le `-application` paramètre du `security login` les commandes spécifie la méthode d'accès pour un compte utilisateur. Pour plus d'informations, reportez-vous à la section `security login` pages de manuel.

### Description de la tâche

- RSH n'est pas un protocole sécurisé.

Vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive.

- ONTAP prend en charge un maximum de 50 sessions RSH simultanées par nœud.

Si la LIF de cluster management réside sur le nœud, il partage cette limite avec la LIF de node management.

Si le taux de connexions entrantes est supérieur à 10 par seconde, le service est temporairement désactivé pendant 60 secondes.

- Les commandes RSH nécessitent des privilèges avancés.

### Étapes

1. Vérifiez que le protocole de sécurité RSH est activé :

```
security protocol show
```

- a. Si le protocole de sécurité RSH est activé, passez à l'étape suivante.
- b. Si le protocole de sécurité RSH n'est pas activé, utilisez la commande suivante pour l'activer :

```
security protocol modify -application rsh -enabled true
```

2. Vérifier que le `management-rsh-server` service existe sur les LIFs de management :

```
network interface show -services management-rsh-server
```

- a. Si le `management-rsh-server` service existe, passez à l'étape suivante.
- b. Si le `management-rsh-server` service n'existe pas, utilisez la commande suivante pour l'ajouter :

```
network interface service-policy add-service -vserver cluster1 -policy
default-management -service management-rsh-server
```

### Exemple de demande de RSH

L'exemple suivant montre comment l'utilisateur nommé « joe », qui a été configuré avec l'accès RSH, peut émettre une demande RSH pour exécuter l' `cluster show` commande :

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show
```

```
Node Health Eligibility

node1 true true
node2 true true
2 entries were displayed.

admin_host$
```

## ONTAP 9.5 ou version antérieure

### Avant de commencer

Les conditions suivantes doivent être remplies pour que vous puissiez utiliser RSH pour accéder au cluster :

- Vous devez disposer d'un compte utilisateur local de cluster configuré pour utiliser la fonction RSH comme méthode d'accès.

Le paramètre `-application` des commandes de connexion de sécurité spécifie la méthode d'accès pour un compte utilisateur. Pour plus d'informations, consultez les pages de manuel de connexion de sécurité.

- RSH doit déjà être activé dans la politique de pare-feu de gestion utilisée par les LIFs de cluster ou de node management afin que les requêtes RSH puissent passer par le pare-feu.

Par défaut, RSH est désactivé. La commande `system services firewall policy show` avec le `-service rsh` paramètre indique si RSH a été activé dans une stratégie de pare-feu. Pour plus d'informations, consultez les `system services firewall policy pages man`.

- Si vous utilisez des connexions IPv6, vous devez déjà configurer et activer IPv6 sur le cluster, et les politiques de pare-feu doivent déjà être configurées avec des adresses IPv6.

La `network options ipv6 show` commande indique si IPv6 est activé ou non. ``system services firewall policy show`` La commande affiche les politiques de pare-feu.

### Description de la tâche

- RSH n'est pas un protocole sécurisé.

Vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive.

- ONTAP prend en charge un maximum de 50 sessions RSH simultanées par nœud.

Si la LIF de cluster management réside sur le nœud, il partage cette limite avec la LIF de node management.

Si le taux de connexions en cours est supérieur à 10 par seconde, le service est temporairement désactivé pendant 60 secondes.



## Étapes

1. Depuis un hôte d'administration, entrez la commande suivante :

```
rsh hostname_or_IP -l username:passwordcommand
```

`hostname_or_IP` Est le nom d'hôte ou l'adresse IP de la LIF de cluster management ou d'une LIF de node management. Il est recommandé d'utiliser la LIF de cluster management. Vous pouvez utiliser une adresse IPv4 ou IPv6.

`command` Est la commande que vous souhaitez exécuter sur RSH.

## Exemple de demande de RSH

L'exemple suivant montre comment l'utilisateur nommé « joe », qui a été configuré avec un accès RSH, peut émettre une requête RSH pour exécuter la commande `cluster show` :

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show
```

```
Node Health Eligibility
```

```

```

```
node1 true true
```

```
node2 true true
```

```
2 entries were displayed.
```

```
admin_host
```

## Utilisez l'interface de ligne de commandes ONTAP

### Utilisation de l'interface de ligne de commandes ONTAP

L'interface de ligne de commande ONTAP fournit une vue basée sur les commandes de l'interface de gestion. Vous saisissez les commandes à l'invite du système de stockage et les résultats des commandes s'affichent dans un texte.

L'invite de commande CLI est représentée sous la forme `cluster_name::>`.

Si vous définissez le niveau de privilège (c'est-à-dire, le `-privilege` paramètre du `set` commande) à `advanced`, l'invite comprend un astérisque (\*), par exemple :

```
cluster_name::*>
```

### À propos des différents shells pour la présentation des commandes CLI (administrateurs de cluster uniquement)

Le cluster a trois shells différents pour les commandes CLI, le *clustershell*, le *nodeshell* et le *systemshell*. Les coques sont à des fins différentes, et elles ont chacune un jeu de commandes différent.

- Le clustershell est le shell natif qui démarre automatiquement lorsque vous vous connectez au cluster.

Il fournit toutes les commandes dont vous avez besoin pour configurer et gérer le cluster. L'aide CLI clustershell (déclenchée par ? à l'invite clustershell) affiche les commandes clustershell disponibles. Le `man command_name` commande dans le clustershell affiche la page man pour la commande clustershell spécifiée.

- Le nodeshell est un shell spécial pour les commandes qui prennent effet uniquement au niveau du nœud.

Le nodeshell est accessible via le `system node run` commande.

Aide de l'interface de ligne de commande du nodeshell (déclenchée par ? ou `help` à l'invite nodeshell) affiche les commandes disponibles du nodeshell. Le `man command_name` la commande dans le nodeshell affiche la page man pour la commande nodeshell spécifiée.

De nombreuses commandes et options de nodeshell couramment utilisées sont regroupées ou alitées dans le clustershell et peuvent également être exécutées à partir du clustershell.

- Le systemshell est un shell de bas niveau qui est utilisé uniquement pour le diagnostic et la résolution de problèmes.

Le systemshell et le compte "diag" associé sont destinés à des fins de diagnostic de bas niveau. Leur accès requiert le niveau de privilège de diagnostic et est réservé uniquement au support technique pour effectuer les tâches de dépannage.

#### Accès aux commandes et options du nodeshell dans le clustershell

Les commandes et options de Nodeshell sont accessibles via le nodeshell:

```
system node run -node nodename
```

De nombreuses commandes et options de nodeshell couramment utilisées sont regroupées ou alitées dans le clustershell et peuvent également être exécutées à partir du clustershell.

Les options Nodeshell prises en charge dans le clustershell sont accessibles à l'aide du `vserver options clustershell` commande. Pour voir ces options, vous pouvez effectuer l'une des opérations suivantes :

- Interroger la CLI clustershell avec `vserver options -vserver nodename_or_clustername -option-name ?`
- Accédez au `vserver options` Page man dans la CLI clustershell avec `man vserver options`

Si vous saisissez une commande ou une option nodeshell ou hérité dans le clustershell et que la commande ou l'option a une commande clustershell équivalente, ONTAP vous informe de la commande clustershell à utiliser.

Si vous entrez une commande ou une option de nodeshell ou hérité qui n'est pas prise en charge dans le clustershell, ONTAP vous informe de l'état « non pris en charge » pour la commande ou l'option.

#### Affiche les commandes nodeshell disponibles

Vous pouvez obtenir la liste des commandes du nodeshell disponibles en utilisant l'aide de la CLI du nodeshell.

## Étapes

1. Pour accéder au nodeshell, entrez la commande suivante à l'invite du système du clustershell :

```
system node run -node {nodename|local}
```

local est le nœud que vous utilisez pour accéder au cluster.



Le `system node run` la commande a une commande alias, `run`.

2. Entrez la commande suivante dans le nodeshell pour voir la liste des commandes disponibles du nodeshell :

```
[commandname] help
```

``_commandname_`` est le nom de la commande dont vous souhaitez afficher la disponibilité. Si vous n'incluez pas ``_commandname_``, La CLI affiche toutes les commandes du nodeshell disponibles.

Vous entrez `exit` Ou tapez `Ctrl-d` pour revenir à la CLI clustershell.

### Exemple d'affichage des commandes de nodeshell disponibles

L'exemple suivant accède au nodeshell d'un nœud nommé node2 et affiche les informations relatives à la commande nodeshell `environment`:

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
 [status] [shelf [<adapter>[.<shelf-number>]]] |
 [status] [shelf_log] |
 [status] [shelf_stats] |
 [status] [shelf_power_status] |
 [status] [chassis [all | list-sensors | Temperature | PSU 1 |
PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

### Méthodes de navigation dans les répertoires de commandes CLI

Les commandes de l'interface de ligne de commande sont organisées en hiérarchie par répertoires de commandes. Vous pouvez exécuter des commandes dans la hiérarchie en entrant le chemin de commande complet ou en parcourant la structure du répertoire.

Lorsque vous utilisez l'interface de ligne de commande, vous pouvez accéder à un répertoire de commandes en saisissant le nom du répertoire à l'invite, puis en appuyant sur entrée. Le nom du répertoire est alors inclus dans le texte d'invite pour indiquer que vous interagissez avec le répertoire de commande approprié. Pour aller plus loin dans la hiérarchie de commandes, entrez le nom d'un sous-répertoire de commandes, puis appuyez sur entrée. Le nom du sous-répertoire est alors inclus dans le texte d'invite et le contexte passe à ce sous-

répertoire.

Vous pouvez naviguer dans plusieurs répertoires de commandes en entrant la commande entière. Par exemple, vous pouvez afficher des informations sur les disques en entrant dans le `storage disk show` commande à l'invite. Vous pouvez également exécuter la commande en parcourant un seul répertoire de commandes à la fois, comme illustré dans l'exemple suivant :

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

Vous pouvez abrégier les commandes en n'entrant que le nombre minimal de lettres dans une commande qui rend la commande unique au répertoire courant. Par exemple, pour abrégier la commande dans l'exemple précédent, vous pouvez entrer `st d sh`. Vous pouvez également utiliser la touche Tab pour développer des commandes abrégées et afficher les paramètres d'une commande, y compris les valeurs des paramètres par défaut.

Vous pouvez utiliser le `top` commande pour accéder au niveau supérieur de la hiérarchie de commandes et au `up` commande ou `..` commande permettant d'atteindre un niveau dans la hiérarchie de commandes.



Les commandes et les options de commande précédées d'un astérisque (\*) dans l'interface de ligne de commande ne peuvent être exécutées qu'au niveau de privilège avancé ou supérieur.

## Règles d'indication des valeurs dans l'interface de ligne de commandes

La plupart des commandes comprennent un ou plusieurs paramètres obligatoires ou facultatifs. De nombreux paramètres exigent que vous spécifiez une valeur pour eux. Un certain nombre de règles doivent être respectées dans l'interface de ligne de commandes.

- Une valeur peut être un nombre, un spécificateur booléen, une sélection dans une liste de valeurs prédéfinies énumérées ou une chaîne de texte.

Certains paramètres acceptent une liste séparée par des virgules de deux valeurs ou plus. Les listes de valeurs séparées par des virgules n'ont pas besoin d'être entre guillemets (" "). Chaque fois que vous spécifiez du texte, un espace ou un caractère de requête (s'il ne s'agit pas d'une requête ou d'un texte commençant par un symbole inférieur ou supérieur à), vous devez inclure l'entité entre guillemets.

- L'ILC interprète une marque d'interrogation ("?»?») comme commande permettant d'afficher les informations d'aide pour une commande particulière.
- Certains textes que vous entrez dans l'interface de ligne de commande, par exemple les noms des commandes, les paramètres et certaines valeurs, ne sont pas sensibles à la casse.

Par exemple, lorsque vous saisissez des valeurs de paramètre pour le `vserver cifs` les commandes, majuscules sont ignorées. Cependant, la plupart des valeurs de paramètres, telles que les noms des nœuds, des serveurs virtuels de stockage (SVM), des agrégats, des volumes et des interfaces logiques, sont sensibles à la casse.

- Si vous souhaitez effacer la valeur d'un paramètre qui prend une chaîne ou une liste, vous devez spécifier un ensemble vide de guillemets ("") ou un tiret ("-").

- Le signe dièse ("#"), également appelé signe dièse, indique un commentaire pour une entrée de ligne de commande; s'il est utilisé, il doit apparaître après le dernier paramètre d'une ligne de commande.

La CLI ignore le texte entre ""#"" et la fin de la ligne.

Dans l'exemple suivant, un SVM est créé avec un commentaire texte. Le SVM est ensuite modifié pour supprimer le commentaire :

```
cluster1::> vsriver create -vsriver vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipspaze ipspazeA -comment "My SVM"
cluster1::> vsriver modify -vsriver vs0 -comment ""
```

Dans l'exemple suivant, un commentaire de ligne de commande utilisant le signe ""#"" indique ce que fait la commande.

```
cluster1::> security login create -vsriver vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

## Méthodes d'affichage de l'historique des commandes et de réémission des commandes

Chaque session de l'interface de ligne de commande conserve un historique de toutes les commandes qui y sont émises. Vous pouvez afficher l'historique des commandes de la session dans laquelle vous vous trouvez. Vous pouvez également réémettre des commandes.

Pour afficher l'historique des commandes, vous pouvez utiliser le `history` commande.

Pour réémettre une commande, vous pouvez utiliser le `redo` commande avec l'un des arguments suivants :

- Chaîne correspondant à une partie d'une commande précédente

Par exemple, si le seul volume la commande que vous avez exécutée est `volume show`, vous pouvez utiliser l' `redo volume` pour réexécuter la commande.

- L'ID numérique d'une commande précédente, comme indiqué par le `history` commande

Par exemple, vous pouvez utiliser le `redo 4` commande permettant de réémettre la quatrième commande dans la liste de l'historique.

- Décalage négatif par rapport à la fin de la liste d'historique

Par exemple, vous pouvez utiliser le `redo -2` commande pour réémettre la commande que vous avez exécutée il y a deux commandes.

Par exemple, pour rétablir la commande troisième depuis la fin de l'historique des commandes, entrez la commande suivante :

```
cluster1::> redo -3
```

### Raccourcis clavier pour la modification des commandes CLI

La commande à l'invite de commande en cours est la commande active. L'utilisation des raccourcis clavier vous permet de modifier rapidement la commande active. Ces raccourcis clavier sont similaires à ceux du shell `tcsh` UNIX et de l'éditeur Emacs.

Le tableau suivant répertorie les raccourcis clavier permettant de modifier les commandes de l'interface de ligne de commande. « Ctrl- » indique que vous maintenez la touche Ctrl enfoncée tout en tapant le caractère spécifié après. « Échap- » indique que vous appuyez sur la touche Échap et relâchez-la, puis saisissez le caractère spécifié après.

| Les fonctions que vous recherchez...                                                                                                                                                                                                                                             | Utilisez le raccourci clavier suivant...        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| Déplacez le curseur d'un caractère vers l'arrière                                                                                                                                                                                                                                | Ctrl-B                                          |
| Flèche vers l'arrière                                                                                                                                                                                                                                                            | Déplacez le curseur d'un caractère vers l'avant |
| Ctrl-F                                                                                                                                                                                                                                                                           | Flèche vers l'avant                             |
| Déplacez le curseur d'un mot vers l'arrière                                                                                                                                                                                                                                      | ESC-B                                           |
| Déplacez le curseur d'un mot vers l'avant                                                                                                                                                                                                                                        | ESC-F                                           |
| Déplacez le curseur au début de la ligne                                                                                                                                                                                                                                         | Ctrl-A                                          |
| Déplacez le curseur jusqu'à la fin de la ligne                                                                                                                                                                                                                                   | Ctrl-E                                          |
| Supprimez le contenu de la ligne de commande du début de la ligne jusqu'au curseur et enregistrez-le dans le tampon de coupe. La mémoire tampon de coupure agit comme une mémoire temporaire, similaire à ce que l'on appelle un <i>presse-papiers</i> dans certains programmes. | Ctrl-U                                          |
| Supprimez le contenu de la ligne de commande du curseur jusqu'à la fin de la ligne et enregistrez-le dans le tampon de découpe                                                                                                                                                   | Ctrl-K                                          |
| Supprimez le contenu de la ligne de commande du curseur jusqu'à la fin du mot suivant et enregistrez-le dans le tampon de découpe                                                                                                                                                | ESC-D                                           |

| Les fonctions que vous recherchez...                                                                                                                                                   | Utilisez le raccourci clavier suivant...                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supprimez le mot devant le curseur et enregistrez-le dans le tampon de coupe                                                                                                           | Ctrl-W                                                                                                                                                                                                            |
| Ank le contenu du tampon de coupe, et le pousser dans la ligne de commande au niveau du curseur                                                                                        | Ctrl + y                                                                                                                                                                                                          |
| Supprimer le caractère avant le curseur                                                                                                                                                | Ctrl-H                                                                                                                                                                                                            |
| Retour arrière                                                                                                                                                                         | Supprimez le caractère où se trouve le curseur                                                                                                                                                                    |
| Ctrl-D.                                                                                                                                                                                | Effacez la ligne                                                                                                                                                                                                  |
| Ctrl-C                                                                                                                                                                                 | Effacez l'écran                                                                                                                                                                                                   |
| Ctrl-L                                                                                                                                                                                 | Remplacez le contenu actuel de la ligne de commande par l'entrée précédente de la liste d'historique.<br><br>À chaque répétition du raccourci clavier, le curseur historique se déplace vers l'entrée précédente. |
| Ctrl-P                                                                                                                                                                                 | ESC-P                                                                                                                                                                                                             |
| Flèche vers le haut                                                                                                                                                                    | Remplacez le contenu actuel de la ligne de commande par l'entrée suivante de la liste de l'historique. À chaque répétition du raccourci clavier, le curseur historique se déplace vers l'entrée suivante.         |
| Ctrl-N                                                                                                                                                                                 | ESC-N                                                                                                                                                                                                             |
| Flèche vers le bas                                                                                                                                                                     | Développer une commande partiellement saisie ou répertorier une entrée valide à partir de la position d'édition actuelle                                                                                          |
| Onglet                                                                                                                                                                                 | Ctrl-I                                                                                                                                                                                                            |
| Afficher l'aide contextuelle                                                                                                                                                           | ?                                                                                                                                                                                                                 |
| Échapper à la cartographie spéciale de la marque de question ("»?") character. For instance, to enter a question mark into a command's argument, press Esc and then the "»" caractère. | ESC- ?                                                                                                                                                                                                            |
| Démarrez la sortie TTY                                                                                                                                                                 | Ctrl-Q                                                                                                                                                                                                            |

| Les fonctions que vous recherchez... | Utilisez le raccourci clavier suivant... |
|--------------------------------------|------------------------------------------|
| Arrêter la sortie TTY                | Ctrl-S                                   |

## Utilisation des niveaux de privilège administratif

Les commandes et paramètres ONTAP sont définis à trois niveaux de privilèges : *admin*, *Advanced* et *diagnostic*. Les niveaux de privilège reflètent les niveaux de compétence requis pour exécuter les tâches.

- **admin**

La plupart des commandes et des paramètres sont disponibles à ce niveau. Ils sont utilisés pour les tâches courantes ou de routine.

- **avancé**

Les commandes et les paramètres à ce niveau sont rarement utilisés, nécessitent des connaissances avancées et peuvent causer des problèmes s'ils sont utilisés de façon inappropriée.

Vous utilisez des commandes ou des paramètres avancés uniquement avec les conseils du personnel de support.

- **diagnostic**

Les paramètres et les commandes de diagnostic sont potentiellement sources de perturbation. Ils sont utilisés uniquement par le personnel de support pour diagnostiquer et corriger les problèmes.

## Définissez le niveau de privilège dans l'interface de ligne de commandes

Vous pouvez définir le niveau de privilège dans l'interface de ligne de commandes en utilisant la `set` commande. Les modifications apportées aux paramètres de niveau de privilège s'appliquent uniquement à la session dans laquelle vous vous trouvez. Elles ne sont pas persistantes d'une session à l'autre.

### Étapes

1. Pour définir le niveau de privilège dans l'interface de ligne de commandes, utilisez le `set` commande avec `-privilege paramètre`.

### Exemple de définition du niveau de privilège

L'exemple suivant définit le niveau de privilège sur avancé, puis sur admin :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```



## Définissez les préférences d’affichage dans la CLI

Vous pouvez définir les préférences d’affichage d’une session CLI à l’aide de `set` commande et `rows` commande. Les préférences définies s’appliquent uniquement à la session dans laquelle vous vous trouvez. Elles ne sont pas persistantes d’une session à l’autre.

### Description de la tâche

Vous pouvez définir les préférences d’affichage CLI suivantes :

- Niveau de privilège de la session de commande
- Indique si des confirmations sont émises pour des commandes potentiellement perturbatrices
- Si `show` les commandes affichent tous les champs
- Le ou les caractères à utiliser comme séparateur de champ
- Unité par défaut lors du reporting des tailles de données
- Le nombre de lignes que l’écran affiche dans la session CLI en cours avant que l’interface n’interrompt la sortie

Si le nombre de rangées préféré n’est pas spécifié, il est automatiquement ajusté en fonction de la hauteur réelle du terminal. Si la hauteur réelle n’est pas définie, le nombre de lignes par défaut est 24.

- Le nœud ou la machine virtuelle de stockage par défaut
- Si une commande continue doit s’arrêter s’il rencontre une erreur

### Étapes

1. Pour définir les préférences d’affichage CLI, utilisez le `set` commande.

Pour définir le nombre de lignes que l’écran affiche dans la session CLI en cours, vous pouvez également utiliser le `rows` commande.

Pour plus d’informations, consultez les pages de manuel du `set` commande et `rows` commande.

### Exemple de définition des préférences d’affichage dans l’interface de ligne de commande

L’exemple suivant définit une virgule comme étant le séparateur de champ, définit GB comme unité de taille de données par défaut, et définit le nombre de lignes sur 50 :

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

### Méthodes d’utilisation des opérateurs de requête

L’interface de gestion prend en charge les requêtes, les modèles de style UNIX et les caractères génériques pour vous permettre de faire correspondre plusieurs valeurs dans les arguments de paramètres de commande.

Le tableau suivant décrit les opérateurs de requête pris en charge :

| Opérateur         | Description                                                                                                                                                                                                                                |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| *                 | <p>Caractère générique correspondant à toutes les entrées.</p> <p>Par exemple, la commande <code>volume show -volume *tmp*</code> affiche la liste de tous les volumes dont le nom inclut la chaîne <code>tmp</code>.</p>                  |
| !                 | <p>PAS opérateur.</p> <p>Indique une valeur qui ne doit pas être comparée ; par exemple, <b>!vs0</b> indique de ne pas correspondre à la valeur <code>vs0</code>.</p>                                                                      |
| OU opérateur<br>. | <p><code>vs2*</code> correspond soit à <code>vs0</code>, soit à <code>vs2</code>. Vous pouvez spécifier plusieurs instructions OU ; par exemple, <code>`a</code></p> <p>Sépare deux valeurs à comparer, par exemple <code>`*vs0</code></p> |
| b*                | <code>*c*</code> correspond à l'entrée <code>a</code> , toute entrée commençant par <code>b</code> , et toute entrée qui inclut <code>c</code> .                                                                                           |
| ..                | <p>Opérateur de gamme.</p> <p>Par exemple : <b>5..10</b> correspond à n'importe quelle valeur de 5 à 10, inclus.</p>                                                                                                                       |
| <                 | <p>Moins que l'opérateur.</p> <p>Par exemple : <b>&lt;20</b> correspond à toute valeur inférieure à 20.</p>                                                                                                                                |
| >                 | <p>Opérateur supérieur à.</p> <p>Par exemple : <b>&gt;5</b> correspond à toute valeur supérieure à 5.</p>                                                                                                                                  |
| <=                | <p>Inférieur ou égal à l'opérateur.</p> <p>Par exemple : <b>≤5</b> correspond à toute valeur inférieure ou égale à 5.</p>                                                                                                                  |
| >=                | <p>Supérieur à ou égal à l'opérateur.</p> <p>Par exemple : <b>≥5</b> correspond à toute valeur supérieure ou égale à 5.</p>                                                                                                                |

| Opérateur | Description                                                                                                                                                                                                                                                                                                                         |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {query}   | <p>Requête étendue.</p> <p>Une requête étendue doit être spécifiée comme premier argument après le nom de la commande, avant tout autre paramètre.</p> <p>Par exemple, la commande <code>volume modify {-volume *tmp*} -state offline</code> définit hors ligne tous les volumes dont le nom inclut la chaîne <code>tmp</code>.</p> |

Si vous voulez analyser les caractères de requête en tant que littéraux, vous devez les inclure entre guillemets (par exemple, "<10", "0..100", "\*abc\*", ou "a|b") pour que les résultats corrects soient renvoyés.

Vous devez inclure des noms de fichiers bruts entre guillemets pour empêcher l'interprétation des caractères spéciaux. Cela s'applique également aux caractères spéciaux utilisés par le cluster shell.

Vous pouvez utiliser plusieurs opérateurs de requête dans une seule ligne de commande. Par exemple, la commande `volume show -size >1GB -percent-used <50 -vserver !vs1` Affiche tous les volumes dont la taille est supérieure à 1 Go, inférieurs à 50 % utilisés et non sur la machine virtuelle de stockage (SVM) nommée « vs1 ».

#### Informations associées

["Raccourcis clavier pour la modification des commandes CLI"](#)

#### Méthodes d'utilisation des requêtes étendues

Vous pouvez utiliser des requêtes étendues pour faire correspondre et exécuter des opérations sur des objets ayant des valeurs spécifiées.

Vous spécifiez les requêtes étendues en les enfermant entre crochets (`{}`). Une requête étendue doit être spécifiée comme premier argument après le nom de la commande, avant tout autre paramètre. Par exemple, pour mettre hors ligne tous les volumes dont le nom inclut la chaîne `tmp`, vous exécutez la commande dans l'exemple suivant :

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

Les requêtes étendues ne sont généralement utiles qu'avec `modify` et `delete` commandes. Ils n'ont aucun sens en `create` ou `show` commandes.

La combinaison de requêtes et d'opérations de modification est un outil utile. Toutefois, il peut être source de confusion et d'erreurs si la mise en œuvre est incorrecte. Par exemple, à l'aide du (privilège avancé) `system node image modify` commande permettant de définir automatiquement l'image logicielle par défaut d'un nœud définit l'autre image logicielle comme non la valeur par défaut. La commande dans l'exemple suivant est effectivement une opération nulle :

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

Cette commande définit l'image par défaut actuelle comme image non par défaut, puis définit la nouvelle

image par défaut (l'image précédente non par défaut) sur l'image non par défaut, ce qui entraîne la conservation des paramètres par défaut d'origine. Pour effectuer l'opération correctement, vous pouvez utiliser la commande comme indiqué dans l'exemple suivant :

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

### Méthodes de personnalisation de la commande show à l'aide des champs

Lorsque vous utilisez le `-instance` paramètre avec un `show` commande pour afficher les détails, le résultat peut être long et inclure plus d'informations qu'il ne vous en faut. Le `-fields` paramètre de la `show` vous permet d'afficher uniquement les informations que vous spécifiez.

Par exemple, en cours d'exécution `volume show -instance` est susceptible de donner lieu à plusieurs écrans d'information. Vous pouvez utiliser `volume show -fields fieldname[,fieldname...]` pour personnaliser la sortie de sorte qu'elle inclut uniquement le ou les champs spécifiés (en plus des champs par défaut qui sont toujours affichés). Vous pouvez utiliser `-fields ?` pour afficher des champs valides pour un `show` commande.

L'exemple suivant montre la différence de sortie entre le `-instance` paramètre et le `-fields` paramètre :

```

cluster1::> volume show -instance

Vserver Name: cluster1-1
Volume Name: vol0
Aggregate Name: aggr0
Volume Size: 348.3GB
Volume Data Set ID: -
Volume Master Data Set ID: -
Volume State: online
Volume Type: RW
Volume Style: flex
...
Space Guarantee Style: volume
Space Guarantee in Effect: true
...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver volume space-guarantee space-guarantee-enabled
----- -
cluster1-1 vol0 volume true
cluster1-2 vol0 volume true
vs1 root_vol
 volume true
vs2 new_vol
 volume true
vs2 root_vol
 volume true
...
cluster1::>

```

## A propos des paramètres de position

Vous pouvez utiliser la fonctionnalité des paramètres de position de l'interface de ligne de commande ONTAP pour améliorer l'efficacité de l'entrée de commande. Vous pouvez interroger une commande pour identifier les paramètres qui sont de position pour la commande.

### Définition d'un paramètre de position

- Un paramètre de position est un paramètre qui ne vous demande pas de spécifier le nom du paramètre avant de spécifier la valeur du paramètre.

- Un paramètre de position peut être intercalé avec des paramètres non positionnels dans l'entrée de commande, tant qu'il observe sa séquence relative avec d'autres paramètres de position dans la même commande, comme indiqué dans l' **`command_name ?`** sortie.
- Un paramètre de position peut être un paramètre obligatoire ou facultatif pour une commande.
- Un paramètre peut être positionné pour une commande mais non positionnel pour une autre.



L'utilisation de la fonctionnalité des paramètres de position dans les scripts n'est pas recommandée, en particulier lorsque les paramètres de position sont facultatifs pour la commande ou si des paramètres facultatifs sont répertoriés avant eux.

### Identifiez un paramètre de position

Vous pouvez identifier un paramètre de position dans l' **`command_name ?`** sortie de la commande. Un paramètre de position comporte des crochets autour de son nom de paramètre, dans l'un des formats suivants :

- `[-parameter_name] parameter_value` affiche un paramètre requis qui est positionnel.
- `[[[-parameter_name] parameter_value]` affiche un paramètre facultatif qui est positionnel.

Par exemple, lorsqu'il s'affiche comme suit dans le **`command_name ?`** sortie, le paramètre est positionné pour la commande dans laquelle il apparaît :

- `[-lif] <lif-name>`
- `[[[-lif] <lif-name>]`

Toutefois, lorsqu'il est affiché comme suit, le paramètre n'est pas positionné pour la commande dans laquelle il apparaît :

- `-lif <lif-name>`
- `[-lif <lif-name>]`

### Exemples d'utilisation de paramètres de position

Dans l'exemple suivant, le **`volume create ?`** le résultat indique que trois paramètres sont en position pour la commande : `-volume`, `-aggregate`, et `-size`.

```

cluster1::> volume create ?
 -vserver <vserver name> Vserver Name
 [-volume] <volume name> Volume Name
 [-aggregate] <aggregate name> Aggregate Name
 [[-size] {<integer>[KB|MB|GB|TB|PB]] Volume Size
 [-state {online|restricted|offline|force-online|force-offline|mixed}]
 Volume State (default: online)
 [-type {RW|DP|DC}] Volume Type (default: RW)
 [-policy <text>] Export Policy
 [-user <user name>] User ID
 ...
 [-space-guarantee|-s {none|volume}] Space Guarantee Style (default:
volume)
 [-percent-snapshot-space <percent>] Space Reserved for Snapshot
Copies
 ...

```

Dans l'exemple suivant, le `volume create` la commande est spécifiée sans utiliser la fonctionnalité des paramètres de position :

```

cluster1::> volume create -vserver svml -volume voll -aggregate aggr1 -size 1g
-percent-snapshot-space 0

```

Les exemples suivants utilisent la fonctionnalité des paramètres de position pour augmenter l'efficacité de l'entrée de commande. Les paramètres de position sont entrelatés avec des paramètres non positionnels dans `volume create` la commande et les valeurs des paramètres de position sont spécifiées sans les noms des paramètres. Les paramètres de position sont spécifiés dans la même séquence que celle indiquée par le **volume create ?** sortie. C'est-à-dire la valeur de `-volume` est spécifié avant celle de `-aggregate`, qui est à son tour spécifié avant celle de `-size`.

```

cluster1::> volume create vol2 aggr1 1g -vserver svml -percent-snapshot-space 0

```

```

cluster1::> volume create -vserver svml vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none

```

## Méthodes d'accès aux pages de manuel ONTAP

Les pages de manuel ONTAP expliquent comment utiliser les commandes de l'interface de ligne de commande ONTAP. Ces pages sont disponibles sur la ligne de commande et sont également publiées dans *command references* spécifique à la version.

Sur la ligne de commande ONTAP, utilisez `man command_name` pour afficher la page man de la commande spécifiée. Si vous ne spécifiez pas de nom de commande, l'index de page manuelle s'affiche. Vous pouvez utiliser le `man man` pour afficher les informations relatives à man commande elle-même. Vous pouvez quitter une page man en entrant `q`.

Reportez-vous à la [Référence des commandes pour votre version de ONTAP 9](#) Pour en savoir plus sur les commandes ONTAP de niveau administrateur et avancé disponibles dans votre version.

## Gérer les sessions CLI

Vous pouvez enregistrer une session CLI dans un fichier dont le nom et la taille sont définis, puis télécharger le fichier vers une destination FTP ou HTTP. Vous pouvez également afficher ou supprimer des fichiers dans lesquels vous avez déjà enregistré des sessions CLI.

### Enregistrez une session CLI

Un enregistrement d'une session CLI se termine lorsque vous arrêtez l'enregistrement ou que vous mettez fin à la session CLI, ou lorsque le fichier atteint la limite de taille spécifiée. La taille de fichier par défaut est de 1 Mo. La taille maximale des fichiers est de 2 Go.

L'enregistrement d'une session CLI est utile, par exemple, si vous dépannez un problème et souhaitez enregistrer des informations détaillées ou si vous souhaitez créer un enregistrement permanent de l'utilisation de l'espace à un moment donné.

#### Étapes

1. Démarrer l'enregistrement de la session CLI en cours dans un fichier :

```
system script start
```

Pour plus d'informations sur l'utilisation du `system script start` voir la page man.

ONTAP commence à enregistrer votre session CLI dans le fichier spécifié.

2. Passez à la session CLI.
3. Lorsque vous avez terminé, arrêtez l'enregistrement de la session :

```
system script stop
```

Pour plus d'informations sur l'utilisation du `system script stop` voir la page man.

ONTAP arrête l'enregistrement de votre session CLI.

### Commandes permettant de gérer les enregistrements des sessions CLI

Vous utilisez le `system script` Commandes permettant de gérer les enregistrements des sessions CLI.

| Les fonctions que vous recherchez...                                          | Utilisez cette commande...       |
|-------------------------------------------------------------------------------|----------------------------------|
| Démarrez l'enregistrement de la session CLI en cours dans un fichier spécifié | <code>system script start</code> |
| Arrêter l'enregistrement de la session CLI en cours                           | <code>system script stop</code>  |



| Les fonctions que vous recherchez...                                             | Utilisez cette commande...        |
|----------------------------------------------------------------------------------|-----------------------------------|
| Affiche des informations sur les enregistrements des sessions CLI                | <code>system script show</code>   |
| Télécharger un enregistrement d'une session CLI vers une destination FTP ou HTTP | <code>system script upload</code> |
| Supprimer un enregistrement d'une session CLI                                    | <code>system script delete</code> |

#### Informations associées

["Référence de commande ONTAP"](#)

### Commandes permettant de gérer la période de temporisation automatique des sessions de l'interface de ligne de commande

La valeur du délai d'attente spécifie la durée pendant laquelle une session de l'interface de ligne de commande reste inactive avant d'être automatiquement arrêtée. La valeur du délai d'expiration de l'interface de ligne de commandes correspond à l'ensemble du cluster C'est-à-dire que chaque nœud d'un cluster utilise la même valeur de temporisation de l'interface de ligne de commandes.

Par défaut, le délai d'expiration automatique des sessions de l'interface de ligne de commande est de 30 minutes.

Vous utilisez le `system timeout` Commandes permettant de gérer la période de temporisation automatique des sessions de l'interface de ligne de commande.

| Les fonctions que vous recherchez...                                                                   | Utilisez cette commande...         |
|--------------------------------------------------------------------------------------------------------|------------------------------------|
| Affiche la période de temporisation automatique pour les sessions CLI                                  | <code>system timeout show</code>   |
| Modifier la période de temporisation automatique pour les sessions de l'interface de ligne de commande | <code>system timeout modify</code> |

#### Informations associées

["Référence de commande ONTAP"](#)

## Gestion du cluster (administrateurs du cluster uniquement)

### Affiche des informations relatives aux nœuds dans un cluster

Vous pouvez afficher les noms des nœuds, que les nœuds soient sains et si ils sont éligibles au cluster. Au niveau de privilège avancé, vous pouvez également afficher si un nœud contient epsilon.

#### Étapes

1. Pour afficher des informations sur les nœuds d'un cluster, utilisez le `cluster show` commande.

Si vous souhaitez que la sortie indique si un nœud contient epsilon, lancer la commande au niveau de

privilège avancé.

### Exemples d’affichage des nœuds dans un cluster

L’exemple suivant affiche des informations sur tous les nœuds d’un cluster à quatre nœuds :

```
cluster1::> cluster show
Node Health Eligibility

node1 true true
node2 true true
node3 true true
node4 true true
```

L’exemple suivant affiche des informations détaillées sur le nœud nommé « node1 » au niveau de privilège avancé :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

Node: node1
Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
Epsilon: false
Eligibility: true
Health: true
```

### Afficher les attributs du cluster

Vous pouvez afficher l’identifiant unique d’un cluster (UUID), son nom, son numéro de série, son emplacement et ses informations de contact.

#### Étapes

1. Pour afficher les attributs d’un cluster, utilisez le `cluster identity show` commande.

### Exemple d’affichage des attributs du cluster

L’exemple suivant affiche le nom, le numéro de série, l’emplacement et les informations de contact d’un cluster.

```
cluster1::> cluster identity show
```

```
Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
Cluster Name: cluster1
Cluster Serial Number: 1-80-123456
Cluster Location: Sunnyvale
Cluster Contact: jsmith@example.com
```

## Modifier les attributs du cluster

Vous pouvez modifier les attributs d'un cluster, comme le nom du cluster, l'emplacement et les informations de contact.

### Description de la tâche

Vous ne pouvez pas modifier l'UUID d'un cluster, qui est défini lors de sa création.

### Étapes

1. Pour modifier les attributs du cluster, utilisez le `cluster identity modify` commande.

Le `-name` le paramètre spécifie le nom du cluster. Le `cluster identity modify` la page man décrit les règles à respecter lorsque vous spécifiez le nom du cluster.

Le `-location` le paramètre spécifie l'emplacement pour le cluster.

Le `-contact` paramètre spécifie les informations de contact telles qu'un nom ou une adresse e-mail.

### Exemple de changement de nom d'un cluster

La commande suivante renomme le cluster actuel (« cluster1 ») en « cluster2 » :

```
cluster1::> cluster identity modify -name cluster2
```

## Afficher l'état des anneaux de réplication de cluster

Vous pouvez afficher l'état des anneaux de réplication du cluster pour vous aider à diagnostiquer les problèmes au niveau du cluster. Si votre cluster rencontre des problèmes, le personnel de support peut vous demander d'effectuer cette tâche afin de vous aider dans les opérations de dépannage.

### Étapes

1. Pour afficher l'état des anneaux de réplication de cluster, utilisez le `cluster ring show` commande au niveau de privilège avancé.

### Exemple d'affichage de l'état de réplication-anneau du cluster

L'exemple suivant affiche l'état de l'anneau de réplication VLDB sur un nœud nommé node0 :

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1::*> cluster ring show -node node0 -unitname vldb
 Node: node0
 Unit Name: vldb
 Status: master
 Epoch: 5
Master Node: node0
 Local Node: node0
 DB Epoch: 5
DB Transaction: 56
 Number Online: 4
 RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412

```

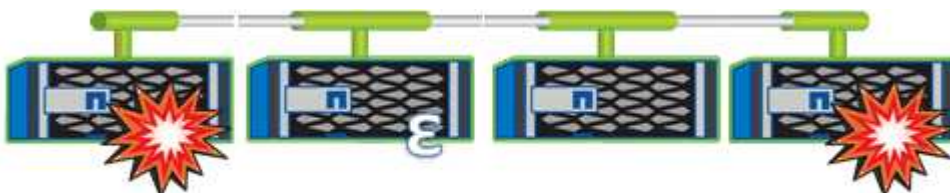
### À propos du quorum et de l'épsilon

Le quorum et l'épsilon sont des mesures importantes de l'état de santé du cluster et des fonctions qui indiquent ensemble que les clusters répondent aux problèmes potentiels de communication et de connectivité.

*Quorum* est une condition préalable à un cluster pleinement opérationnel. Lorsqu'un cluster est au quorum, une simple majorité de nœuds sont en bon état et peuvent communiquer entre eux. En cas de perte du quorum, le cluster n'a plus la possibilité d'effectuer des opérations normales sur le cluster. Un seul ensemble de nœuds peut avoir le quorum à la fois car tous les nœuds partagent collectivement une vue unique des données. Par conséquent, si deux nœuds qui ne communiquent pas sont autorisés à modifier les données de manière divergentes, il n'est plus possible de réconcilier les données en une seule vue de données.

Chaque nœud du cluster participe à un protocole de vote qui sélectionne un nœud *master* ; chaque nœud restant est un *Secondary*. Le nœud maître est chargé de synchroniser les informations sur le cluster. Lorsque le quorum est formé, il est maintenu par vote continu. Si le nœud maître se met hors ligne et que le cluster est encore au quorum, un nouveau maître est élu par les nœuds qui restent en ligne.

Étant donné qu'il y a la possibilité d'une TIE dans un cluster qui a un nombre pair de nœuds, un nœud a un poids fractionnaire supplémentaire appelé *epsilon*. Si la connectivité entre deux portions égales d'un grand cluster tombe en panne, le groupe de nœuds contenant epsilon maintient le quorum, en supposant que tous les nœuds sont en bon état. Par exemple, l'illustration suivante montre un cluster à quatre nœuds où deux des nœuds ont échoué. Cependant, comme l'un des nœuds survivants contient epsilon, le cluster reste dans le quorum même s'il n'y a pas une simple majorité de nœuds sains.



Epsilon est automatiquement affecté au premier nœud lors de la création du cluster. Si le nœud qui contient epsilon devient défectueux, prend le relais de son partenaire haute disponibilité ou est repris par son partenaire haute disponibilité, puis il est automatiquement réaffecté à un nœud saine dans une paire haute disponibilité différente.

La mise hors ligne d'un nœud peut affecter la capacité du cluster à rester dans le quorum. Par conséquent, ONTAP émet un message d'avertissement si vous tentez une opération qui détiendra le cluster du quorum ou qui le mettra hors service de la perte du quorum. Vous pouvez désactiver les messages d'avertissement de quorum à l'aide du `cluster quorum-service options modify` commande au niveau de privilège avancé.

De manière générale, en supposant une connectivité fiable entre les nœuds du cluster, un cluster plus grand est plus stable qu'un cluster plus petit. Le quorum nécessaire à une simple majorité de moitié des nœuds plus epsilon est plus facile à maintenir dans un cluster de 24 nœuds que dans un cluster de deux nœuds.

Un cluster à deux nœuds présente des défis uniques pour le maintien du quorum. Les clusters à deux nœuds utilisent *cluster HA*, dans lesquels aucun nœud ne contient epsilon ; les deux nœuds sont plutôt interrogés en continu afin de s'assurer que si un nœud tombe en panne, l'autre dispose d'un accès en lecture/écriture complet aux données, ainsi que de l'accès aux interfaces logiques et aux fonctions de gestion.

### **De quels volumes système sont-ils**

Les volumes système sont des volumes FlexVol qui contiennent des métadonnées spéciales, comme les métadonnées pour les journaux d'audit des services de fichiers. Ces volumes sont visibles dans le cluster, de sorte que vous puissiez entièrement prendre en compte l'utilisation du stockage dans votre cluster.

Les volumes système sont détenus par le serveur de gestion de cluster (également appelé SVM d'administration) et ils sont créés automatiquement lorsque l'audit des services de fichiers est activé.

Vous pouvez afficher les volumes système à l'aide du `volume show` mais la plupart des autres opérations de volume ne sont pas autorisées. Par exemple, vous ne pouvez pas modifier un volume système à l'aide de `volume modify` commande.

Cet exemple présente quatre volumes système sur le SVM d'administration, qui ont été automatiquement créés lorsque les audits des services de fichiers ont été activés pour un SVM de données dans le cluster :

```
cluster1::> volume show -vserver cluster1
```

| Vserver  | Volume                                   | Aggregate | State  | Type  | Size  | Available |
|----------|------------------------------------------|-----------|--------|-------|-------|-----------|
| Used%    |                                          |           |        |       |       |           |
| -----    | -----                                    | -----     | -----  | ----- | ----- | -----     |
| -----    |                                          |           |        |       |       |           |
| cluster1 | MDV_aud_1d0131843d4811e296fc123478563412 | aggr0     | online | RW    | 2GB   | 1.90GB    |
| 5%       |                                          |           |        |       |       |           |
| cluster1 | MDV_aud_8be27f813d7311e296fc123478563412 | root_vs0  | online | RW    | 2GB   | 1.90GB    |
| 5%       |                                          |           |        |       |       |           |
| cluster1 | MDV_aud_9dc4ad503d7311e296fc123478563412 | aggr1     | online | RW    | 2GB   | 1.90GB    |
| 5%       |                                          |           |        |       |       |           |
| cluster1 | MDV_aud_a4b887ac3d7311e296fc123478563412 | aggr2     | online | RW    | 2GB   | 1.90GB    |
| 5%       |                                          |           |        |       |       |           |

4 entries were displayed.

## Gérer des nœuds

### Ajout de nœuds au cluster

Une fois le cluster créé, vous pouvez le développer en ajoutant des nœuds. Vous n'ajoutez qu'un seul nœud à la fois.

#### Ce dont vous avez besoin

- Si vous ajoutez des nœuds à un cluster à plusieurs nœuds, tous les nœuds existants du cluster doivent être en bon état (indiqué par la `cluster show`).
- Si vous ajoutez des nœuds à un cluster sans commutateur à deux nœuds, vous devez convertir le cluster sans commutateur à deux nœuds en cluster à connexion par commutateur à l'aide d'un commutateur de cluster pris en charge par NetApp.

La fonctionnalité de cluster sans commutateur n'est prise en charge que dans un cluster à deux nœuds.

- Si vous ajoutez un second nœud à un cluster à un seul nœud, le second nœud doit avoir été installé et le réseau de clusters doit avoir été configuré.
- Si la configuration automatique du processeur de service est activée sur le cluster, le sous-réseau spécifié pour le processeur de service doit disposer de ressources disponibles pour permettre au nœud de jonction d'utiliser le sous-réseau spécifié pour configurer automatiquement le processeur de service.
- Vous devez avoir collecté les informations suivantes pour le LIF de gestion des nœuds du nouveau nœud :
  - Port
  - Adresse IP
  - Masque de réseau
  - Passerelle par défaut

## Description de la tâche

Les nœuds doivent être numériques de manière à pouvoir former des paires haute disponibilité. Une fois que vous avez commencé à ajouter un nœud au cluster, vous devez terminer le processus. Le nœud doit faire partie du cluster avant de pouvoir ajouter un autre nœud.

## Étapes

1. Mettez le nœud que vous souhaitez ajouter au cluster sous tension.

Le nœud démarre et l'assistant de configuration du nœud démarre sur la console.

```
Welcome to node setup.
```

```
You can enter the following commands at any time:
```

```
"help" or "?" - if you want to have a question clarified,
```

```
"back" - if you want to change previously answered questions, and
```

```
"exit" or "quit" - if you want to quit the setup wizard.
```

```
Any changes you made before quitting will be saved.
```

```
To accept a default or omit a question, do not enter a value.
```

```
Enter the node management interface port [e0M]:
```

2. Quittez l'assistant de configuration des nœuds : `exit`

L'assistant de configuration du nœud se ferme et une invite de connexion s'affiche, vous avertissant que vous n'avez pas terminé les tâches de configuration.

3. Connectez-vous au compte admin à l'aide de `admin` nom d'utilisateur.
4. Démarrez l'assistant de configuration du cluster :

```
cluster setup
```

```
::> cluster setup
```

Welcome to the cluster setup wizard.

You can enter the following commands at any time:

"help" or "?" - if you want to have a question clarified,  
"back" - if you want to change previously answered questions, and  
"exit" or "quit" - if you want to quit the cluster setup wizard.  
Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".  
To accept a default or omit a question, do not enter a value....

Use your web browser to complete cluster setup by accessing  
`https://<node_mgmt_or_e0M_IP_address>`

Otherwise, press Enter to complete cluster setup using the  
command line interface:



Pour plus d'informations sur la configuration d'un cluster à l'aide de l'interface graphique de configuration, consultez le ["System Manager" aide en ligne](#).

- Appuyez sur entrée pour effectuer cette tâche à l'aide de l'interface de ligne de commande. Lorsque vous êtes invité à créer un cluster ou à vous joindre à un cluster existant, entrez **join**.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
join
```

Si la version de ONTAP exécutée sur le nouveau nœud est différente de celle exécutée sur le cluster existant, le système signale un `System checks Error: Cluster join operation cannot be performed at this time` erreur. Il s'agit du comportement attendu. Pour continuer, exécutez le `add-node -allow-mixed-version-join new_node_name` au niveau de privilège avancé à partir d'un nœud existant dans le cluster.

- Suivez les invites pour configurer le nœud et le joindre au cluster :
  - Pour accepter la valeur par défaut d'une invite, appuyez sur entrée.
  - Pour saisir votre propre valeur pour une invite, entrez la valeur, puis appuyez sur entrée.
- Répétez les étapes précédentes pour chaque nœud ajouté.

### Une fois que vous avez terminé

Une fois les nœuds ajoutés au cluster, il est conseillé d'activer le basculement du stockage pour chaque paire haute disponibilité.

### Informations associées



## Retirer des nœuds du cluster

Vous pouvez supprimer les nœuds non souhaités d'un cluster ou d'un nœud à la fois. Après avoir supprimé un nœud, vous devez également supprimer son partenaire de basculement. Si vous supprimez un nœud, ses données deviennent inaccessibles ou effacées.

### Avant de commencer

Les conditions suivantes doivent être remplies avant de supprimer des nœuds du cluster :

- Plus de la moitié des nœuds du cluster doivent être en bon état.
- Toutes les données du nœud que vous souhaitez supprimer doivent avoir été évacuées.
  - Cela peut inclure ["purge des données d'un volume chiffré"](#).
- Tous les volumes non-root ont été ["déplacé"](#) à partir d'agrégats détenus par le nœud.
- Tous les agrégats non racines ont été ["supprimé"](#) à partir du nœud.
- Si le nœud est propriétaire de disques FIPS (Federal Information Processing Standards) ou de disques à autocryptage (SED), ["le chiffrement de disque a été supprimé"](#) en retournant les disques en mode non protégé.
  - Pour aller plus avant ["Procédez à la suppression des disques FIPS ou des disques SED"](#).
- Les LIF de données l'ont été ["supprimé"](#) ou ["déplacé"](#) à partir du nœud.
- Les LIF de Cluster Management ont été ["déplacé"](#) à partir du nœud et des ports de rattachement modifiés.
- Toutes les LIFs intercluster ont été ["supprimé"](#).
  - Lorsque vous supprimez les LIFs intercluster, un avertissement qui peut être ignoré est affiché.
- Le basculement du stockage a été effectué ["désactivé"](#) pour le nœud.
- Toutes les règles de basculement LIF ont été ["modifié"](#) pour supprimer les ports sur le nœud.
- Tous les VLAN sur le nœud ont été ["supprimé"](#).
- Si vous souhaitez supprimer des LUN sur le nœud, vous devez ["Modifiez la liste des nœuds de rapport SLM \(Selective LUN Map\)"](#) avant de supprimer le nœud.

Si vous ne supprimez pas le nœud et son partenaire HA de la liste des nœuds-rapports SLM, l'accès aux LUN précédemment sur le nœud peut être perdu, même si les volumes contenant les LUN ont été déplacés vers un autre nœud.

Il est recommandé d'émettre un message AutoSupport pour informer le support technique NetApp que la suppression de nœud est en cours.



Vous ne devez pas effectuer d'opérations telles que `cluster remove-node`, `cluster unjoin`et `node rename` lorsqu'une mise à niveau automatique de ONTAP est en cours.

### Description de la tâche

- Si vous exécutez un cluster à versions mixtes, vous pouvez supprimer le dernier nœud à version faible à l'aide de l'une des commandes de privilège avancées commençant par ONTAP 9.3 :
  - ONTAP 9.3 : `cluster unjoin -skip-last-low-version-node-check`

- ONTAP 9.4 et versions ultérieures : `cluster remove-node -skip-last-low-version-node -check`

- Si vous dissociez 2 nœuds d'un cluster à 4 nœuds, la haute disponibilité du cluster est automatiquement activée sur les deux nœuds restants.



Toutes les données système et utilisateur de tous les disques connectés au nœud doivent être inaccessibles aux utilisateurs avant de supprimer un nœud du cluster. Si un nœud n'a pas été correctement rejoint à partir d'un cluster, contactez le support NetApp pour obtenir de l'aide concernant les options de restauration.

## Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Vérifier si un nœud sur le cluster contient epsilon :

```
cluster show -epsilon true
```

3. Si un nœud sur le cluster contient epsilon et que ce nœud va être rejoint, déplacer epsilon vers un nœud qui ne va pas être dissocié :

- a. Déplacer epsilon depuis le nœud qui va être désrejoint

```
cluster modify -node <name_of_node_to_be_unjoined> -epsilon false
```

- b. Déplacer epsilon vers un nœud qui ne va pas être dissocié :

```
cluster modify -node <node_name> -epsilon true
```

4. Identifiez le nœud maître actuel :

```
cluster ring show
```

Le nœud maître est le nœud qui contient des processus tels que «mgmt», «vldb», «vifmgr», «bcomd» et «crs».

5. Si le nœud que vous souhaitez supprimer est le nœud maître actuel, activez un autre nœud du cluster pour qu'il soit choisi comme nœud maître :

- a. Rendre le nœud maître actuel inéligible pour participer au cluster :

```
cluster modify -node <node_name> -eligibility false
```

Lorsque le nœud maître devient inéligible, l'un des nœuds restants est choisi par le quorum du cluster comme nouveau maître.

- b. Rendez le nœud maître précédent éligible pour participer à nouveau au cluster :

```
cluster modify -node <node_name> -eligibility true
```

6. Connectez-vous à la LIF de Remote node management ou à la LIF cluster-management sur un autre nœud que celui en cours de suppression.
7. Supprimer le nœud du cluster :

| Pour cette version ONTAP...       | Utilisez cette commande...      |
|-----------------------------------|---------------------------------|
| ONTAP 9.3                         | <pre>cluster unjoin</pre>       |
| ONTAP 9.4 et versions ultérieures | <pre>cluster remove-node*</pre> |

Si vous avez une version mixte de cluster et que vous supprimez le dernier nœud inférieur, utilisez le `-skip-last-low-version-node-check` paramètre avec ces commandes.

Le système vous informe des informations suivantes :

- Vous devez également supprimer le partenaire de basculement du nœud du cluster.
- Après avoir retiré le nœud et avant de le réintégrer, vous devez utiliser l'option du menu de démarrage (4) nettoyer la configuration et initialiser tous les disques ou l'option (9) configurer le partitionnement de disque avancé pour effacer la configuration du nœud et initialiser tous les disques.

Un message de panne est généré si des conditions que vous devez traiter avant de supprimer le nœud. Par exemple, le message peut indiquer que le nœud dispose de ressources partagées que vous devez supprimer ou que le nœud se trouve dans une configuration de basculement du stockage ou de la configuration haute disponibilité du cluster que vous devez désactiver.

Si le nœud est le maître de quorum, le cluster sera brièvement perdu et reviendra ensuite au quorum. Cette perte de quorum est temporaire et n'affecte aucune opération de données.

8. Si un message d'erreur indique des conditions d'erreur, traitez ces conditions et relancez le `cluster remove-node` ou `cluster unjoin` commande.

Le nœud est redémarré automatiquement après sa suppression réussie du cluster.

9. Si vous requalifiez le nœud, effacez la configuration du nœud et initialisez tous les disques :
- Pendant le processus de démarrage, appuyez sur Ctrl-C pour afficher le menu de démarrage lorsque vous y êtes invité.
  - Sélectionner l'option de menu d'amorçage (4) nettoyer la configuration et initialiser tous les disques.
10. Retour au niveau de privilège admin :

```
set -privilege admin
```

11. Répétez la procédure précédente pour supprimer le partenaire de basculement du cluster.

### Accédez aux fichiers log, core dump et MIB d'un noeud à l'aide d'un navigateur Web

L'infrastructure du processeur de service (`spi`) Le service web est activé par défaut pour permettre à un navigateur web d'accéder aux fichiers log, core dump et MIB d'un noeud du cluster. Les fichiers restent accessibles même lorsque le nœud est en panne, à condition que le nœud soit pris en charge par son partenaire.

#### Ce dont vous avez besoin

- La LIF de cluster management doit être active.

Vous pouvez utiliser la LIF de gestion du cluster ou un nœud pour accéder à la `spi` service web. Toutefois, il est recommandé d'utiliser la LIF de gestion du cluster.

Le `network interface show` La commande affiche le statut de toutes les LIFs du cluster.

- Vous devez utiliser un compte utilisateur local pour accéder à l' `spi` service web, les comptes utilisateur de domaine ne sont pas pris en charge.
- Si votre compte utilisateur n'a pas le rôle « admin » (qui a accès à l' `spi` service web par défaut), votre rôle de contrôle d'accès doit avoir accès au système `spi` service web.

Le `vserver services web access show` commande affiche les rôles auxquels les services web ont accès.

- Si vous n'utilisez pas le compte d'utilisateur « admin » (qui inclut `http` méthode d'accès par défaut), votre compte utilisateur doit être configuré avec le `http` méthode d'accès.

Le `security login show` la commande affiche les méthodes d'accès et de connexion des comptes utilisateur ainsi que leurs rôles de contrôle d'accès.

- Si vous souhaitez utiliser HTTPS pour un accès Web sécurisé, SSL doit être activé et un certificat numérique doit être installé.

Le `system services web show` la commande affiche la configuration du moteur de protocole web au niveau du cluster.

#### Description de la tâche

Le `spi` le service web est activé par défaut et le service peut être désactivé manuellement (`vserver services web modify -vserver * -name spi -enabled false`).

Le rôle « admin » est accordé à l' `spi` le service web par défaut peut être désactivé manuellement (`services web access delete -vserver cluster_name -name spi -role admin`).

#### Étapes

1. Pointez le navigateur Web sur `spi` URL du service web dans l'un des formats suivants :

- `http://cluster-mgmt-LIF/spi/`
- `https://cluster-mgmt-LIF/spi/`

`cluster-mgmt-LIF` Est l'adresse IP de la LIF de management du cluster.

2. Lorsque le navigateur vous y invite, entrez votre compte utilisateur et votre mot de passe.

Une fois votre compte authentifié, le navigateur affiche des liens vers le `/mroot/etc/log/`, `/mroot/etc/crash/`, et `/mroot/etc/mib/` répertoires de chaque nœud du cluster.

## Accéder à la console système d'un nœud

Si un nœud est suspendu au menu de démarrage ou à l'invite de l'environnement de démarrage, vous pouvez y accéder uniquement via la console système (également appelée *série console*). Vous pouvez accéder à la console système d'un nœud depuis une connexion SSH vers le processeur de service du nœud ou vers le cluster.

### Description de la tâche

Le processeur de service et ONTAP proposent des commandes qui vous permettent d'accéder à la console système. Toutefois, depuis le processeur de service, vous pouvez accéder uniquement à la console système de son propre nœud. Dans le cluster, vous pouvez accéder à la console système de n'importe quel nœud du cluster.

### Étapes

1. Accéder à la console système d'un nœud :

| Si vous êtes dans le...                                          | Entrez cette commande...             |
|------------------------------------------------------------------|--------------------------------------|
| Interface de ligne de commandes du processeur de service du nœud | <code>system console</code>          |
| INTERFACE DE LIGNE DE COMMANDES DE ONTAP                         | <code>system node run-console</code> |

2. Connectez-vous à la console du système lorsque vous y êtes invité.
3. Pour quitter la console du système, appuyez sur Ctrl-D.

### Exemples d'accès à la console du système

L'exemple suivant montre le résultat de la saisie du `system console` Commande à l'invite "Enregistrer node2". La console système indique que le noeud 2 est suspendu à l'invite de l'environnement d'amorçage. Le `boot_ontap` La commande est entrée sur la console pour démarrer le nœud sur ONTAP. Ctrl-D est ensuite enfoncé pour quitter la console et retourner au processeur de service.

```

SP node2> system console
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap

...

*
* Press Ctrl-C for Boot Menu. *
*

...

```

(La touche Ctrl-D est enfoncée pour quitter la console du système.)

```

Connection to 123.12.123.12 closed.
SP node2>

```

L'exemple suivant montre le résultat de la saisie du `system node run-console` Commande provenant de ONTAP pour accéder à la console système du nœud 2, qui est suspendue à l'invite de l'environnement de démarrage. Le `boot_ontap` La commande a été saisie au niveau de la console pour démarrer le nœud 2 vers ONTAP. Appuyez ensuite sur Ctrl-D pour quitter la console et revenir à ONTAP.

```

cluster1::> system node run-console -node node2
Pressing Ctrl-D will end this session and any further sessions you might
open on top of this session.
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap

...

*
* Press Ctrl-C for Boot Menu. *
*

...

```

(La touche Ctrl-D est enfoncée pour quitter la console du système.)

```

Connection to 123.12.123.12 closed.
cluster1::>

```

## Gestion des volumes root et des agrégats root des nœuds

Le volume racine d'un nœud est un volume FlexVol installé en usine ou par le logiciel d'installation. Il est réservé aux fichiers système, aux fichiers journaux et aux fichiers core. Le nom du répertoire est `/mroot`, qui n'est accessible que via le systemshell par le support technique. La taille minimale du volume racine d'un nœud dépend du modèle de plateforme.

### Présentation des règles qui régissent les volumes racine des nœuds et les agrégats racine

Le volume racine d'un nœud contient des répertoires et des fichiers spéciaux pour ce nœud. L'agrégat root contient le volume root. Quelques règles régissent le volume racine d'un nœud et l'agrégat racine.

- Les règles suivantes régissent le volume racine du nœud :
  - À moins d'en recevoir l'instruction du support technique, ne modifiez pas la configuration ou le contenu du volume racine.
  - Ne stockez pas les données utilisateur sur le volume racine.

Le stockage des données utilisateur dans le volume racine augmente le temps de rétablissement du stockage entre les nœuds d'une paire haute disponibilité.

- Vous pouvez déplacer le volume root vers un autre agrégat. Voir [\[relocate-root\]](#).
- L'agrégat root est dédié uniquement au volume root du nœud.

ONTAP vous empêche de créer d'autres volumes dans l'agrégat racine.

## "NetApp Hardware Universe"

### Libérez de l'espace sur le volume racine d'un nœud

Un message d'avertissement s'affiche lorsque le volume racine d'un nœud est saturé ou presque plein. Le nœud ne peut pas fonctionner correctement lorsque son volume racine est plein. Vous pouvez libérer de l'espace sur le volume racine d'un nœud en supprimant les fichiers « core dump », les fichiers de trace des paquets et les copies Snapshot de volume racine.

### Étapes

1. Afficher les fichiers core dump du nœud et leur nom :

```
system node coredump show
```

2. Supprimez les fichiers core dump indésirables du nœud :

```
system node coredump delete
```

3. Accès au nodeshell :

```
system node run -node nodename
```

*nodename* est le nom du nœud dont vous souhaitez libérer l'espace du volume racine.

4. Passez au niveau de privilège avancé du nodeshell à partir du nodeshell :

**priv set advanced**

5. Afficher et supprimer les fichiers de trace des paquets du nœud via le nodeshell :

a. Afficher tous les fichiers dans le volume root du nœud :

**ls /etc**

b. Si des fichiers de trace de paquets sont enregistrés (\*.trc) sont dans le volume racine du nœud, supprimez-les individuellement :

**rm /etc/log/packet\_traces/file\_name.trc**

6. Identifiez et supprimez les copies Snapshot du volume racine du nœud via le nodeshell :

a. Identifiez le nom du volume root :

**vol status**

Le volume racine est indiqué par le mot « root » dans la colonne « Options » du `vol status` sortie de la commande.

Dans l'exemple suivant, le volume root est `vol0`:

```
node1*> vol status
```

| Volume | State  | Status                  | Options         |
|--------|--------|-------------------------|-----------------|
| vol0   | online | raid_dp, flex<br>64-bit | root, nvfail=on |

a. Afficher les copies Snapshot du volume racine :

**snap list root\_vol\_name**

b. Supprimez les copies Snapshot de volume racine non souhaitées :

**snap delete root\_vol\_namesnapshot\_name**

7. Quittez le nodeshell et retournez au clustershell :

**exit**

### Transfert des volumes racines vers de nouveaux agrégats

La procédure de remplacement racine migre l'agrégat racine actuel vers un autre jeu de disques sans interruption.

### Description de la tâche

Le basculement du stockage doit être activé pour transférer les volumes root. Vous pouvez utiliser le `storage failover modify -node nodename -enable true` commande permettant d'activer le basculement.

Vous pouvez modifier l'emplacement du volume root vers un nouvel agrégat dans les scénarios suivants :



- Lorsque les agrégats racines ne sont pas sur le disque de votre choix
- Lorsque vous souhaitez réorganiser les disques connectés au nœud
- Lorsque vous effectuez un remplacement des tiroirs disques EOS

## Étapes

1. Définissez le niveau de privilège sur avancé :

```
set privilege advanced
```

2. Transférer l'agrégat racine :

```
system node migrate-root -node nodename -disklist disklist -raid-type raid-type
```

- **-noeud**

Spécifie le nœud qui possède l'agrégat racine que vous souhaitez migrer.

- **-disklist**

Spécifie la liste des disques sur lesquels le nouvel agrégat racine sera créé. Tous les disques doivent être des disques de secours et appartenir au même nœud. Le nombre minimum de disques requis dépend du type RAID.

- **-raid-type**

Spécifie le type RAID de l'agrégat racine. La valeur par défaut est `raid-dp`.

3. Surveiller la progression de la tâche :

```
job show -id jobid -instance
```

## Résultats

Si toutes les vérifications préalables ont réussi, la commande démarre un travail de remplacement de volume racine et se ferme. Le nœud devrait redémarrer.

## Démarrer ou arrêter la présentation d'un nœud

Pour des raisons de maintenance ou de dépannage, vous pouvez avoir besoin de démarrer ou d'arrêter un nœud. Vous pouvez le faire via l'interface de ligne de commandes de ONTAP, l'invite de l'environnement de démarrage ou l'interface de ligne de commandes du processeur de service.

Utilisation de la commande de l'interface de ligne de commandes du processeur `system power off` ou `system power cycle` Pour mettre hors/sous tension un nœud peut provoquer un arrêt inapproprié du nœud (également appelé *shutdown*) et n'a pas vocation à remplacer un arrêt normal à l'aide du ONTAP `system node halt` commande.

## Redémarrez un nœud à l'invite du système

Vous pouvez redémarrer un nœud en mode normal depuis l'invite du système. Un nœud est configuré pour démarrer à partir du périphérique d'amorçage, tel qu'une carte CompactFlash pour PC.

## Étapes

1. Si le cluster contient quatre nœuds ou plus, vérifier que le nœud à redémarrer ne contient pas epsilon :

- a. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

- b. Déterminer quel nœud contient epsilon :

```
cluster show
```

L'exemple suivant montre que « node1 » possède epsilon :

```
cluster1::*> cluster show
Node Health Eligibility Epsilon

node1 true true true
node2 true true false
node3 true true false
node4 true true false
4 entries were displayed.
```

- a. Si le nœud à redémarrer contient epsilon, retirer epsilon du nœud :

```
cluster modify -node node_name -epsilon false
```

- b. Assigner epsilon à un nœud différent qui demeurera en service :

```
cluster modify -node node_name -epsilon true
```

- c. Retour au niveau de privilège admin :

```
set -privilege admin
```

2. Utilisez le `system node reboot` commande permettant de redémarrer le nœud.

Si vous ne spécifiez pas le `-skip-lif-migration` Paramètre, la commande tente de migrer les LIF de gestion du cluster et des données de manière synchrone vers un autre nœud avant le redémarrage. Si la migration de LIF échoue ou se trouve en dehors des délais, le processus de redémarrage est interrompu et ONTAP affiche une erreur pour indiquer l'échec de la migration de LIF.

```
cluster1::> system node reboot -node node1 -reason "software upgrade"
```

Le processus de redémarrage du nœud démarre. L'invite de connexion ONTAP apparaît, indiquant que le processus de redémarrage est terminé.

**Démarrez ONTAP à l'invite de l'environnement de démarrage**

Vous pouvez démarrer la version actuelle ou la version de sauvegarde de ONTAP lorsque vous êtes à l'invite d'environnement d'amorçage d'un nœud.

**Étapes**

- 1. Accédez à l'invite de l'environnement d'initialisation à partir de l'invite du système de stockage à l'aide de la `system node halt` commande.

La console du système de stockage affiche l'invite de l'environnement de démarrage.

- 2. À l'invite de l'environnement de démarrage, entrez l'une des commandes suivantes :

| Pour démarrer...                                                | Entrer...                 |
|-----------------------------------------------------------------|---------------------------|
| La dernière version de ONTAP                                    | <code>boot_ontap</code>   |
| Image principale ONTAP à partir du périphérique de démarrage    | <code>boot_primary</code> |
| Image de sauvegarde ONTAP à partir du périphérique de démarrage | <code>boot_backup</code>  |

Si vous n'êtes pas certain de l'image à utiliser, vous devez utiliser `boot_ontap` dans la première instance.

**Arrêtez un nœud**

Vous pouvez arrêter un nœud s'il ne répond plus, ou si le personnel de support vous y dirige, dans le cadre des opérations de dépannage.

**Étapes**

- 1. Si le cluster contient quatre nœuds ou plus, vérifier que le nœud à arrêter ne contient pas epsilon :
  - a. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

- b. Déterminer quel nœud contient epsilon :

```
cluster show
```

L'exemple suivant montre que « node1 » possède epsilon :

```
cluster1::*> cluster show
Node Health Eligibility Epsilon

node1 true true true
node2 true true false
node3 true true false
node4 true true false
4 entries were displayed.
```

- a. Si le nœud à arrêter contient epsilon, retirer epsilon du nœud :

```
cluster modify -node node_name -epsilon false
```

- b. Assigner epsilon à un nœud différent qui demeurera en service :

```
cluster modify -node node_name -epsilon true
```

- c. Retour au niveau de privilège admin :

```
set -privilege admin
```

2. Utilisez le `system node halt` commande permettant d'arrêter le nœud.

Si vous ne spécifiez pas le `-skip-lif-migration` Paramètre, la commande tente de migrer les LIF de gestion des données et du cluster de manière synchrone vers un autre nœud avant l'arrêt. Si la migration de LIF échoue ou se trouve en dehors des délais, le processus d'arrêt est interrompu et ONTAP affiche une erreur pour indiquer l'échec de la migration de LIF.

Vous pouvez déclencher manuellement un « core dump » avec l'arrêt en utilisant les deux `-dump` paramètre.

L'exemple suivant arrête le nœud nommé « node1 » pour la maintenance matérielle :

```
cluster1::> system node halt -node node1 -reason 'hardware maintenance'
```

## Gérer un nœud à l'aide du menu de démarrage

Vous pouvez utiliser le menu de démarrage pour corriger les problèmes de configuration sur un nœud, réinitialiser le mot de passe d'administration, initialiser les disques, réinitialiser la configuration du nœud et restaurer les informations de configuration du nœud sur le périphérique d'amorçage.



Si une paire haute disponibilité est utilisée "[Cryptage SAS ou disques NVMe \(SED, NSE, FIPS\)](#)", vous devez suivre les instructions de la rubrique "[Retour d'un lecteur FIPS ou SED en mode non protégé](#)" Pour tous les disques de la paire HA avant d'initialiser le système (options de démarrage 4 ou 9). Si vous ne le faites pas, vous risquez de subir des pertes de données si les disques sont requalifiés.

Étapes

- 1. Redémarrez le nœud pour accéder au menu de démarrage à l'aide de `system node reboot` commande à l'invite du système.

Le processus de redémarrage du nœud démarre.

- 2. Pendant le processus de redémarrage, appuyez sur Ctrl-C pour afficher le menu de démarrage lorsque vous y êtes invité.

Le nœud affiche les options suivantes pour le menu de démarrage :


```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set onboard key management recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```



Option de menu d'amorçage (2) l'amorçage sans `/etc/rc` est obsolète et n'a aucun effet sur le système.

- 3. Sélectionnez l'une des options suivantes en saisissant le numéro correspondant :

| Pour...                                                                              | Sélectionner...                 |
|--------------------------------------------------------------------------------------|---------------------------------|
| Continuer à démarrer le nœud en mode normal                                          | 1) démarrage normal             |
| Modifier le mot de passe du noeud, qui est aussi le mot de passe du compte ""admin"" | 3) modification du mot de passe |

| Pour...                                                                                                                                                   | Sélectionner...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Initialiser les disques du nœud et créer un volume racine pour le nœud                                                                                    | <p>4) nettoyer la configuration et initialiser tous les disques</p> <div data-bbox="678 258 730 315">  </div> <p>Cette option de menu efface toutes les données sur les disques du nœud et réinitialise la configuration par défaut de votre nœud.</p> <p>Sélectionnez cette option de menu uniquement après que le nœud a été supprimé d'un cluster (non joint) et qu'il n'est pas joint à un autre cluster.</p> <p>Dans le cas d'un nœud avec des tiroirs disques internes ou externes, le volume racine des disques internes est initialisé. S'il n'y a pas de tiroirs disques internes, le volume root sur les disques externes est initialisé.</p> <p>Dans le cas d'un système exécutant la virtualisation FlexArray avec des tiroirs disques internes ou externes, les LUN de baie ne sont pas initialisées. Tout disque natif sur des tiroirs internes ou externes est initialisé.</p> <p>Dans le cas d'un système exécutant la virtualisation FlexArray avec uniquement DES LUN de baie et aucun tiroir disque interne ou externe, le volume racine DES LUN de la baie de stockage est initialisé, voir "<a href="#">Installation de FlexArray</a>".</p> <p>Si le nœud que vous souhaitez initialiser contient des disques qui sont partitionnés pour le partitionnement données-racines, les disques doivent être départitionnés avant que le nœud puisse être initialisé, voir <b>9) configurer le partitionnement de disque avancé</b> et "<a href="#">Gestion des disques et des agrégats</a>".</p> |
| Opérations de maintenance des agrégats et des disques pour obtenir des informations détaillées sur les agrégats et les disques                            | <p>5) démarrage du mode maintenance</p> <p>Pour quitter le mode Maintenance, utilisez le <code>halt</code> commande.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Restaurez les informations de configuration à partir du volume racine du nœud vers le périphérique d'amorçage, par exemple une carte CompactFlash pour PC | <p>6) mettre à jour la mémoire flash à partir de la configuration de sauvegarde</p> <p>ONTAP stocke des informations de configuration des nœuds sur le périphérique de démarrage. Au redémarrage du nœud, les informations du périphérique de démarrage sont automatiquement sauvegardées sur le volume racine du nœud. Si le périphérique d'amorçage est corrompu ou doit être remplacé, vous devez utiliser cette option de menu pour restaurer les informations de configuration du volume racine du nœud vers le périphérique d'amorçage.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| Pour...                                                                                                                                                                      | Sélectionner...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Installez le nouveau logiciel sur le nœud                                                                                                                                    | <p>7) installer le nouveau logiciel en premier</p> <p>Si le logiciel ONTAP du périphérique d'amorçage n'inclut pas la prise en charge de la matrice de stockage que vous souhaitez utiliser pour le volume racine, vous pouvez utiliser cette option de menu pour obtenir une version du logiciel qui prend en charge votre matrice de stockage et l'installer sur le nœud.</p> <p>Cette option de menu permet uniquement d'installer une version plus récente du logiciel ONTAP sur un nœud sur lequel aucun volume racine n'est installé. Do <i>NOT</i> utiliser cette option de menu pour mettre à niveau ONTAP.</p>                                                                                                                        |
| Redémarrez le nœud                                                                                                                                                           | 8) redémarrez le nœud                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Départitionner tous les disques et supprimer leurs informations de propriété ou nettoyer la configuration et initialiser le système avec des disques entiers ou partitionnés | <p>9) Configuration du partitionnement de disque avancé</p> <p>Depuis ONTAP 9.2, l'option de partitionnement de disque avancé fournit des fonctionnalités de gestion supplémentaires pour les disques configurés pour le partitionnement données-racines ou données-racines. Les options suivantes sont disponibles à partir de l'option de démarrage 9 :</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>(9a) Unpartition all disks and remove their ownership information.</p> <p>(9b) Clean configuration and initialize system with partitioned disks.</p> <p>(9c) Clean configuration and initialize system with whole disks.</p> <p>(9d) Reboot the node.</p> <p>(9e) Return to main boot menu.</p> </div> |

## Affiche les attributs du nœud

Vous pouvez afficher les attributs d'un ou plusieurs nœuds du cluster, par exemple le nom, le propriétaire, l'emplacement, numéro de modèle, numéro de série, durée pendant laquelle le nœud s'exécute, état de santé et éligibilité à un cluster.

### Étapes

1. Pour afficher les attributs d'un nœud spécifié ou à propos de tous les nœuds d'un cluster, utilisez le `system node show` commande.

### Exemple d'affichage des informations relatives à un nœud

L'exemple suivant affiche des informations détaillées sur le nœud 1 :

```
cluster1::> system node show -node node1
 Node: node1
 Owner: Eng IT
 Location: Lab 5
 Model: model_number
 Serial Number: 12345678
 Asset Tag: -
 Uptime: 23 days 04:42
 NVRAM System ID: 118051205
 System ID: 0118051205
 Vendor: NetApp
 Health: true
 Eligibility: true
 Differentiated Services: false
 All-Flash Optimized: true
 Capacity Optimized: false
 QLC Optimized: false
 All-Flash Select Optimized: false
 SAS2/SAS3 Mixed Stack Support: none
```

## Modifier les attributs du nœud

Vous pouvez modifier les attributs d'un nœud si nécessaire. Les attributs que vous pouvez modifier incluent les informations sur le propriétaire du nœud, les informations d'emplacement, le numéro d'inventaire et l'éligibilité à participer au cluster.

### Description de la tâche

L'éligibilité d'un nœud à participer au cluster peut être modifiée au niveau de privilège avancé à l'aide de `-eligibility` paramètre du `system node modify` ou `cluster modify` commande. Si vous définissez l'éligibilité d'un nœud sur `false`, le nœud est inactif dans le cluster.



Vous ne pouvez pas modifier l'éligibilité des nœuds localement. Il doit être modifié depuis un autre nœud. L'éligibilité des nœuds ne peut pas non plus être modifiée avec une configuration haute disponibilité du cluster.



Vous ne devez pas définir l'éligibilité d'un nœud sur `false`, à l'exception de cas tels que la restauration de la configuration de nœuds ou la maintenance prolongée des nœuds. L'accès aux données SAN et NAS au nœud peut être affecté lorsque ce dernier n'est pas éligible.

## Étapes

1. Utilisez le `system node modify` commande permettant de modifier les attributs d'un nœud.

### Exemple de modification des attributs du nœud

La commande suivante modifie les attributs du nœud « node1 ». Le propriétaire du nœud est défini sur « Joe Smith » et son numéro d'inventaire est défini sur « js1234 » :



```
cluster1::> system node modify -node node1 -owner "Joe Smith" -assettag
js1234
```

## Renommez un nœud

Vous pouvez modifier le nom d'un nœud si nécessaire.

### Étapes

1. Pour renommer un nœud, utilisez `system node rename` commande.

Le `-newname` paramètre spécifie le nouveau nom pour le nœud. Le `system node rename` la page man décrit les règles à respecter lorsque vous spécifiez le nom du nœud.

Si vous souhaitez renommer plusieurs nœuds du cluster, vous devez exécuter la commande de chaque nœud séparément.



Le nom du nœud ne peut pas être « tous » car « tous » est un nom réservé au système.

### Exemple de modification du nom d'un nœud

La commande suivante renomme le nœud « node1 » en « node1a » :

```
cluster1::> system node rename -node node1 -newname node1a
```

## Gérez des clusters à un seul nœud

Un cluster à un seul nœud est une implémentation spéciale d'un cluster exécuté sur un nœud autonome. Les clusters à un seul nœud ne sont pas recommandés, car ils n'offrent pas de redondance. En cas de panne du nœud, l'accès aux données est perdu.



Pour la tolérance aux pannes et la continuité de l'activité, il est fortement recommandé de configurer votre cluster avec "[Haute disponibilité \(paires haute disponibilité\)](#)".

Si vous choisissez de configurer ou de mettre à niveau un cluster à un seul nœud, vous devez connaître les points suivants :

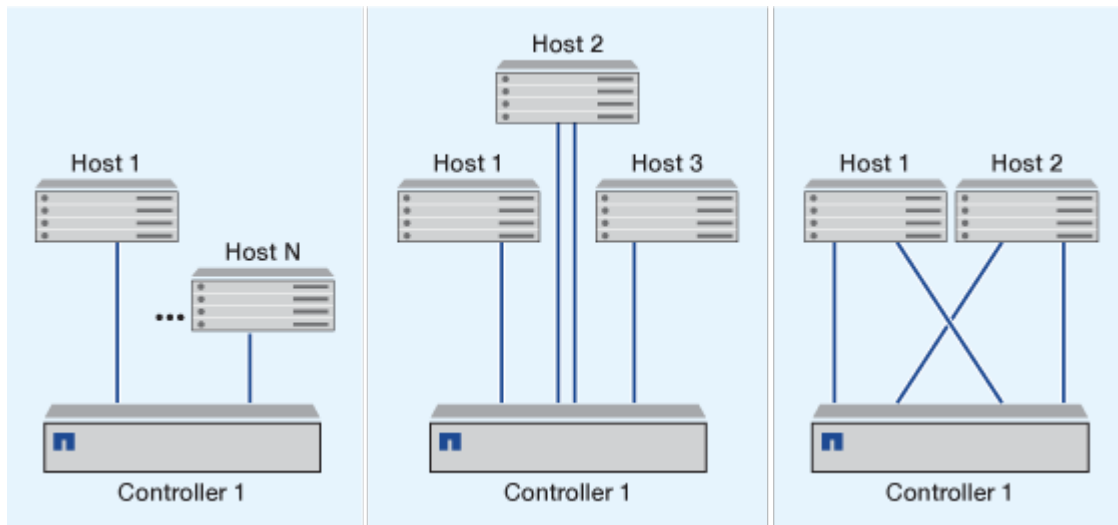
- Le chiffrement du volume racine n'est pas pris en charge sur les clusters à un seul nœud.
- Si vous supprimez des nœuds devant disposer d'un cluster à un seul nœud, vous devez modifier les ports de cluster pour transmettre le trafic de données en modifiant les ports de cluster en tant que ports de données, puis en créant des LIFs de données sur les ports de données.
- Pour les clusters à un seul nœud, vous pouvez spécifier la destination de sauvegarde de la configuration lors de l'installation du logiciel. Une fois l'installation effectuée, ces paramètres peuvent être modifiés à l'aide des commandes ONTAP.
- Si plusieurs hôtes se connectent au nœud, chaque hôte peut être configuré avec un système d'exploitation différent, tel que Windows ou Linux. Si plusieurs chemins s'offrent à l'hôte vers le contrôleur, ALUA doit être activé sur l'hôte.

## Méthodes de configuration des hôtes SAN iSCSI avec des nœuds uniques

Vous pouvez configurer des hôtes SAN iSCSI pour qu'ils se connectent directement à un seul nœud ou via un ou plusieurs commutateurs IP. Le nœud peut avoir plusieurs connexions iSCSI au commutateur.

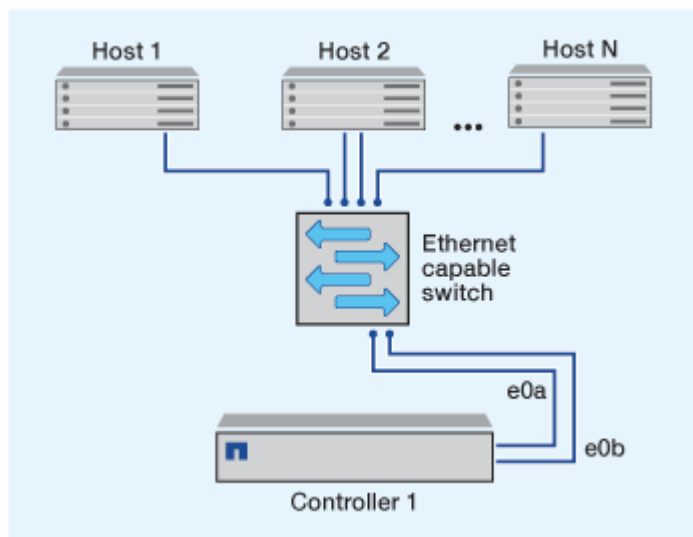
### Configurations à un seul nœud en attachement direct

Dans les configurations à un seul nœud à connexion directe, un ou plusieurs hôtes sont directement connectés au nœud.



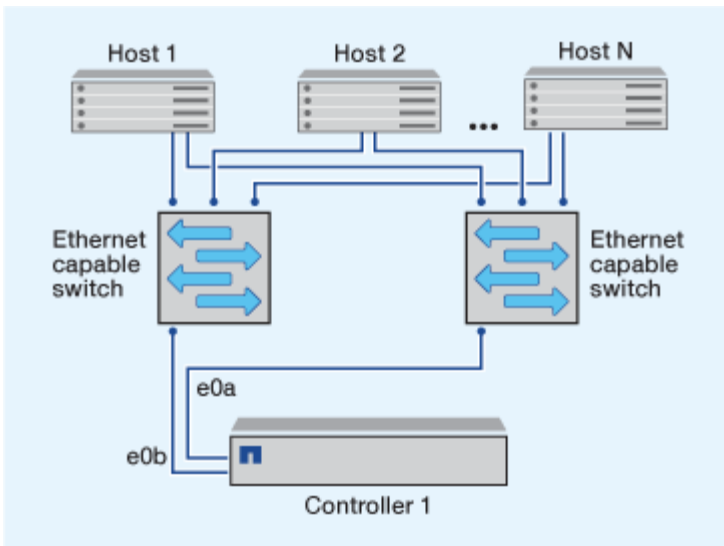
### Configurations à un seul réseau sans nœud

Dans les configurations à un seul réseau et à un seul nœud, un commutateur connecte un seul nœud à un ou plusieurs hôtes. Comme il y a un seul commutateur, cette configuration n'est pas entièrement redondante.



### Configurations à nœud unique multi-réseau

Dans les configurations à un nœud multi-réseau, deux commutateurs ou plus connectent un nœud à un ou plusieurs hôtes. Étant donné qu'il y a plusieurs commutateurs, cette configuration est totalement redondante.



### Méthodes de configuration des hôtes SAN FC et FC-NVMe avec des nœuds uniques

Vous pouvez configurer des hôtes SAN FC et FC-NVMe avec des nœuds uniques via une ou plusieurs structures. La virtualisation NPIV (N-Port ID Virtualization) est requise et doit être activée sur tous les commutateurs FC de la structure. Vous ne pouvez pas relier directement des hôtes SAN FC ou FC-NVMe aux nœuds uniques sans utiliser de commutateur FC.

#### Configurations à 1 nœud et structure unique

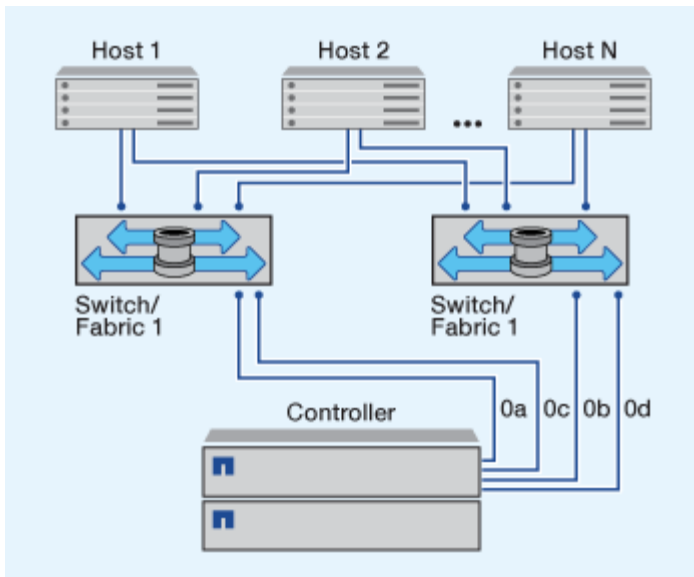
Dans les configurations à un seul nœud de la structure unique, un commutateur connecte un seul nœud à un ou plusieurs hôtes. Comme il y a un seul commutateur, cette configuration n'est pas entièrement redondante.

Dans les configurations à un seul nœud de la structure unique, vous n'avez pas besoin de logiciels de chemins d'accès multiples si vous disposez uniquement d'un chemin d'accès unique de l'hôte vers le nœud.

#### Configurations multifabriques à un nœud

Dans les configurations multifabriques à un nœud, il existe deux commutateurs ou plus qui connectent un nœud à un ou plusieurs hôtes. Dans une optique de simplicité, la figure suivante présente une configuration multistrukture à un seul nœud avec seulement deux fabriques. Elle présente également au moins deux fabrics dans une configuration multi-fabric. Dans cette figure, le contrôleur de stockage est monté dans le châssis supérieur et le châssis inférieur peut être vide ou comporter un module IOMX, comme dans cet exemple.

Les ports cibles FC (0a, 0C, 0b, 0d) dans les illustrations sont des exemples. Les numéros de port réels varient selon le modèle de votre nœud de stockage et si vous utilisez des adaptateurs d'extension.



### Informations associées

"Rapport technique NetApp 4684 : implémentation et configuration de SAN modernes avec NVMe-of"

### Mise à niveau de ONTAP pour un cluster à un seul nœud

Depuis la version ONTAP 9.2, vous pouvez utiliser l'interface de ligne de commandes ONTAP pour effectuer une mise à jour automatisée d'un cluster à un seul nœud. Les clusters à un seul nœud ne manquent pas de redondance. Les mises à jour restent donc toujours perturbées. Les mises à niveau entraînant des interruptions ne peuvent pas être réalisées avec System Manager.

### Avant de commencer

Vous devez terminer la mise à niveau "préparation" étapes.

### Étapes

1. Supprimez le pack logiciel ONTAP précédent :

```
cluster image package delete -version <previous_package_version>
```

2. Téléchargez le pack logiciel ONTAP cible :

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.7/image.tgz
```

```
Package download completed.
Package processing completed.
```

3. Vérifiez que le pack logiciel est disponible dans le référentiel du package de cluster :

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version Package Build Time

9.7 M/DD/YYYY 10:32:15
```

4. Vérifiez que le cluster est prêt à être mis à niveau :

```
cluster image validate -version <package_version_number>
```

```
cluster1::> cluster image validate -version 9.7
```

WARNING: There are additional manual upgrade validation checks that must be performed after these automated validation checks have completed...

5. Surveiller la progression de la validation :

```
cluster image show-update-progress
```

6. Effectuez toutes les actions requises identifiées par la validation.

7. Générer une estimation de mise à niveau logicielle si vous le souhaitez :

```
cluster image update -version <package_version_number> -estimate-only
```

L'estimation de la mise à niveau logicielle affiche des détails sur chaque composant à mettre à jour, ainsi que la durée estimée de la mise à niveau.

8. Effectuez la mise à niveau logicielle :

```
cluster image update -version <package_version_number>
```



En cas de problème, la mise à jour s'interrompt et vous êtes invité à prendre les mesures correctives nécessaires. Vous pouvez utiliser la commande `cluster image show-update-progress` pour afficher les détails de tous les problèmes et la progression de la mise à jour. Après avoir résolu le problème, vous pouvez reprendre la mise à jour à l'aide de la commande `cluster image resume-update`.

9. Afficher la progression de la mise à jour du cluster :

```
cluster image show-update-progress
```

Le nœud est redémarré dans le cadre de la mise à jour et ne peut pas être accédé durant le redémarrage.

10. Déclencher une notification :

```
autosupport invoke -node * -type all -message "Finishing_Upgrade"
```

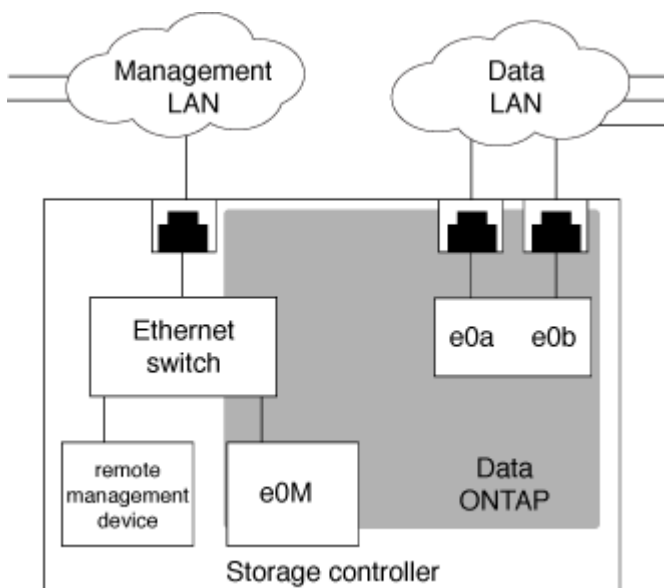
Si votre cluster n'est pas configuré pour envoyer des messages, une copie de la notification est enregistrée localement.

## Configuration du réseau SP/BMC

### Isolez le trafic du réseau de gestion

Il est recommandé de configurer le processeur de service/BMC et l'interface de gestion e0M sur un sous-réseau dédié au trafic de gestion. L'exécution du trafic de données sur le réseau de gestion peut entraîner des problèmes de dégradation des performances et de routage.

Le port Ethernet de gestion de la plupart des contrôleurs de stockage (indiqué par une icône de clé anglaise à l'arrière du châssis) est connecté à un commutateur Ethernet interne. Le commutateur interne fournit la connectivité au SP/BMC et à l'interface de gestion e0M, que vous pouvez utiliser pour accéder au système de stockage via les protocoles TCP/IP tels que Telnet, SSH et SNMP.



Si vous prévoyez d'utiliser à la fois le périphérique de gestion à distance et le e0M, vous devez les configurer sur le même sous-réseau IP. Étant donné qu'il s'agit d'interfaces à faible bande passante, il est recommandé de configurer le processeur de service/BMC et e0M sur un sous-réseau dédié au trafic de gestion.

Si vous ne pouvez pas isoler le trafic de gestion ou si votre réseau de gestion dédié est exceptionnellement grand, vous devez essayer de maintenir le volume de trafic réseau le plus bas possible. Un trafic de diffusion

ou de multidiffusion excessif peut dégrader les performances du SP/BMC.



Certains contrôleurs de stockage, comme le AFF A800, disposent de deux ports externes, l'un pour BMC et l'autre pour e0M. Pour ces contrôleurs, il n'est pas nécessaire de configurer BMC et e0M sur le même sous-réseau IP.

### Considérations relatives à la configuration réseau SP/BMC

Vous pouvez activer une configuration réseau automatique au niveau du cluster pour le processeur de service (recommandé). Vous pouvez également désactiver la configuration réseau automatique du processeur de service (par défaut) et gérer manuellement la configuration réseau du processeur de service au niveau du nœud. Il existe quelques considérations pour chaque cas.



Cette rubrique s'applique à la fois au processeur de service et au contrôleur BMC.

La configuration réseau automatique du processeur de service permet au processeur de service d'utiliser les ressources d'adresse (y compris l'adresse IP, le masque de sous-réseau et l'adresse de passerelle) du sous-réseau spécifié pour configurer automatiquement son réseau. Grâce à la configuration réseau automatique du processeur de service, vous n'avez pas besoin d'attribuer manuellement des adresses IP au processeur de service de chaque nœud. Par défaut, la configuration réseau automatique du processeur de service est désactivée, car l'activation de la configuration nécessite que le sous-réseau soit d'abord défini dans le cluster.

Si vous activez la configuration réseau automatique du processeur de service, les scénarios et considérations suivants s'appliquent :

- Si le processeur de service n'a jamais été configuré, le réseau du processeur de service est configuré automatiquement en fonction du sous-réseau spécifié pour la configuration réseau automatique du processeur de service.
- Si le processeur de service a déjà été configuré manuellement, ou si la configuration réseau du processeur de service existante est basée sur un autre sous-réseau, le réseau SP de tous les nœuds du cluster est reconfiguré en fonction du sous-réseau que vous spécifiez dans la configuration réseau automatique du processeur de service.

La reconfiguration peut affecter une autre adresse au processeur de service, ce qui peut avoir un impact sur votre configuration DNS et sa capacité à résoudre les noms d'hôtes du processeur de service. Par conséquent, vous devrez peut-être mettre à jour votre configuration DNS.

- Un nœud qui rejoint le cluster utilise le sous-réseau spécifié pour configurer automatiquement son réseau SP.
- Le `system service-processor network modify` La commande ne vous permet pas de modifier l'adresse IP du processeur de service.

Lorsque la configuration réseau automatique du processeur de service est activée, la commande ne vous permet que d'activer ou de désactiver l'interface réseau du processeur de service.

- Si la configuration réseau automatique du processeur de service était auparavant activée, la désactivation de l'interface réseau du processeur de service entraîne la libération de la ressource d'adresse attribuée et son renvoi au sous-réseau.
- Si vous désactivez l'interface réseau du processeur de service, puis le réactivez, il est possible que le processeur de service soit reconfiguré à une adresse différente.

Si la configuration réseau automatique du processeur de service est désactivée (par défaut), les scénarios et considérations suivants s'appliquent :

- Si le processeur de service n'a jamais été configuré, la configuration réseau IPv4 du processeur de service utilise par défaut DHCP IPv4 et IPv6 est désactivé.

Un nœud qui rejoint le cluster utilise également le DHCP IPv4 pour sa configuration réseau du processeur de service par défaut.

- Le `system service-processor network modify` Commande vous permet de configurer l'adresse IP du processeur de service d'un nœud.

Un message d'avertissement apparaît lorsque vous tentez de configurer manuellement le réseau du processeur de service avec des adresses allouées à un sous-réseau. Si vous ignorez l'avertissement et que vous procédez à l'attribution manuelle d'adresse, vous risquez d'entraîner un scénario avec des adresses en double.

Si la configuration réseau automatique du processeur de service est désactivée après avoir été activée précédemment, les scénarios et considérations suivants s'appliquent :

- Si la configuration réseau automatique du processeur de service possède la famille d'adresses IPv4 désactivée, le réseau IPv4 du processeur de service utilise par défaut DHCP, et le `system service-processor network modify` La commande vous permet de modifier la configuration IPv4 du processeur de service pour les nœuds individuels.
- Si la famille d'adresses IPv6 est désactivée dans la configuration réseau automatique du processeur de service, le réseau IPv6 du processeur de service est également désactivé et le `system service-processor network modify` Vous permet d'activer et de modifier la configuration IPv6 du processeur de service pour les nœuds individuels.

### Activez la configuration réseau automatique SP/BMC

Pour permettre au processeur de service d'utiliser la configuration réseau automatique, il est préférable de ne pas configurer le réseau du processeur de service manuellement. Étant donné que la configuration réseau automatique du processeur de service est à l'échelle du cluster, vous n'avez pas besoin de gérer manuellement le réseau du processeur de service pour les nœuds individuels.



Cette tâche s'applique à la fois au processeur de service et au contrôleur BMC.

- Le sous-réseau que vous souhaitez utiliser pour la configuration réseau automatique du processeur de service doit déjà être défini dans le cluster et ne doit pas avoir de conflit de ressources avec l'interface réseau du processeur de service.

Le `network subnet show` la commande affiche les informations de sous-réseau du cluster.

Le paramètre qui force l'association de sous-réseau (le `-force-update-lif-associations` paramètre du `network subnet` Commandes) est pris en charge uniquement sur les LIFs réseau et non sur l'interface réseau du processeur de service.

- Si vous souhaitez utiliser des connexions IPv6 pour le processeur de service, IPv6 doit déjà être configuré et activé pour ONTAP.



Le `network options ipv6 show` Commande affiche l'état actuel des paramètres IPv6 pour ONTAP.

## Étapes

1. Spécifiez la famille d'adresses IPv4 ou IPv6 et le nom du sous-réseau que vous souhaitez que le processeur de service utilise `system service-processor network auto-configuration enable` commande.
2. Affiche la configuration réseau automatique du processeur de service à l'aide de `system service-processor network auto-configuration show` commande.
3. Si vous souhaitez par la suite désactiver ou réactiver l'interface réseau IPv4 ou IPv6 du processeur de service pour tous les nœuds qui se trouvent dans le quorum, utilisez le `system service-processor network modify` commande avec `-address-family [IPv4|IPv6]` et `-enable [true|false]` paramètres.

Lorsque la configuration réseau automatique du processeur de service est activée, vous ne pouvez pas modifier l'adresse IP du processeur de service pour un nœud qui se trouve au quorum. Vous pouvez activer ou désactiver uniquement l'interface réseau IPv4 ou IPv6 du processeur de service.

Si un nœud est hors quorum, vous pouvez modifier la configuration réseau du processeur de service du nœud, y compris l'adresse IP du processeur de service, en exécutant `system service-processor network modify` Depuis le nœud et confirmer que vous souhaitez remplacer la configuration réseau automatique du processeur de service pour le nœud. Cependant, lorsque le nœud rejoint le quorum, la reconfiguration automatique du processeur de service est effectuée pour le nœud en fonction du sous-réseau spécifié.

## Configurez le réseau SP/BMC manuellement

Si vous ne disposez pas d'une configuration réseau automatique définie pour le processeur de service, vous devez configurer manuellement le réseau SP d'un nœud pour que ce dernier soit accessible via une adresse IP.

### Ce dont vous avez besoin

Si vous souhaitez utiliser des connexions IPv6 pour le processeur de service, IPv6 doit déjà être configuré et activé pour ONTAP. Le `network options ipv6` Les commandes gèrent les paramètres IPv6 pour ONTAP.



Cette tâche s'applique à la fois au processeur de service et au contrôleur BMC.

Vous pouvez configurer le processeur de service pour qu'il utilise IPv4, IPv6 ou les deux. La configuration IPv4 du processeur de service prend en charge l'adressage statique et DHCP, et la configuration IPv6 du processeur de service prend uniquement en charge l'adressage statique.

Si la configuration réseau automatique du processeur de service a été configurée, vous n'avez pas besoin de configurer manuellement le réseau SP pour des nœuds individuels, et le `system service-processor network modify` La commande vous permet d'activer ou de désactiver uniquement l'interface réseau du processeur de service.

## Étapes

1. Configurez le réseau du processeur de service d'un nœud en utilisant le `system service-processor network modify` commande.
  - Le `-address-family` Le paramètre spécifie si la configuration IPv4 ou IPv6 du processeur de service doit être modifiée.

- Le `-enable` Paramètre active l'interface réseau de la famille d'adresses IP spécifiée.
- Le `-dhcp` Paramètre indique si la configuration réseau doit être utilisée depuis le serveur DHCP ou l'adresse réseau que vous fournissez.

Vous pouvez activer DHCP (par paramètre) `-dhcp` à v4) Uniquement si vous utilisez IPv4. Vous ne pouvez pas activer DHCP pour les configurations IPv6.

- Le `-ip-address` Le paramètre spécifie l'adresse IP publique pour le processeur de service.

Un message d'avertissement apparaît lorsque vous tentez de configurer manuellement le réseau du processeur de service avec des adresses allouées à un sous-réseau. L'omission de l'avertissement et la poursuite de l'attribution manuelle d'adresse peuvent entraîner une affectation d'adresse en double.

- Le `-netmask` Le paramètre spécifie le masque de réseau du processeur de service (si vous utilisez IPv4).
- Le `-prefix-length` Paramètre spécifie la longueur du préfixe réseau du masque de sous-réseau pour le processeur de service (si vous utilisez IPv6).
- Le `-gateway` Le paramètre spécifie l'adresse IP de passerelle pour le processeur de service.

2. Configurez le réseau SP pour les nœuds restants du cluster en répétant l'étape 1.
3. Affiche la configuration réseau du processeur de service et vérifie le statut de configuration du processeur de service à l'aide de `system service-processor network show` commande avec `-instance` ou `-field setup-status` paramètres.

Le statut de configuration du processeur de service d'un nœud peut être l'un des suivants :

- `not-setup` — non configuré
- `succeeded` — Configuration réussie
- `in-progress` — Configuration en cours
- `failed` — Echec de la configuration

### Exemple de configuration du réseau du processeur de service

L'exemple suivant configure le processeur de service d'un nœud pour utiliser IPv4, active le processeur de service et affiche la configuration réseau du processeur de service pour vérifier les paramètres :

```

cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

Node: node1
Address Type: IPv4
Interface Enabled: true
Type of Device: SP
Status: online
Link Status: up
DHCP Status: none
IP Address: 192.168.123.98
MAC Address: ab:cd:ef:fe:ed:02
Netmask: 255.255.255.0
Prefix Length of Subnet Mask: -
Router Assigned IP Address: -
Link Local IP Address: -
Gateway IP Address: 192.168.123.1
Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
Subnet Name: -
Enable IPv6 Router Assigned Address: -
SP Network Setup Status: succeeded
SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>

```

## Modifiez la configuration du service d'API du processeur de service

L'API du processeur de service est une API réseau sécurisée qui permet à ONTAP de communiquer avec le processeur de service sur le réseau. Vous pouvez modifier le port utilisé par le service API SP, renouveler les certificats que le service utilise pour les communications internes ou désactiver entièrement le service. Vous ne devez modifier la configuration que dans de rares cas.

### Description de la tâche

- Le service d'API du processeur de service utilise le port 50000 par défaut.

Vous pouvez modifier la valeur du port si, par exemple, vous êtes dans un paramètre réseau où port 50000 Est utilisé pour la communication par une autre application réseau ou pour différencier le trafic des autres applications et le trafic généré par le service API SP.

- Les certificats SSL et SSH utilisés par le service API du processeur de service sont internes au cluster et

ne sont pas distribués en externe.

Dans le cas peu probable où les certificats sont compromis, vous pouvez les renouveler.

- Le service API du processeur de service est activé par défaut.

Il vous suffit de désactiver le service API du processeur de service dans de rares cas, par exemple dans un LAN privé où le processeur de service n'est pas configuré ou utilisé et que vous souhaitez désactiver ce service.

Si le service d'API du processeur de service est désactivé, l'API n'accepte aucune connexion entrante. En outre, des fonctionnalités telles que les mises à jour de micrologiciel SP basées sur le réseau et la collecte de journaux de SP « `down system` » basée sur le réseau deviennent indisponibles. Le système passe à l'aide de l'interface série.

## Étapes

1. Passez au niveau de privilège avancé à l'aide du `set -privilege advanced` commande.
2. Modifiez la configuration du service d'API du processeur de service :

| Les fonctions que vous recherchez...                                                                  | Utiliser la commande suivante...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modifiez le port utilisé par le service d'API du processeur de service                                | <code>system service-processor api-service modify</code> avec le <code>-port {49152..`65535`paramètre }</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Renouvelez les certificats SSL et SSH utilisés par le service API SP pour les communications internes | <ul style="list-style-type: none"><li>• Pour ONTAP 9.5 ou une utilisation ultérieure<br/><code>system service-processor api-service renew-internal-certificate</code></li><li>• Pour ONTAP 9.4 et une utilisation antérieure<br/><code>system service-processor api-service renew-certificates</code></li></ul> <p>Si aucun paramètre n'est spécifié, seuls les certificats d'hôte (y compris les certificats client et serveur) sont renouvelés.</p> <p>Si le <code>-renew-all true</code> Le paramètre est spécifié, les certificats d'hôte et le certificat d'autorité de certification racine sont renouvelés.</p> |
| comm                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Désactivez ou réactivez le service API du processeur de service                                       | <code>system service-processor api-service modify</code> avec le <code>-is-enabled {true</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

3. Affichez la configuration du service API du processeur de service à l'aide de `system service-processor api-service show` commande.

## Gérez les nœuds à distance à l'aide du processeur de service/contrôleur BMC

### Gérez un nœud à distance à l'aide de la présentation SP/BMC

Vous pouvez gérer un nœud à distance à l'aide d'un contrôleur intégré, appelé processeur de service (SP) ou contrôleur BMC (Baseboard Management Controller). Ce contrôleur de gestion à distance est inclus dans tous les modèles de plate-forme actuels. Le contrôleur reste opérationnel quel que soit l'état de fonctionnement du nœud.

Les plates-formes suivantes prennent en charge BMC au lieu de SP :

- FAS 8700
- FAS 8300
- Prise de l'extension
- AFF A800
- AFF A700s
- AFF A400
- A320 de AFF
- AVEC AFF A220
- Baie AFF C190

### À propos du processeur de service

Le processeur de service (SP) est un périphérique de gestion à distance qui vous permet d'accéder à, de contrôler et de dépanner un nœud à distance.

Le processeur de service offre les fonctionnalités suivantes :

- Le processeur de service permet d'accéder à un nœud à distance pour diagnostiquer, arrêter, mettre hors/sous tension ou redémarrer le nœud, quel que soit l'état du contrôleur.

Le processeur de service est alimenté par une tension de veille, disponible tant qu'au moins une de ses alimentations est alimentée.

Vous pouvez vous connecter au processeur de service à l'aide d'une application cliente Secure Shell sur un hôte d'administration. Vous pouvez ensuite utiliser l'interface de ligne de commande du processeur de service pour surveiller et dépanner le nœud à distance. Vous pouvez également utiliser le processeur de service pour accéder à la console série et exécuter des commandes ONTAP à distance.

Vous pouvez accéder au processeur de service à partir de la console série de ou accéder à la console série à partir du processeur de service. Le processeur de service vous permet d'ouvrir simultanément une session d'interface de ligne de commandes du processeur de service et une autre session de console.

Par exemple, lorsqu'un capteur de température devient critique ou faible, ONTAP déclenche l'arrêt normal du processeur de service de la carte mère. La console série ne répond plus, mais vous pouvez tout de même utiliser la combinaison de touches Ctrl-G sur la console pour accéder à l'interface de ligne de commandes du processeur de service. Vous pouvez ensuite utiliser le `system power on` ou `system power cycle` Commande du processeur de service pour mettre le nœud sous tension ou hors tension.

- Le processeur de service surveille les capteurs environnementaux et les journaux d'événements pour vous aider à prendre des mesures de service efficaces et en temps opportun.

Le processeur de service surveille les capteurs environnementaux tels que les températures des nœuds, les tensions, les courants et la vitesse des ventilateurs. Lorsqu'un capteur environnemental a atteint un état anormal, le processeur de service consigne les lectures anormales, informe ONTAP du problème et envoie des alertes et des notifications « système propre » si nécessaire via un message AutoSupport, que le nœud puisse envoyer des messages AutoSupport ou non.

Le processeur de service consigne également des événements tels que la progression du démarrage, les modifications des unités remplaçables sur site, les événements générés par ONTAP et l'historique des commandes du processeur de service. Vous pouvez appeler manuellement un message AutoSupport pour inclure les fichiers journaux du processeur de service collectés à partir d'un nœud spécifié.

Autre que la génération de ces messages pour le compte d'un nœud qui est en panne et la connexion d'informations de diagnostic supplémentaires aux messages AutoSupport, le processeur de service n'a aucun impact sur la fonctionnalité AutoSupport. Les paramètres de configuration de AutoSupport et le comportement du contenu des messages sont hérités de ONTAP.



Le processeur de service ne repose pas sur le `-transport` paramètre du `system node autosupport modify` commande permettant d'envoyer des notifications. Le processeur de service utilise uniquement le protocole SMTP (simple Mail transport Protocol) et requiert la configuration AutoSupport de son hôte pour inclure les informations relatives à l'hôte de messagerie.

Si le protocole SNMP est activé, le processeur de service génère des interruptions SNMP vers des hôtes d'interruption configurés pour tous les événements "système propriétaire".

- Le processeur de service dispose d'un tampon de mémoire non volatile qui stocke jusqu'à 4,000 événements dans un journal des événements du système (SEL) pour vous aider à diagnostiquer les problèmes.

Le journal des événements système enregistre chaque entrée du journal d'audit en tant qu'événement d'audit. Il est stocké dans la mémoire flash intégrée sur le processeur de service. La liste des événements du journal des événements est automatiquement envoyée par le processeur de service aux destinataires spécifiés via un message AutoSupport.

Le journal des événements du système contient les informations suivantes :

- Événements matériels détectés par le processeur de service --par exemple, statut d'un capteur concernant les alimentations, la tension ou d'autres composants
  - Erreurs détectées par le processeur de service—par exemple, une erreur de communication, une panne de ventilateur ou une erreur de la mémoire ou de l'UC
  - Événements logiciels critiques envoyés au SP par le nœud—par exemple, une panique, une panne de communication, une panne de démarrage ou un "système propre" déclenché par l'utilisateur à la suite de l'émission du SP `system reset` ou `system power cycle` commande
- Le processeur de service surveille la console série, que les administrateurs soient connectés ou non à la console, que ce soit.

Lorsque des messages sont envoyés à la console, le processeur de service les stocke dans le journal de la console. Le journal de la console est conservé tant que le processeur de service est alimenté à partir d'une des alimentations du nœud. Du fait que le processeur de service fonctionne avec une alimentation de veille, il demeure disponible même lorsque le nœud est mis hors tension puis sous tension ou lorsqu'il

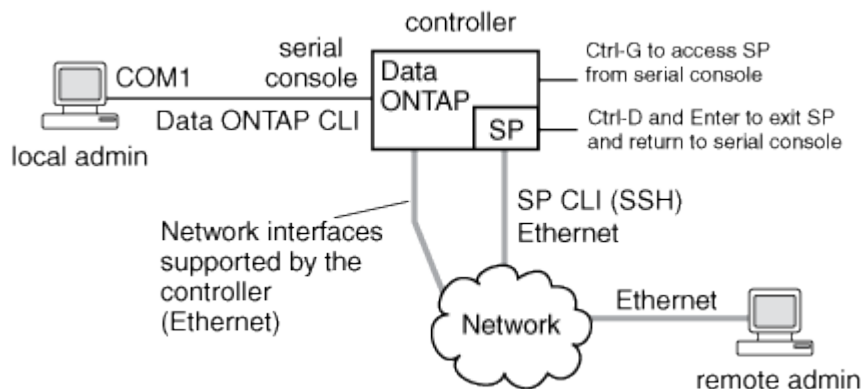
est arrêté.

- Le basculement assisté par matériel est disponible si le SP est configuré.
- Le service d'API du processeur de service permet à ONTAP de communiquer avec le processeur de service sur le réseau.

Le service améliore la gestion ONTAP du processeur de service en prenant en charge des fonctionnalités réseau telles que l'interface réseau de la mise à jour du firmware du processeur de service, ce qui permet à un nœud d'accéder à la fonctionnalité du processeur de service ou à la console système d'un autre nœud, et de charger le journal du processeur de service à partir d'un autre nœud.

Vous pouvez modifier la configuration du service API SP en modifiant le port utilisé par le service, en renouvelant les certificats SSL et SSH utilisés par le service pour une communication interne ou en désactivant entièrement le service.

Le schéma suivant illustre l'accès à ONTAP et au processeur de service d'un nœud. L'interface du processeur de service est accessible via le port Ethernet (indiqué par une icône de clé anglaise à l'arrière du châssis) :



### Rôle du contrôleur de gestion de la carte mère

Depuis ONTAP 9.1, sur certaines plateformes matérielles, le logiciel est personnalisé pour prendre en charge un nouveau contrôleur intégré dans le contrôleur BMC (Baseboard Management Controller). Le contrôleur BMC dispose de commandes d'interface de ligne de commande (CLI) que vous pouvez utiliser pour gérer le périphérique à distance.

Le contrôleur BMC fonctionne de la même manière que le processeur de service et utilise plusieurs des mêmes commandes. Le BMC vous permet de faire les opérations suivantes :

- Configurez les paramètres réseau du contrôleur BMC.
- Accéder à un nœud à distance et effectuer des tâches de gestion de nœud, telles que diagnostiquer, arrêter, mettre hors/sous tension ou redémarrer le nœud.

Il existe certaines différences entre le processeur de service et le contrôleur BMC :

- Le contrôleur BMC contrôle entièrement la surveillance environnementale des éléments d'alimentation, des éléments de refroidissement, des capteurs de température, des capteurs de tension et des capteurs de courant. Le contrôleur BMC signale les informations relatives aux capteurs à ONTAP via IPMI.

- Certaines des commandes de stockage et de haute disponibilité sont différentes.
- Le contrôleur BMC n'envoie pas de messages AutoSupport.

Des mises à jour automatiques du firmware sont également disponibles lors de l'exécution de ONTAP 9.2 GA ou version ultérieure avec les conditions suivantes :

- La version 1.15 ou ultérieure du micrologiciel BMC doit être installée.



Une mise à jour manuelle est nécessaire pour mettre à niveau le micrologiciel du contrôleur BMC de la version 1.12 à la version 1.15 ou ultérieure.

- BMC redémarre automatiquement une fois la mise à jour du micrologiciel terminée.



Les opérations de nœud ne sont pas affectées lors du redémarrage de BMC.

### Méthodes de gestion des mises à jour du micrologiciel SP/BMC

ONTAP inclut une image du micrologiciel du processeur de service appelée *baseline image*. Si une nouvelle version du firmware du processeur de service est disponible par la suite, vous pouvez la télécharger et mettre à jour le firmware du processeur de service vers la version téléchargée sans mettre à niveau la version ONTAP.



Cette rubrique s'applique à la fois au processeur de service et au contrôleur BMC.

ONTAP propose les méthodes suivantes pour gérer les mises à jour du firmware du processeur de service :

- La fonctionnalité de mise à jour automatique du processeur de service est activée par défaut, ce qui permet la mise à jour automatique du firmware du processeur de service dans les scénarios suivants :
  - Lorsque vous effectuez une mise à niveau vers une nouvelle version de ONTAP

Le processus de mise à niveau du ONTAP inclut automatiquement la mise à jour du firmware du processeur de service, à condition que la version du firmware du processeur de service fournie avec ONTAP soit plus récente que la version du processeur de service exécutée sur le nœud.



ONTAP détecte une mise à jour automatique du processeur de service défectueuse et déclenche une action corrective pour retry la mise à jour automatique du processeur de service jusqu'à trois fois. Si les trois tentatives échouent, consultez le lien de l'article de la base de connaissances : [Health Monitor SPAutoUpgradeFailedMajorAlert la mise à niveau du SP échoue - message AutoSupport](#).

- Lorsque vous téléchargez une version du firmware du processeur de service depuis le site de support NetApp et que la version téléchargée est plus récente que celle actuellement exécutée par le processeur de service
- Lorsque vous rétrogradez ou restaurez à une version antérieure de ONTAP

Le micrologiciel du processeur de service est automatiquement mis à jour vers la dernière version compatible prise en charge par la version ONTAP que vous avez rétablie ou rétrogradée. Une mise à jour manuelle du firmware du processeur de service n'est pas requise.

Vous pouvez désactiver la fonctionnalité de mise à jour automatique du processeur de service à l'aide de



`system service-processor image modify` commande. Toutefois, il est recommandé de ne pas activer cette fonctionnalité. La désactivation de cette fonctionnalité peut entraîner des combinaisons sous-optimales ou non qualifiées entre l'image ONTAP et l'image du firmware du processeur de service.

- ONTAP vous permet de déclencher manuellement une mise à jour du processeur de service et de spécifier comment la mise à jour doit avoir lieu à l'aide du `system service-processor image update` commande.

Vous pouvez spécifier les options suivantes :

- Le pack du firmware du processeur de service à utiliser (`-package`)

Vous pouvez mettre à jour le firmware du processeur de service sur un pack téléchargé en indiquant le nom du fichier d'image. L'avance `system image package show` La commande affiche tous les fichiers d'image (y compris les fichiers du pack du firmware du processeur de service) disponibles sur un nœud.

- Indique si vous souhaitez utiliser le pack du firmware du processeur de service de base pour la mise à jour du processeur de service (`-baseline`)

Vous pouvez mettre à jour le firmware du processeur de service vers la version de base fournie avec la version en cours d'exécution de ONTAP.



Si vous utilisez certaines des options ou paramètres de mise à jour les plus avancés, les paramètres de configuration du contrôleur BMC peuvent être temporairement effacés. Après le redémarrage, ONTAP peut restaurer la configuration du contrôleur BMC pendant 10 minutes.

- ONTAP vous permet d'afficher l'état de la dernière mise à jour du firmware du processeur de service déclenchée par ONTAP à l'aide de `system service-processor image update-progress show` commande.

Toute connexion existante au processeur de service est interrompue lors de la mise à jour du firmware du processeur de service. Voici si la mise à jour du firmware du processeur de service est automatique ou déclenchée manuellement.

#### Informations associées

["Téléchargements NetApp : firmware système et diagnostics"](#)

#### Lorsque le SP/BMC utilise l'interface réseau pour les mises à jour du micrologiciel

Une mise à jour du firmware du processeur de service déclenchée par ONTAP avec le processeur de service qui exécute les versions 1.5, 2.5, 3.1 ou ultérieures prend en charge l'utilisation d'un mécanisme de transfert de fichiers IP sur l'interface réseau du processeur de service.



Cette rubrique s'applique à la fois au processeur de service et au contrôleur BMC.

La mise à jour du firmware du processeur de service sur l'interface réseau est plus rapide qu'une mise à jour via l'interface série. Il réduit la fenêtre de maintenance pendant laquelle le firmware du processeur de service est mis à jour, et le fonctionnement de la ONTAP ne génère aucune interruption. Des versions du processeur de service qui prennent en charge cette fonctionnalité sont incluses avec ONTAP. Ils sont également

disponibles sur le site de support NetApp et peuvent être installés sur les contrôleurs qui exécutent une version compatible de ONTAP.

Lorsque vous exécutez SP version 1.5, 2.5, 3.1 ou ultérieure, les comportements de mise à niveau du micrologiciel suivants s'appliquent :

- Une mise à jour du firmware du processeur de service qui est *automatiquement* déclenchée par ONTAP par défaut par l'utilisation de l'interface réseau pour la mise à jour. Toutefois, le processeur de service passe à l'utilisation de l'interface série pour la mise à jour du firmware si l'une des conditions suivantes se produit :
  - L'interface réseau du processeur de service n'est pas configurée ou n'est pas disponible.
  - Le transfert de fichier IP échoue.
  - Le service API du processeur de service est désactivé.

Quelle que soit la version du processeur de service que vous exécutez, une mise à jour du firmware du processeur de service déclenchée par l'interface de ligne de commandes du processeur de service utilise toujours l'interface réseau du processeur de service pour la mise à jour.

### Informations associées

["Téléchargements NetApp : firmware système et diagnostics"](#)

### Comptes pouvant accéder au processeur de service

Lorsque vous tentez d'accéder au processeur de service, vous êtes invité à fournir des informations d'identification. Comptes utilisateurs du cluster créés avec le `service-processor` Le type d'application a accès à l'interface de ligne de commandes du processeur de service sur n'importe quel nœud du cluster. Les comptes utilisateurs du processeur de service sont gérés à partir de ONTAP et authentifiés par mot de passe. Depuis ONTAP 9.9.1, les comptes utilisateurs de SP doivent avoir le `admin` rôle.

Les comptes utilisateurs permettant d'accéder au processeur de service sont gérés à partir de ONTAP au lieu de l'interface de ligne de commandes du processeur de service. Un compte utilisateur du cluster peut accéder au processeur de service s'il est créé avec le `-application` paramètre du `security login create` commande définie sur `service-processor` et le `-authmethod` paramètre défini sur `password`. Le processeur de service prend uniquement en charge l'authentification par mot de passe.

Vous devez spécifier le `-role` Paramètre lors de la création d'un compte utilisateur du processeur de service.

- Dans ONTAP 9.9.1 et versions ultérieures, vous devez spécifier `admin` pour le `-role` et toute modification d'un compte nécessite le `admin` rôle. Les autres rôles ne sont plus autorisés pour des raisons de sécurité.
  - Si vous effectuez une mise à niveau vers ONTAP 9.9.1 ou une version ultérieure, reportez-vous à la section ["Modifier les comptes utilisateur pouvant accéder au Service Processor"](#).
  - Si vous rétablir ONTAP 9.8 ou des versions antérieures, consultez ["Vérifiez les comptes utilisateurs pouvant accéder au Service Processor"](#).
- Dans ONTAP 9.8 et les versions antérieures, tout rôle peut accéder au processeur de service, mais `admin` est recommandé.

Par défaut, le compte d'utilisateur du cluster nommé « admin » inclut le `service-processor` Le type d'application et a accès au processeur de service.

ONTAP vous empêche de créer des comptes utilisateur avec des noms réservés au système (tels que « root » et « naroot »). Vous ne pouvez pas utiliser un nom réservé système pour accéder au cluster ou au processeur de service.

Vous pouvez afficher les comptes utilisateurs actuels du processeur de service à l'aide de `-application service-processor` paramètre du `security login show` commande.

## Accéder au SP/BMC à partir d'un hôte d'administration

Vous pouvez vous connecter au processeur de service d'un nœud à partir d'un hôte d'administration pour effectuer des tâches de gestion des nœuds à distance.

### Ce dont vous avez besoin

Les conditions suivantes doivent être remplies :

- L'hôte d'administration que vous utilisez pour accéder au processeur de service doit prendre en charge SSHv2.
- Votre compte utilisateur doit déjà être configuré pour l'accès au processeur de service.

Pour accéder au processeur de service, votre compte utilisateur doit avoir été créé avec le `-application` paramètre du `security login create` commande définie sur `service-processor` et le `-authmethod` paramètre défini sur `password`.



Cette tâche s'applique à la fois au processeur de service et au contrôleur BMC.

Si le processeur de service est configuré pour utiliser une adresse IPv4 ou IPv6 et si cinq tentatives de connexion SSH d'un hôte échouent consécutivement en 10 minutes, le processeur de service rejette les demandes de connexion SSH et suspend la communication avec l'adresse IP de l'hôte pendant 15 minutes. La communication reprend au bout de 15 minutes, et vous pouvez essayer de vous reconnecter au processeur de service.

ONTAP vous empêche de créer ou d'utiliser des noms réservés au système (tels que « root » et « naroot ») pour accéder au cluster ou au processeur de service.

### Étapes

1. Depuis l'hôte d'administration, connectez-vous au processeur de service :

```
ssh username@SP_IP_address
```

2. Lorsque vous êtes invité, saisissez le mot de passe pour `username`.

L'invite du processeur de service apparaît, indiquant que vous avez accès à l'interface de ligne de commandes du processeur de service.

### Exemples d'accès au processeur de service à partir d'un hôte d'administration

L'exemple suivant montre comment vous connecter au processeur de service avec un compte utilisateur `joe`, Qui a été configuré pour accéder au processeur de service.

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

Les exemples suivants montrent comment utiliser l'adresse globale IPv6 ou l'adresse annoncée du routeur IPv6 pour vous connecter au processeur de service sur un nœud sur lequel SSH est configuré pour IPv6 et le processeur de service configuré pour IPv6.

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

## Accédez au processeur de service/BMC à partir de la console système

Vous pouvez accéder au processeur de service à partir de la console système (également appelée *console série*) pour effectuer des tâches de surveillance ou de dépannage.

### Description de la tâche

Cette tâche s'applique à la fois au processeur de service et au contrôleur BMC.

### Étapes

1. Accédez à l'interface de ligne de commandes du processeur de service à partir de la console système en appuyant sur Ctrl-G à l'invite de.
2. Connectez-vous à l'interface de ligne de commandes du processeur de service lorsque vous êtes invité.

L'invite du processeur de service apparaît, indiquant que vous avez accès à l'interface de ligne de commandes du processeur de service.

3. Quittez l'interface de ligne de commandes du processeur de service et revenez à la console du système en appuyant sur Ctrl-D, puis appuyez sur entrée.

### Exemple d'accès à l'interface de ligne de commandes du processeur de service à partir de la console système

L'exemple suivant montre le résultat d'une pression sur Ctrl-G depuis la console système pour accéder à l'interface de ligne de commandes du processeur de service. Le `help system power` La commande est entrée à l'invite du processeur de service, suivie d'une pression sur Ctrl-D, puis entrée pour revenir à la console du système.

```
cluster1::>
```

(Appuyez sur Ctrl-G pour accéder à l'interface de ligne de commandes du processeur de service.)

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

(Appuyez sur Ctrl-D, puis entrée pour revenir à la console du système.)

```
cluster1::>
```

### Relations entre l'interface de ligne de commandes du processeur de service, la console du processeur de service et les sessions de console système

Vous pouvez ouvrir une session de l'interface de ligne de commandes du processeur de service afin de gérer un nœud à distance et d'ouvrir une session de console distincte du processeur de service pour accéder à la console du nœud. La session de la console du processeur de service met en miroir les valeurs de sortie affichées dans une session de console système simultanée. Le processeur de service et la console du système disposent d'environnements shell indépendants avec une authentification de connexion indépendante.

La présentation de la façon dont les sessions de l'interface de ligne de commandes du processeur de service, de la console du processeur de service et de la console système sont associées permet de gérer un nœud à distance. Voici une description de la relation entre les sessions :

- Un seul administrateur peut se connecter à la session de l'interface de ligne de commandes du processeur de service à la fois. Toutefois, le processeur de service vous permet d'ouvrir simultanément une session de l'interface de ligne de commandes du processeur de service et une autre session de console du processeur de service.

L'interface de ligne de commandes du processeur de service est indiquée avec l'invite du processeur de service (SP>). Dans une session de l'interface de ligne de commandes du processeur de service, vous pouvez utiliser ce dernier `system console` Commande pour lancer une session de console du processeur de service. En même temps, vous pouvez démarrer une session de l'interface de ligne de commandes du processeur de service distincte via SSH. Si vous appuyez sur Ctrl-D pour quitter la session de console du processeur de service, vous revenez automatiquement à la session de l'interface de ligne de commandes du processeur de service. Si une session de l'interface de ligne de commandes du processeur de service existe déjà, un message vous demande si vous souhaitez mettre fin à la session de l'interface de ligne de commandes du processeur de service existante. Si vous saisissez « y », la session de l'interface de ligne de commandes du processeur de service existante est interrompue, ce qui vous permet de revenir de la console du processeur de service à l'interface de ligne de commandes du

processeur de service. Cette action est enregistrée dans le journal des événements du processeur de service.

Dans une session de l'interface de ligne de commandes ONTAP connectée via SSH, vous pouvez basculer sur la console système d'un nœud en exécutant `ONTAP system node run-console` commande provenant d'un autre nœud.

- Pour des raisons de sécurité, la session de l'interface de ligne de commandes du processeur de service et la session de console du système ont une authentification de connexion indépendante.

Lorsque vous lancez une session de console du processeur de service à partir de l'interface de ligne de commandes du processeur de service (en utilisant le processeur de service) `system console` commande), vous êtes invité à fournir les informations d'identification de la console du système. Lorsque vous accédez à l'interface de ligne de commandes du processeur de service à partir d'une session de console système (en appuyant sur Ctrl-G), vous êtes invité à fournir les informations d'identification de l'interface de ligne de commandes du processeur de service.

- La session de console du processeur de service et la session de console du système ont des environnements de shell indépendants.

La session de la console du processeur de service met en miroir les valeurs de sortie affichées dans une session de console simultanée du système. Cependant, la session de console simultanée du système ne met pas en miroir la session de console du processeur de service.

La session de la console du processeur de service ne met pas en miroir les valeurs de sortie des sessions SSH simultanées.

## Gérez les adresses IP pouvant accéder au processeur de service

Par défaut, le processeur de service accepte les requêtes de connexion SSH des hôtes d'administration de n'importe quelle adresse IP. Vous pouvez configurer le processeur de service pour qu'il accepte les requêtes de connexion SSH depuis uniquement les hôtes d'administration qui possèdent les adresses IP que vous spécifiez. Les modifications que vous apportez s'appliquent à l'accès SSH au processeur de service de n'importe quel nœud du cluster.

### Étapes

1. Accordez au processeur de service l'accès aux adresses IP que vous spécifiez via le `system service-processor ssh add-allowed-addresses` commande avec `-allowed-addresses` paramètre.

- La valeur du `-allowed-addresses` le paramètre doit être spécifié au format de `address/netmask`, et multiple `address/netmask` les paires doivent être séparées par des virgules, par exemple `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`.

Réglage du `-allowed-addresses` paramètre à `0.0.0.0/0, ::/0` Permet à toutes les adresses IP d'accéder au processeur de service (par défaut).

- Lorsque vous modifiez la valeur par défaut en limitant l'accès au SP aux adresses IP que vous spécifiez, ONTAP vous invite à confirmer que vous souhaitez que les adresses IP spécifiées remplacent le paramètre par défaut « Autoriser tous » (`0.0.0.0/0, ::/0`).
- Le `system service-processor ssh show` La commande affiche les adresses IP pouvant accéder au processeur de service.

2. Si vous souhaitez bloquer l'accès au processeur de service à une adresse IP spécifiée, utilisez le `system service-processor ssh remove-allowed-addresses` commande avec `-allowed-addresses` paramètre.

Si vous bloquez l'accès à toutes les adresses IP, le processeur de service devient inaccessible depuis n'importe quel hôte d'administration.

### Exemples de gestion des adresses IP pouvant accéder au processeur de service

Les exemples suivants montrent le paramètre par défaut pour l'accès SSH au processeur de service, modifiez la valeur par défaut en limitant l'accès du processeur de service aux adresses IP spécifiées, en supprimant les adresses IP spécifiées de la liste d'accès, puis en restaurant l'accès du processeur de service pour toutes les adresses IP :

```
cluster1::> system service-processor ssh show
Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
 with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
 addresses will be denied access. To restore the "allow all"
default,
 use the "system service-processor ssh add-allowed-addresses
 -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
 {y|n}: y

cluster1::> system service-processor ssh show
Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
Allowed Addresses: 0.0.0.0/0, ::/0
```

Utilisez l'aide en ligne de la CLI SP/BMC

L'aide en ligne affiche les commandes et options de la CLI du processeur de service/BMC.

Description de la tâche

Cette tâche s'applique à la fois au processeur de service et au contrôleur BMC.

Étapes

- 1. Pour afficher les informations d'aide pour les commandes SP/BMC, entrez les suivantes :

| Pour accéder à l'aide du processeur de service...           | Pour accéder à l'aide de BMC...          |
|-------------------------------------------------------------|------------------------------------------|
| Type <code>help</code> À l'invite du processeur de service. | Type <code>system</code> À l'invite BMC. |

L'exemple suivant montre l'aide en ligne de l'interface de ligne de commandes du processeur de service.

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

L'exemple suivant montre l'aide en ligne de BMC CLI.

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```



2. Pour afficher les informations d'aide relatives à l'option d'une commande SP/BMC, entrez `help` Avant ou après la commande SP/BMC.

L'exemple suivant montre l'aide en ligne de l'interface de ligne de commandes du processeur de service pour le processeur de service `events` commande.

```
SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events
```

L'exemple suivant montre l'aide en ligne de BMC CLI pour le BMC `system power` commande.

```
BMC> system power help
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status

BMC>
```

**Commandes permettant de gérer à distance un nœud**

Vous pouvez gérer un nœud à distance en accédant à son processeur de service et en exécutant des commandes de l'interface de ligne de commandes du processeur de service afin d'effectuer des tâches de gestion des nœuds. Dans le cas de plusieurs tâches courantes de gestion des nœuds à distance, vous pouvez également utiliser les commandes ONTAP d'un autre nœud du cluster. Certaines commandes du processeur de service sont spécifiques à la plateforme et peuvent ne pas être disponibles sur votre plateforme.


| Les fonctions que vous recherchez...                                                                     | Utilisez cette commande du processeur de service... | Utilisez cette commande BMC... | Ou cette commande ONTAP ... |
|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------|--------------------------------|-----------------------------|
| Affiche les commandes ou sous-commandes du processeur de service disponibles d'une commande SP spécifiée | help [command]                                      |                                |                             |


| Les fonctions que vous recherchez...                                                                                                                                                                                  | Utilisez cette commande du processeur de service... | Utilisez cette commande BMC...                                                                                                                                                                                        | Ou cette commande ONTAP ...                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| Affiche le niveau de privilège actuel pour l'interface de ligne de commandes du processeur de service                                                                                                                 | <code>priv show</code>                              |                                                                                                                                                                                                                       |                                            |
| Définissez le niveau de privilège pour accéder au mode spécifié pour l'interface de ligne de commandes du processeur de service                                                                                       | <code>priv set {admin</code>                        | <code>advanced</code>                                                                                                                                                                                                 | <code>diag}</code>                         |
|                                                                                                                                                                                                                       |                                                     | Afficher la date et l'heure du système                                                                                                                                                                                | <code>date</code>                          |
|                                                                                                                                                                                                                       | <code>date</code>                                   | Affiche les événements consignés par le processeur de service                                                                                                                                                         | <code>events {all</code>                   |
| <code>info</code>                                                                                                                                                                                                     | <code>newest number</code>                          | <code>oldest number</code>                                                                                                                                                                                            | <code>search keyword}</code>               |
|                                                                                                                                                                                                                       |                                                     | Affiche l'état du processeur de service et les informations de configuration réseau                                                                                                                                   | <code>sp status [-v</code>                 |
| <code>-d]</code><br>Le <code>-v</code> Option affiche les statistiques du processeur de service sous forme détaillée. Le <code>-d</code> Option ajoute le journal de débogage du processeur de service à l'affichage. | <code>bmc status [-v</code>                         | <code>-d]</code><br>Le <code>-v</code> Option affiche les statistiques du processeur de service sous forme détaillée. Le <code>-d</code> Option ajoute le journal de débogage du processeur de service à l'affichage. | <code>system service-processor show</code> |
| Affiche la durée de mise en service du processeur de service et le nombre moyen de tâches de la file d'attente d'exécution au cours des 1, 5 et 15 dernières minutes                                                  | <code>sp uptime</code>                              | <code>bmc uptime</code>                                                                                                                                                                                               |                                            |
| Affiche les journaux de la console du système                                                                                                                                                                         | <code>system log</code>                             |                                                                                                                                                                                                                       |                                            |

| Les fonctions que vous recherchez...                                                   | Utilisez cette commande du processeur de service... | Utilisez cette commande BMC...                                            | Ou cette commande ONTAP ...                                                                       |
|----------------------------------------------------------------------------------------|-----------------------------------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Affiche les archives du journal du processeur de service ou les fichiers d'une archive | sp log history show [-archive {latest               | {all                                                                      | archive-name}}] [-dump {all                                                                       |
| file-name}}                                                                            | bmc log history show [-archive {latest              | {all                                                                      | archive-name}}] [-dump {all                                                                       |
| file-name}}                                                                            |                                                     | Affiche l'état de mise sous tension du contrôleur d'un nœud               | system power status                                                                               |
|                                                                                        | system node power show                              | Afficher les informations sur la batterie                                 | system battery show                                                                               |
|                                                                                        |                                                     | Affiche les informations ACP ou l'état des capteurs du module d'extension | system acp [show                                                                                  |
| sensors show]                                                                          |                                                     |                                                                           | Répertorier toutes les unités remplaçables sur site et leurs ID                                   |
| system fru list                                                                        |                                                     |                                                                           | Affiche les informations produit pour l'unité remplaçable sur site spécifiée                      |
| system fru show fru_id                                                                 |                                                     |                                                                           | Affiche le journal d'historique des données FRU                                                   |
| system fru log show (niveau de privilège avancé)                                       |                                                     |                                                                           | Affiche le statut des capteurs environnementaux, y compris leurs États et leurs valeurs actuelles |
| system sensors ou system sensors show                                                  |                                                     | system node environment sensors show                                      | Affiche l'état et les détails du capteur spécifié                                                 |

| Les fonctions que vous recherchez...                                                                                                                                                     | Utilisez cette commande du processeur de service...        | Utilisez cette commande BMC...                   | Ou cette commande ONTAP ...                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>system sensors get sensor_name</code><br><br>Vous pouvez obtenir <code>sensor_name</code> à l'aide du <code>system sensors</code> ou le <code>system sensors show</code> commande. |                                                            |                                                  | Affiche les informations de version du firmware du processeur de service                                                                                                                                                                                                                     |
| <code>version</code>                                                                                                                                                                     |                                                            | <code>system service-processor image show</code> | Affiche l'historique des commandes du processeur de service                                                                                                                                                                                                                                  |
| <code>sp log audit</code> (niveau de privilège avancé)                                                                                                                                   | <code>bmc log audit</code>                                 |                                                  | Affiche les informations de débogage du processeur de service                                                                                                                                                                                                                                |
| <code>sp log debug</code> (niveau de privilège avancé)                                                                                                                                   | <code>bmc log debug</code> (niveau de privilège avancé)    |                                                  | Affiche le fichier des messages du processeur de service                                                                                                                                                                                                                                     |
| <code>sp log messages</code> (niveau de privilège avancé)                                                                                                                                | <code>bmc log messages</code> (niveau de privilège avancé) |                                                  | Affiche les paramètres de collecte d'analyses système lors d'un événement de réinitialisation de la surveillance, affiche les informations d'analyse système recueillies lors d'un événement de réinitialisation de la surveillance ou efface les informations d'analyse système recueillies |
| <code>system forensics [show</code>                                                                                                                                                      | <code>log dump</code>                                      | <code>log clear]</code>                          |                                                                                                                                                                                                                                                                                              |
|                                                                                                                                                                                          | Connectez-vous à la console du système                     | <code>system console</code>                      |                                                                                                                                                                                                                                                                                              |

| Les fonctions que vous recherchez... | Utilisez cette commande du processeur de service...                          | Utilisez cette commande BMC...                                                                                                       | Ou cette commande ONTAP ... |
|--------------------------------------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| system node run-console              | Vous devez appuyer sur Ctrl-D pour quitter la session de console du système. | Mise sous tension ou hors tension du nœud, ou réalisation d'une mise hors/sous tension (mise hors tension, puis remise sous tension) | system power on             |
|                                      | system node power on (niveau de privilège avancé)                            | system power off                                                                                                                     |                             |
|                                      | system power cycle                                                           |                                                                                                                                      |                             |

| Les fonctions que vous recherchez...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Utilisez cette commande du processeur de service...    | Utilisez cette commande BMC...                                                                                                             | Ou cette commande ONTAP ... |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| <p>L'alimentation de veille reste allumée pour maintenir le processeur de service en fonctionnement sans interruption. Pendant la mise hors/sous tension, une brève pause se produit avant de remettre l'alimentation en marche.</p> <div data-bbox="167 1014 220 1066">  </div> <p>À l'aide de ces commandes, la mise hors/sous tension du nœud peut provoquer un arrêt incorrect du nœud (également appelé <i>shutdown</i>) et ne remplace pas un arrêt normal à l'aide de ONTAP <code>system node halt</code> commande.</p> | <p>Créer un « core dump » et réinitialiser le nœud</p> | <p><code>system core [-f]</code></p> <p>Le <code>-f</code> option force la création d'un « core dump » et la réinitialisation du nœud.</p> |                             |

| Les fonctions que vous recherchez...                                        | Utilisez cette commande du processeur de service...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Utilisez cette commande BMC...                                                                                                                                                                                                                                                                                                                                                                   | Ou cette commande ONTAP ...                                                                                                                                                                |
|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>system node<br/>coredump trigger</p> <p>(niveau de privilège avancé)</p> | <p>Ces commandes ont le même effet que d'appuyer sur le bouton non masquable Interrupt (NMI) d'un nœud, provoquant un arrêt non planifié du nœud et forçant un vidage des fichiers core lors de l'arrêt du nœud. Ces commandes sont utiles lorsque ONTAP sur le nœud est arrêté ou ne répond pas aux commandes telles que system node shutdown. Les fichiers core dump générés sont affichés dans la sortie du system node coredump show commande. Le processeur de service reste opérationnel tant que l'alimentation en entrée du nœud n'est pas interrompue.</p> | <p>Redémarrez le nœud à l'aide d'une image du micrologiciel du BIOS (primaire, de sauvegarde ou de courant) spécifiée en option pour effectuer une restauration suite à des problèmes tels qu'une image corrompue du périphérique d'amorçage du nœud</p>                                                                                                                                         | <p>system reset<br/>{primary}</p>                                                                                                                                                          |
| <p>backup</p>                                                               | <p>current}</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                  | <p>system node reset<br/>avec le -firmware<br/>{primary}</p>                                                                                                                               |
| <p>backup</p>                                                               | <p>current} paramètre<br/>(niveau de privilège avancé)</p> <p>system node reset</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <div>  <p>Cette opération provoque un arrêt non planifié du nœud.</p> </div> <p>Si aucune image du micrologiciel du BIOS n'est spécifiée, l'image actuelle est utilisée pour le redémarrage. Le processeur de service reste opérationnel tant que l'alimentation en entrée du nœud n'est pas interrompue.</p> | <p>Affiche l'état de la mise à jour automatique du firmware des batteries ou active ou désactive la mise à jour automatique du firmware des batteries lors du prochain démarrage du SP</p> |

| Les fonctions que vous recherchez...     | Utilisez cette commande du processeur de service...                                              | Utilisez cette commande BMC...                                                                                                                                                                                              | Ou cette commande ONTAP ...                                               |
|------------------------------------------|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| system battery<br>auto_update [status]   | enable                                                                                           | disable]<br><br>(niveau de privilège avancé)                                                                                                                                                                                |                                                                           |
|                                          | Comparez l'image actuelle du micrologiciel de la batterie à une image de micrologiciel spécifiée | system battery<br>verify [image_URL]<br><br>(niveau de privilège avancé)<br><br>Si image_URL n'est pas spécifié, l'image du micrologiciel de la batterie par défaut est utilisée pour la comparaison.                       |                                                                           |
|                                          | Mettez à jour le micrologiciel de la batterie à partir de l'image à l'emplacement spécifié       | system battery<br>flash image_URL<br><br>(niveau de privilège avancé)<br><br>Vous utilisez cette commande si le processus de mise à niveau automatique du micrologiciel de la batterie a échoué pour une raison quelconque. |                                                                           |
|                                          | Mettez à jour le firmware du processeur de service en utilisant l'image à l'emplacement spécifié | sp update image_URL<br>image_URL il ne doit pas dépasser 200 caractères.                                                                                                                                                    | bmc update image_URL<br>image_URL il ne doit pas dépasser 200 caractères. |
| system service-processor image<br>update | Redémarre le processeur de service                                                               | sp reboot                                                                                                                                                                                                                   |                                                                           |



| Les fonctions que vous recherchez...            | Utilisez cette commande du processeur de service...                | Utilisez cette commande BMC...                                                                                                                                                               | Ou cette commande ONTAP ... |
|-------------------------------------------------|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| <code>system service-processor reboot-sp</code> | Effacez le contenu Flash de la mémoire NVRAM                       | <code>system nvram flash clear</code> (niveau de privilège avancé)<br><br>Cette commande ne peut pas être démarrée lorsque le contrôleur est hors tension ( <code>system power off</code> ). |                             |
|                                                 | Quittez l'interface de ligne de commandes du processeur de service | <code>exit</code>                                                                                                                                                                            |                             |

### À propos des mesures du capteur du processeur de service à seuil et des valeurs d'état du résultat de la commande des capteurs du système

Les capteurs à seuils prélèvent des mesures périodiques des différents composants du système. Le processeur de service compare la mesure d'un capteur à seuil par rapport aux limites de seuil prédéfinies qui définissent les conditions de fonctionnement acceptables d'un composant.

En fonction de la mesure du capteur, le processeur de service affiche l'état du capteur pour vous aider à contrôler l'état du composant.

Les capteurs de température, de tension, de courant et de vitesse des ventilateurs du système sont des exemples de capteurs à seuils. La liste spécifique des capteurs à seuils dépend de la plateforme.

Les seuils des capteurs à seuils sont les suivants, affichés dans le résultat du processeur de service `system sensors` commande :

- Valeur critique inférieure (LCR)
- Valeur non critique inférieure (LNC)
- Valeur non critique supérieure (UNC)
- Valeur critique supérieure (UCR)

Une mesure de capteur entre LNC et LCR ou entre UNC et UCR indique des signes d'un problème et une panne du système. Par conséquent, vous devez prévoir rapidement un entretien du composant.

Une mesure de capteur inférieure à LCR ou supérieure à UCR indique un dysfonctionnement du composant et une panne imminente du système. Le composant requiert donc une intervention immédiate.

Le schéma suivant illustre les plages de gravité spécifiées par les seuils :



La mesure d'un capteur à seuil se trouve sous le `Current` dans le `system sensors` sortie de la commande. Le `system sensors get sensor_name` la commande affiche des détails supplémentaires pour le capteur spécifié. Lorsque la mesure d'un capteur à seuil franchit les plages de seuils non critique et critique, le capteur signale un problème d'augmentation de la gravité. Lorsque la mesure dépasse une limite de seuil, l'état du capteur dans le `system sensors` la sortie de la commande change de `ok` à `nc` (non critique) ou `cr` (Critique) selon le seuil dépassé et un message d'événement est enregistré dans le journal des événements du journal des événements du système.

Certains capteurs à seuils ne possèdent pas les quatre niveaux de seuil. Les seuils manquants indiquent concernant ces capteurs `na` comme leurs limites dans le `system sensors` Le résultat de la commande, indiquant que le capteur particulier n'a aucune limite ou problème de gravité pour le seuil donné, et que le processeur de service ne surveille pas le capteur pour ce seuil.

### Exemple de sortie de la commande System Sensors

L'exemple suivant montre certaines des informations affichées par `system sensors` Commande dans l'interface de ligne de commandes du processeur de service :

```
SP node1> system sensors
```

| Sensor Name                    | Current | Unit      | Status | LCR   | LNC    |
|--------------------------------|---------|-----------|--------|-------|--------|
| UNC                            | UCR     |           |        |       |        |
| -----+-----+-----+-----+-----+ |         |           |        |       |        |
| -----+-----+-----+             |         |           |        |       |        |
| CPU0_Temp_Margin               | -55.000 | degrees C | ok     | na    | na     |
| -5.000                         | 0.000   |           |        |       |        |
| CPU1_Temp_Margin               | -56.000 | degrees C | ok     | na    | na     |
| -5.000                         | 0.000   |           |        |       |        |
| In_Flow_Temp                   | 32.000  | degrees C | ok     | 0.000 | 10.000 |
| 42.000                         | 52.000  |           |        |       |        |
| Out_Flow_Temp                  | 38.000  | degrees C | ok     | 0.000 | 10.000 |
| 59.000                         | 68.000  |           |        |       |        |
| CPU1_Error                     | 0x0     | discrete  | 0x0180 | na    | na     |
| na                             | na      |           |        |       |        |
| CPU1_Therm_Trip                | 0x0     | discrete  | 0x0180 | na    | na     |
| na                             | na      |           |        |       |        |
| CPU1_Hot                       | 0x0     | discrete  | 0x0180 | na    | na     |
| na                             | na      |           |        |       |        |
| IO_Mid1_Temp                   | 30.000  | degrees C | ok     | 0.000 | 10.000 |
| 55.000                         | 64.000  |           |        |       |        |
| IO_Mid2_Temp                   | 30.000  | degrees C | ok     | 0.000 | 10.000 |
| 55.000                         | 64.000  |           |        |       |        |
| CPU_VTT                        | 1.106   | Volts     | ok     | 1.028 | 1.048  |
| 1.154                          | 1.174   |           |        |       |        |
| CPU0_VCC                       | 1.154   | Volts     | ok     | 0.834 | 0.844  |
| 1.348                          | 1.368   |           |        |       |        |
| 3.3V                           | 3.323   | Volts     | ok     | 3.053 | 3.116  |
| 3.466                          | 3.546   |           |        |       |        |
| 5V                             | 5.002   | Volts     | ok     | 4.368 | 4.465  |
| 5.490                          | 5.636   |           |        |       |        |
| STBY_1.8V                      | 1.794   | Volts     | ok     | 1.678 | 1.707  |
| 1.892                          | 1.911   |           |        |       |        |
| ...                            |         |           |        |       |        |

### Exemple de sortie de la commande `sensor_name` des capteurs système pour un capteur à seuils

L'exemple suivant montre le résultat de la saisie `system sensors get sensor_name` Dans l'interface de ligne de commandes du processeur de service pour le capteur à seuil 5V :

```

SP node1> system sensors get 5V

Locating sensor record...
Sensor ID : 5V (0x13)
Entity ID : 7.97
Sensor Type (Analog) : Voltage
Sensor Reading : 5.002 (+/- 0) Volts
Status : ok
Lower Non-Recoverable : na
Lower Critical : 4.246
Lower Non-Critical : 4.490
Upper Non-Critical : 5.490
Upper Critical : 5.758
Upper Non-Recoverable : na
Assertion Events :
Assertions Enabled : lnc- lcr- ucr+
Deassertions Enabled : lnc- lcr- ucr+

```

### Informations sur les valeurs d'état du capteur SP discrètes du résultat de la commande des capteurs du système

Les capteurs discrets ne possèdent pas de seuils. Leurs relevés, affichés sous le `Current` Dans l'interface de ligne de commandes du processeur de service `system sensors` La sortie de la commande, ne portent pas de significations réelles et sont ainsi ignorées par le processeur de service. Le `Status` dans le `system sensors` le résultat de la commande affiche les valeurs d'état des capteurs discrets au format hexadécimal.

Les capteurs de panne des ventilateurs, des unités d'alimentation et du système sont des exemple de capteurs discrets. La liste spécifique des capteurs discrets dépend de la plateforme.

Vous pouvez utiliser l'interface de ligne de commandes du processeur de service `system sensors get sensor_name` commande d'aide à l'interprétation des valeurs d'état de la plupart des capteurs discrets. Les exemples suivants montrent les résultats de la saisie `system sensors get sensor_name` Pour les capteurs discrets `CPU0_Error` et `IO_Slot1_PRESENT` :

```

SP node1> system sensors get CPU0_Error

Locating sensor record...
Sensor ID : CPU0_Error (0x67)
Entity ID : 7.97
Sensor Type (Discrete): Temperature
States Asserted : Digital State
 [State Deasserted]

```

```

SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID : IO_Slot1_Present (0x74)
Entity ID : 11.97
Sensor Type (Discrete): Add-in Card
States Asserted : Availability State
 [Device Present]

```

Bien que le `system sensors get sensor_name` La commande affiche les informations d'état de la plupart des capteurs discrets ; elle ne fournit pas d'informations d'état pour les capteurs discrets `System_FW_Status`, `System_Watchdog`, `PSU1_Input_Type` et `PSU2_Input_Type`. Vous pouvez utiliser les informations suivantes pour interpréter les valeurs d'état de ces capteurs.

### System\_FW\_Status

L'état du capteur `System_FW_Status` s'affiche sous la forme de `0xAABB`. Vous pouvez combiner les informations de `AA` et `BB` pour déterminer l'état du capteur.

`AA` peut avoir l'une des valeurs suivantes :

| Valeurs | État du capteur                    |
|---------|------------------------------------|
| 01      | Erreur du firmware du système      |
| 02      | Blocage du firmware du système     |
| 04      | Progression du firmware du système |

`BB` peut avoir l'une des valeurs suivantes :

| Valeurs | État du capteur                                                                                      |
|---------|------------------------------------------------------------------------------------------------------|
| 00      | Le logiciel système s'est arrêté correctement                                                        |
| 01      | Initialisation de la mémoire en cours                                                                |
| 02      | Initialisation de la NVMEM en cours (lorsque la mémoire NVMEM est présente)                          |
| 04      | Restauration des valeurs du concentrateur du contrôleur de mémoire (MCH) (lorsque NVMEM est présent) |
| 05      | L'utilisateur a accédé à la configuration                                                            |

| Valeurs | État du capteur                                                                                        |
|---------|--------------------------------------------------------------------------------------------------------|
| 13      | Démarrage du système d'exploitation ou DU CHARGEUR                                                     |
| 1F      | Le BIOS est en cours de démarrage                                                                      |
| 20      | LE CHARGEUR est en cours d'exécution                                                                   |
| 21      | LE CHARGEUR programme le firmware du BIOS principal. Vous ne devez pas mettre le système hors tension. |
| 22      | LE CHARGEUR programme l'autre firmware du BIOS. Vous ne devez pas mettre le système hors tension.      |
| 2E      | ONTAP est en cours d'exécution                                                                         |
| 60      | Le processeur de service est hors tension du système                                                   |
| 61      | Le processeur de service est mis sous tension sur le système                                           |
| 62      | Le processeur de service a réinitialisé le système                                                     |
| 63      | Cycle d'alimentation du chien de garde du processeur de service                                        |
| 64      | Réinitialisation à froid du processeur de service                                                      |

Par exemple, l'état du capteur System\_FW\_Status 0x042F signifie « progression du micrologiciel du système (04), ONTAP est en cours d'exécution (2F) ».

#### Surveillance\_système

Le capteur System\_Watchdog peut avoir l'une des conditions suivantes :

- **0x0080**

L'état de ce capteur n'a pas changé

| Valeurs | État du capteur               |
|---------|-------------------------------|
| 0x0081  | Interruption du temporisateur |
| 0x0180  | Temporisation expirée         |

| Valeurs | État du capteur             |
|---------|-----------------------------|
| 0x0280  | Réinitialisation matérielle |
| 0x0480  | Hors tension                |
| 0x0880  | Cycle d'alimentation        |

Par exemple, l'état 0x0880 du capteur System\_Watchdog indique qu'un délai de surveillance est expiré et provoque un cycle d'alimentation du système.

#### PSU1\_Input\_Type et PSU2\_Input\_Type

Pour les alimentations à courant continu (CC), les capteurs PSU1\_Input\_Type et PSU2\_Input\_Type ne s'appliquent pas. Pour les alimentations à courant alternatif (CA), l'état des capteurs peut avoir l'une des valeurs suivantes :

| Valeurs | État du capteur           |
|---------|---------------------------|
| 0x01 xx | Type d'alimentation 220 V |
| 0x02 xx | Type d'alimentation 110 V |

Par exemple, l'état du capteur PSU1\_Input\_Type 0x0280 indique que le capteur indique que le type d'alimentation est 110 V.

#### Commandes de gestion du processeur de service à partir de ONTAP

ONTAP fournit des commandes de gestion du processeur de service, y compris la configuration réseau du processeur de service, l'image du firmware du processeur de service, l'accès SSH au processeur de service et l'administration générale du processeur de service.

#### Commandes permettant de gérer la configuration réseau du processeur de service

| Les fonctions que vous recherchez...                                                                                                                                  | Exécuter cette commande ONTAP...                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Activez la configuration réseau automatique du processeur de service pour que ce dernier utilise la famille d'adresse IPv4 ou IPv6 du sous-réseau spécifié            | <code>system service-processor network auto-configuration enable</code>  |
| Désactivez la configuration réseau automatique du processeur de service pour la famille d'adresses IPv4 ou IPv6 du sous-réseau spécifié pour le processeur de service | <code>system service-processor network auto-configuration disable</code> |
| Affiche la configuration réseau automatique du processeur de service                                                                                                  | <code>system service-processor network auto-configuration show</code>    |


| Les fonctions que vous recherchez...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Exécuter cette commande ONTAP...                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Configurez manuellement le réseau du processeur de service d'un nœud, y compris les éléments suivants :</p> <ul style="list-style-type: none"> <li>• La famille d'adresses IP (IPv4 ou IPv6)</li> <li>• Indique si l'interface réseau de la famille d'adresses IP spécifiée doit être activée</li> <li>• Si vous utilisez IPv4, que vous utilisiez la configuration réseau depuis le serveur DHCP ou l'adresse réseau que vous spécifiez</li> <li>• Adresse IP publique du processeur de service</li> <li>• Le masque de réseau du processeur de service (si vous utilisez IPv4)</li> <li>• Longueur du préfixe réseau du masque de sous-réseau pour le processeur de service (en cas d'utilisation d'IPv6)</li> <li>• Adresse IP de la passerelle pour le processeur de service</li> </ul>                                                                                                                                                                                                                                                        | <p><code>system service-processor network modify</code></p>                                                                                                                         |
| <p>Affichage de la configuration réseau du processeur de service, y compris les éléments suivants :</p> <ul style="list-style-type: none"> <li>• La famille d'adresses configurée (IPv4 ou IPv6) et si elle est activée ou non</li> <li>• Type de périphérique de gestion à distance</li> <li>• État actuel du processeur de service et état de la liaison</li> <li>• Configuration du réseau, comme l'adresse IP, l'adresse MAC, le masque de réseau, la longueur du préfixe du masque de sous-réseau, l'adresse IP attribuée par le routeur, l'adresse IP locale de liaison et l'adresse IP de la passerelle</li> <li>• Heure à laquelle le processeur de service a été mis à jour pour la dernière fois</li> <li>• Nom du sous-réseau utilisé pour la configuration automatique du processeur de service</li> <li>• Indique si l'adresse IP attribuée par le routeur IPv6 est activée</li> <li>• État de configuration du réseau du processeur de service</li> <li>• Raison de l'échec de configuration réseau du processeur de service</li> </ul> | <p><code>system service-processor network show</code></p> <p>L'affichage des détails complets du réseau du processeur de service nécessite le <code>-instance</code> paramètre.</p> |



| Les fonctions que vous recherchez...                                                                                                                                                                                                                                                                | Exécuter cette commande ONTAP...                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Modifiez la configuration du service API du processeur de service, notamment :</p> <ul style="list-style-type: none"> <li>• Modification du port utilisé par le service d'API du processeur de service</li> <li>• Activation ou désactivation du service API du processeur de service</li> </ul> | <pre>system service-processor api-service modify</pre> <p>(niveau de privilège avancé)</p>                                                                                                                                                                                                                                      |
| <p>Affiche la configuration du service API du processeur de service</p>                                                                                                                                                                                                                             | <pre>system service-processor api-service show</pre> <p>(niveau de privilège avancé)</p>                                                                                                                                                                                                                                        |
| <p>Renouvelez les certificats SSL et SSH utilisés par le service API SP pour les communications internes</p>                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• Pour ONTAP 9.5 ou version ultérieure : <pre>system service-processor api-service renew-internal-certificates</pre></li> <li>• Pour ONTAP 9.4 ou version antérieure : <pre>system service-processor api-service renew-certificates</pre></li> </ul> <p>(niveau de privilège avancé)</p> |

#### Commandes permettant de gérer l'image du firmware du processeur de service

| Les fonctions que vous recherchez...                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Exécuter cette commande ONTAP...                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Afficher les détails de l'image du firmware du processeur de service actuellement installée, y compris les éléments suivants :</p> <ul style="list-style-type: none"> <li>• Type de périphérique de gestion à distance</li> <li>• Image (principale ou de sauvegarde) à partir de laquelle le processeur de service démarre, son état et la version du firmware</li> <li>• Indique si la mise à jour automatique du micrologiciel est activée et que l'état de la dernière mise à jour est activé</li> </ul> | <pre>system service-processor image show</pre> <p>Le <code>-is-current</code> Paramètre indique l'image (principale ou de sauvegarde) à partir de laquelle le processeur de service est actuellement démarré, pas si la version du firmware installée est la plus récente.</p> |

| Les fonctions que vous recherchez...                                                                                                                                                                                                                                                                                                                                             | Exécuter cette commande ONTAP...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Activez ou désactivez la mise à jour automatique du firmware du processeur de service                                                                                                                                                                                                                                                                                            | <pre>system service-processor image modify</pre> <p>Par défaut, le firmware du processeur de service est automatiquement mis à jour avec la mise à jour du ONTAP ou lorsqu'une nouvelle version du firmware du processeur de service est téléchargée manuellement. La désactivation de la mise à jour automatique n'est pas recommandée, car cela peut entraîner des combinaisons sous-optimales ou non qualifiées entre l'image ONTAP et l'image du firmware du processeur de service.</p>                                                                                                                                                              |
| Téléchargez manuellement une image du firmware du processeur de service sur un nœud                                                                                                                                                                                                                                                                                              | <pre>system node image get</pre> <div>  <p>Avant d'exécuter le <code>system node image</code> commandes, vous devez définir le niveau de privilège sur avancé (<code>set -privilege advanced</code>), saisissez <b>y</b> lorsque vous êtes invité à continuer.</p> </div> <p>L'image du firmware du processeur de service est fournie avec ONTAP. Vous n'avez pas besoin de télécharger manuellement le firmware du processeur de service, sauf si vous souhaitez utiliser une version du firmware du processeur de service différente de celle fournie avec ONTAP.</p> |
| <p>Affichez le statut de la dernière mise à jour du firmware du processeur de service déclenchée par ONTAP, y compris les informations suivantes :</p> <ul style="list-style-type: none"> <li>• Heure de début et de fin de la dernière mise à jour du firmware du processeur de service</li> <li>• Indique si une mise à jour est en cours et le pourcentage terminé</li> </ul> | <pre>system service-processor image update-progress show</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

#### Commandes permettant de gérer l'accès SSH au processeur de service

| Les fonctions que vous recherchez...                                  | Exécuter cette commande ONTAP...                                 |
|-----------------------------------------------------------------------|------------------------------------------------------------------|
| Accordez au SP un accès uniquement aux adresses IP spécifiées         | <pre>system service-processor ssh add-allowed-addresses</pre>    |
| Bloc les adresses IP spécifiées pour l'accès au processeur de service | <pre>system service-processor ssh remove-allowed-addresses</pre> |

| Les fonctions que vous recherchez...                             | Exécuter cette commande ONTAP...               |
|------------------------------------------------------------------|------------------------------------------------|
| Affiche les adresses IP pouvant accéder au processeur de service | <code>system service-processor ssh show</code> |

#### Commandes d'administration générale du processeur de service

| Les fonctions que vous recherchez...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Exécuter cette commande ONTAP...                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Affichage des informations générales sur le processeur de service, notamment :</p> <ul style="list-style-type: none"> <li>• Type de périphérique de gestion à distance</li> <li>• État actuel du processeur de service</li> <li>• Indique si le réseau du processeur de service est configuré ou non</li> <li>• Informations sur le réseau, telles que l'adresse IP publique et l'adresse MAC</li> <li>• Version du firmware du processeur de service et version de l'interface IPMI (Intelligent Platform Management interface)</li> <li>• Indique si la mise à jour automatique du firmware du processeur de service est activée</li> </ul> | <p><code>system service-processor show</code> L'affichage des informations complètes du processeur de service nécessite le <code>-instance</code> paramètre.</p> |
| Redémarre le processeur de service sur un nœud                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <code>system service-processor reboot-sp</code>                                                                                                                  |
| Générez et envoyez un message AutoSupport qui inclut les fichiers journaux du processeur de service collectés à partir d'un nœud spécifié                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <code>system node autosupport invoke-splog</code>                                                                                                                |
| Affiche la carte d'allocation des fichiers journaux du processeur de service collectés dans le cluster, y compris les numéros de séquence des fichiers journaux du processeur de service qui résident dans chaque nœud de collecte                                                                                                                                                                                                                                                                                                                                                                                                               | <code>system service-processor log show-allocations</code>                                                                                                       |

#### Informations associées

["Référence de commande ONTAP"](#)

#### Commandes ONTAP pour la gestion BMC

Ces commandes ONTAP sont prises en charge sur le contrôleur BMC (Baseboard Management Controller).

Le BMC utilise certaines des mêmes commandes que le processeur de service. Les commandes suivantes du processeur de service sont prises en charge sur le contrôleur BMC.

| Les fonctions que vous recherchez...                                                                                                | Utilisez cette commande                                            |
|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Affiche les informations BMC                                                                                                        | <b>system service-processor show</b>                               |
| Afficher/modifier la configuration réseau du BMC                                                                                    | <b>system service-processor network show/modify</b>                |
| Réinitialisez le contrôleur BMC                                                                                                     | <b>system service-processor reboot-sp</b>                          |
| Affiche/modifie les détails de l'image du micrologiciel BMC actuellement installée                                                  | <b>system service-processor image show/modify</b>                  |
| Mettre à jour le micrologiciel du contrôleur BMC                                                                                    | <b>system service-processor image update</b>                       |
| Affiche l'état de la dernière mise à jour du micrologiciel du contrôleur BMC                                                        | <b>system service-processor image update-progress show</b>         |
| Activez la configuration réseau automatique pour que le contrôleur BMC utilise une adresse IPv4 ou IPv6 sur le sous-réseau spécifié | <b>system service-processor network auto-configuration enable</b>  |
| Désactivez la configuration réseau automatique pour une adresse IPv4 ou IPv6 sur le sous-réseau spécifié pour le contrôleur BMC     | <b>system service-processor network auto-configuration disable</b> |
| Afficher la configuration réseau automatique du contrôleur BMC                                                                      | <b>system service-processor network auto-configuration show</b>    |

Pour les commandes qui ne sont pas prises en charge par le micrologiciel du contrôleur BMC, le message d'erreur suivant est renvoyé.

```
::> Error: Command not supported on this platform.
```

## Commandes BMC CLI

Vous pouvez vous connecter au contrôleur BMC à l'aide de SSH. Les commandes suivantes sont prises en charge à partir de la ligne de commande BMC.

| Commande        | Fonction                                                                                          |
|-----------------|---------------------------------------------------------------------------------------------------|
| systeme         | Affiche la liste de toutes les commandes.                                                         |
| console systeme | Effectue la connexion à la console du système.<br>Utiliser <b>Ctrl+D</b> pour quitter la session. |

| Commande                              | Fonction                                                                     |
|---------------------------------------|------------------------------------------------------------------------------|
| cœur du système                       | Vide le « core » du système et effectue une réinitialisation.                |
| cycle de mise sous tension du système | Mettez le système hors tension, puis sous tension.                           |
| le système est hors tension           | Mettez le système hors tension.                                              |
| le système est sous tension           | Mettez le système sous tension.                                              |
| état de l'alimentation du système     | État de l'alimentation du système d'impression.                              |
| réinitialisation du système           | Réinitialisez le système.                                                    |
| journal système                       | Imprimer les journaux de la console du système                               |
| affichage des fru du système [id]     | Vidage des informations sur l'unité remplaçable sur site (FRU) sélectionnée. |

## Gestion de l'heure du cluster (administrateurs du cluster uniquement)

Les problèmes peuvent survenir lorsque l'heure du cluster est incorrecte. Bien que ONTAP vous permet de définir manuellement le fuseau horaire, la date et l'heure sur le cluster, vous devez configurer les serveurs NTP (Network Time Protocol) pour synchroniser l'heure du cluster.

Depuis ONTAP 9.5, vous pouvez configurer votre serveur NTP avec une authentification symétrique.

NTP est toujours activé. Toutefois, la synchronisation du cluster avec une source de temps externe nécessite toujours une configuration. ONTAP vous permet de gérer la configuration NTP du cluster de l'une des manières suivantes :

- Vous pouvez associer un maximum de 10 serveurs NTP externes au cluster (`cluster time-service ntp server create`).
  - Pour la redondance et la qualité du service de temps, vous devez associer au moins trois serveurs NTP externes au cluster.
  - Vous pouvez spécifier un serveur NTP à l'aide de son adresse IPv4 ou IPv6 ou de son nom d'hôte complet.
  - Vous pouvez spécifier manuellement la version NTP (v3 ou v4) à utiliser.

Par défaut, ONTAP sélectionne automatiquement la version NTP prise en charge pour un serveur NTP externe donné.

Si la version NTP que vous spécifiez n'est pas prise en charge pour le serveur NTP, le service de change ne peut pas avoir lieu.

- Au niveau de privilège avancé, vous pouvez spécifier un serveur NTP externe associé au cluster

comme source de temps principale pour corriger et ajuster l'heure du cluster.

- Vous pouvez afficher les serveurs NTP associés au cluster (`cluster time-service ntp server show`).
- Vous pouvez modifier la configuration NTP du cluster (`cluster time-service ntp server modify`).
- Vous pouvez dissocier le cluster d'un serveur NTP externe (`cluster time-service ntp server delete`).
- Au niveau de privilège avancé, vous pouvez réinitialiser la configuration en désactivant toute association de serveurs NTP externes au cluster (`cluster time-service ntp server reset`).

Un nœud qui rejoint un cluster adopte automatiquement la configuration NTP du cluster.

Outre l'utilisation du protocole NTP, ONTAP vous permet également de gérer manuellement l'heure du cluster. Cette fonctionnalité est utile pour corriger une heure erronée (par exemple, l'heure d'un nœud est devenue très incorrecte après un redémarrage). Dans ce cas, vous pouvez indiquer une heure approximative du cluster jusqu'à ce que NTP puisse se synchroniser avec un serveur de temps externe. Le temps que vous définissez manuellement prend effet sur tous les nœuds du cluster.

Vous pouvez gérer manuellement l'heure du cluster des manières suivantes :

- Vous pouvez définir ou modifier le fuseau horaire, la date et l'heure sur le cluster (`cluster date modify`).
- Vous pouvez afficher les paramètres actuels du fuseau horaire, de date et d'heure du cluster (`cluster date show`).



Les planifications des tâches ne s'adaptent pas aux modifications manuelles de la date et de l'heure du cluster. Ces travaux sont planifiés pour s'exécuter en fonction de l'heure actuelle du cluster au moment de la création du travail ou de l'exécution du travail le plus récent. Par conséquent, si vous modifiez manuellement la date ou l'heure du cluster, vous devez utiliser le `job show` et `job history show` commandes permettant de vérifier que tous les travaux planifiés sont mis en file d'attente et terminés en fonction de vos besoins.



## Commandes de gestion de l'heure du cluster

Vous utilisez le `cluster time-service ntp server` Commandes permettant de gérer les serveurs NTP du cluster. Vous utilisez le `cluster date` commandes permettant de gérer manuellement l'heure du cluster.

Depuis ONTAP 9.5, vous pouvez configurer votre serveur NTP avec une authentification symétrique.

Les commandes suivantes vous permettent de gérer les serveurs NTP du cluster :

| Les fonctions que vous recherchez...                                          | Utilisez cette commande...                                              |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Associez le cluster à un serveur NTP externe sans authentification symétrique | <code>cluster time-service ntp server create -server server_name</code> |

| Les fonctions que vous recherchez...                                                                                                                                                                                                      | Utilisez cette commande...                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Associez le cluster à un serveur NTP externe avec une authentification symétrique disponible dans ONTAP 9.5 ou version ultérieure                                                                                                         | <pre>cluster time-service ntp server create -server server_ip_address -key-id key_id</pre> <div>  <p>Le <code>key_id</code> doit faire référence à une clé partagée existante configurée avec « clé ntp de service de cluster ».</p> </div>                          |
| <p>Activer l'authentification symétrique pour un serveur NTP existant le serveur NTP existant peut être modifié pour activer l'authentification en ajoutant l'ID de clé requis</p> <p>Disponible dans ONTAP 9.5 ou version ultérieure</p> | <pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre>                                                                                                                                                                                                                                                                  |
| Désactiver l'authentification symétrique                                                                                                                                                                                                  | <pre>cluster time-service ntp server modify -server server_name -is-authentication -enabled false</pre>                                                                                                                                                                                                                                               |
| Configurez une clé NTP partagée                                                                                                                                                                                                           | <pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <div>  <p>Les clés partagées sont désignées par un ID. L'ID, son type et la valeur doivent être identiques sur le nœud et le serveur NTP</p> </div> |
| Affiche les informations relatives aux serveurs NTP associés au cluster                                                                                                                                                                   | <pre>cluster time-service ntp server show</pre>                                                                                                                                                                                                                                                                                                       |
| Modifier la configuration d'un serveur NTP externe associé au cluster                                                                                                                                                                     | <pre>cluster time-service ntp server modify</pre>                                                                                                                                                                                                                                                                                                     |
| Dissociez un serveur NTP du cluster                                                                                                                                                                                                       | <pre>cluster time-service ntp server delete</pre>                                                                                                                                                                                                                                                                                                     |
| Réinitialise la configuration en désactivant l'association de tous les serveurs NTP externes au cluster                                                                                                                                   | <pre>cluster time-service ntp server reset</pre> <div>  <p>Cette commande nécessite le niveau de privilège avancé.</p> </div>                                                                                                                                      |

Les commandes suivantes vous permettent de gérer manuellement l'heure du cluster :

| Les fonctions que vous recherchez...                                    | Utilisez cette commande...       |
|-------------------------------------------------------------------------|----------------------------------|
| Définissez ou modifiez le fuseau horaire, la date et l'heure            | <code>cluster date modify</code> |
| Affiche les paramètres de fuseau horaire, de date et d'heure du cluster | <code>cluster date show</code>   |

#### Informations associées

["Référence de commande ONTAP"](#)

## Gérer la bannière et la MOTD

### Gérer la bannière et la vue d'ensemble de la MOTD

ONTAP vous permet de configurer une bannière de connexion ou un message du jour (MOTD) pour communiquer des informations administratives aux utilisateurs de l'interface de ligne de commande du cluster ou de la machine virtuelle de stockage (SVM).

Une bannière s'affiche dans une session de console (pour l'accès au cluster uniquement) ou dans une session SSH (pour l'accès au cluster ou au SVM) avant qu'un utilisateur soit invité à authentification par exemple. Par exemple, vous pouvez utiliser la bannière pour afficher un message d'avertissement comme les éléments suivants à une personne qui tente de se connecter au système :

```
$ ssh admin@cluster1-01
```

```
This system is for authorized users only. Your IP Address has been logged.
```

```
Password:
```

Une MOTD s'affiche dans une session de console (pour l'accès au cluster uniquement) ou une session SSH (pour l'accès au cluster ou au SVM) après l'authentification d'un utilisateur, mais avant l'affichage de l'invite `clustershell`. Par exemple, vous pouvez utiliser le MOTD pour afficher un message d'accueil ou d'information comme les éléments suivants que seuls les utilisateurs authentifiés verront :

```
$ ssh admin@cluster1-01
```

```
Password:
```

```
Greetings. This system is running ONTAP 9.0.
```

```
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015
from 10.72.137.28.
```

Vous pouvez créer ou modifier le contenu de la bannière ou de la MOTD en utilisant le `security login banner modify` ou `security login motd modify` les commandes, respectivement, de l'une des



manières suivantes :

- Vous pouvez utiliser la CLI de manière interactive ou non interactive pour spécifier le texte à utiliser pour la bannière ou la MOTD.

Le mode interactif, lancé lorsque la commande est utilisée sans l' `-message` ou `-uri` paramètre, vous permet d'utiliser des nouvelles lignes (également appelées fin de lignes) dans le message.

Le mode non interactif, qui utilise le `-message` paramètre pour spécifier la chaîne de message, ne prend pas en charge les nouvelles lignes.

- Vous pouvez télécharger du contenu à partir d'un emplacement FTP ou HTTP à utiliser pour la bannière ou le MOTD.
- Vous pouvez configurer le MOTD pour qu'il affiche du contenu dynamique.

Voici des exemples de ce que vous pouvez configurer le MOTD pour qu'il s'affiche de façon dynamique :

- Nom du cluster, nom de nœud ou nom SVM
- Date et heure du cluster
- Nom de l'utilisateur connecté
- Dernière connexion de l'utilisateur sur n'importe quel nœud du cluster
- Nom ou adresse IP du périphérique de connexion
- Nom du système d'exploitation
- Version du logiciel
- Chaîne de version effective du cluster

Le `security login motd modify` La page man décrit les séquences d'échappement que vous pouvez utiliser pour permettre au MOTD d'afficher du contenu généré dynamiquement.

La bannière ne prend pas en charge le contenu dynamique.

Vous pouvez gérer la bannière et la MOTD au niveau du cluster ou du SVM :

- Les faits suivants s'appliquent à la bannière :
  - La bannière configurée pour le cluster est également utilisée pour tous les SVM qui ne possèdent pas de message de bannière défini.
  - Une bannière SVM peut être configurée pour chaque SVM.

Si une bannière au niveau du cluster a été configurée, elle est remplacée par la bannière SVM-level pour la SVM donnée.

- Les faits suivants s'appliquent à la MOTD :
  - Par défaut, la MOTD configurée pour le cluster est également activée pour tous les SVM.
  - En outre, un MOTD au niveau d'un SVM peut être configuré pour chaque SVM.

Dans ce cas, les utilisateurs qui se connectent à la SVM verront deux MOTDS, l'un défini au niveau du cluster et l'autre au niveau du SVM.

- La fonction MOTD au niveau du cluster peut être activée ou désactivée par SVM par l'administrateur du cluster.

Si l'administrateur du cluster désactive la MOTD au niveau du cluster pour un SVM, un utilisateur qui se connecte à la SVM ne voit pas la MOTD au niveau du cluster.

## Créez une bannière

Vous pouvez créer une bannière pour afficher un message à quelqu'un qui tente d'accéder au cluster ou à un SVM. La bannière s'affiche dans une session de console (pour l'accès au cluster uniquement) ou dans une session SSH (pour l'accès au cluster ou SVM) avant qu'un utilisateur soit invité à s'authentifier.

### Étapes

1. Utilisez le `security login banner modify` Commande pour créer une bannière pour le cluster ou le SVM :

| Les fonctions que vous recherchez...                                            | Alors...                                                                                                                                |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Spécifiez un message à une seule ligne                                          | Utilisez le <code>-message «text" paramètre pour spécifier le texte.</code>                                                             |
| Inclure les nouvelles lignes (également appelées fin de lignes) dans le message | Utiliser la commande sans <code>-message</code> ou <code>-uri</code> paramètre pour lancer le mode interactif d'édition de la bannière. |
| Téléchargez le contenu depuis un emplacement pour l'utiliser pour la bannière   | Utilisez le <code>-uri</code> Paramètre pour spécifier l'emplacement FTP ou HTTP du contenu.                                            |

La taille maximale d'une bannière est de 2,048 octets, y compris les newlines.

Bannière créée à l'aide du `-uri` paramètre statique. Elle n'est pas mise à jour automatiquement pour refléter les modifications ultérieures du contenu source.

La bannière créée pour le cluster est également affichée pour tous les SVM qui ne disposent pas de bannière existante. Toute bannière créée pour un SVM remplace la bannière de niveau cluster pour ce SVM. Spécification du `-message` paramètre avec un tiret dans les guillemets doubles ("`-`") Pour la SVM réinitialise le SVM pour l'utilisation de la bannière cluster.

2. Vérifiez que la bannière a été créée en l'affichant avec le `security login banner show` commande.

Spécification du `-message` paramètre avec une chaîne vide ("`"`") affiche des bannières qui n'ont pas de contenu.

Spécification du `-message` paramètre avec "`-`" Affiche tous les SVM (admin ou data) ne disposant pas de bannière configurée.

### Exemples de bannières de création

L'exemple suivant utilise le mode non interactif pour créer une bannière pour le cluster « cluster1 » :

```
cluster1::> security login banner modify -message "Authorized users only!"

cluster1::>
```

L'exemple suivant utilise le mode interactif pour créer une bannière pour le SVM "svm1":

```
cluster1::> security login banner modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0 1 2 3 4 5 6 7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
The svm1 SVM is reserved for authorized users only!

cluster1::>
```

L'exemple suivant montre les bannières créées :

```
cluster1::> security login banner show
Vserver: cluster1
Message

Authorized users only!

Vserver: svm1
Message

The svm1 SVM is reserved for authorized users only!

2 entries were displayed.

cluster1::>
```

## Informations associées

[Gestion de la bannière](#)

## Gestion de la bannière

Vous pouvez gérer la bannière au niveau du cluster ou de la SVM. La bannière configurée pour le cluster est également utilisée pour tous les SVM qui ne possèdent pas de message de bannière défini. Une bannière créée par la suite pour un SVM remplace la bannière de cluster pour ce SVM.

### Choix

- Gérez la bannière au niveau du cluster :

| Les fonctions que vous recherchez...                                                                                                     | Alors...                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Créez une bannière à afficher pour toutes les sessions de connexion de l'interface de ligne de commande                                  | Définissez une bannière au niveau du cluster :<br><br><code>`*security login banner modify -vserver <i>cluster_name</i> { [-message "text"]</code> |
| <code>[-uri <i>ftp_or_http_addr</i>] }*</code>                                                                                           | Supprimer la bannière pour toutes les connexions (cluster et SVM)                                                                                  |
| Définissez la bannière sur une chaîne vide ("") :<br><br><code><b>security login banner modify -vserver * -message ""</b></code>         | Remplacer une bannière créée par un administrateur du SVM                                                                                          |
| Modifier le message de la bannière SVM :<br><br><code>`*security login banner modify -vserver <i>svm_name</i> { [-message "text"]</code> | <code>[-uri <i>ftp_or_http_addr</i>] }*</code>                                                                                                     |

- Gestion de la bannière au niveau du SVM :

Spécification `-vserver svm_name` N'est pas requis dans le contexte SVM.

| Les fonctions que vous recherchez...                                                              | Alors...                                                                                                                         |
|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Remplacer la bannière fournie par l'administrateur du cluster avec une autre bannière pour le SVM | Créer une bannière pour le SVM :<br><br><code>`*security login banner modify -vserver <i>svm_name</i> { [-message "text"]</code> |
| <code>[-uri <i>ftp_or_http_addr</i>] }*</code>                                                    | Supprime la bannière fournie par l'administrateur du cluster afin qu'aucune bannière ne s'affiche pour la SVM                    |

| Les fonctions que vous recherchez...                                                                                               | Alors...                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Définir la bannière SVM sur une chaîne vide pour le SVM :<br><br><b>security login banner modify -vserver svm_name -message ""</b> | Utilisez la bannière cluster lorsque le SVM utilise actuellement une bannière de niveau SVM |

## Créer un MOTD

Vous pouvez créer un message du jour (MOTD) pour communiquer des informations aux utilisateurs authentifiés de CLI. Le mot MOTD s'affiche dans une session de console (pour l'accès au cluster uniquement) ou dans une session SSH (pour l'accès au cluster ou SVM) après l'authentification d'un utilisateur, mais avant l'affichage de l'invite clustershell.

### Étapes

1. Utilisez le `security login motd modify` Commande pour créer un MOTD pour le cluster ou le SVM :

| Les fonctions que vous recherchez...                           | Alors...                                                                                                                             |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Spécifiez un message à une seule ligne                         | Utilisez le <code>-message «text" paramètre pour spécifier le texte.</code>                                                          |
| Inclure les nouvelles lignes (également appelée fin de lignes) | Utiliser la commande sans <code>-message</code> ou <code>-uri</code> Paramètre pour lancer le mode interactif pour modifier le MOTD. |
| Téléchargez le contenu à partir d'un emplacement pour le MOTD  | Utilisez le <code>-uri</code> Paramètre pour spécifier l'emplacement FTP ou HTTP du contenu.                                         |

La taille maximale d'un MOTD est de 2,048 octets, y compris les nouvelles lignes.

Le `security login motd modify` La page man décrit les séquences d'échappement que vous pouvez utiliser pour permettre au MOTD d'afficher du contenu généré dynamiquement.

Un MOTD créé à l'aide du `-uri` paramètre statique. Elle n'est pas mise à jour automatiquement pour refléter les modifications ultérieures du contenu source.

Un MOTD créé pour le cluster est également affiché pour toutes les connexions de SVM par défaut, ainsi qu'un MOTD de niveau SVM que vous pouvez créer séparément pour un SVM donné. Réglage du `-is -cluster-message-enabled` paramètre à `false` Pour un SVM, il n'est pas possible de visualiser la MOTD niveau du cluster pour ce SVM.

2. Vérifiez que le MOTD a été créé en l'affichant avec le `security login motd show` commande.

Spécification du `-message` paramètre avec une chaîne vide ("" ) Affiche les MOTDS qui ne sont pas configurés ou n'ont pas de contenu.

Voir la "[code de connexion de sécurité motd modifier](#)" Page de manuel de commande pour une liste de paramètres à utiliser pour permettre au MOTD d'afficher le contenu généré dynamiquement. Assurez-vous de consulter la page de manuel spécifique à votre version de ONTAP.

### Exemples de création de MOTDS

L'exemple suivant utilise le mode non interactif pour créer un MOTD pour le cluster « cluster1 » :

```
cluster1::> security login motd modify -message "Greetings!"
```

L'exemple suivant utilise le mode interactif pour créer un MOTD pour le SVM "svm1" qui utilise les séquences d'échappement pour afficher le contenu généré dynamiquement :

```
cluster1::> security login motd modify -vserver svm1
```

Enter the message of the day for Vserver "svm1".

Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to abort.

0            1            2            3            4            5            6            7  
8

1234567890123456789012345678901234567890123456789012345678901234  
567890

Welcome to the \n SVM. Your user ID is '\N'. Your last successful login  
was \L.

L'exemple suivant affiche les MOTDS qui ont été créés :

```
cluster1::> security login motd show
```

Vserver: cluster1

Is the Cluster MOTD Displayed?: true

Message

-----

---

Greetings!

Vserver: svm1

Is the Cluster MOTD Displayed?: true

Message

-----

---

Welcome to the \n SVM. Your user ID is '\N'. Your last successful login  
was \L.

2 entries were displayed.

## Gérer la DPE

Vous pouvez gérer le message du jour (MOTD) au niveau du cluster ou de la SVM. Par défaut, la MOTD configurée pour le cluster est également activée pour tous les SVM. En outre, un MOTD au niveau d'un SVM peut être configuré pour chaque SVM. La fonction MOTD au niveau du cluster peut être activée ou désactivée pour chaque SVM par l'administrateur du cluster.

Pour obtenir la liste des séquences d'échappement pouvant être utilisées pour générer dynamiquement du contenu pour le MOTD, reportez-vous au ["référence de commande"](#).

### Choix

- Gérer la DPE au niveau du cluster :

| Les fonctions que vous recherchez...                                                                                                                                                  | Alors...                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Créez un MOTD pour toutes les connexions lorsqu'il n'existe pas de MOTD                                                                                                               | Définir un mot de travail au niveau du cluster :<br><br><code>`*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"]</code>                                                                                                                 |
| <code>[-uri <i>ftp_or_http_addr</i>] }*</code>                                                                                                                                        | Modifiez le MOTD pour toutes les connexions lorsqu'aucun MOTD au niveau des SVM n'est configuré                                                                                                                                                                           |
| Modifier la DPE au niveau du cluster :<br><br><code>`*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"] }</code>                                     | <code>[-uri <i>ftp_or_http_addr</i>] }*</code>                                                                                                                                                                                                                            |
| Supprimer le MOTD pour toutes les connexions lorsqu'aucun MOTD au niveau des SVM n'est configuré                                                                                      | Définissez le mot-symbole MOTD au niveau du cluster sur une chaîne vide ("") :<br><br><code><b>security login motd modify -vserver <i>cluster_name</i> -message ""</b></code>                                                                                             |
| Demandez à chaque SVM d'afficher la MOTD au niveau du cluster au lieu d'utiliser la MOTD au niveau du SVM                                                                             | Définissez un MOTD au niveau du cluster, puis définissez tous les MOTD au niveau du SVM sur une chaîne vide lorsque le MOTD au niveau du cluster est activé :<br><br>a. <code>`*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"]</code> |
| <code>[-uri <i>ftp_or_http_addr</i>] }*</code><br><code><b>.. security login motd modify { -vserver !"<i>cluster_name</i>" } -message "" -is -cluster-message-enabled true</b></code> | Avoir un MOTD affiché uniquement pour les SVM sélectionnés et n'utiliser aucun MOTD au niveau du cluster                                                                                                                                                                  |

| Les fonctions que vous recherchez...                                                                                                                                                                                                                                                                                                   | Alors...                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Définissez la MOTD au niveau du cluster sur une chaîne vide, puis définissez les MOTDS au niveau du SVM pour les SVM sélectionnés :</p> <p>a. <b>security login motd modify -vserver <i>cluster_name</i> -message ""</b></p> <p>b. <code>*security login motd modify -vserver <i>svm_name</i> { [-message "<i>text</i>"]</code></p> | <p><code>[-uri <i>ftp_or_http_addr</i>] }*</code><br/>+<br/>Vous pouvez répéter cette étape pour chaque SVM si nécessaire.</p>                                                                                   |
| <p>Utilisez la même MOTD au niveau du SVM pour toutes les SVM (données et admin</p>                                                                                                                                                                                                                                                    | <p>Définir le cluster et tous les SVM afin d'utiliser le même MOTD :</p> <p><code>*security login motd modify -vserver * { [-message "<i>text</i>"]</code></p>                                                   |
| <p><code>[-uri <i>ftp_or_http_addr</i>] }*</code></p> <p>[NOTE]<br/>====<br/>Si vous utilisez le mode interactif, la CLI vous invite à entrer la MOTD individuellement pour le cluster et chaque SVM. Vous pouvez coller le même MOTD dans chaque instance lorsque vous êtes invité à le faire.<br/><br/>=====</p>                     | <p>Disposer d'une MOTD au niveau du cluster disponible en option pour tous les SVM, mais ne pas vouloir que la MOTD soit affichée pour les connexions de cluster</p>                                             |
| <p>Définissez un MOTD au niveau du cluster, mais désactivez son affichage pour le cluster :</p> <p><code>*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"]</code></p>                                                                                                                                | <p><code>[-uri <i>ftp_or_http_addr</i>] } -is-cluster-message-enabled false*</code></p>                                                                                                                          |
| <p>Supprimer tous les MOTD au niveau du cluster et des SVM lorsque seuls certains SVM ont des MOTD au niveau du cluster et des SVM</p>                                                                                                                                                                                                 | <p>Définissez le cluster et tous les SVM de manière à utiliser une chaîne vide pour le MOTD :</p> <p><b>security login motd modify -vserver *<br/>-message ""</b></p>                                            |
| <p>Modifiez la MOTD uniquement pour les SVM qui ont une chaîne non vide, lorsque d'autres SVM utilisent une chaîne vide, et lorsqu'un autre MOTD est utilisé au niveau du cluster</p>                                                                                                                                                  | <p>Utilisez les requêtes étendues pour modifier la MOTD de façon sélective :</p> <p><code>*security login motd modify { -vserver<br/>!"<i>cluster_name</i>" -message !"" } { [-message "<i>text</i>"]</code></p> |



| Les fonctions que vous recherchez...                                                                                  | Alors...                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>[-uri ftp_or_http_addr] }*</code>                                                                               | Afficher tous les MOTD contenant du texte spécifique (par exemple, « janvier » suivi de « 2015 ») n'importe où dans un message unique ou multiligne, même si le texte est divisé entre différentes lignes |
| Utilisez une requête pour afficher les MOTDS :<br><br><b>security login motd show -message<br/>*"January"*"2015"*</b> | Créer de manière interactive un MOTD qui inclut plusieurs nouvelles lignes consécutives (également appelées fin de lignes, ou EOLs)                                                                       |

- Gestion de la MOTD au niveau de la SVM :

Spécification `-vserver svm_name` N'est pas requis dans le contexte SVM.

| Les fonctions que vous recherchez...                                                                                                                                                                                                                                                                                            | Alors...                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Utilisez une DPE différente au niveau du SVM lorsque le SVM possède déjà une DPE au niveau du SVM                                                                                                                                                                                                                               | Modifier la MOTD au niveau du SVM :<br><br><code>*security login motd modify -vserver svm_name { [-message "text"]</code> |
| <code>[-uri ftp_or_http_addr] }*</code>                                                                                                                                                                                                                                                                                         | Utiliser uniquement la MOTD de niveau cluster pour le SVM, lorsque le SVM possède déjà une MOTD de niveau SVM             |
| Définir la MOTD au niveau du SVM sur une chaîne vide, puis faire activer la MOTD au niveau du cluster pour la SVM :<br><br>a. <b>security login motd modify -vserver svm_name -message ""</b><br><br>b. (Pour l'administrateur du cluster) <b>security login motd modify -vserver svm_name -is-cluster-message-enabled true</b> | Pas que le SVM n'affiche de DPE, lorsque les DPE au niveau du cluster et du SVM sont actuellement affichées pour la SVM   |

## Gestion des tâches et planification

Les travaux sont placés dans une file d'attente de travaux et exécutés en arrière-plan lorsque des ressources sont disponibles. Si une tâche consomme trop de ressources de cluster, vous pouvez l'arrêter ou le mettre en pause jusqu'à ce que la demande sur le cluster soit moins élevée. Vous pouvez également surveiller et redémarrer les travaux.

### Catégories de travail

Il existe trois catégories de travaux que vous pouvez gérer : affilié au serveur, affilié au cluster et privé.

Un travail peut se trouver dans l'une des catégories suivantes :

- **Travaux affiliés au serveur**

Ces travaux sont mis en file d'attente par l'infrastructure de gestion vers un nœud spécifique à exécuter.

- **Emplois affiliés à un groupe**

Ces travaux sont mis en file d'attente par l'infrastructure de gestion vers n'importe quel nœud du cluster à exécuter.

- **Emplois privés**

Ces jobs sont spécifiques à un nœud et n'utilisent pas la base de données répliquée (RDB) ou tout autre mécanisme du cluster. Les commandes qui gèrent les travaux privés nécessitent un niveau de privilège avancé ou supérieur.

## Commandes de gestion des travaux

Lorsque vous entrez une commande qui appelle un travail, généralement, la commande vous informe que le travail a été mis en file d'attente, puis revient à l'invite de commande CLI. Toutefois, certaines commandes indiquent plutôt la progression du travail et ne reviennent pas à l'invite de commande CLI tant que le travail n'a pas été terminé. Dans ce cas, vous pouvez appuyer sur Ctrl-C pour déplacer le travail en arrière-plan.

| Les fonctions que vous recherchez...                           | Utilisez cette commande...                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Affiche des informations sur tous les travaux                  | <code>job show</code>                                                                                                                                                                                                                                                                                                                                                                               |
| Affiche des informations sur les travaux par nœud              | <code>job show bynode</code>                                                                                                                                                                                                                                                                                                                                                                        |
| Affiche des informations sur les travaux affiliés à un cluster | <code>job show-cluster</code>                                                                                                                                                                                                                                                                                                                                                                       |
| Affiche des informations sur les tâches terminées              | <code>job show-completed</code>                                                                                                                                                                                                                                                                                                                                                                     |
| Affiche des informations sur l'historique des travaux          | <code>job history show</code><br><br>Jusqu'à 25,000 enregistrements de tâche sont stockés pour chaque nœud du cluster. Par conséquent, toute tentative d'affichage de l'historique complet du travail peut prendre beaucoup de temps. Pour éviter les temps d'attente potentiellement longs, il est conseillé d'afficher les tâches par nœud, machine virtuelle de stockage ou ID d'enregistrement. |
| Affiche la liste des travaux privés                            | <code>job private show</code> (niveau de privilège avancé)                                                                                                                                                                                                                                                                                                                                          |
| Affiche des informations sur les travaux privés terminés       | <code>job private show-completed</code> (niveau de privilège avancé)                                                                                                                                                                                                                                                                                                                                |

| Les fonctions que vous recherchez...                                                                                                                    | Utilisez cette commande...                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| Affiche des informations sur l'état d'initialisation des gestionnaires de travaux                                                                       | <code>job initstate show</code> (niveau de privilège avancé)         |
| Surveiller la progression d'une tâche                                                                                                                   | <code>job watch-progress</code>                                      |
| Surveiller la progression d'un travail privé                                                                                                            | <code>job private watch-progress</code> (niveau de privilège avancé) |
| Interrompre un travail                                                                                                                                  | <code>job pause</code>                                               |
| Interrompre un travail privé                                                                                                                            | <code>job private pause</code> (niveau de privilège avancé)          |
| Reprendre un travail en pause                                                                                                                           | <code>job resume</code>                                              |
| Reprendre un travail privé en pause                                                                                                                     | <code>job private resume</code> (niveau de privilège avancé)         |
| Arrêter un travail                                                                                                                                      | <code>job stop</code>                                                |
| Arrêter un travail privé                                                                                                                                | <code>job private stop</code> (niveau de privilège avancé)           |
| Supprimer un travail                                                                                                                                    | <code>job delete</code>                                              |
| Supprimer un travail privé                                                                                                                              | <code>job private delete</code> (niveau de privilège avancé)         |
| Dissociez un travail affilié à un cluster avec un nœud non disponible qui le possède, de sorte qu'un autre nœud puisse prendre possession de ce travail | <code>job unclaim</code> (niveau de privilège avancé)                |



Vous pouvez utiliser le `event log show` commande permettant de déterminer le résultat d'un travail terminé.

## Informations associées

["Référence de commande ONTAP"](#)

## Commandes de gestion des planifications de travaux

De nombreuses tâches, par exemple, les copies Snapshot de volume, peuvent être configurées pour s'exécuter sur des planifications spécifiées. Les planifications qui s'exécutent à des heures spécifiques sont appelées *cron* planifications (similaires à UNIX) *cron* planifications). Les horaires exécutés à intervalles sont appelés *interval* planifications. Vous utilisez le `job schedule` commandes permettant de gérer les planifications de tâches.

Les planifications de tâches ne s'adaptent pas aux modifications manuelles apportées à la date et à l'heure du cluster. Ces travaux sont planifiés pour s'exécuter en fonction de l'heure actuelle du cluster au moment de la création du travail ou de l'exécution du travail le plus récent. Par conséquent, si vous modifiez manuellement la

date ou l'heure du cluster, vous devez utiliser le `job show` et `job history show` commandes permettant de vérifier que tous les travaux planifiés sont mis en file d'attente et terminés en fonction de vos besoins.

Si le cluster fait partie d'une configuration MetroCluster, la planification de tâches sur les deux clusters doit être identique. Par conséquent, si vous créez, modifiez ou supprimez un Job planning, vous devez effectuer la même opération sur le cluster distant.

| Les fonctions que vous recherchez...                     | Utilisez cette commande...                                                                                                                                                                                |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Affiche des informations sur tous les horaires           | <code>job schedule show</code>                                                                                                                                                                            |
| Affiche la liste des travaux par planning                | <code>job schedule show-jobs</code>                                                                                                                                                                       |
| Affiche des informations sur les planifications cron     | <code>job schedule cron show</code>                                                                                                                                                                       |
| Affiche des informations sur les plannings d'intervalles | <code>job schedule interval show</code>                                                                                                                                                                   |
| Créez une planification cron                             | <code>job schedule cron create</code><br><br>À partir de ONTAP 9.10.1, vous pouvez inclure le SVM pour votre planification de tâches.                                                                     |
| Créer un planning d'intervalles                          | <code>job schedule interval create</code><br><br>Vous devez spécifier au moins un des paramètres suivants : <code>-days</code> , <code>-hours</code> , <code>-minutes</code> , ou <code>-seconds</code> . |
| Modifier une planification cron                          | <code>job schedule cron modify</code>                                                                                                                                                                     |
| Modifier un planning d'intervalles                       | <code>job schedule interval modify</code>                                                                                                                                                                 |
| Supprimer un planning                                    | <code>job schedule delete</code>                                                                                                                                                                          |
| Supprimez une planification cron                         | <code>job schedule cron delete</code>                                                                                                                                                                     |
| Supprimer un planning d'intervalles                      | <code>job schedule interval delete</code>                                                                                                                                                                 |

#### Informations associées

["Référence de commande ONTAP"](#)

## Sauvegarde et restauration des configurations de cluster (administrateurs de cluster uniquement)

## Quels sont les fichiers de sauvegarde de configuration

Les fichiers de sauvegarde de configuration sont des fichiers d'archive (.7z) qui contiennent des informations sur toutes les options configurables qui sont nécessaires pour que le cluster et les nœuds qu'il contient fonctionnent correctement.

Ces fichiers stockent la configuration locale de chaque nœud, plus la configuration répliquée au niveau du cluster. Vous utilisez les fichiers de sauvegarde de configuration pour sauvegarder et restaurer la configuration de votre cluster.

Il existe deux types de fichiers de sauvegarde de configuration :

- **Fichier de sauvegarde de configuration de nœud**

Chaque nœud sain du cluster inclut un fichier de sauvegarde de configuration de nœud, qui contient toutes les informations de configuration et les métadonnées nécessaires au fonctionnement du nœud sur le cluster.

- **Fichier de sauvegarde de configuration de cluster**

Ces fichiers incluent une archive de tous les fichiers de sauvegarde de configuration des nœuds du cluster, ainsi que des informations de configuration du cluster répliqué (base de données répliquée ou fichier RDB). Les fichiers de sauvegarde de configuration de cluster vous permettent de restaurer la configuration de tout le cluster ou de tout nœud du cluster. Les planifications de sauvegarde de configuration de cluster créent ces fichiers automatiquement et les stockent sur plusieurs nœuds du cluster.



Les fichiers de sauvegarde de configuration contiennent uniquement des informations sur la configuration. Elles n'incluent aucune donnée utilisateur. Pour plus d'informations sur la restauration des données utilisateur, reportez-vous à la section "[La protection des données](#)".

## Sauvegarde automatique des configurations de nœuds et de clusters

Trois planifications distinctes créent automatiquement les fichiers de sauvegarde des configurations de cluster et de nœud et les répliquent entre les nœuds du cluster.

Les fichiers de sauvegarde de configuration sont automatiquement créés en fonction des planifications suivantes :



- Toutes les 8 heures
- Tous les jours
- Hebdomadaire

À chaque fois, un fichier de sauvegarde de configuration de nœud est créé sur chaque nœud en bon état du cluster. Tous ces fichiers de sauvegarde de configuration de nœud sont ensuite rassemblés dans un fichier de sauvegarde de configuration de cluster unique avec la configuration de cluster répliquée et enregistrés sur un ou plusieurs nœuds du cluster.

## Commandes de gestion des planifications de sauvegarde de configuration

Vous pouvez utiliser le `system configuration backup settings` commandes permettant de gérer les planifications de sauvegarde de configuration.

Ces commandes sont disponibles au niveau de privilège avancé.



| Les fonctions que vous recherchez...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Utilisez cette commande...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Modifiez les paramètres d'un planning de sauvegarde de configuration :</p> <ul style="list-style-type: none"><li>• Spécifiez une URL distante (HTTP, HTTPS, FTP, FTPS ou TFTP ) où les fichiers de sauvegarde de configuration seront chargés en plus des emplacements par défaut dans le cluster</li><li>• Spécifiez un nom d'utilisateur à utiliser pour se connecter à l'URL distante</li><li>• Définissez le nombre de sauvegardes à conserver pour chaque planning de sauvegarde de configuration</li></ul> | <p><code>system configuration backup settings modify</code></p> <p>Lorsque vous utilisez HTTPS dans l'URL distante, utilisez le <code>-validate-certification</code> option permettant d'activer ou de désactiver la validation de certificats numériques. La validation du certificat est désactivée par défaut.</p> <div><p>Le serveur Web sur lequel vous téléchargez le fichier de sauvegarde de configuration doit avoir ACTIVÉ les opérations HTTP et LES opérations DE POST activées pour HTTPS. Pour plus d'informations, consultez la documentation de votre serveur Web.</p></div> |
| <p>Définissez le mot de passe à utiliser pour vous connecter à l'URL distante</p>                                                                                                                                                                                                                                                                                                                                                                                                                                   | <p><code>system configuration backup settings set-password</code></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <p>Afficher les paramètres du programme de sauvegarde de la configuration</p>                                                                                                                                                                                                                                                                                                                                                                                                                                       | <p><code>system configuration backup settings show</code></p> <div><p>Vous définissez le <code>-instance</code> paramètre pour afficher le nom d'utilisateur et le nombre de sauvegardes à conserver pour chaque planning.</p></div>                                                                                                                                                                                                                                                                                                                                                       |

### Commandes de gestion des fichiers de sauvegarde de configuration

Vous utilisez le `system configuration backup` commandes permettant de gérer les fichiers de sauvegarde de la configuration du cluster et des nœuds.

Ces commandes sont disponibles au niveau de privilège avancé.

| Les fonctions que vous recherchez...                                                            | Utilisez cette commande...                             |
|-------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| <p>Créer un nouveau fichier de sauvegarde de configuration de nœud ou de cluster</p>            | <p><code>system configuration backup create</code></p> |
| <p>Copiez un fichier de sauvegarde de configuration d'un nœud vers un autre nœud du cluster</p> | <p><code>system configuration backup copy</code></p>   |

| Les fonctions que vous recherchez...                                                                                                                       | Utilisez cette commande...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Charger un fichier de sauvegarde de configuration à partir d'un nœud du cluster vers une URL distante (FTP, HTTP, HTTPS, TFTP ou FTPS)                     | <p data-bbox="820 163 1390 191"><code>system configuration backup upload</code></p> <p data-bbox="820 228 1471 396">Lorsque vous utilisez HTTPS dans l'URL distante, utilisez le <code>-validate-certification</code> option permettant d'activer ou de désactiver la validation de certificats numériques. La validation du certificat est désactivée par défaut.</p> <div data-bbox="850 653 904 709">  </div> <p data-bbox="964 447 1455 919">Le serveur Web sur lequel vous téléchargez le fichier de sauvegarde de configuration doit avoir ACTIVÉ les opérations HTTP et LES opérations DE POST activées pour HTTPS. Certains serveurs Web peuvent nécessiter l'installation d'un module supplémentaire. Pour plus d'informations, consultez la documentation de votre serveur Web. Les formats d'URL pris en charge varient en fonction de la version d'ONTAP. Consultez l'aide en ligne de commandes de votre version ONTAP.</p> |
| Téléchargez un fichier de sauvegarde de configuration à partir d'une URL distante vers un nœud du cluster et, si spécifié, validez le certificat numérique | <p data-bbox="820 989 1422 1016"><code>system configuration backup download</code></p> <p data-bbox="820 1054 1471 1222">Lorsque vous utilisez HTTPS dans l'URL distante, utilisez le <code>-validate-certification</code> option permettant d'activer ou de désactiver la validation de certificats numériques. La validation du certificat est désactivée par défaut.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Renommez un fichier de sauvegarde de configuration sur un nœud du cluster                                                                                  | <p data-bbox="820 1283 1386 1310"><code>system configuration backup rename</code></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Afficher les fichiers de sauvegarde de configuration de nœud et de cluster pour un ou plusieurs nœuds du cluster                                           | <p data-bbox="820 1398 1354 1425"><code>system configuration backup show</code></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Supprime un fichier de sauvegarde de configuration sur un noeud                                                                                            | <div data-bbox="850 1694 904 1751">  </div> <p data-bbox="964 1623 1455 1822">Cette commande supprime le fichier de sauvegarde de configuration sur le nœud spécifié uniquement. Si le fichier de sauvegarde de configuration existe également sur d'autres noeuds du cluster, il reste sur ces noeuds.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Recherchez un fichier de sauvegarde de configuration à utiliser pour restaurer un noeud

Vous utilisez un fichier de sauvegarde de configuration situé sur une URL distante ou sur un nœud du cluster pour restaurer une configuration de nœud.

### Description de la tâche

Vous pouvez utiliser un fichier de sauvegarde de configuration de cluster ou de nœud pour restaurer une configuration de nœud.

### Étape

1. Rendez le fichier de sauvegarde de configuration disponible pour le noeud pour lequel vous devez restaurer la configuration.

| Si le fichier de sauvegarde de configuration se trouve... | Alors...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sur une URL distante                                      | Utilisez le <code>system configuration backup download</code> commande au niveau de privilège avancé pour le télécharger sur le nœud restauré.                                                                                                                                                                                                                                                                                                                                                                                 |
| Sur un nœud du cluster                                    | <ol style="list-style-type: none"><li>a. Utilisez le <code>system configuration backup show</code> commande au niveau de privilège avancé pour afficher la liste des fichiers de sauvegarde de configuration disponibles dans le cluster contenant la configuration du nœud de restauration.</li><li>b. Si le fichier de sauvegarde de configuration que vous identifiez n'existe pas sur le nœud de récupération, utilisez le <code>system configuration backup copy</code> commande de copie sur le nœud restauré.</li></ol> |

Si vous avez précédemment recréé-crée le cluster, vous devez choisir un fichier de sauvegarde de configuration qui a été créé après la création du cluster. Si vous devez utiliser un fichier de sauvegarde de configuration qui a été créé avant le regroupement de loisirs, après avoir restauré le nœud, vous devez recréer le cluster.

## Restaurez la configuration du nœud à l'aide d'un fichier de sauvegarde de configuration

Vous restaurez la configuration du nœud à l'aide du fichier de sauvegarde de configuration que vous avez identifié et mis à la disposition du nœud de récupération.

### Description de la tâche

Vous ne devez effectuer cette tâche que pour effectuer une restauration suite à un incident entraînant la perte des fichiers de configuration locale du nœud.

### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```



2. Si le nœud fonctionne correctement, utilisez le au niveau de privilège avancé d'un autre nœud `cluster modify` commande avec `-node` et `-eligibility` paramètres pour le signaler non éligible et l'isoler du cluster.

Si le nœud n'est pas sain, ignorez cette étape.

Dans cet exemple, le nœud 2 est modifié pour ne pas participer au cluster afin que sa configuration puisse être restaurée :

```
cluster1::*> cluster modify -node node2 -eligibility false
```

3. Utilisez le `system configuration recovery node restore` commande au niveau de privilège avancé pour restaurer la configuration du nœud à partir d'un fichier de sauvegarde de configuration.

Si le nœud a perdu son identité, y compris son nom, vous devez utiliser le `-nodename-in-backup` paramètre pour spécifier le nom du nœud dans le fichier de sauvegarde de configuration.

Cet exemple restaure la configuration du nœud à l'aide de l'un des fichiers de sauvegarde de configuration stockés sur le nœud :

```
cluster1::*> system configuration recovery node restore -backup
cluster1.8hour.2011-02-22.18_15_00.7z
```

```
Warning: This command overwrites local configuration files with
files contained in the specified backup file. Use this
command only to recover from a disaster that resulted
in the loss of the local configuration files.
The node will reboot after restoring the local configuration.
Do you want to continue? {y|n}: y
```

La configuration est restaurée et le nœud redémarre.

4. Si vous avez indiqué que le nœud n'est pas éligible, utilisez le `system configuration recovery cluster sync` commande pour marquer le nœud comme éligible et le synchroniser avec le cluster.
5. Si vous travaillez dans un environnement SAN, utilisez le `system node reboot` Commande permettant de redémarrer le nœud et de rétablir le quorum SAN.

### Une fois que vous avez terminé

Si vous avez précédemment recréés le cluster, et si vous restaurez la configuration du nœud à l'aide d'un fichier de sauvegarde de configuration créé avant la recréation du cluster, vous devez recréer le cluster.

### Recherchez une configuration à utiliser pour la récupération d'un cluster

Vous utilisez la configuration à partir d'un nœud du cluster ou d'un fichier de sauvegarde de configuration de cluster pour restaurer un cluster.

### Étapes

1. Choisissez un type de configuration pour restaurer le cluster.

- Un nœud dans le cluster

Si le cluster se compose de plusieurs nœuds et que l'un des deux nœuds dispose d'une configuration de cluster depuis laquelle le cluster était dans la configuration souhaitée, vous pouvez restaurer le cluster à l'aide de la configuration stockée sur ce nœud.

Dans la plupart des cas, le nœud contenant l'anneau de réplication avec l'ID de transaction le plus récent est le nœud le plus adapté à la restauration de la configuration du cluster. Le `cluster ring show` la commande au niveau de privilège avancé vous permet d'afficher la liste des anneaux répliqués disponibles sur chaque nœud du cluster.

- Fichier de sauvegarde de la configuration du cluster

Si vous ne pouvez pas identifier un nœud avec la configuration de cluster appropriée ou si le cluster est composé d'un seul nœud, vous pouvez utiliser un fichier de sauvegarde de configuration de cluster pour restaurer le cluster.

Si vous récupérez le cluster à partir d'un fichier de sauvegarde de configuration, toute modification de configuration effectuée depuis la sauvegarde sera perdue. Après la restauration, vous devez résoudre tout écart entre le fichier de sauvegarde de configuration et la configuration actuelle. Consultez l'article de la base de connaissances ["Guide de résolution des sauvegardes de configuration ONTAP"](#) pour des conseils de dépannage.

2. Si vous choisissez d'utiliser un fichier de sauvegarde de configuration de cluster, mettez le fichier à disposition du nœud que vous prévoyez d'utiliser pour restaurer le cluster.

| Si le fichier de sauvegarde de configuration se trouve... | Alors...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sur une URL distante                                      | Utilisez le <code>system configuration backup download</code> commande au niveau de privilège avancé pour le télécharger sur le nœud restauré.                                                                                                                                                                                                                                                                                                                                                                                                         |
| Sur un nœud du cluster                                    | <ol style="list-style-type: none"> <li>Utilisez le <code>system configuration backup show</code> commande au niveau de privilège avancé pour trouver un fichier de sauvegarde de la configuration du cluster qui a été créé lorsque le cluster était dans la configuration souhaitée.</li> <li>Si le fichier de sauvegarde de configuration de cluster n'est pas situé sur le nœud que vous souhaitez utiliser pour restaurer le cluster, utilisez le <code>system configuration backup copy</code> commande de copie sur le nœud restauré.</li> </ol> |

## Restaurer une configuration de cluster à partir d'une configuration existante

Pour restaurer une configuration de cluster à partir d'une configuration existante après une défaillance de cluster, vous devez recréer le cluster à l'aide de la configuration de cluster que vous avez choisie et mise à disposition du nœud de récupération, puis vous devez relier chaque nœud supplémentaire au nouveau cluster.

## Description de la tâche

Vous ne devez effectuer cette tâche que pour effectuer une restauration après un incident ayant entraîné la perte de la configuration du cluster.



Si vous créez à nouveau le cluster à partir d'un fichier de sauvegarde de configuration, vous devez contacter le support technique pour résoudre tout écart entre le fichier de sauvegarde de configuration et la configuration présente dans le cluster.

Si vous récupérez le cluster à partir d'un fichier de sauvegarde de configuration, toute modification de configuration effectuée depuis la sauvegarde sera perdue. Après la restauration, vous devez résoudre tout écart entre le fichier de sauvegarde de configuration et la configuration actuelle. Consultez l'article de la base de connaissances ["Guide de résolution des sauvegardes de configuration ONTAP pour des conseils de dépannage"](#).

## Étapes

1. Désactiver le basculement du stockage pour chaque paire haute disponibilité :

```
storage failover modify -node node_name -enabled false
```

Il n'est nécessaire de désactiver qu'une seule fois le basculement du stockage pour chaque paire haute disponibilité. Lorsque vous désactivez le basculement du stockage pour un nœud, le basculement du stockage est également désactivé sur le partenaire du nœud.

2. Arrêtez chaque nœud sauf pour le nœud qui récupère :

```
system node halt -node node_name -reason "text"
```

```
cluster1::*> system node halt -node node0 -reason "recovering cluster"

Warning: Are you sure you want to halt the node? {y|n}: y
```

3. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

4. Sur le nœud de récupération, utilisez **system configuration recovery cluster recreate** commande pour recréer le cluster.

Cet exemple recrée le cluster à l'aide des informations de configuration stockées sur le nœud lors de la restauration :

```
cluster1::~*> configuration recovery cluster recreate -from node
```

```
Warning: This command will destroy your existing cluster. It will
 rebuild a new single-node cluster consisting of this node
 and its current configuration. This feature should only be
 used to recover from a disaster. Do not perform any other
 recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

Un nouveau cluster est créé sur le nœud restauré.

5. Si vous recréez le cluster à partir d'un fichier de sauvegarde de configuration, vérifiez que le cluster Recovery est toujours en cours :

**system configuration recovery cluster show**

Il n'est pas nécessaire de vérifier l'état de restauration du cluster si vous recréez le cluster à partir d'un nœud sain.

```
cluster1::~*> system configuration recovery cluster show
Recovery Status: in-progress
Is Recovery Status Persisted: false
```

6. Démarrez chaque nœud qui doit être rejoint au cluster recréé-crée.

Vous devez redémarrer les nœuds un par un.

7. Pour chaque nœud qui doit être joint au cluster recréé-crée, procédez comme suit :

- a. A partir d'un nœud sain sur le cluster recréé-crée, rrejoignez le nœud cible :

**system configuration recovery cluster rejoin -node node\_name**

Cet exemple rejoint le nœud cible « node2 » au cluster recréé-crée :

```
cluster1::~*> system configuration recovery cluster rejoin -node node2

Warning: This command will rejoin node "node2" into the local
 cluster, potentially overwriting critical cluster
 configuration files. This command should only be used
 to recover from a disaster. Do not perform any other
 recovery operations while this operation is in progress.
 This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

Le nœud cible redémarre, puis rejoint le cluster.

- b. Vérifier que le nœud cible est en bon état et qu'il a formé le quorum avec le reste des nœuds du cluster :

```
cluster show -eligibility true
```

Le nœud cible doit rejoindre à nouveau le cluster créé avant de pouvoir rejoindre un autre nœud.

```
cluster1::*> cluster show -eligibility true
Node Health Eligibility Epsilon

node0 true true false
node1 true true false
2 entries were displayed.
```

8. Si vous avez créé à nouveau le cluster à partir d'un fichier de sauvegarde de configuration, définissez l'état de restauration sur terminé :

```
system configuration recovery cluster modify -recovery-status complete
```

9. Retour au niveau de privilège admin :

```
set -privilege admin
```

10. Si le cluster comprend seulement deux nœuds, utilisez le **cluster ha modify** Commande pour réactiver le cluster HA.
11. Utilisez le **storage failover modify** Commande permettant de réactiver le basculement du stockage pour chaque paire haute disponibilité.

### Une fois que vous avez terminé

Si le cluster a des relations de paires SnapMirror, vous devez également les recréer. Pour plus d'informations, voir ["La protection des données"](#).

### Synchroniser un nœud avec le cluster

Si le quorum au niveau du cluster est atteint mais qu'un ou plusieurs nœuds ne sont pas synchronisés avec le cluster, il faut synchroniser le nœud pour restaurer la base de données répliquée (RDB) sur le nœud et la mettre au quorum.

#### Étape

1. Depuis un nœud sain, utilisez le `system configuration recovery cluster sync` commande au niveau de privilège avancé pour synchroniser le nœud qui est hors synchronisation avec la configuration du cluster.

Cet exemple synchronise un nœud (*node2*) avec le reste du cluster :

```
cluster1::*> system configuration recovery cluster sync -node node2
```

Warning: This command will synchronize node "node2" with the cluster configuration, potentially overwriting critical cluster configuration files on the node. This feature should only be used to recover from a disaster. Do not perform any other recovery operations while this operation is in progress. This command will cause all the cluster applications on node "node2" to restart, interrupting administrative CLI and Web interface on that node.

Do you want to continue? {y|n}: y

All cluster applications on node "node2" will be restarted. Verify that the cluster applications go online.

## Résultat

Le RDB est répliqué sur le nœud et le nœud devient éligible au cluster.

## Gestion des « core dumps » (administrateurs du cluster uniquement)

Lorsqu'un nœud fonctionne de façon incohérente, un « core dump » se produit et le système crée un fichier « core dump » que le support technique peut utiliser pour résoudre le problème. Vous pouvez configurer ou afficher les attributs de core dump. Vous pouvez également enregistrer, afficher, segmenter, charger ou supprimer un fichier de vidage de mémoire.

Vous pouvez gérer des « core dumps » des manières suivantes :

- Configuration des « core dumps » et affichage des paramètres de configuration
- Affichage des informations de base, de l'état et des attributs des « core dumps »

Les fichiers core dump et les rapports sont stockés dans le `/mroot/etc/crash/` répertoire d'un nœud. Vous pouvez afficher le contenu du répertoire à l'aide du `system node coredump commandes` ou un navigateur web.




- Enregistrement du contenu du core dump et chargement du fichier enregistré à un emplacement spécifié ou au support technique

ONTAP vous empêche de lancer l'enregistrement d'un fichier « core dump » lors d'un basculement, d'un transfert d'agrégat ou d'un rétablissement.

- Suppression des fichiers « core dump » qui ne sont plus nécessaires

## Commandes pour la gestion des « core dumps »

Vous utilisez le `system node coredump config commandes` permettant de gérer la configuration des « core dumps », le `system node coredump commandes` pour gérer les fichiers « core dump » et `system node coredump reports commandes` permettant de gérer les rapports de base de l'application.

| Les fonctions que vous recherchez...                                                       | Utilisez cette commande...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configurer les « core dumps »                                                              | <code>system node coredump config modify</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Affiche les paramètres de configuration des « core dumps »                                 | <code>system node coredump config show</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Affiche les informations de base relatives aux « core dumps »                              | <code>system node coredump show</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Déclenche manuellement un « core dump » lorsque vous redémarrez un nœud                    | <p><code>system node reboot</code> avec les deux <code>-dump</code> et <code>-skip-lif-migration-before-reboot</code> paramètres</p> <div>  <p>Le lien:<a href="https://docs.netapp.com/us-en/ontap-cli/system-node-reboot.html#parameters[skip-lif-migration-before-reboot]">https://docs.netapp.com/us-en/ontap-cli/system-node-reboot.html#parameters[skip-lif-migration-before-reboot]</a> Le paramètre spécifie que la migration de LIF avant un redémarrage sera ignorée.</p> </div> |
| Déclenche manuellement un « core dump » lorsque vous arrêtez un nœud                       | <p><code>system node halt</code> avec les deux <code>-dump</code> et <code>-skip-lif-migration-before-shutdown</code> paramètres</p> <div>  <p>Le lien:<a href="https://docs.netapp.com/us-en/ontap-cli/system-node-halt.html#parameters[skip-lif-migration-before-shutdown]">https://docs.netapp.com/us-en/ontap-cli/system-node-halt.html#parameters[skip-lif-migration-before-shutdown]</a> Le paramètre spécifie que la migration de LIF avant un arrêt sera ignorée.</p> </div>     |
| Enregistrer un « core dump » spécifié                                                      | <code>system node coredump save</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Enregistrez tous les « core dumps » non enregistrés sur un nœud spécifié                   | <code>system node coredump save-all</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Générez et envoyez un message AutoSupport avec un fichier « core dump » que vous spécifiez | <p><code>system node autosupport invoke-core-upload</code></p> <div>  <p>Le <code>-uri</code> Le paramètre facultatif indique une destination alternative pour le message AutoSupport.</p> </div>                                                                                                                                                                                                                                                                                        |
| Affiche les informations d'état relatives aux « core dumps »                               | <code>system node coredump status</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Les fonctions que vous recherchez...                                                                    | Utilisez cette commande...                       |
|---------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| Supprime un « core dump » spécifié                                                                      | <code>system node coredump delete</code>         |
| Supprimez tous les « core dumps » non enregistrés ou tous les fichiers « core » enregistrés sur un nœud | <code>system node coredump delete-all</code>     |
| Affiche les rapports de vidage de mémoire de l'application                                              | <code>system node coredump reports show</code>   |
| Supprimer un rapport de vidage de mémoire de l'application                                              | <code>system node coredump reports delete</code> |

#### Informations associées

["Référence de commande ONTAP"](#)

## Gestion des disques et des niveaux (agrégat)

### Présentation des disques et des niveaux locaux (agrégats)

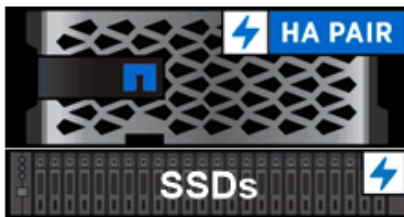
System Manager et l'interface de ligne de commandes vous permettent de gérer le stockage physique ONTAP. Vous pouvez créer, développer et gérer des niveaux locaux (agrégats), travailler avec les niveaux locaux Flash Pool (agrégats), gérer les disques et gérer les règles RAID.

#### De quels niveaux locaux (agrégats) sont-ils

*Local tiers* (également appelé *Aggregates*) sont des conteneurs pour les disques gérés par un nœud. Vous pouvez utiliser des niveaux locaux pour isoler des charges de travail présentant différents besoins en performances, hiérarchiser les données selon différents modèles d'accès ou isoler les données à des fins réglementaires.

- Vous pouvez créer un niveau local composé exclusivement de SSD pour les applications stratégiques qui nécessitent une latence la plus faible et des performances maximales.
- Pour hiérarchiser les données selon différents modèles d'accès, vous pouvez créer un *niveau local hybride* en déployant Flash comme cache haute performance pour un jeu de données de travail, tout en utilisant des disques durs à moindre coût ou un stockage objet pour les données moins fréquemment utilisées.
  - *Flash Pool* est composé à la fois de SSD et de disques durs.
  - Un *FabricPool* consiste en un niveau local tout SSD avec un magasin d'objets attaché.
- Si vous devez isoler les données archivées de données actives à des fins réglementaires, vous pouvez utiliser un niveau local composé de disques durs haute capacité ou encore une combinaison de disques durs performants et haute capacité.





Datacenter



Cloud

*You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed “hot” data and object storage for rarely accessed “cold” data.*

### Utilisation des niveaux locaux (agrégats)

Vous pouvez effectuer les tâches suivantes :

- ["Gestion des niveaux locaux \(agrégats\)"](#)
- ["Gérer les disques"](#)
- ["Gérer les configurations RAID"](#)
- ["Gestion des niveaux Flash Pool"](#)

Vous pouvez effectuer ces tâches si les conditions suivantes sont vraies :

- Vous ne souhaitez pas utiliser un outil de script automatique.
- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.
- Vous disposez d'une configuration MetroCluster et vous suivez les procédures décrites dans ["MetroCluster"](#) documentation sur la configuration initiale et les instructions relatives aux niveaux locaux (agrégats) et à la gestion des disques.

### Informations associées

- ["Gérer les niveaux clouds FabricPool"](#)

## Gestion des niveaux locaux (agrégats)

### Gestion des niveaux locaux (agrégats)

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour ajouter des tiers locaux (agrégats), gérer leur utilisation et leur ajouter de la capacité (disques).

Vous pouvez effectuer les tâches suivantes :

- ["Ajouter \(créer\) un niveau local \(agrégat\)"](#)

Pour ajouter un niveau local, suivez un flux de travail spécifique. Déterminez le nombre de disques ou de partitions de disque requis pour le niveau local et choisissez la méthode à utiliser pour créer le niveau local. Vous pouvez ajouter des niveaux locaux automatiquement en laissant à ONTAP l'attribuer ou vous pouvez spécifier manuellement la configuration.

- ["Gestion de l'utilisation de niveaux locaux \(agrégats\)"](#)

Pour les niveaux locaux existants, vous pouvez les renommer, définir les coûts des supports ou déterminer leurs informations de disque et de groupe RAID. Vous pouvez modifier la configuration RAID d'un niveau local et attribuer des niveaux locaux aux SVM (Storage VM).

Vous pouvez modifier la configuration RAID d'un niveau local et attribuer des niveaux locaux aux SVM (Storage VM). Vous pouvez déterminer quels volumes résident sur un niveau local, ainsi que la quantité d'espace qu'ils utilisent sur un niveau local. Vous pouvez contrôler la quantité d'espace que les volumes peuvent utiliser. Vous pouvez transférer la propriété des niveaux locaux avec une paire haute disponibilité. Vous pouvez également supprimer un niveau local.

- ["Ajout de capacité \(disques\) à un niveau local \(agrégat\)"](#)

En utilisant différentes méthodes, vous suivez un flux de travail spécifique pour ajouter de la capacité. Vous pouvez ajouter des disques à un niveau local et ajouter des disques à un nœud ou à un tiroir. Si nécessaire, vous pouvez corriger les partitions de rechange mal alignées.

## **Ajouter (créer) un niveau local (agrégat)**

### **Ajout d'un niveau local (création d'un agrégat)**

Pour ajouter un niveau local (créer un agrégat), il faut suivre un workflow spécifique.

Déterminez le nombre de disques ou de partitions de disque requis pour le niveau local et choisissez la méthode à utiliser pour créer le niveau local. Vous pouvez ajouter des niveaux locaux automatiquement en laissant à ONTAP l'attribuer ou vous pouvez spécifier manuellement la configuration.

- ["Flux de production pour l'ajout d'un niveau local \(agrégat\)"](#)
- ["Détermination du nombre de disques ou de partitions de disque requis pour un niveau local \(agrégat\)"](#)
- ["Choisissez la méthode de création du niveau local \(agrégat\) à utiliser "](#)
- ["Ajout automatique de niveaux locaux \(agrégats\)"](#)
- ["Ajoutez manuellement des niveaux locaux \(agrégats\)"](#)

### **Flux de production pour l'ajout d'un niveau local (agrégat)**

La création de niveaux locaux (agrégats) permet de stocker les volumes de votre système.

Le flux de production permettant de créer des niveaux locaux (agrégats) est spécifique à l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## **Workflow de System Manager**

### **Utilisez System Manager pour ajouter (créer) un niveau local**

System Manager crée des niveaux locaux en se basant sur les meilleures pratiques recommandées pour la configuration des niveaux locaux.

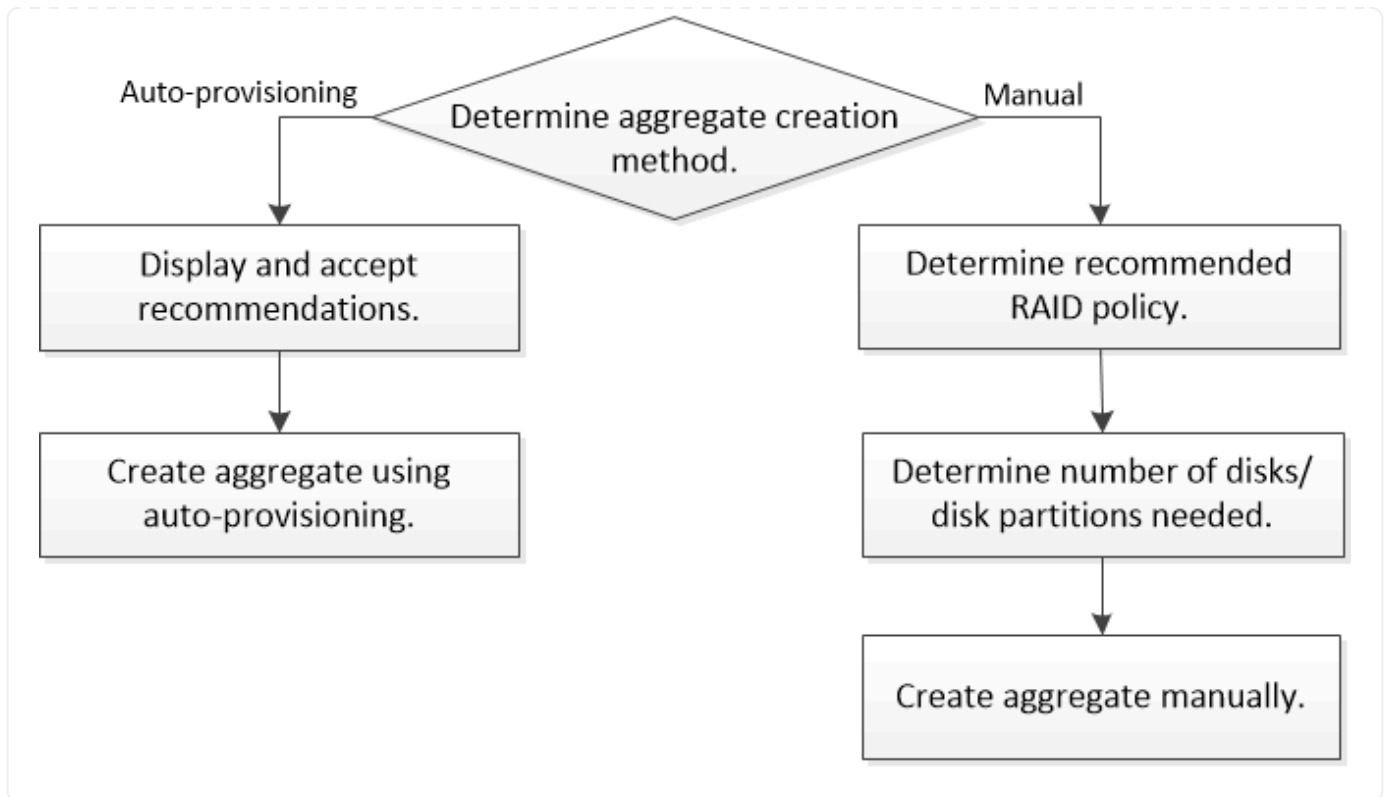
Depuis ONTAP 9.11.1, vous pouvez décider de configurer manuellement les niveaux locaux si vous souhaitez une configuration différente de celle recommandée lors du processus automatique pour ajouter un niveau local.



#### Flux de travail de l'interface de

#### Utilisez l'interface de ligne de commande pour ajouter (créer) un agrégat

Depuis ONTAP 9.2, ONTAP peut fournir des configurations recommandées lors de la création d'agrégats (provisionnement automatique). Si les configurations recommandées, en fonction des meilleures pratiques, sont appropriées dans votre environnement, vous pouvez les accepter de créer les agrégats. Sinon, vous pouvez créer des agrégats manuellement.



#### Détermination du nombre de disques ou de partitions de disque requis pour un niveau local (agrégat)

Vous devez disposer d'un nombre suffisant de disques ou de partitions de disque dans votre niveau local (agrégat) pour répondre aux exigences système et métier. Vous devez également disposer du nombre recommandé de disques de secours ou de partitions de disque de secours pour minimiser le risque de perte de données.

Le partitionnement données-racines est activé par défaut sur certaines configurations. Les systèmes sur lesquels le partitionnement données-racines est activé utilisent des partitions de disque pour créer des niveaux locaux. Les systèmes sur lesquels le partitionnement données-racines n'est pas activé utilisent des disques non partitionnés.

Vous devez disposer de suffisamment de disques ou de partitions de disque pour répondre au nombre minimal requis pour votre stratégie RAID et suffisant pour répondre à vos besoins en termes de capacité minimale.



Dans ONTAP, l'espace utilisable du disque est inférieur à la capacité physique du disque. Vous pouvez trouver l'espace utilisable d'un lecteur spécifique et le nombre minimal de disques ou de partitions de disque requis pour chaque stratégie RAID dans ["Hardware Universe"](#).

#### Détermination de l'espace utilisable d'un disque spécifique

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## System Manager

### Utilisez System Manager pour déterminer l'espace utilisable des disques

Procédez comme suit pour afficher la taille utilisable d'un disque :

#### Étapes

1. Accédez à **stockage > niveaux**
2. Cliquez sur  en regard du nom du niveau local.
3. Sélectionnez l'onglet **Disk information**.

#### CLI

### Utilisez l'interface de ligne de commande pour déterminer l'espace utilisable des disques

Pour afficher la taille utilisable d'un disque, procédez comme suit :

#### Étape

1. Affichage des informations sur le disque de spare :

```
storage aggregate show-spare-disks
```

Outre le nombre de disques ou de partitions de disque nécessaire pour créer votre groupe RAID et répondre à vos besoins en termes de capacité, vous devez également disposer du nombre minimal de disques de secours ou de partitions de disque de secours recommandé pour votre agrégat :

- Pour tous les agrégats Flash, vous devez disposer d'au moins un disque de secours ou une partition de disque.



La baie AFF C190 n'utilise par défaut aucun disque de spare. Cette exception est entièrement prise en charge.

- Pour les agrégats homogènes non Flash, vous devez disposer d'au moins deux disques de secours ou partitions de disque.
- Pour les pools de stockage SSD, vous devez disposer d'au moins un disque de secours pour chaque paire haute disponibilité.
- Pour les agrégats Flash Pool, vous devez disposer d'au moins deux disques de spare par paire haute disponibilité. Pour plus d'informations sur les règles RAID prises en charge pour les agrégats Flash Pool, consultez la ["Hardware Universe"](#).
- Pour prendre en charge l'utilisation du Maintenance Center et éviter les problèmes causés par plusieurs pannes simultanées de disques, vous devez disposer d'au moins quatre disques de secours dans des supports multiples.

#### Informations associées

["NetApp Hardware Universe"](#)

["Rapport technique NetApp 3838 : Guide de configuration du sous-système de stockage"](#)

## Choisir la méthode à utiliser pour créer des tiers locaux (agrégats)

Bien que ONTAP recommande l'ajout automatique de niveaux locaux (création d'agrégats avec provisionnement automatique) conformément aux meilleures pratiques, vous devez déterminer si les configurations recommandées sont prises en charge dans votre environnement. Si ce n'est pas le cas, vous devez prendre des décisions sur la stratégie RAID et la configuration du disque, puis créer les niveaux locaux manuellement.

Lors de la création automatique d'un niveau local, ONTAP analyse les disques de spare du cluster et génère une recommandation sur la façon d'utiliser les disques disponibles pour ajouter des tiers locaux conformément aux meilleures pratiques. ONTAP affiche les configurations recommandées. Vous pouvez accepter les recommandations ou ajouter les tiers locaux manuellement.

### Avant d'accepter les recommandations ONTAP

Si l'une des conditions de disque suivantes est présente, elles doivent être résolues avant d'accepter les recommandations de ONTAP :

- Disques manquants
- Fluctuation des numéros de disque disponibles
- Disques non assignés
- Pièces de rechange non remises à zéro
- Les disques sont soumis à un test de maintenance

Le `storage aggregate auto-provision` la page man contient plus d'informations sur ces exigences.

### Lorsque vous devez utiliser la méthode manuelle

Dans de nombreux cas, l'organisation recommandée du niveau local sera optimale pour votre environnement. Cependant, si votre cluster exécute ONTAP 9.1 ou une version antérieure, ou si votre environnement inclut les configurations suivantes, vous devez créer le niveau local à l'aide de la méthode manuelle.



Depuis ONTAP 9.11.1, vous pouvez ajouter manuellement des niveaux locaux avec System Manager.

- Agrégats utilisant des LUN de baies tierces
- Disques virtuels avec Cloud Volumes ONTAP ou ONTAP Select
- Système MetroCluster
- SyncMirror
- Disques MSATA
- Niveaux Flash Pool (agrégats)
- Plusieurs types ou tailles de disques sont connectés au nœud

### Sélectionnez la méthode de création des niveaux locaux (agrégats).

Choisissez la méthode que vous souhaitez utiliser :

- ["Ajoutez \(créez\) automatiquement des niveaux locaux \(agrégats\)"](#)

- ["Ajoutez \(créez\) des niveaux locaux \(agrégats\) manuellement"](#)

#### Informations associées

- ["Référence de commande ONTAP"](#)

#### Ajout automatique de niveaux locaux (création d'agrégats avec provisionnement automatique)

Ajout automatique d'un niveau local (création d'un agrégat avec auto-provisionnement) grâce aux recommandations de bonnes pratiques ONTAP

S'il convient à votre environnement, vous pouvez accepter la recommandation et laisser ONTAP ajouter le niveau local.

#### Avant de commencer

Les disques doivent être au sein d'un nœud avant de pouvoir être utilisés dans un niveau local (agrégat). Si votre cluster n'est pas configuré pour utiliser l'affectation automatique de propriété des disques, vous devez ["attribuer la propriété manuellement"](#).



## System Manager

### Étapes

1. Dans System Manager, cliquez sur **stockage > niveaux**.
2. Dans la page **tiers**, cliquez sur [+ Add Local Tier](#) pour créer un nouveau niveau local :

La page **Ajouter un niveau local** affiche le nombre recommandé de niveaux locaux qui peuvent être créés sur les nœuds et le stockage utilisable disponible.

3. Cliquez sur **Détails recommandés** pour afficher la configuration recommandée par System Manager.

System Manager affiche les informations suivantes à partir de ONTAP 9.8 :

- **Nom de niveau local** (vous pouvez modifier le nom de niveau local à partir de ONTAP 9.10.1)
- **Nom du nœud**
- **Taille utilisable**
- **Type de stockage**

À partir de ONTAP 9.10.1, des informations supplémentaires s'affichent :

- **Disques** : indique le nombre, la taille et le type des disques
- **Layout** : affiche la disposition du groupe RAID, y compris les disques de parité ou de données et les emplacements inutilisés.
- **Disques de rechange** : indique le nom du nœud, le nombre et la taille des disques de spare et le type de stockage.

4. Effectuez l'une des opérations suivantes :

| Si vous voulez...                                                                                        | Puis faites cela...                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Acceptez les recommandations de System Manager.                                                          | Passez à la section <a href="#">Étape de configuration du gestionnaire de clés intégré pour le chiffrement</a> .                                                                                                                                                                                                                                        |
| Configurez manuellement les niveaux locaux et <b>NOT</b> utilisez les recommandations de System Manager. | <p>Passez à la section <a href="#">"Ajout manuel d'un niveau local (création d'agrégat)"</a>:</p> <ul style="list-style-type: none"><li>• Pour ONTAP 9.10.1 et versions antérieures, suivez la procédure d'utilisation de l'interface de ligne de commandes.</li><li>• Depuis ONTAP 9.11.1, suivez la procédure pour utiliser System Manager.</li></ul> |

5. (facultatif) : si le gestionnaire de clés intégré a été installé, vous pouvez le configurer pour le chiffrement. Cochez la case **configurer le gestionnaire de clés intégré pour le chiffrement**.
  - a. Saisissez une phrase de passe.
  - b. Saisissez de nouveau la phrase de passe pour la confirmer.
  - c. Enregistrez la phrase de passe pour une utilisation ultérieure au cas où le système doit être restauré.

d. Sauvegarder la base de données clé pour une utilisation ultérieure.

6. Cliquez sur **Enregistrer** pour créer le niveau local et l'ajouter à votre solution de stockage.

## CLI

Vous exécutez le `storage aggregate auto-provision` commande permettant de générer des recommandations de disposition des agrégats. Vous pouvez ensuite créer des agrégats après la vérification et l'approbation des recommandations ONTAP.

### Ce dont vous avez besoin

ONTAP 9.2 ou version ultérieure doit être exécuté sur le cluster.

### Description de la tâche

Le récapitulatif par défaut généré avec le `storage aggregate auto-provision` commande répertorie les agrégats recommandés à créer, y compris les noms et la taille utilisable. Vous pouvez afficher la liste et déterminer si vous souhaitez créer les agrégats recommandés lorsque vous y êtes invité.

Vous pouvez également afficher un récapitulatif détaillé à l'aide de `-verbose` qui affiche les rapports suivants :

- Un récapitulatif par nœud des nouveaux agrégats permet de créer, découvrir des unités de rechange et les disques et partitions de rechange restants après la création de l'agrégat
- Nouveaux agrégats de données à créer avec le nombre de disques et de partitions à utiliser
- Disposition des groupes RAID montrant comment les disques et partitions de rechange seront utilisés dans les nouveaux agrégats de données à créer
- Détails sur les disques de spare et partitions restants après la création d'un agrégat

Si vous connaissez bien la méthode de provisionnement automatique et que votre environnement est correctement préparé, vous pouvez utiliser le `-skip-confirmation` option pour créer l'agrégat recommandé sans afficher ni confirmation. Le `storage aggregate auto-provision` La commande n'est pas affectée par la session de l'interface de ligne de commande `-confirmations` réglage.

Le lien:<https://docs.netapp.com/us-en/ontap-cli/storage-aggregate-auto-provision.html>[`storage aggregate auto-provision page man^`] contient des informations supplémentaires sur les recommandations de mise en page globale.

### Étapes

1. Exécutez le `storage aggregate auto-provision` commande avec les options d'affichage souhaitées.
  - Aucune option : afficher le résumé standard
  - `-verbose` Option : affiche un récapitulatif détaillé
  - `-skip-confirmation` Option : créez des agrégats recommandés sans afficher ni confirmation
2. Effectuez l'une des opérations suivantes :

|                   |                     |
|-------------------|---------------------|
| Si vous voulez... | Puis faites cela... |
|-------------------|---------------------|

|                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Acceptez les recommandations de ONTAP.</p>                                                                                                                                                     | <p>Vérifiez l'affichage des agrégats recommandés, puis répondez à l'invite pour créer les agrégats recommandés.</p> <pre> myA400-44556677::&gt; storage aggregate auto- provision Node                               New Data Aggregate Usable Size ----- ----- myA400-364                         myA400_364_SSD_1 3.29TB myA400-363                         myA400_363_SSD_1 1.46TB ----- ----- Total:                             2      new data aggregates 4.75TB  Do you want to create recommended aggregates? {y </pre> |
| <p>n}): y</p> <p>Info: Aggregate auto provision has started. Use the "storage aggregate show-auto-provision-progress" command to track the progress.</p> <p>myA400-44556677::&gt;</p> <p>----</p> | <p>Configurez manuellement les niveaux locaux et <b>NOT</b> utilisez les recommandations de ONTAP.</p>                                                                                                                                                                                                                                                                                                                                                                                                                          |

### Informations associées

- ["Référence de commande ONTAP"](#)

### Ajout manuel de niveaux locaux (création d'agrégats

Si vous ne souhaitez pas ajouter de niveau local (créer un agrégat) en suivant les recommandations sur les meilleures pratiques de ONTAP, vous pouvez effectuer la procédure manuellement.

### Avant de commencer

Les disques doivent être au sein d'un nœud avant de pouvoir être utilisés dans un niveau local (agrégat). Si votre cluster n'est pas configuré pour utiliser l'affectation automatique de propriété des disques, vous devez ["attribuer la propriété manuellement"](#).

## System Manager

Depuis ONTAP 9.11.1, si vous ne souhaitez pas utiliser la configuration recommandée par System Manager pour créer un niveau local, vous pouvez spécifier la configuration souhaitée.

### Étapes

1. Dans System Manager, cliquez sur **stockage > niveaux**.
2. Dans la page **tiers**, cliquez sur  **Add Local Tier** pour créer un nouveau niveau local :

La page **Ajouter un niveau local** affiche le nombre recommandé de niveaux locaux qui peuvent être créés sur les nœuds et le stockage utilisable disponible.

3. Lorsque System Manager affiche la recommandation de stockage pour le niveau local, cliquez sur **basculer vers création manuelle de niveau local** dans la section **disques de rechange**.

La page **Ajouter un niveau local** affiche les champs que vous utilisez pour configurer le niveau local.

4. Dans la première section de la page **Ajouter un niveau local**, procédez comme suit :
  - a. Entrez le nom du niveau local.
  - b. (Facultatif) : cochez la case **Symétrie de ce niveau local** si vous souhaitez mettre en miroir le niveau local.
  - c. Sélectionnez un type de disque.
  - d. Sélectionnez le nombre de disques.
5. Dans la section **Configuration RAID**, procédez comme suit :
  - a. Sélectionnez le type de RAID.
  - b. Sélectionnez la taille du groupe RAID.
  - c. Cliquez sur allocation RAID pour afficher la manière dont les disques sont alloués dans le groupe.
6. (Facultatif) : si le gestionnaire de clés intégré a été installé, vous pouvez le configurer pour le chiffrement dans la section **chiffrement** de la page. Cochez la case **configurer le gestionnaire de clés intégré pour le chiffrement**.
  - a. Saisissez une phrase de passe.
  - b. Saisissez de nouveau la phrase de passe pour la confirmer.
  - c. Enregistrez la phrase de passe pour une utilisation ultérieure au cas où le système doit être restauré.
  - d. Sauvegarder la base de données clé pour une utilisation ultérieure.
7. Cliquez sur **Enregistrer** pour créer le niveau local et l'ajouter à votre solution de stockage.

### CLI

Avant de créer des agrégats manuellement, il est recommandé de vérifier les options de configuration de disque et de simuler la création.

Vous pouvez alors lancer le `storage aggregate create` command et vérifier les résultats.

### Ce dont vous avez besoin

Vous devez avoir déterminé le nombre de disques et le nombre de disques de secours dont vous avez besoin dans l'agrégat.

### Description de la tâche

Si le partitionnement données-racines est activé et que votre configuration compte au moins 24 disques SSD, il est recommandé d'attribuer des partitions de données à différents nœuds.

La procédure de création d'agrégats sur des systèmes avec le partitionnement données-racines et le partitionnement données-racines est identique à la procédure de création d'agrégats sur des systèmes utilisant des disques non partitionnés. Si le partitionnement données-racines est activé sur votre système, vous devez utiliser le nombre de partitions de disque pour le système `-diskcount` option. Pour le partitionnement données-racines, le `-diskcount` spécifie le nombre de disques à utiliser.



Lors de la création de plusieurs agrégats à des fins d'utilisation avec FlexGroups, les agrégats doivent être de taille aussi proche que possible.

Le `storage aggregate create` la page man contient plus d'informations sur les options et les exigences de création d'agrégats.

### Étapes

1. Afficher la liste des partitions de disque de spare pour vérifier que vous avez assez pour créer votre agrégat :

```
storage aggregate show-spare-disks -original-owner node_name
```

Les partitions de données sont affichées sous `Local Data Usable`. Une partition racine ne peut pas être utilisée comme partition de rechange.

2. Simuler la création de l'agrégat :

```
storage aggregate create -aggregate aggregate_name -node node_name
-raidtype raid_dp -diskcount number_of_disks_or_partitions -simulate true
```

3. Si des avertissements s'affichent à partir de la commande simulée, ajustez la commande et répétez la simulation.

4. Créer l'agrégat :

```
storage aggregate create -aggregate aggr_name -node node_name -raidtype
raid_dp -diskcount number_of_disks_or_partitions
```

5. Afficher l'agrégat pour vérifier qu'il a été créé :

```
storage aggregate show-status aggregate_name
```

### Informations associées

- ["Référence de commande ONTAP"](#)

### Gestion de l'utilisation de niveaux locaux (agrégats)

#### Gestion de l'utilisation de niveaux locaux (agrégats)

Une fois que vous avez créé des niveaux locaux (agrégats), vous pouvez gérer leur utilisation.

Vous pouvez effectuer les tâches suivantes :

- "Renommer un niveau local (agrégat)"
- "Définir le coût du support pour un niveau local (agrégat)"
- "Déterminer les informations sur les disques et les groupes RAID pour un niveau local (agrégat)"
- "Assignation de niveaux locaux (agrégats) à des VM de stockage (SVM)"
- "Déterminer les volumes qui résident sur un niveau local (agrégat)"
- "Déterminer et contrôler l'utilisation de l'espace d'un volume dans un niveau local (agrégat)"
- "Déterminer l'utilisation de l'espace au niveau local (agrégat)"
- "Transférer la propriété de niveau local (agrégat) au sein d'une paire haute disponibilité"
- "Supprimer un niveau local (agrégat)"

### Renommer un niveau local (agrégat)


Vous pouvez renommer un niveau local (agrégat). La méthode à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

#### System Manager

##### Utilisez System Manager pour renommer un niveau local (agrégat)

Depuis ONTAP 9.10.1, vous pouvez modifier le nom d'un niveau local (agrégat).

#### Étapes

1. Dans System Manager, cliquez sur **stockage > niveaux**.
2. Cliquez sur  en regard du nom du niveau local.
3. Sélectionnez **Renommer**.
4. Spécifiez un nouveau nom pour le niveau local.

#### CLI

##### Utilisez l'interface de ligne de commande pour renommer un niveau local (agrégat)

#### Étape

1. À l'aide de l'interface de ligne de commandes, renommer le niveau local (agrégat) :

```
storage aggregate rename -aggregate aggr-name -newname aggr-new-name
```

L'exemple suivant renomme un agrégat nommé « aggr5 » en « sales-aggr » :

```
> storage aggregate rename -aggregate aggr5 -newname sales-aggr
```

### Définir le coût du support pour un niveau local (agrégat)

Depuis ONTAP 9.11.1, System Manager permet de définir le coût du support pour un niveau local (agrégat).

## Étapes

1. Dans System Manager, cliquez sur **stockage > niveaux**, puis sur **définir le coût du support** dans les mosaïques de niveau local (agrégat) souhaitées.
2. Sélectionnez **niveaux actifs et inactifs** pour activer la comparaison.
3. Entrez un type de devise et un montant.

Lorsque vous saisissez ou modifiez le coût du support, la modification est effectuée dans tous les types de support.

## Lecteurs à zéro rapide manuellement

Sur les systèmes récemment installés avec ONTAP 9.4 ou version ultérieure et les systèmes réinitialisés avec ONTAP 9.4 ou version ultérieure, *FAST remise à zéro* est utilisé pour zéro disque.

Avec *FAST remise à zéro*, les entraînements sont remis à zéro en secondes. Cette opération est effectuée automatiquement avant le provisionnement et réduit considérablement le temps nécessaire pour initialiser le système, créer des agrégats ou développer des agrégats lors de l'ajout de disques de rechange.

*Fast Rremise à zéro* est pris en charge à la fois sur les disques SSD et les disques durs.



*Fast remise à zéro* n'est pas pris en charge sur les systèmes mis à niveau à partir de ONTAP 9.3 ou version antérieure. ONTAP 9.4 ou version ultérieure doit être récemment installé ou le système doit être réinitialisé. Dans ONTAP 9.3 et versions antérieures, le processus de mise à zéro des disques est également automatique par ONTAP, mais ce processus prend plus de temps.

Si vous devez mettre manuellement à zéro un lecteur, vous pouvez utiliser l'une des méthodes suivantes. Dans ONTAP 9.4 et versions ultérieures, la remise à zéro manuelle d'un disque ne prend également que quelques secondes.

## Commande CLI

### Utilisez une commande CLI pour les disques rapides à zéro

#### Description de la tâche

Des privilèges d'administrateur sont requis pour utiliser cette commande.

#### Étapes

1. Entrez la commande CLI :

```
storage disk zerospares
```

## Options du menu de démarrage

### Sélectionnez les options du menu de démarrage sur disques rapides à zéro

#### Description de la tâche

- L'amélioration de la remise à zéro rapide ne prend pas en charge les systèmes mis à niveau depuis une version antérieure à ONTAP 9.4.
- Si un nœud du cluster contient un niveau local (agrégat) avec des disques à remise à zéro rapide, vous ne pouvez pas rétablir le cluster à la version ONTAP 9.2 ou antérieure.

#### Étapes

1. Dans le menu de démarrage, sélectionnez l'une des options suivantes :
  - (4) nettoyer la configuration et initialiser tous les disques
  - (9a) départition de tous les disques et suppression de leurs informations de propriété
  - (9b) nettoyer la configuration et initialiser le nœud avec des disques entiers

## Attribuer manuellement la propriété des disques

Les disques doivent être au sein d'un nœud avant de pouvoir être utilisés dans un niveau local (agrégat).

#### Description de la tâche

- Si vous attribuez manuellement la propriété d'une paire haute disponibilité qui n'est pas initialisée et ne dispose pas uniquement de tiroirs DS460C, utilisez l'option 1.
- Si vous initialisez une paire haute disponibilité ne comportant que des tiroirs DS460C, utilisez l'option 2 pour attribuer manuellement la propriété des disques racines.



## Option 1 : la plupart des paires haute disponibilité

Si vous disposez d'une paire haute disponibilité qui n'est pas initialisée et ne dispose pas uniquement de tiroirs DS460C, utilisez cette procédure pour attribuer manuellement la propriété.

### Description de la tâche

- Les disques pour lesquels vous attribuez la propriété doivent se trouver dans un tiroir physiquement connecté au nœud auquel vous êtes propriétaire.
- Si vous utilisez des disques d'un niveau local (agrégat) :
  - Les disques doivent être au sein d'un nœud avant de pouvoir être utilisés dans un niveau local (agrégat).
  - Vous ne pouvez pas réaffecter la propriété d'un disque utilisé dans un niveau local (agrégat).

### Étapes

1. Utiliser l'interface de ligne de commande pour afficher tous les disques non détenus :

```
storage disk show -container-type unassigned
```

2. Affectez chaque disque :

```
storage disk assign -disk disk_name -owner owner_name
```

Vous pouvez utiliser le caractère générique pour attribuer plusieurs disques à la fois. Si vous réassignez un disque de réserve qui appartient déjà à un nœud différent, vous devez utiliser l'option "-force".

## Option 2 : une paire haute disponibilité avec seulement des tiroirs DS460C

Pour une paire haute disponibilité que vous initialisez et qui ne possède que des tiroirs DS460C, utilisez cette procédure pour attribuer manuellement la propriété des disques racine.

### Description de la tâche

- Lorsque vous initialisez une paire haute disponibilité ne comportant que des tiroirs DS460C, vous devez attribuer manuellement les disques racines afin de respecter la règle relative au demi-tiroir.

Après l'initialisation (démarrage) des paires haute disponibilité, l'assignation automatique de la propriété des disques est automatiquement activée et utilise la règle du demi-tiroir pour attribuer la propriété aux disques restants (autres que les disques racines) et à tous les disques ajoutés à l'avenir, comme le remplacement des disques défectueux, répondant au message de « faible capacité », ou en ajoutant de la capacité.

Pour en savoir plus sur la politique de demi-tiroir, consultez le sujet ["À propos de l'assignation automatique de Disk Ownership"](#).

- La technologie RAID nécessite un minimum de 10 disques par paire haute disponibilité (5 pour chaque nœud) pour tout disque NL-SAS de plus de 8 To dans un tiroir DS460C.

### Étapes

1. Si vos étagères DS460C ne sont pas entièrement remplies, procédez comme suit ; sinon, passez à l'étape suivante.

- a. Installez tout d'abord les lecteurs dans la rangée avant (baies de lecteurs 0, 3, 6 et 9) de chaque tiroir.

L'installation des entraînements dans la rangée avant de chaque tiroir permet un débit d'air correct et empêche la surchauffe.

- b. Pour les disques restants, répartissez-les uniformément entre les tiroirs.

Remplissez les rangées de tiroirs d'avant en arrière. Si vous ne disposez pas de suffisamment de disques pour remplir les rangées, installez-les par paires de sorte que les disques occupent les côtés gauche et droit d'un tiroir de manière uniforme.

L'illustration suivante montre la numérotation et les emplacements des baies de lecteur dans un tiroir DS460C.



2. Connectez-vous au cluster shell en utilisant la LIF node-management ou la LIF cluster-management.
3. Attribuez manuellement les lecteurs racine de chaque tiroir pour qu'ils soient conformes à la stratégie demi-tiroir à l'aide des sous-étapes suivantes :

La règle demi-tiroir vous permet d'affecter la moitié gauche des lecteurs d'un tiroir (baies 0 à 5) au nœud A et la moitié droite des lecteurs d'un tiroir (baies 6 à 11) au nœud B.

- a. Afficher tous les disques non possédés :

```
storage disk show -container-type unassigned`
```

- b. Assigner les disques root:

```
storage disk assign -disk disk_name -owner owner_name
```

Vous pouvez utiliser le caractère générique pour attribuer plusieurs disques à la fois.

#### Déterminer les informations sur les disques et les groupes RAID pour un niveau local (agrégat)

Certaines tâches d'administration de niveau local (agrégat) nécessitent de savoir quels types de disques composent le niveau local, leur taille, leur checksum et leur état, qu'ils soient partagés avec d'autres niveaux locaux, ainsi que la taille et la composition des groupes RAID.

#### Étape

1. Afficher les disques de l'agrégat, par groupe RAID :

```
storage aggregate show-status aggr_name
```

Les disques sont affichés pour chaque groupe RAID de l'agrégat.

Vous pouvez afficher le type RAID du disque (données, parité, parité) dans le `Position` colonne. Si le `Position` s'affiche `shared`, Le lecteur est ensuite partagé : s'il s'agit d'un disque dur, il s'agit d'un disque partitionné ; s'il s'agit d'un disque SSD, il fait partie d'un pool de stockage.

```
cluster1::> storage aggregate show-status nodeA_fp_1
```

Owner Node: cluster1-a

Aggregate: nodeA\_fp\_1 (online, mixed\_raid\_type, hybrid) (block checksums)

Plex: /nodeA\_fp\_1/plex0 (online, normal, active, pool0)

RAID Group /nodeA\_fp\_1/plex0/rg0 (normal, block checksums, raid\_dp)

| Position | Disk   | Pool | Type | RPM   | Usable Size | Physical Size | Status   |
|----------|--------|------|------|-------|-------------|---------------|----------|
| shared   | 2.0.1  | 0    | SAS  | 10000 | 472.9GB     | 547.1GB       | (normal) |
| shared   | 2.0.3  | 0    | SAS  | 10000 | 472.9GB     | 547.1GB       | (normal) |
| shared   | 2.0.5  | 0    | SAS  | 10000 | 472.9GB     | 547.1GB       | (normal) |
| shared   | 2.0.7  | 0    | SAS  | 10000 | 472.9GB     | 547.1GB       | (normal) |
| shared   | 2.0.9  | 0    | SAS  | 10000 | 472.9GB     | 547.1GB       | (normal) |
| shared   | 2.0.11 | 0    | SAS  | 10000 | 472.9GB     | 547.1GB       | (normal) |

RAID Group /nodeA\_flashpool\_1/plex0/rg1

(normal, block checksums, raid4) (Storage Pool: SmallSP)

| Position | Disk   | Pool | Type | RPM | Usable Size | Physical Size | Status   |
|----------|--------|------|------|-----|-------------|---------------|----------|
| shared   | 2.0.13 | 0    | SSD  | -   | 186.2GB     | 745.2GB       | (normal) |
| shared   | 2.0.12 | 0    | SSD  | -   | 186.2GB     | 745.2GB       | (normal) |

8 entries were displayed.

### Assignation de niveaux locaux (agrégats) à des VM de stockage (SVM)

Si vous attribuez un ou plusieurs niveaux locaux (agrégats) à une machine virtuelle de stockage (Storage VM ou SVM, anciennement appelée Vserver), vous pouvez uniquement utiliser les niveaux locaux pour contenir des volumes pour cette machine virtuelle de stockage (SVM).

#### Ce dont vous avez besoin

La machine virtuelle de stockage et les niveaux locaux que vous souhaitez attribuer à cette machine virtuelle de stockage doivent déjà exister.

#### Description de la tâche

En attribuant des niveaux locaux à vos VM de stockage, il est important d'isoler les VM de stockage les uns des autres. C'est particulièrement important dans un environnement en colocation.

#### Étapes

1. Vérifier la liste des niveaux locaux (agrégats) déjà affectés à la SVM :

```
vserver show -fields aggr-list
```

Les agrégats actuellement affectés au SVM sont affichés. Si aucun agrégat n'est attribué, "-" s'affiche.

2. Ajoutez ou supprimez des agrégats affectés, selon vos besoins :

| Les fonctions que vous recherchez...   | Utilisez cette commande...             |
|----------------------------------------|----------------------------------------|
| Attribuez des agrégats supplémentaires | <code>vserver add-aggregates</code>    |
| Annuler l'attribution des agrégats     | <code>vserver remove-aggregates</code> |

Les agrégats répertoriés sont affectés ou supprimés du SVM. Si le SVM possède déjà des volumes qui utilisent un agrégat qui n'est pas affecté à la SVM, un message d'avertissement est affiché, mais la commande se termine avec succès. Tous les agrégats qui ont déjà été affectés au SVM et qui n'ont pas été nommés dans la commande ne sont pas affectés.

### Exemple

Dans l'exemple suivant, les agrégats `aggr1` et `aggr2` sont affectés à SVM `svm1` :

```
vserver add-aggregates -vserver svm1 -aggregates aggr1,aggr2
```

### Déterminer les volumes qui résident sur un niveau local (agrégat)

Vous devrez peut-être déterminer quels volumes résident sur un niveau local (agrégat) avant d'effectuer des opérations sur le niveau local, par exemple le déplacer ou le mettre hors ligne.

### Étapes

1. Pour afficher les volumes qui résident sur un agrégat, entrez

```
volume show -aggregate aggregate_name
```

Tous les volumes qui résident sur l'agrégat spécifié sont affichés.

### Déterminer et contrôler l'utilisation de l'espace d'un volume dans un niveau local (agrégat)

Vous pouvez déterminer quels volumes FlexVol utilisent le plus d'espace d'un niveau local (agrégat) et, plus précisément, les fonctionnalités du volume.

Le `volume show-footprint` la commande fournit des informations sur l'empreinte d'un volume ou son utilisation de l'espace dans l'agrégat contenant.

Le `volume show-footprint` la commande affiche des détails sur l'utilisation de l'espace pour chaque volume d'un agrégat, y compris les volumes offline. Cette commande permet de rapprocher l'écart entre la sortie du `volume show-space` et `aggregate show-space` commandes. Tous les pourcentages sont calculés en pourcentage de la taille de l'agrégat.

L'exemple suivant montre le `volume show-footprint` sortie de la commande pour un volume appelé `testvol` :

```
cluster1::> volume show-footprint testvol
```

```
Vserver : thevs
Volume : testvol
```

| Feature                  | Used    | Used% |
|--------------------------|---------|-------|
| -----                    | -----   | ----- |
| Volume Data Footprint    | 120.6MB | 4%    |
| Volume Guarantee         | 1.88GB  | 71%   |
| Flexible Volume Metadata | 11.38MB | 0%    |
| Delayed Frees            | 1.36MB  | 0%    |
| Total Footprint          | 2.01GB  | 76%   |

Le tableau suivant explique certaines lignes clés de la sortie du `volume show-footprint` commande et ce que vous pouvez faire pour essayer de réduire l'utilisation de l'espace grâce à cette fonctionnalité :

| Nom de ligne/fonction    | Description/contenu de la ligne                                                                                                                                                                                       | D'autres façons de diminuer                                                                                                              |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Volume Data Footprint    | Quantité totale d'espace utilisé dans l'agrégat contenant les données d'un volume dans le système de fichiers actif et l'espace utilisé par les copies Snapshot du volume. Cette ligne n'inclut pas l'espace réservé. | <ul style="list-style-type: none"> <li>Suppression des données du volume.</li> <li>Suppression des copies Snapshot du volume.</li> </ul> |
| Volume Guarantee         | Quantité d'espace réservé par le volume dans l'agrégat pour les écritures ultérieures. La quantité d'espace réservé dépend du type de garantie du volume.                                                             | Modification du type de garantie du volume à <code>none</code> .                                                                         |
| Flexible Volume Metadata | Quantité totale d'espace utilisé dans l'agrégat par les fichiers de métadonnées du volume.                                                                                                                            | Pas de méthode directe de contrôle.                                                                                                      |
| Delayed Frees            | Les blocs utilisés par ONTAP pour la performance et qui ne peuvent pas être immédiatement libérés. Pour les destinations SnapMirror, cette ligne a une valeur 0 et ne s'affiche pas.                                  | Pas de méthode directe de contrôle.                                                                                                      |
| File Operation Metadata  | Quantité totale d'espace réservé pour les métadonnées de l'opération de fichier.                                                                                                                                      | Pas de méthode directe de contrôle.                                                                                                      |

|                 |                                                                                                     |                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Total Footprint | Quantité totale d'espace que le volume utilise dans l'agrégat. C'est la somme de toutes les lignes. | Toutes les méthodes utilisées pour diminuer l'espace utilisé par un volume. |
|-----------------|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|

### Informations associées

"Rapport technique NetApp 3483 : « Thin Provisioning » dans un environnement d'entreprise NetApp SAN ou IP SAN"

### Déterminer l'utilisation de l'espace au niveau local (agrégat)

Vous pouvez afficher la quantité d'espace utilisée par tous les volumes d'un ou plusieurs niveaux locaux (agrégats) afin de libérer de l'espace.

WAFL réserve un pourcentage de l'espace disque total pour les métadonnées et les performances au niveau de l'agrégat. L'espace utilisé pour la maintenance des volumes de l'agrégat vient de la réserve WAFL et ne peut pas être modifié.

Dans les agrégats de moins de 30 To, WAFL réserve 10 % de l'espace disque total pour les métadonnées et les performances au niveau de l'agrégat.

À partir de ONTAP 9.12.1, dans des agrégats de 30 To ou plus, la quantité d'espace disque réservé pour les métadonnées et les performances au niveau de l'agrégat diminue. L'espace utilisable des agrégats est donc 5 % plus important. La disponibilité de ces économies d'espace varie en fonction de votre plateforme et de votre version d'ONTAP.

| Espace disque réservé par ONTAP dans les agrégats de 30 To ou plus | S'applique aux plates-formes      | Dans les versions ONTAP              |
|--------------------------------------------------------------------|-----------------------------------|--------------------------------------|
| 5 %                                                                | Toutes les plateformes AFF et FAS | ONTAP 9.14.1 et versions ultérieures |
| 5 %                                                                | Plateformes AFF et FAS500f        | ONTAP 9.12.1 et versions ultérieures |
| 10 %                                                               | Toutes les plateformes            | ONTAP 9.11.1 et versions ultérieures |

Vous pouvez afficher l'utilisation de l'espace par tous les volumes d'un ou plusieurs agrégats avec `aggregate show-space` commande. Cela vous permet de déterminer quels volumes consomment le plus d'espace de leurs agrégats contenant afin de pouvoir mettre en œuvre des actions pour libérer plus d'espace.

L'espace utilisé d'un agrégat est directement affecté par l'espace utilisé sur les volumes FlexVol qu'il contient. Les mesures que vous prenez pour augmenter l'espace d'un volume affectent également l'espace de l'agrégat.



À partir de ONTAP 9.15.1, deux nouveaux compteurs de métadonnées sont disponibles. En plus des modifications apportées à plusieurs compteurs existants, vous pouvez obtenir une vue plus claire de la quantité de données utilisateur allouées. Voir "[Détermination de l'espace dans un volume ou un agrégat](#)" pour en savoir plus.

Les lignes suivantes sont incluses dans le `aggregate show-space` sortie de la commande :

- **Empreintes de volume**

Total de l'ensemble des empreintes des volumes de l'agrégat. Il inclut tout l'espace utilisé ou réservé par

toutes les données et métadonnées de tous les volumes de l'agrégat contenant.

- **Métadonnées agrégées**

L'ensemble des métadonnées du système de fichiers requises par l'agrégat, telles que les bitmaps d'allocation et les fichiers d'inodes.

- **Réserve snapshot**

Quantité d'espace réservé pour les copies Snapshot de l'agrégat, sur la base de la taille du volume. Elle est considérée comme un espace utilisé et n'est pas disponible pour le volume, l'agrégat des données ou des métadonnées.

- **Réserve snapshot inutilisable**

Quantité d'espace initialement allouée à la réserve Snapshot de l'agrégat non disponible pour les copies Snapshot de l'agrégat, car elle est utilisée par les volumes associés à l'agrégat. Ne peut avoir lieu que pour les agrégats avec une réserve Snapshot d'agrégat non nulle.

- **Total utilisé**

Somme de l'espace utilisé ou réservé dans l'agrégat par volumes, métadonnées ou copies Snapshot.

- **Physique totale utilisée**

Quantité d'espace utilisée pour les données actuellement (au lieu d'être exclusivement réservée à une utilisation ultérieure). Inclut l'espace utilisé par les copies Snapshot de l'agrégat.

L'exemple suivant montre le `aggregate show-space` Sortie de la commande d'un agrégat dont la réserve Snapshot est de 5 %. Si la réserve Snapshot était 0, la ligne ne s'affiche pas.

```
cluster1::> storage aggregate show-space
```

Aggregate : wqa\_gx106\_aggr1

| Feature             | Used       | Used%  |
|---------------------|------------|--------|
| -----               | -----      | -----  |
| Volume Footprints   | 101.0MB    | 0%     |
| Aggregate Metadata  | 300KB      | 0%     |
| Snapshot Reserve    | 5.98GB     | 5%     |
| <br>Total Used      | <br>6.07GB | <br>5% |
| Total Physical Used | 34.82KB    | 0%     |

#### Informations associées

- ["Article de la base de connaissances : utilisation de l'espace"](#)
- ["Libérez jusqu'à 5 % de capacité en passant à ONTAP 9.12.1"](#)



## Transférer la propriété d'un niveau local (agrégat) au sein d'une paire haute disponibilité

Vous pouvez modifier la propriété des niveaux locaux (agrégats) entre les nœuds d'une paire haute disponibilité sans interrompre les services des niveaux locaux.

Les deux nœuds d'une paire haute disponibilité sont physiquement connectés aux disques ou aux LUN de baie des autres. Chaque LUN de disque ou de baie est détenue par un des nœuds.

La propriété de tous les disques ou LUN de baie au sein d'un niveau local (agrégat) passe temporairement d'un nœud à l'autre lorsqu'un basculement se produit. Cependant, les opérations de relocalisation des niveaux locaux peuvent également modifier définitivement la propriété (par exemple, si elles sont effectuées pour équilibrer la charge). La propriété change sans processus de copie des données ni déplacement physique des disques ou des LUN de baies.

### Description de la tâche

- Comme les limites de nombre de volumes sont validées par programmation lors des opérations de relocalisation de niveau local, il n'est pas nécessaire de vérifier cette valeur manuellement.

Si le nombre de volumes dépasse la limite prise en charge, l'opération de transfert de niveau local échoue et un message d'erreur s'affiche.

- Vous ne devez pas lancer le transfert de niveau local lorsque des opérations au niveau du système sont en cours sur le nœud source ou de destination ; de même, vous ne devez pas démarrer ces opérations pendant le transfert de niveau local.

Ces opérations peuvent inclure les opérations suivantes :

- Basculement
- Rétablissement
- Arrêt
- Une autre opération de transfert de niveau local
- Évolution de la propriété des disques
- Opérations locales de configuration du niveau ou des volumes
- Remplacement du contrôleur de stockage
- Mise à niveau de ONTAP
- Restauration de ONTAP
- Si vous disposez d'une configuration MetroCluster, vous ne devez pas lancer la relocalisation des niveaux locaux pendant que les opérations de reprise sur incident (*basculement*, *rétablissement* ou *rétablissement*) sont en cours.
- Si vous disposez d'une configuration MetroCluster et que vous lancez une relocalisation des niveaux locaux sur un niveau local commuté, l'opération peut échouer car elle dépasse le nombre maximal de volumes du partenaire de DR.
- Vous ne devez pas lancer le transfert de niveau local sur des agrégats corrompus ou soumis à des opérations de maintenance.
- Avant de lancer la relocalisation des niveaux locaux, vous devez enregistrer les « core dumps » sur les nœuds source et de destination.

### Étapes

1. Afficher les agrégats du nœud pour vérifier quels agrégats déplacer et vérifier qu'ils sont en ligne et en bon état :

```
storage aggregate show -node source-node
```

La commande suivante montre six agrégats sur les quatre nœuds du cluster. Tous les agrégats sont en ligne. NODE1 et NODE3 forment une paire HA, tandis que les nœuds 2 et Node4 forment une paire HA.

```
cluster::> storage aggregate show
Aggregate Size Available Used% State #Vols Nodes RAID Status

aggr_0 239.0GB 11.13GB 95% online 1 node1 raid_dp, normal
aggr_1 239.0GB 11.13GB 95% online 1 node1 raid_dp, normal
aggr_2 239.0GB 11.13GB 95% online 1 node2 raid_dp, normal
aggr_3 239.0GB 11.13GB 95% online 1 node2 raid_dp, normal
aggr_4 239.0GB 238.9GB 0% online 5 node3 raid_dp, normal
aggr_5 239.0GB 239.0GB 0% online 4 node4 raid_dp, normal
6 entries were displayed.
```

2. Lancer la commande pour démarrer le transfert d'agrégat :

```
storage aggregate relocation start -aggregate-list aggregate-1, aggregate-2...
-node source-node -destination destination-node
```

La commande suivante déplace les agrégats aggr\_1 et aggr\_2 du nœud 1 vers le nœud 3. Node4 est le partenaire HA de Node1. Les agrégats ne peuvent être déplacés qu'au sein de la paire haute disponibilité.

```
cluster::> storage aggregate relocation start -aggregate-list aggr_1,
aggr_2 -node node1 -destination node3
Run the storage aggregate relocation show command to check relocation
status.
node1::storage aggregate>
```

3. Suivre la progression du transfert d'agrégats avec le storage aggregate relocation show commande :

```
storage aggregate relocation show -node source-node
```

La commande suivante affiche la progression des agrégats en cours de déplacement vers le nœud 3 :

```
cluster::> storage aggregate relocation show -node node1
Source Aggregate Destination Relocation Status

node1
 aggr_1 node3 In progress, module: waf1
 aggr_2 node3 Not attempted yet
2 entries were displayed.
node1::storage aggregate>
```

Lorsque la relocalisation est terminée, la sortie de cette commande affiche chaque agrégat avec un statut de relocalisation "Done".

### Supprimer un niveau local (agrégat)

Vous pouvez supprimer un niveau local (agrégat) s'il n'y a pas de volumes au niveau local.

Le `storage aggregate delete` commande supprime un agrégat de stockage. La commande échoue si des volumes sont présents sur l'agrégat. Si l'agrégat dispose d'un magasin d'objets associé, alors en plus de supprimer l'agrégat, la commande supprime également les objets du magasin d'objets. Aucune modification n'a été apportée à la configuration du magasin d'objets dans le cadre de cette commande.

L'exemple suivant supprime un agrégat nommé « aggr1 » :

```
> storage aggregate delete -aggregate aggr1
```

### Commandes de transfert d'agrégats

Il existe des commandes ONTAP spécifiques pour déplacer la propriété des agrégats au sein d'une paire haute disponibilité.

| Les fonctions que vous recherchez...            | Utilisez cette commande...                      |
|-------------------------------------------------|-------------------------------------------------|
| Démarrer le processus de transfert d'agrégats   | <code>storage aggregate relocation start</code> |
| Surveiller le processus de transfert d'agrégats | <code>storage aggregate relocation show</code>  |

### Informations associées

- ["Référence de commande ONTAP"](#)

### Commandes de gestion des agrégats

Vous utilisez le `storage aggregate` commande de gestion de vos agrégats.

| Les fonctions que vous recherchez...                             | Utilisez cette commande...                                                                         |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Afficher la taille du cache pour tous les agrégats Flash Pool    | <code>storage aggregate show -fields hybrid-cache-size-total -hybrid-cache-size-total &gt;0</code> |
| Affichage des informations et de l'état des disques d'un agrégat | <code>storage aggregate show-status</code>                                                         |
| Affiche les disques de spare par nœud                            | <code>storage aggregate show-spare-disks</code>                                                    |
| Afficher les agrégats racine dans le cluster                     | <code>storage aggregate show -has-mroot true</code>                                                |
| Affiche les informations de base et l'état des agrégats          | <code>storage aggregate show</code>                                                                |
| Afficher le type de stockage utilisé dans un agrégat             | <code>storage aggregate show -fields storage-type</code>                                           |
| Mettre un agrégat en ligne                                       | <code>storage aggregate online</code>                                                              |
| Supprimer un agrégat                                             | <code>storage aggregate delete</code>                                                              |
| Placer un agrégat dans l'état restreint                          | <code>storage aggregate restrict</code>                                                            |
| Renommer un agrégat                                              | <code>storage aggregate rename</code>                                                              |
| Mettre un agrégat hors ligne                                     | <code>storage aggregate offline</code>                                                             |
| Modifier le type RAID d'un agrégat                               | <code>storage aggregate modify -raidtype</code>                                                    |

#### Informations associées

- ["Référence de commande ONTAP"](#)

#### Ajout de capacité (disques) à un niveau local (agrégat)

##### Ajout de capacité (disques) à un niveau local (agrégat)

En utilisant différentes méthodes, vous suivez un flux de travail spécifique pour ajouter de la capacité.

- ["Flux de production permettant d'ajouter de la capacité à un niveau local \(agrégat\)"](#)
- ["Méthodes de création d'espace au niveau local \(agrégat\)"](#)

Vous pouvez ajouter des disques à un niveau local et ajouter des disques à un nœud ou à un tiroir.

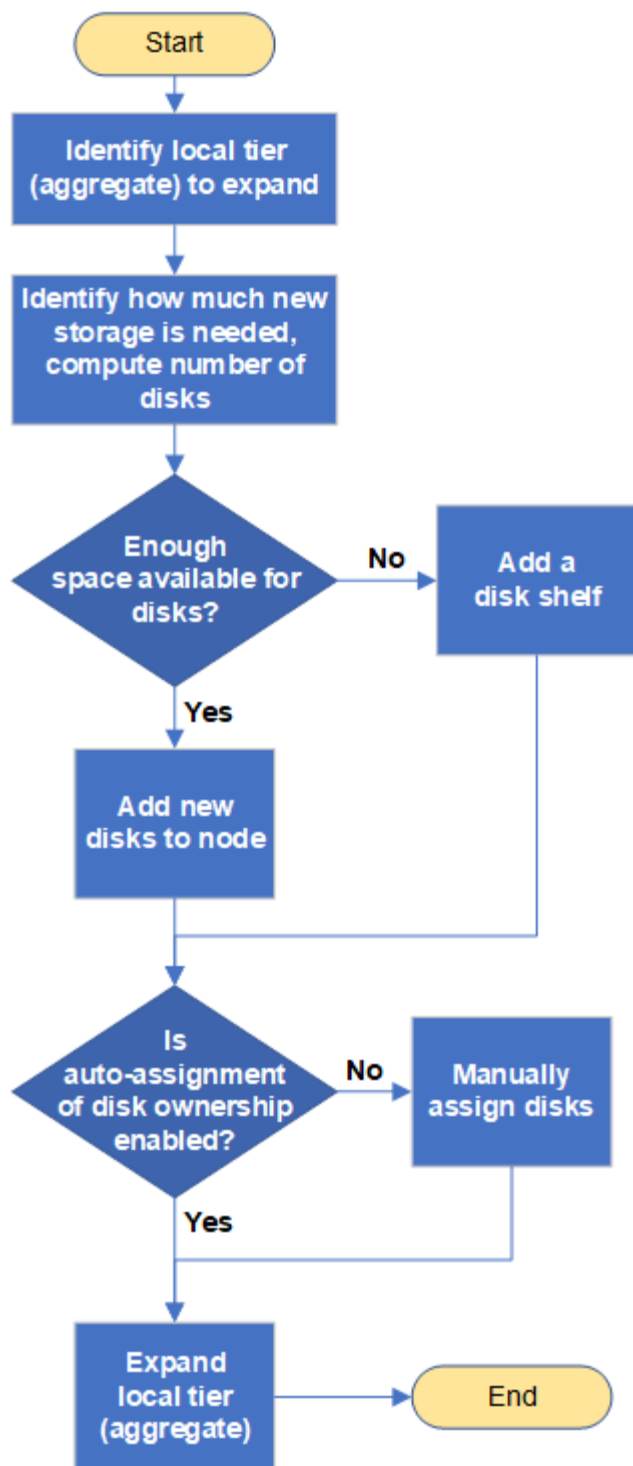
Si nécessaire, vous pouvez corriger les partitions de rechange mal alignées.

- "Ajout de disques à un niveau local (agrégat)"
- "Ajout de disques à un nœud ou un tiroir"
- "Corrigez les partitions de rechange mal alignées"

**Flux de production : ajout de capacité à un niveau local (développement d'un agrégat)**

Pour ajouter de la capacité à un niveau local (développez un agrégat), vous devez d'abord identifier le niveau local à ajouter, déterminer la quantité de stockage nécessaire, installer de nouveaux disques, attribuer la propriété du disque et créer un nouveau groupe RAID, le cas échéant.

Vous pouvez ajouter de la capacité via System Manager ou l'interface de ligne de commandes.



#### Méthodes de création d'espace au niveau local (agrégat)

Si un niveau local (agrégat) vient à manquer d'espace disponible, plusieurs problèmes peuvent survenir pendant la perte de données ou la désactivation de la garantie d'un volume. Il existe plusieurs façons de libérer de l'espace dans un niveau local.

Toutes les méthodes ont des conséquences diverses. Avant de prendre des mesures, vous devez lire la section appropriée de la documentation.

Les méthodes suivantes permettent de créer de l'espace dans le niveau local, en fonction des conséquences

les plus fréquentes :

- Ajouter des disques au niveau local.
- Déplacez certains volumes vers un autre niveau local avec l'espace disponible.
- Réduisez la taille des volumes garantis par volume dans le Tier local.
- Supprimez les copies Snapshot du volume inutiles si le type de garantie du volume est « none ».
- Supprimez les volumes inutiles.
- Activation de fonctionnalités gain d'espace, comme la déduplication ou la compression
- (Temporairement) désactivez les fonctions qui utilisent un grand nombre de métadonnées .

**Ajout de capacité à un niveau local (ajout de disques à un agrégat)**

Vous pouvez ajouter des disques à un niveau local (agrégat), afin d'augmenter le stockage des volumes qui lui sont associés.

## System Manager (ONTAP 9.8 et versions ultérieures)

### Utilisez System Manager pour ajouter de la capacité (ONTAP 9.8 et versions ultérieures)

Vous pouvez ajouter de la capacité à un niveau local en ajoutant des disques de capacité.




Depuis ONTAP 9.12.1, vous pouvez utiliser System Manager pour afficher la capacité engagée d'un niveau local afin de déterminer si la capacité supplémentaire est requise pour le niveau local. Voir "[Contrôle de la capacité dans System Manager](#)".

#### Description de la tâche

Cette tâche n'est effectuée que si vous avez installé ONTAP 9.8 ou une version ultérieure. Si vous avez installé une version antérieure de ONTAP, reportez-vous à l'onglet (ou à la section) intitulé « Gestionnaire système (ONTAP 9.7 et versions antérieures) ».

«.

#### Étapes

1. Cliquez sur **stockage > niveaux**.
2. Cliquez sur  en regard du nom du niveau local auquel vous souhaitez ajouter de la capacité.
3. Cliquez sur **Ajouter capacité**.



S'il n'y a pas de disques de réserve que vous pouvez ajouter, l'option **Ajouter capacité** n'est pas affichée et vous ne pouvez pas augmenter la capacité du niveau local.

4. Effectuer les étapes suivantes, en fonction de la version de ONTAP installée :

| Si cette version de ONTAP est installée... | Procédez comme suit...                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ONTAP 9.8, 9.9 ou 9.10.1                   | <ol style="list-style-type: none"><li>a. Si le nœud contient plusieurs niveaux de stockage, sélectionnez le nombre de disques que vous souhaitez ajouter au niveau local. Sinon, si le nœud contient uniquement un seul niveau de stockage, la capacité ajoutée est estimée automatiquement.</li><li>b. Cliquez sur <b>Ajouter</b>.</li></ol> |
| À partir d'ONTAP 9.11.1                    | <ol style="list-style-type: none"><li>a. Sélectionnez le type et le nombre de disques.</li><li>b. Si vous souhaitez ajouter des disques à un nouveau groupe RAID, cochez la case. L'allocation RAID s'affiche.</li><li>c. Cliquez sur <b>Enregistrer</b>.</li></ol>                                                                           |

5. (Facultatif) le processus prend un certain temps. Si vous souhaitez exécuter le processus en arrière-plan, sélectionnez **Exécuter en arrière-plan**.
6. Une fois le processus terminé, vous pouvez afficher la capacité accrue dans les informations de niveau local à **Storage > tiers**.

## System Manager (ONTAP 9.7 et versions antérieures)

### Utilisez System Manager pour ajouter de la capacité (ONTAP 9.7 et versions antérieures)

Vous pouvez ajouter de la capacité à un niveau local (agrégat) en ajoutant des disques de capacité.



## Description de la tâche

Cette tâche n'est effectuée que si vous avez installé ONTAP 9.7 ou une version antérieure. Si vous avez installé ONTAP 9.8 ou une version ultérieure, reportez-vous à [Utilisez System Manager pour ajouter de la capacité \(ONTAP 9.8 ou version ultérieure\)](#).

## Étapes

1. (Pour ONTAP 9.7 uniquement) cliquez sur \* (revenir à la version classique)\*.
2. Cliquez sur **matériel et diagnostics > agrégats**.
3. Sélectionnez l'agrégat auquel vous souhaitez ajouter des disques de capacité, puis cliquez sur **actions > Ajouter de la capacité**.



Il faut ajouter des disques de la même taille que les autres disques de l'agrégat.

4. (Pour ONTAP 9.7 uniquement) cliquez sur **passer à la nouvelle expérience**.
5. Cliquez sur **stockage > niveaux** pour vérifier la taille du nouvel agrégat.

## CLI

### Utilisez l'interface de ligne de commande pour ajouter de la capacité

La procédure d'ajout de disques partitionnés à un agrégat est similaire à la procédure d'ajout de disques non partitionnés.

### Ce dont vous avez besoin

Vous devez savoir à quelle taille de groupe RAID est destinée à l'agrégat que vous ajoutez le stockage.

## Description de la tâche

Lorsque vous développez un agrégat, vous devez savoir si vous ajoutez des partitions ou des disques non partitionnés à cet agrégat. Lorsque vous ajoutez des disques non partitionnés à un agrégat existant, la taille des groupes RAID existants est héritée par le nouveau groupe RAID, ce qui peut affecter le nombre de disques de parité requis. Si un disque non partitionné est ajouté à un groupe RAID composé de disques partitionnés, le nouveau disque est partitionné, laissant ainsi une partition de rechange inutilisée.

Lorsque vous provisionnez des partitions, vous devez vous assurer que vous ne laissez pas le nœud sans un disque dont les deux partitions sont de rechange. Dans ce cas, et le nœud subit une perturbation du contrôleur, des informations précieuses sur le problème (le fichier « core ») risquent de ne pas être disponibles pour le support technique.



N'utilisez pas le `disklist` commande d'extension de vos agrégats. Cela pourrait entraîner un mauvais alignement de la partition.

## Étapes

1. Afficher le stockage disponible de réserve sur le système qui possède l'agrégat :

```
storage aggregate show-spare-disks -original-owner node_name
```

Vous pouvez utiliser le `-is-disk-shared` paramètre permettant d'afficher uniquement les disques partitionnés ou les disques non partitionnés.

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true
```

Original Owner: cl1-s2

Pool0

Shared HDD Spares

|                           |         |        |      | Local |                 |
|---------------------------|---------|--------|------|-------|-----------------|
| Local                     |         |        |      | Data  |                 |
| Root Physical             |         |        |      |       |                 |
| Disk                      |         |        | Type | RPM   | Checksum Usable |
| Usable                    | Size    | Status |      |       |                 |
| -----                     |         |        |      |       |                 |
| 1.0.1                     |         |        | BSAS | 7200  | block 753.8GB   |
| 73.89GB                   | 828.0GB | zeroed |      |       |                 |
| 1.0.2                     |         |        | BSAS | 7200  | block 753.8GB   |
| 0B                        | 828.0GB | zeroed |      |       |                 |
| 1.0.3                     |         |        | BSAS | 7200  | block 753.8GB   |
| 0B                        | 828.0GB | zeroed |      |       |                 |
| 1.0.4                     |         |        | BSAS | 7200  | block 753.8GB   |
| 0B                        | 828.0GB | zeroed |      |       |                 |
| 1.0.8                     |         |        | BSAS | 7200  | block 753.8GB   |
| 0B                        | 828.0GB | zeroed |      |       |                 |
| 1.0.9                     |         |        | BSAS | 7200  | block 753.8GB   |
| 0B                        | 828.0GB | zeroed |      |       |                 |
| 1.0.10                    |         |        | BSAS | 7200  | block 0B        |
| 73.89GB                   | 828.0GB | zeroed |      |       |                 |
| 2 entries were displayed. |         |        |      |       |                 |

## 2. Afficher les groupes RAID actuels de l'agrégat :

```
storage aggregate show-status aggr_name
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1
```

Owner Node: cl1-s2

Aggregate: data\_1 (online, raid\_dp) (block checksums)

Plex: /data\_1/plex0 (online, normal, active, pool0)

RAID Group /data\_1/plex0/rg0 (normal, block checksums)

|          | Position | Disk  | Pool | Type | RPM     | Usable Size | Physical Size | Status |
|----------|----------|-------|------|------|---------|-------------|---------------|--------|
|          | -----    | ----- | ---- | ---- | -----   | -----       | -----         |        |
| -----    |          |       |      |      |         |             |               |        |
| shared   | 1.0.10   | 0     | BSAS | 7200 | 753.8GB | 828.0GB     |               |        |
| (normal) |          |       |      |      |         |             |               |        |
| shared   | 1.0.5    | 0     | BSAS | 7200 | 753.8GB | 828.0GB     |               |        |
| (normal) |          |       |      |      |         |             |               |        |
| shared   | 1.0.6    | 0     | BSAS | 7200 | 753.8GB | 828.0GB     |               |        |
| (normal) |          |       |      |      |         |             |               |        |
| shared   | 1.0.11   | 0     | BSAS | 7200 | 753.8GB | 828.0GB     |               |        |
| (normal) |          |       |      |      |         |             |               |        |
| shared   | 1.0.0    | 0     | BSAS | 7200 | 753.8GB | 828.0GB     |               |        |
| (normal) |          |       |      |      |         |             |               |        |

5 entries were displayed.

### 3. Simuler l'ajout du stockage à l'agrégat :

```
storage aggregate add-disks -aggregate aggr_name -diskcount
number_of_disks_or_partitions -simulate true
```

Vous pouvez voir le résultat de l'ajout de stockage sans provisionner réellement du stockage. Si des avertissements s'affichent à partir de la commande simulée, vous pouvez régler la commande et répéter la simulation.

```
cl1-s2::> storage aggregate add-disks -aggregate aggr_test
-diskcount 5 -simulate true
```

Disks would be added to aggregate "aggr\_test" on node "cl1-s2" in the following manner:

First Plex

```
RAID Group rg0, 5 disks (block checksum, raid_dp)

Physical Usable
Position Disk Type Size
Size

shared 1.11.4 SSD 415.8GB
415.8GB
shared 1.11.18 SSD 415.8GB
415.8GB
shared 1.11.19 SSD 415.8GB
415.8GB
shared 1.11.20 SSD 415.8GB
415.8GB
shared 1.11.21 SSD 415.8GB
415.8GB
```

Aggregate capacity available for volume use would be increased by 1.83TB.

#### 4. Ajouter le stockage à l'agrégat :

```
storage aggregate add-disks -aggregate aggr_name -raidgroup new -diskcount
number_of_disks_or_partitions
```

Lorsque vous créez un agrégat Flash Pool, si vous ajoutez des disques avec un checksum différent de celui de l'agrégat, ou si vous ajoutez des disques à un checksum mixte, vous devez utiliser le `-checksumstyle` paramètre.

Si vous ajoutez des disques à un agrégat Flash Pool, vous devez utiliser le `-disktype` paramètre pour spécifier le type de disque.

Vous pouvez utiliser le `-disksize` paramètre permettant de spécifier la taille des disques à ajouter. Seuls les disques avec une taille spécifiée approximativement sont sélectionnés pour être supplémentaires à l'agrégat.

```
cl1-s2::> storage aggregate add-disks -aggregate data_1 -raidgroup
new -diskcount 5
```

5. Vérifiez que l'ajout du stockage a réussi :

```
storage aggregate show-status -aggregate aggr_name
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1
```

Owner Node: c11-s2

```
Aggregate: data_1 (online, raid_dp) (block checksums)
```

```
Plex: /data 1/plex0 (online, normal, active, pool0)
```

```
RAID Group /data_1/plex0/rg0 (normal, block checksums)
```

| Physical                   |        |      |       |       |         | Usable |
|----------------------------|--------|------|-------|-------|---------|--------|
| Position                   | Disk   | Pool | Type  | RPM   | Size    |        |
| Size                       | Status |      |       |       |         |        |
| -----                      | -----  | ---- | ----- | ----- | -----   |        |
| shared                     | 1.0.10 | 0    | BSAS  | 7200  | 753.8GB |        |
| 828.0GB (normal)           |        |      |       |       |         |        |
| shared                     | 1.0.5  | 0    | BSAS  | 7200  | 753.8GB |        |
| 828.0GB (normal)           |        |      |       |       |         |        |
| shared                     | 1.0.6  | 0    | BSAS  | 7200  | 753.8GB |        |
| 828.0GB (normal)           |        |      |       |       |         |        |
| shared                     | 1.0.11 | 0    | BSAS  | 7200  | 753.8GB |        |
| 828.0GB (normal)           |        |      |       |       |         |        |
| shared                     | 1.0.0  | 0    | BSAS  | 7200  | 753.8GB |        |
| 828.0GB (normal)           |        |      |       |       |         |        |
| shared                     | 1.0.2  | 0    | BSAS  | 7200  | 753.8GB |        |
| 828.0GB (normal)           |        |      |       |       |         |        |
| shared                     | 1.0.3  | 0    | BSAS  | 7200  | 753.8GB |        |
| 828.0GB (normal)           |        |      |       |       |         |        |
| shared                     | 1.0.4  | 0    | BSAS  | 7200  | 753.8GB |        |
| 828.0GB (normal)           |        |      |       |       |         |        |
| shared                     | 1.0.8  | 0    | BSAS  | 7200  | 753.8GB |        |
| 828.0GB (normal)           |        |      |       |       |         |        |
| shared                     | 1.0.9  | 0    | BSAS  | 7200  | 753.8GB |        |
| 828.0GB (normal)           |        |      |       |       |         |        |
| 10 entries were displayed. |        |      |       |       |         |        |

6. Vérifiez que le nœud dispose toujours d'au moins un lecteur avec la partition racine et la partition de données en tant que disque de rechange :

```
storage aggregate show-spare-disks -original-owner node name
```

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true
```

Original Owner: cl1-s2

Pool0

Shared HDD Spares

|                           |          |                | Local |              |
|---------------------------|----------|----------------|-------|--------------|
|                           |          |                |       | Data         |
| Root                      | Physical |                |       |              |
| Disk                      |          |                | Type  | RPM Checksum |
| Usable                    | Size     | Status         |       | Usable       |
| 1.0.1                     | 73.89GB  | 828.0GB zeroed | BSAS  | 7200 block   |
| 1.0.10                    | 73.89GB  | 828.0GB zeroed | BSAS  | 7200 block   |
| 2 entries were displayed. |          |                |       |              |

#### Ajout de disques à un nœud ou un tiroir

Vous ajoutez des disques à un nœud ou un tiroir pour augmenter le nombre de disques de secours ou ajouter de l'espace au niveau local (agrégat).

#### Avant de commencer

Le lecteur que vous souhaitez ajouter doit être pris en charge par votre plate-forme. Vous pouvez confirmer à l'aide du ["NetApp Hardware Universe"](#).

Le nombre minimum de disques que vous devez ajouter en une seule procédure est de six. L'ajout d'un disque unique peut réduire les performances.

#### Étapes pour le NetApp Hardware Universe

1. Dans le menu déroulant **produits**, sélectionnez votre configuration matérielle
2. Sélectionnez votre plate-forme.
3. Sélectionnez la version de ONTAP que vous exécutez, puis **Afficher les résultats**.
4. Sous le graphique, sélectionnez **cliquez ici pour voir d'autres vues**. Choisissez la vue qui correspond à votre configuration.



### Procédure d'installation des lecteurs

1. Vérifier le ["Site de support NetApp"](#) Pour les derniers fichiers de firmware de tiroir et de disque et de package de qualification de disque.

Si vos nœuds ou tiroirs ne disposent pas des dernières versions, mettez-les à jour avant d'installer le nouveau disque.

Le firmware des disques est automatiquement mis à jour (sans interruption) sur les nouveaux lecteurs qui ne disposent pas de versions de micrologiciel actuelles.

2. Mettez-vous à la terre.
3. Retirez délicatement le cache de l'avant de la plate-forme.
4. Identifiez le logement approprié pour le nouveau lecteur.



Les emplacements appropriés pour l'ajout de disques varient en fonction du modèle de plate-forme et de la version ONTAP. Dans certains cas, vous devez ajouter des lecteurs à des slots spécifiques dans l'ordre indiqué. Par exemple, dans un AFF A800, vous ajoutez les disques à des intervalles spécifiques, en laissant les clusters de slots vides. Ensuite, dans une solution AFF A220, vous ajoutez de nouveaux disques aux emplacements vides suivants, de l'extérieur vers le milieu du shelf.

Reportez-vous aux étapes de la section **avant de commencer** pour identifier les emplacements appropriés pour votre configuration dans le ["NetApp Hardware Universe"](#).

5. Insérez le nouveau lecteur :
  - a. Avec la poignée de came en position ouverte, utilisez les deux mains pour insérer le nouvel entraînement.
  - b. Poussez jusqu'à ce que l'entraînement s'arrête.
  - c. Fermez la poignée de came de façon à ce que le lecteur soit bien en place dans le plan médian et que la poignée s'enclenche. Assurez-vous de fermer lentement la poignée de came de manière à ce qu'elle s'aligne correctement sur la face de l'entraînement.
6. Vérifiez que le voyant d'activité du lecteur (vert) est allumé.

Lorsque le voyant d'activité du lecteur est allumé, cela signifie que le lecteur est alimenté. Lorsque le voyant d'activité du lecteur clignote, cela signifie que le lecteur est alimenté et que les E/S sont en cours. Si le micrologiciel du lecteur est mis à jour automatiquement, le voyant clignote.

7. Pour ajouter un autre lecteur, répétez les étapes 4 à 6.

Les nouveaux disques ne sont pas reconnus tant qu'ils ne sont pas attribués à un nœud. Vous pouvez attribuer les nouveaux disques manuellement ou patienter jusqu'à ce que ONTAP affecte automatiquement les nouveaux disques si le nœud respecte les règles d'affectation automatique des disques.

8. Une fois tous les nouveaux disques identifiés, vérifiez qu'ils ont été ajoutés et que leur propriété est correctement spécifiée.

## Étapes de confirmation de l'installation

1. Afficher la liste des disques :

```
storage aggregate show-spare-disks
```

Vous devez voir les nouveaux disques, qui appartiennent au nœud approprié.

2. **En option (pour ONTAP 9.3 et versions antérieures uniquement)**, mettre à zéro les nouveaux lecteurs ajoutés :

```
storage disk zerospares
```

Les disques utilisés précédemment dans un niveau local ONTAP (agrégat) doivent être mis à zéro avant de pouvoir être ajoutés à un autre agrégat. Dans la version ONTAP 9.3 et antérieure, la remise à zéro peut prendre des heures, en fonction de la taille des disques non mis à zéro dans le nœud. La mise à zéro des disques évite les retards si vous devez augmenter rapidement la taille d'un niveau local. Ce n'est pas un problème dans ONTAP 9.4 ou version ultérieure où les disques sont remis à zéro à l'aide de *FAST remise à zéro* qui ne prend que quelques secondes.

## Résultats

Les nouveaux disques sont prêts. Vous pouvez les ajouter à un niveau local (agrégat), les placer dans la liste des disques de secours ou les ajouter lors de la création d'un niveau local.

### Corrigez les partitions de rechange mal alignées

Lorsque vous ajoutez des disques partitionnés à un niveau local (agrégat), vous devez laisser un disque dont la partition racine et la partition de données sont disponibles en tant que réserve pour chaque nœud. Si ce n'est pas le cas et que le nœud subit une perturbation, ONTAP ne peut pas transférer le « core » vers la partition de données de secours.

### Avant de commencer

Vous devez disposer d'une partition de données libre et d'une partition racine libre sur le même type de disque appartenant au même nœud.

## Étapes

1. À l'aide de l'interface de ligne de commande, affichez les partitions de rechange pour le nœud :

```
storage aggregate show-spare-disks -original-owner node_name
```

Notez quel disque dispose d'une partition de données libre (données\_réserve) et quel disque dispose d'une partition racine libre (source\_réserve). La partition de rechange affiche une valeur différente de zéro sous Local Data Usable ou Local Root Usable colonne.

2. Remplacez le disque par une partition de données de rechange par le disque avec la partition racine de rechange :

```
storage disk replace -disk spare_data -replacement spare_root -action start
```



Vous pouvez copier les données dans un sens ou dans l'autre. Toutefois, la copie de la partition racine prend moins de temps.

3. Surveillez la progression du remplacement des disques :

```
storage aggregate show-status -aggregate aggr_name
```

4. Une fois l'opération de remplacement terminée, affichez à nouveau les pièces de rechange pour confirmer que vous disposez d'un disque de secours complet :

```
storage aggregate show-spare-disks -original-owner node_name
```

Vous devriez voir un disque de secours avec de l'espace utilisable sous « données locales utilisables » et Local Root Usable.

### Exemple

Vous affichez vos partitions de rechange pour le nœud c1-01 et voyez que vos partitions de rechange ne sont pas alignées :

```
c1::> storage aggregate show-spare-disks -original-owner c1-01
```

Original Owner: c1-01

Pool0

Shared HDD Spares

| Disk   | Type | RPM  | Checksum | Local<br>Data<br>Usable | Local<br>Root<br>Usable | Physical<br>Size |
|--------|------|------|----------|-------------------------|-------------------------|------------------|
| 1.0.1  | BSAS | 7200 | block    | 753.8GB                 | 0B                      | 828.0GB          |
| 1.0.10 | BSAS | 7200 | block    | 0B                      | 73.89GB                 | 828.0GB          |

Vous lancez la tâche de remplacement de disque :

```
c1::> storage disk replace -disk 1.0.1 -replacement 1.0.10 -action start
```

Pendant que vous attendez la fin de l'opération de remplacement, vous affichez la progression de l'opération :

```
c1::> storage aggregate show-status -aggregate aggr0_1
```

Owner Node: c1-01

Aggregate: aggr0\_1 (online, raid\_dp) (block checksums)

Plex: /aggr0\_1/plex0 (online, normal, active, pool0)

RAID Group /aggr0\_1/plex0/rg0 (normal, block checksums)

|          |        |      |      |      |         | Usable Physical | Status                        |
|----------|--------|------|------|------|---------|-----------------|-------------------------------|
| Position | Disk   | Pool | Type | RPM  | Size    | Size            |                               |
| shared   | 1.0.1  | 0    | BSAS | 7200 | 73.89GB | 828.0GB         | (replacing, copy in progress) |
| shared   | 1.0.10 | 0    | BSAS | 7200 | 73.89GB | 828.0GB         | (copy 63% completed)          |
| shared   | 1.0.0  | 0    | BSAS | 7200 | 73.89GB | 828.0GB         | (normal)                      |
| shared   | 1.0.11 | 0    | BSAS | 7200 | 73.89GB | 828.0GB         | (normal)                      |
| shared   | 1.0.6  | 0    | BSAS | 7200 | 73.89GB | 828.0GB         | (normal)                      |
| shared   | 1.0.5  | 0    | BSAS | 7200 | 73.89GB | 828.0GB         | (normal)                      |

Une fois l'opération de remplacement terminée, vérifiez que vous disposez d'un disque de secours complet :

```
ie2220::> storage aggregate show-spare-disks -original-owner c1-01
```

Original Owner: c1-01

Pool0

Shared HDD Spares

|       |      |      |          | Local   | Local   | Physical |
|-------|------|------|----------|---------|---------|----------|
|       |      |      |          | Data    | Root    |          |
| Disk  | Type | RPM  | Checksum | Usable  | Usable  | Size     |
| 1.0.1 | BSAS | 7200 | block    | 753.8GB | 73.89GB | 828.0GB  |

## Gérer les disques

### Présentation de la gestion des disques

Vous pouvez effectuer diverses procédures de gestion des disques du système.

- **Aspects de la gestion des disques**

- ["Lorsque vous devez mettre à jour le progiciel de qualification des disques"](#)
- ["Fonctionnement des disques de secours"](#)
- ["Quel est le niveau de faible niveau d'avertissement de disque de secours pouvant vous aider à gérer vos disques de secours"](#)
- ["Options supplémentaires de gestion du partitionnement données-racines"](#)

- **Propriété du disque et de la partition**

- ["Propriété du disque et de la partition"](#)
- **Échec du retrait du disque**
  - ["Retirez un disque défectueux"](#)
- **Nettoyage de disque**
  - ["Nettoyage de disque"](#)

## Fonctionnement des disques de secours

Un disque de secours est un disque affecté à un système de stockage et prêt à l'emploi, mais qui n'est pas utilisé par un groupe RAID et ne contient aucune donnée.

Si une panne de disque se produit au sein d'un groupe RAID, le disque de secours est automatiquement affecté au groupe RAID pour remplacer les disques défectueux. Les données du disque défaillant sont reconstruites en arrière-plan sur le disque de remplacement de disque de secours du disque de parité RAID. L'activité de reconstruction est consignée dans le `/etc/message` Fichier et un message AutoSupport est envoyé.

Si le disque de secours disponible n'est pas de la même taille que le disque en panne, un disque de la taille supérieure suivante est choisi, puis inférieur pour correspondre à la taille du disque qu'il remplace.

## Exigences de rechange pour les supports de disques multiples

Pour optimiser la redondance du stockage et réduire au maximum le temps passé par ONTAP à copier les disques, il est essentiel de conserver le nombre de disques de secours sur des supports multiples.

Vous devez maintenir en permanence au moins deux disques de secours pour les disques multi-disques. Pour prendre en charge l'utilisation du Maintenance Center et éviter les problèmes causés par plusieurs pannes simultanées de disques, vous devez conserver au moins quatre disques de secours en vue d'un fonctionnement stable et remplacer rapidement les disques défectueux.

Si deux disques tombent en panne en même temps avec seulement deux disques de secours disponibles, ONTAP risque de ne pas pouvoir échanger le contenu du disque défectueux et de son support s'accoupler avec les disques de rechange. Ce scénario est appelé impasse. Si cela se produit, vous êtes averti par l'intermédiaire de messages EMS et AutoSupport. Lorsque les supports de remplacement sont disponibles, vous devez suivre les instructions fournies par les messages EMS.

Pour plus d'informations, consultez l'article de la base de connaissances ["La mise en page RAID ne peut pas être recrée automatiquement - message AutoSupport"](#)

## Quel est le niveau de faible niveau d'avertissement de disque de secours pouvant vous aider à gérer vos disques de secours

Par défaut, des avertissements sont émis sur la console et des journaux si vous avez moins d'un disque de secours qui correspond aux attributs de chaque disque de votre système de stockage.

Vous pouvez modifier la valeur de seuil de ces messages d'avertissement pour vous assurer que votre système respecte les meilleures pratiques.

## Description de la tâche

Vous devez définir l'option RAID « `min_disrserve_count` » sur « 2 » pour vous assurer que vous disposez toujours du nombre minimum recommandé de disques de rechange.

## Étape

1. Définissez l'option sur « 2 » :

```
storage raid-options modify -node nodename -name min_spare_count -value 2
```

## Options supplémentaires de gestion du partitionnement données-racines

Depuis ONTAP 9.2, une nouvelle option de partitionnement données-racines est disponible dans le menu de démarrage qui fournit des fonctions de gestion supplémentaires pour les disques configurés pour le partitionnement données-racines.

Les fonctions de gestion suivantes sont disponibles sous l'option de menu d'amorçage 9.

- **Départitionner tous les disques et supprimer leurs informations de propriété**

Cette option est utile si votre système est configuré pour le partitionnement données-racines et que vous devez la réinitialiser avec une configuration différente.

- **Nettoyer la configuration et initialiser le nœud avec des disques partitionnés**

Cette option est utile pour les éléments suivants :

- Votre système n'est pas configuré pour le partitionnement données-racines et vous souhaitez le configurer pour le partitionnement données-racines
- Votre système n'est pas correctement configuré pour le partitionnement données-racines et vous devez le corriger
- Vous disposez d'une plateforme AFF ou FAS avec uniquement des disques SSD connectés pour la version précédente du partitionnement données-racines et souhaitez la mettre à niveau vers la version plus récente du partitionnement données-racines afin d'améliorer l'efficacité du stockage

- **Nettoyer la configuration et initialiser le nœud avec des disques entiers**

Cette option est utile si vous devez :

- Départition des partitions existantes
- Supprimez la propriété de disque local
- Réinitialisez votre système avec des disques entiers à l'aide de RAID-DP

## Lorsque vous devez mettre à jour le progiciel de qualification des disques

Le boîtier de qualification des disques (DQP) ajoute un support complet pour les disques nouvellement qualifiés. Avant de mettre à jour le firmware des disques ou d'ajouter de nouveaux types ou tailles de disques à un cluster, vous devez mettre à jour le DQP. Il est également recommandé de mettre à jour régulièrement le DQP, par exemple tous les trimestres ou tous les deux ans.

Vous devez télécharger et installer le DQP dans les situations suivantes :

- Chaque fois que vous ajoutez un nouveau type ou une nouvelle taille de disque au nœud

Par exemple, si vous avez déjà des disques de 1 To et que vous ajoutez des disques de 2 To, vous devez

vérifier la dernière mise à jour du DQP.

- Chaque fois que vous mettez à jour le micrologiciel du disque
- Chaque fois que les fichiers de firmware ou de DQP sont plus récents
- Chaque fois que vous effectuez une mise à niveau vers une nouvelle version de ONTAP.

Le DQP n'a pas été mis à jour dans le cadre d'une mise à niveau ONTAP.

## Informations associées

["Téléchargements NetApp : pack de qualification des disques"](#)

["Téléchargements NetApp : firmware de disque"](#)

## Propriété du disque et de la partition

### Propriété du disque et de la partition

Vous pouvez gérer la propriété des disques et des partitions.

Vous pouvez effectuer les tâches suivantes :

- **"Afficher la propriété du disque et de la partition"**

Vous pouvez afficher la propriété des disques pour déterminer quel nœud contrôle le stockage. Vous pouvez également afficher la propriété de la partition sur les systèmes qui utilisent des disques partagés.

- **"Modifiez les paramètres de l'assignation automatique de Disk Ownership"**

Vous pouvez sélectionner une règle autre que celle par défaut pour l'attribution automatique de la propriété de disque ou pour désactiver l'assignation automatique de la propriété de disque.

- **"Affectation manuelle de la propriété de disques non partitionnés"**

Si votre cluster n'est pas configuré pour utiliser l'affectation automatique de propriété de disque, vous devez attribuer la propriété manuellement.

- **"Affectation manuelle de la propriété de disques partitionnés"**

Vous pouvez définir la propriété du disque de conteneur ou des partitions manuellement ou en utilisant l'affectation automatique, comme pour les disques non partitionnés.

- **"Retirez un disque défectueux"**

Un disque défectueux n'est plus considéré par ONTAP comme un disque utilisable, et vous pouvez immédiatement déconnecter le disque du shelf.

- **"Supprimer la propriété d'un disque"**

ONTAP écrit les informations de propriété du disque sur le disque. Avant de retirer un disque de spare ou son tiroir d'un nœud, vous devez supprimer ses informations de propriété de sorte qu'elles puissent être correctement intégrées à un autre nœud.

## À propos de l'assignation automatique de Disk Ownership

L'assignation automatique des disques qui n'appartiennent pas est activée par défaut. Les attributions automatiques de propriété de disque se produisent 10 minutes après l'initialisation de la paire haute disponibilité et toutes les cinq minutes pendant le fonctionnement normal du système.

Lorsque vous ajoutez un nouveau disque à une paire haute disponibilité, par exemple lors du remplacement d'un disque en panne, de la réponse à un message de « disques de secours faibles » ou de l'ajout de capacité, la règle d'affectation automatique par défaut attribue la propriété du disque à un nœud en tant que disque de secours.

La règle d'allocation automatique par défaut est basée sur des caractéristiques spécifiques à la plateforme ou sur le tiroir DS460C si votre paire haute disponibilité ne dispose que de ces tiroirs et utilise l'une des méthodes (règles) suivantes pour attribuer la propriété des disques :

| Méthode d'affectation                                                                                                                                                                                                               | Effet sur les affectations de nœuds                                                                                                                                                                                                        | Configurations de plate-forme par défaut à la méthode d'affectation                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| baie                                                                                                                                                                                                                                | Les baies à numéro pair sont attribuées au nœud A et aux baies à numéro impair au nœud B.                                                                                                                                                  | Systèmes d'entrée de gamme dans une configuration de paires haute disponibilité avec un seul tiroir partagé.                                                                                       |
| tiroir                                                                                                                                                                                                                              | Tous les disques du tiroir sont affectés au nœud A.                                                                                                                                                                                        | Systèmes d'entrée de gamme dans une configuration de paires haute disponibilité avec une pile de deux tiroirs ou plus et configurations MetroCluster avec une pile par nœud, deux tiroirs ou plus. |
| séparer la tablette<br><br>Cette politique relève de la valeur «par défaut» pour le <code>-autoassign-policy</code> paramètre du <code>storage disk option</code> pour les configurations de plateformes et de tiroirs applicables. | Les disques du côté gauche du shelf sont affectés au nœud A et du côté droit au nœud B. Les tiroirs partiels sur les paires haute disponibilité sont expédiés de l'usine avec des disques remplis depuis le bord du tiroir vers le centre. | La plupart des plateformes AFF et certaines configurations MetroCluster.                                                                                                                           |
| pile                                                                                                                                                                                                                                | Tous les disques de la pile sont affectés au nœud A.                                                                                                                                                                                       | Systèmes d'entrée de gamme autonomes et toutes les autres configurations.                                                                                                                          |

|                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>demi-tiroir</p> <p>Cette politique relève de la valeur «par défaut» pour le <code>-autoassign-policy</code> paramètre du <code>storage disk option</code> pour les configurations de plateformes et de tiroirs applicables.</p> | <p>Tous les disques de la moitié gauche d'un tiroir DS460C (baies de lecteurs 0 à 5) sont affectés au nœud A ; tous les disques de la moitié droite d'un tiroir (baies de lecteurs 6 à 11) sont affectés au nœud B.</p> <p>Lors de l'initialisation d'une paire haute disponibilité avec seulement des tiroirs DS460C, l'assignation automatique de la propriété des disques n'est pas prise en charge. Vous devez attribuer manuellement la propriété des disques contenant des lecteurs racine/conteneur qui possèdent la partition racine en respectant la stratégie demi-tiroir.</p> | <p>Paires HAUTE DISPONIBILITÉ avec tiroirs DS460C uniquement, après l'initialisation des paires haute disponibilité (démarrage).</p> <p>Après le démarrage d'une paire haute disponibilité, l'assignation automatique de la propriété des disques est automatiquement activée et utilise la règle à demi-tiroir pour attribuer la propriété aux disques restants (autres que les disques racine/disques de conteneur sur lesquels la partition racine est installée) et à tous les disques ajoutés ultérieurement.</p> <p>Si votre paire haute disponibilité possède des tiroirs DS460C en plus d'autres modèles de tiroirs, la règle relative au demi-tiroir n'est pas utilisée. La stratégie par défaut utilisée est dictée par les caractéristiques propres à la plateforme.</p> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Paramètres et modifications d'affectation automatique :

- Vous pouvez afficher les paramètres d'affectation automatique actuels (activé/désactivé) avec le `storage disk option show` commande.
- Vous pouvez désactiver l'affectation automatique à l'aide du `storage disk option modify` commande.
- Si la stratégie d'affectation automatique par défaut n'est pas souhaitable dans votre environnement, vous pouvez spécifier (modifier) la méthode d'affectation des baies, des étagères ou des piles à l'aide du `-autoassign-policy` paramètre dans le `storage disk option modify` commande.

Découvrez comment ["Modifiez les paramètres de l'assignation automatique de Disk Ownership"](#).



Les règles d'affectation automatique par défaut des demi-tiroirs et des tiroirs divisés sont uniques car elles ne peuvent pas être définies par des utilisateurs comme les règles de compartiment, de tiroir et de pile le peuvent.

Dans les systèmes ADP (Advanced Drive Partitionnement), l'affectation automatique des disques sur les tiroirs à moitié pleins doit être installée dans les baies de tiroir appropriées en fonction du type de tiroir que vous possédez :

- Si votre étagère n'est pas un tiroir DS460C, installez les disques de manière égale sur le côté gauche et le côté droit, en vous déplaçant vers le milieu. Par exemple, six disques dans les baies 0-5 et six disques dans les baies 18-23 d'un tiroir DS224C.
- Si votre tiroir est un tiroir DS460C, installez les lecteurs dans la rangée avant (baies de lecteur 0, 3, 6 et 9) de chaque tiroir. Pour les disques restants, répartissez-les uniformément dans chaque tiroir en remplissant

les rangées de tiroirs d'avant en arrière. Si vous ne disposez pas de suffisamment de disques pour remplir les rangées, installez-les par paires de sorte que les disques occupent les côtés gauche et droit d'un tiroir de manière uniforme.

L'installation des entraînements dans la rangée avant de chaque tiroir permet un débit d'air correct et empêche la surchauffe.



Si les disques ne sont pas installés dans les baies de tiroir appropriées sur des tiroirs à moitié remplis, lorsqu'un disque de conteneur tombe en panne et est remplacé, ONTAP n'affecte pas automatiquement la propriété. Dans ce cas, l'affectation du nouveau lecteur de conteneur doit être effectuée manuellement. Une fois que vous avez attribué la propriété du disque de conteneur, ONTAP gère automatiquement toute attribution de partitionnement et de partitionnement de disque requise.

Dans certains cas où l'affectation automatique ne fonctionne pas, vous devez attribuer manuellement la propriété du disque à l'aide du `storage disk assign` commande :

- Si vous désactivez l'affectation automatique, les nouveaux disques ne sont pas disponibles en tant que disques de secours tant qu'ils ne sont pas attribués manuellement à un nœud.
- Si vous souhaitez attribuer automatiquement des disques et que vous disposez de plusieurs piles ou tiroirs qui doivent avoir un droit de propriété différent, un disque doit avoir été manuellement affecté à chaque pile ou tiroir afin que l'affectation automatique de la propriété fonctionne sur chaque pile ou tiroir.
- Si l'affectation automatique est activée et que vous affectez manuellement un lecteur à un nœud non spécifié dans la stratégie active, l'affectation automatique cesse de fonctionner et un message EMS s'affiche.

Découvrez comment ["Attribuez manuellement la propriété de disque des disques non partitionnés"](#).

Découvrez comment ["Attribuez manuellement la propriété des disques partitionnés"](#).

#### Afficher la propriété du disque et de la partition

Vous pouvez afficher la propriété des disques pour déterminer quel nœud contrôle le stockage. Vous pouvez également afficher la propriété de la partition sur les systèmes qui utilisent des disques partagés.

#### Étapes

1. Afficher la propriété des disques physiques :

```
storage disk show -ownership
```



```
cluster::> storage disk show -ownership
```

| Disk       | Aggregate | Home  | Owner | DR | Home | Home ID    | Owner ID   | DR |
|------------|-----------|-------|-------|----|------|------------|------------|----|
| Home ID    | Reserver  | Pool  |       |    |      |            |            |    |
| 1.0.0      | aggr0_2   | node2 | node2 | -  |      | 2014941509 | 2014941509 | -  |
| 2014941509 | Pool0     |       |       |    |      |            |            |    |
| 1.0.1      | aggr0_2   | node2 | node2 | -  |      | 2014941509 | 2014941509 | -  |
| 2014941509 | Pool0     |       |       |    |      |            |            |    |
| 1.0.2      | aggr0_1   | node1 | node1 | -  |      | 2014941219 | 2014941219 | -  |
| 2014941219 | Pool0     |       |       |    |      |            |            |    |
| 1.0.3      | -         | node1 | node1 | -  |      | 2014941219 | 2014941219 | -  |
| 2014941219 | Pool0     |       |       |    |      |            |            |    |

2. Si vous disposez d'un système utilisant des disques partagés, vous pouvez afficher la propriété de la partition :

```
storage disk show -partition-ownership
```

```
cluster::> storage disk show -partition-ownership
```

| Container  | Container | Root       | Data       |
|------------|-----------|------------|------------|
| Disk       | Aggregate | Root Owner | Owner ID   |
| Owner ID   |           |            |            |
| 1.0.0      | -         | node1      | 1886742616 |
| 1886742616 |           |            |            |
| 1.0.1      | -         | node1      | 1886742616 |
| 1886742616 |           |            |            |
| 1.0.2      | -         | node2      | 1886742657 |
| 1886742657 |           |            |            |
| 1.0.3      | -         | node2      | 1886742657 |
| 1886742657 |           |            |            |

### Modifiez les paramètres de l'assignation automatique de Disk Ownership

Vous pouvez utiliser le `storage disk option modify` commande pour sélectionner une règle autre que celle par défaut pour l'attribution automatique de propriété de disque ou pour désactiver l'assignation automatique de propriété de disque.

Découvrez "[assignation automatique de la propriété du disque](#)".

### Description de la tâche

Si vous disposez d'une paire haute disponibilité avec seulement des tiroirs DS460C, la règle d'affectation

automatique par défaut est « demi-tiroir ». Vous ne pouvez pas choisir une règle autre que celle par défaut (baie, tiroir, pile).

## Étapes

### 1. Modifier l'affectation automatique des disques :

- a. Si vous souhaitez sélectionner une stratégie autre que celle par défaut, entrez :

```
storage disk option modify -autoassign-policy autoassign_policy -node
node_name
```

- Utiliser `stack` comme le `autoassign_policy` pour configurer la propriété automatique au niveau de la pile ou de la boucle.
- Utiliser `shelf` comme le `autoassign_policy` pour configurer la propriété automatique au niveau du tiroir.
- Utiliser `bay` comme le `autoassign_policy` pour configurer la propriété automatique au niveau de la baie.

- b. Pour désactiver l'affectation automatique de propriété de disque, entrez :

```
storage disk option modify -autoassign off -node node_name
```

### 2. Vérifiez les paramètres d'assignation automatique des disques :

```
storage disk option show
```

```
cluster1::> storage disk option show
```

| Node       | BKg. FW. Upd. | Auto Copy | Auto Assign | Auto Assign Policy |
|------------|---------------|-----------|-------------|--------------------|
| -----      | -----         | -----     | -----       | -----              |
| cluster1-1 | on            | on        | on          | default            |
| cluster1-2 | on            | on        | on          | default            |

## Attribuez manuellement la propriété de disque des disques non partitionnés

Si votre paire haute disponibilité n'est pas configurée pour utiliser l'affectation automatique de propriété des disques, vous devez attribuer manuellement la propriété. Si vous initialisez une paire haute disponibilité ne comportant que des tiroirs DS460C, vous devez attribuer manuellement la propriété des disques racine.

## Description de la tâche

- Si vous attribuez manuellement la propriété d'une paire haute disponibilité qui n'est pas initialisée et ne dispose pas uniquement de tiroirs DS460C, utilisez l'option 1.
- Si vous initialisez une paire haute disponibilité ne comportant que des tiroirs DS460C, utilisez l'option 2 pour attribuer manuellement la propriété des disques racines.

## Option 1 : la plupart des paires haute disponibilité

Si vous disposez d'une paire haute disponibilité qui n'est pas initialisée et ne dispose pas uniquement de tiroirs DS460C, utilisez cette procédure pour attribuer manuellement la propriété.

### Description de la tâche

- Les disques pour lesquels vous attribuez la propriété doivent se trouver dans un tiroir physiquement connecté au nœud auquel vous êtes propriétaire.
- Si vous utilisez des disques d'un niveau local (agrégat) :
  - Les disques doivent être au sein d'un nœud avant de pouvoir être utilisés dans un niveau local (agrégat).
  - Vous ne pouvez pas réaffecter la propriété d'un disque utilisé dans un niveau local (agrégat).

### Étapes

1. Utiliser l'interface de ligne de commande pour afficher tous les disques non détenus :

```
storage disk show -container-type unassigned
```

2. Affectez chaque disque :

```
storage disk assign -disk disk_name -owner owner_name
```

Vous pouvez utiliser le caractère générique pour attribuer plusieurs disques à la fois. Si vous réassignez un disque de réserve qui appartient déjà à un nœud différent, vous devez utiliser l'option "-force".

## Option 2 : une paire haute disponibilité avec seulement des tiroirs DS460C

Pour une paire haute disponibilité que vous initialisez et qui ne possède que des tiroirs DS460C, utilisez cette procédure pour attribuer manuellement la propriété des disques racine.

### Description de la tâche

- Lorsque vous initialisez une paire haute disponibilité ne comportant que des tiroirs DS460C, vous devez attribuer manuellement les disques racines afin de respecter la règle relative au demi-tiroir.

Après l'initialisation (démarrage) des paires haute disponibilité, l'assignation automatique de la propriété des disques est automatiquement activée et utilise la règle du demi-tiroir pour attribuer la propriété aux disques restants (autres que les disques racines) et à tous les disques ajoutés à l'avenir, comme le remplacement des disques défectueux, répondant au message de « faible capacité », ou en ajoutant de la capacité.

Pour en savoir plus sur la politique de demi-tiroir, consultez le sujet ["À propos de l'assignation automatique de Disk Ownership"](#).

- La technologie RAID nécessite un minimum de 10 disques par paire haute disponibilité (5 pour chaque nœud) pour tout disque NL-SAS de plus de 8 To dans un tiroir DS460C.

### Étapes

1. Si vos étagères DS460C ne sont pas entièrement remplies, procédez comme suit ; sinon, passez à l'étape suivante.

- a. Installez tout d'abord les lecteurs dans la rangée avant (baies de lecteurs 0, 3, 6 et 9) de chaque tiroir.

L'installation des entraînements dans la rangée avant de chaque tiroir permet un débit d'air correct et empêche la surchauffe.

- b. Pour les disques restants, répartissez-les uniformément entre les tiroirs.

Remplissez les rangées de tiroirs d'avant en arrière. Si vous ne disposez pas de suffisamment de disques pour remplir les rangées, installez-les par paires de sorte que les disques occupent les côtés gauche et droit d'un tiroir de manière uniforme.

L'illustration suivante montre la numérotation et les emplacements des baies de lecteur dans un tiroir DS460C.



2. Connectez-vous au cluster shell en utilisant la LIF node-management ou la LIF cluster-management.
3. Attribuez manuellement les lecteurs racine de chaque tiroir pour qu'ils soient conformes à la stratégie demi-tiroir à l'aide des sous-étapes suivantes :

La règle demi-tiroir vous permet d'affecter la moitié gauche des lecteurs d'un tiroir (baies 0 à 5) au nœud A et la moitié droite des lecteurs d'un tiroir (baies 6 à 11) au nœud B.

- a. Afficher tous les disques non possédés :

```
storage disk show -container-type unassigned`
```

- b. Assigner les disques root:

```
storage disk assign -disk disk_name -owner owner_name
```

Vous pouvez utiliser le caractère générique pour attribuer plusieurs disques à la fois.

#### Affectation manuelle de la propriété de disques partitionnés

Vous pouvez attribuer manuellement la propriété du disque conteneur ou des partitions sur les systèmes ADP (Advanced Drive Partitioning). Si vous initialisez une paire haute disponibilité ne comportant que des tiroirs DS460C, vous devez attribuer manuellement la propriété des disques de conteneur qui incluront les partitions racine.

#### Description de la tâche

- Le type de système de stockage que vous avez déterminé la méthode ADP prise en charge, les données-racines (RD) ou les données-racines (RD2).

Les systèmes de stockage FAS utilisent les systèmes de stockage RD et AFF RD2.

- Si vous attribuez manuellement la propriété d'une paire haute disponibilité qui n'est pas initialisée et ne dispose pas uniquement de tiroirs DS460C, utilisez l'option 1 pour attribuer manuellement des disques avec partitionnement RD (root-Data) ou l'option 2 pour attribuer manuellement des disques avec partitionnement RD2 (root-Data-Data-Data).
- Si vous initialisez une paire haute disponibilité ne comportant que des tiroirs DS460C, utilisez l'option 3

pour attribuer manuellement la propriété des disques de conteneur qui ont la partition racine.

**Option 1 : affectation manuelle des disques avec partitionnement RD (root-Data)**

Pour le partitionnement données-racines, trois entités détenues sont détenues collectivement (le disque de conteneur et les deux partitions) par la paire haute disponibilité.

**Description de la tâche**

- Le disque de conteneur et les deux partitions ne doivent pas toutes être détenues par le même nœud de la paire haute disponibilité, tant qu'elles appartiennent à un des nœuds de la paire haute disponibilité. Toutefois, lorsque vous utilisez une partition dans un niveau local (agrégat), elle doit être détenue par le même nœud qui possède le niveau local.
- Si un disque conteneur tombe en panne dans un tiroir à moitié rempli et est remplacé, vous devrez peut-être attribuer manuellement la propriété du disque, car ONTAP n'affecte pas toujours automatiquement la propriété dans ce cas.
- Une fois le disque conteneur attribué, le logiciel ONTAP gère automatiquement toute partition et toute attribution de partition requises.

**Étapes**

1. Utilisez l'interface de ligne de commande pour afficher la propriété actuelle du disque partitionné :

```
storage disk show -disk disk_name -partition-ownership
```

2. Définissez le niveau de privilège de l'interface de ligne de commande sur avancé :

```
set -privilege advanced
```

3. Entrez la commande appropriée, en fonction de l'entité de propriété pour laquelle vous souhaitez affecter la propriété :

Si l'une des entités de propriété est déjà détenue, vous devez inclure l'option « force ».

| Si vous souhaitez attribuer la propriété à... | Utilisez cette commande...                                                                  |
|-----------------------------------------------|---------------------------------------------------------------------------------------------|
| Disque de conteneur                           | <code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i></code>            |
| Partition de données                          | <code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -data true</code> |
| Partition racine                              | <code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -root true</code> |

**Option 2 : affectation manuelle des disques avec partitionnement données-racines (RD2)**

Pour le partitionnement données-racines, quatre entités détenues par le système (le disque de conteneur et les trois partitions) sont détenues collectivement par la paire haute disponibilité. Le partitionnement données-racines crée une petite partition en tant que partition racine et deux partitions de taille supérieure égale pour les données.

**Description de la tâche**

- Les paramètres doivent être utilisés avec le `disk assign` commande permettant d'attribuer la partition appropriée d'un disque partitionné données-racines. Vous ne pouvez pas utiliser ces paramètres avec des disques faisant partie d'un pool de stockage. La valeur par défaut est « FALSE ».
  - Le `-data1 true` paramètre attribue la partition "data1" d'un disque partitionné root-data1-data2.
  - Le `-data2 true` paramètre attribue la partition "data2" d'un disque partitionné root-data1-data2.
- Si un disque conteneur tombe en panne dans un tiroir à moitié rempli et est remplacé, vous devrez peut-être attribuer manuellement la propriété du disque, car ONTAP n'affecte pas toujours automatiquement la propriété dans ce cas.
- Une fois le disque conteneur attribué, le logiciel ONTAP gère automatiquement toute partition et toute attribution de partition requises.

**Étapes**

1. Utilisez l'interface de ligne de commande pour afficher la propriété actuelle du disque partitionné :

```
storage disk show -disk disk_name -partition-ownership
```

2. Définissez le niveau de privilège de l'interface de ligne de commande sur avancé :

```
set -privilege advanced
```

3. Entrez la commande appropriée, en fonction de l'entité de propriété pour laquelle vous souhaitez affecter la propriété :

Si l'une des entités de propriété est déjà détenue, vous devez inclure l'option « force ».

| Si vous souhaitez attribuer la propriété à... | Utilisez cette commande...                                                                   |
|-----------------------------------------------|----------------------------------------------------------------------------------------------|
| Disque de conteneur                           | <code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i></code>             |
| Partition de données 1                        | <code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -data1 true</code> |
| Partition Data2                               | <code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -data2 true</code> |
| Partition racine                              | <code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -root true</code>  |

### Option 3 : attribuez manuellement des lecteurs de conteneur DS460C disposant de la partition racine

Si vous initialisez une paire haute disponibilité ne comportant que des tiroirs DS460C, vous devez attribuer manuellement la propriété des disques de conteneur qui disposent de la partition racine en suivant la règle demi-tiroir.

#### Description de la tâche

- Lorsque vous initialisez une paire haute disponibilité ne comportant que des tiroirs DS460C, le menu de démarrage ADP (disponible avec ONTAP 9.2 et versions ultérieures), les options 9a et 9b ne prennent pas en charge l'affectation automatique de propriété de disque. Vous devez affecter manuellement les lecteurs de conteneur qui ont la partition racine en suivant la stratégie demi-tiroir.

Après l'initialisation de la paire haute disponibilité (démarrage), l'affectation automatique de la propriété des disques est automatiquement activée et utilise la règle demi-tiroir pour attribuer la propriété aux disques restants (autres que les disques de conteneur sur lesquels se trouve la partition racine) et à tous les disques ajoutés ultérieurement, tels que le remplacement des disques défectueux, répondre au message de « faibles pièces de rechange » ou ajouter de la capacité.

- Pour en savoir plus sur la politique de demi-tiroir, consultez le sujet ["À propos de l'assignation automatique de Disk Ownership"](#).

#### Étapes

1. Si vos étagères DS460C ne sont pas entièrement remplies, procédez comme suit ; sinon, passez à l'étape suivante.

- a. Installez tout d'abord les lecteurs dans la rangée avant (baies de lecteurs 0, 3, 6 et 9) de chaque tiroir.

L'installation des entraînements dans la rangée avant de chaque tiroir permet un débit d'air correct et empêche la surchauffe.

- b. Pour les disques restants, répartissez-les uniformément entre les tiroirs.

Remplissez les rangées de tiroirs d'avant en arrière. Si vous ne disposez pas de suffisamment de disques pour remplir les rangées, installez-les par paires de sorte que les disques occupent les côtés gauche et droit d'un tiroir de manière uniforme.

L'illustration suivante montre la numérotation et les emplacements des baies de lecteur dans un tiroir DS460C.





2. Connectez-vous au cluster shell en utilisant la LIF node-management ou la LIF cluster-management.
3. Pour chaque tiroir, attribuez manuellement les lecteurs de conteneur qui ont la partition racine en respectant la stratégie demi-tiroir en suivant les sous-étapes suivantes :

La règle demi-tiroir vous permet d'affecter la moitié gauche des lecteurs d'un tiroir (baies 0 à 5) au nœud A et la moitié droite des lecteurs d'un tiroir (baies 6 à 11) au nœud B.

- a. Afficher tous les disques non possédés :

```
storage disk show -container-type unassigned
```

- b. Attribuez les lecteurs de conteneur qui ont la partition racine :

```
storage disk assign -disk disk_name -owner owner_name
```

Vous pouvez utiliser le caractère générique pour attribuer plusieurs lecteurs à la fois.

#### Configurez une configuration actif-passif sur les nœuds à l'aide du partitionnement données-racines

Lorsqu'une paire haute disponibilité est configurée pour utiliser le partitionnement données-racines par l'usine, les partitions de données sont partagées entre les deux nœuds de la paire pour une utilisation dans une configuration active/active. Si vous souhaitez utiliser la paire haute disponibilité dans une configuration active-passive, vous devez mettre à jour la propriété de la partition avant de créer votre niveau de données local (agrégat).

#### Ce dont vous avez besoin

- Vous devriez avoir déterminé quel nœud sera le nœud actif et quel nœud sera le nœud passif.
- Storage failover doit être configuré sur la paire HA.

#### Description de la tâche

Cette tâche est effectuée sur deux nœuds : le nœud A et le nœud B.

Cette procédure est destinée aux nœuds pour lesquels aucun niveau local de données (agrégat) n'a été créé à

partir des disques partitionnés.

Découvrez "[partitionnement de disque avancé](#)".

Étapes

Toutes les commandes sont saisies au niveau du shell du cluster.

- 1. Afficher la propriété actuelle des partitions de données :

```
storage aggregate show-spare-disks
```

Le résultat indique que la moitié des partitions de données appartiennent à un nœud et que la moitié appartiennent à l'autre nœud. Toutes les partitions de données doivent être de rechange.

```
cluster1::> storage aggregate show-spare-disks

Original Owner: cluster1-01
Pool0
Partitioned Spares

Local
Local
Root Physical
Disk
Usable Size

1.0.0
0B 828.0GB
1.0.1
73.89GB 828.0GB
1.0.5
0B 828.0GB
1.0.6
0B 828.0GB
1.0.10
0B 828.0GB
1.0.11
0B 828.0GB

Type RPM Checksum Usable
BSAS 7200 block 753.8GB
BSAS 7200 block 753.8GB
BSAS 7200 block 753.8GB
BSAS 7200 block 753.8GB
BSAS 7200 block 753.8GB
BSAS 7200 block 753.8GB
BSAS 7200 block 753.8GB

Original Owner: cluster1-02
Pool0
Partitioned Spares

Local
Local
Root Physical
Disk
Type RPM Checksum Usable
```

```

Usable Size

1.0.2 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.3 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.4 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.7 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.8 BSAS 7200 block 753.8GB
73.89GB 828.0GB
1.0.9 BSAS 7200 block 753.8GB
0B 828.0GB
12 entries were displayed.

```

2. Saisissez le niveau de privilège avancé :

```
set advanced
```

3. Pour chaque partition de données appartenant au nœud qui sera le nœud passif, affectez-le au nœud actif :

```
storage disk assign -force -data true -owner active_node_name -disk disk_name
```

Il n'est pas nécessaire d'inclure la partition dans le nom du disque.

Vous devez saisir une commande similaire à l'exemple suivant pour chaque partition de données que vous devez réattribuer :

```
storage disk assign -force -data true -owner cluster1-01 -disk 1.0.3
```

4. Vérifiez que toutes les partitions sont affectées au nœud actif.

```

cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
Pool0
Partitioned Spares

Local
Local
Root Physical
Disk
Usable Size

Type RPM Checksum Usable
Data

```

```

1.0.0 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.1 BSAS 7200 block 753.8GB
73.89GB 828.0GB
1.0.2 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.3 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.4 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.5 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.6 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.7 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.8 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.9 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.10 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.11 BSAS 7200 block 753.8GB
0B 828.0GB

```

Original Owner: cluster1-02

Pool0

Partitioned Spares

```

Local
Local
Data
Root Physical
Disk
Usable Size Type RPM Checksum Usable

1.0.8 BSAS 7200 block 0B
73.89GB 828.0GB
13 entries were displayed.

```

Notez que la cluster1-02 est toujours propriétaire d'une partition racine de rechange.

##### 5. Revenir au privilège administratif :

```
set admin
```

##### 6. Créer votre agrégat de données en laissant au moins une partition de données comme spare :

```
storage aggregate create new_aggr_name -diskcount number_of_partitions -node
active_node_name
```

L'agrégat de données est créé et appartient au nœud actif.

### Configurez une configuration actif-passif sur les nœuds à l'aide du partitionnement données-racines

Lorsqu'une paire haute disponibilité est configurée pour utiliser le partitionnement données-racines par l'usine, les partitions de données sont partagées entre les deux nœuds de la paire pour une utilisation dans une configuration active/active. Si vous souhaitez utiliser la paire haute disponibilité dans une configuration active-passive, vous devez mettre à jour la propriété de la partition avant de créer votre niveau de données local (agrégat).

#### Ce dont vous avez besoin

- Vous devriez avoir déterminé quel nœud sera le nœud actif et quel nœud sera le nœud passif.
- Storage failover doit être configuré sur la paire HA.

#### Description de la tâche

Cette tâche est effectuée sur deux nœuds : le nœud A et le nœud B.

Cette procédure est destinée aux nœuds pour lesquels aucun niveau local de données (agrégat) n'a été créé à partir des disques partitionnés.

Découvrez "[partitionnement de disque avancé](#)".

#### Étapes

Toutes les commandes sont des entrées au niveau du shell du cluster.

1. Afficher la propriété actuelle des partitions de données :

```
storage aggregate show-spare-disks -original-owner passive_node_name -fields
local-usable-data1-size, local-usable-data2-size
```

Le résultat indique que la moitié des partitions de données appartiennent à un nœud et que la moitié appartiennent à l'autre nœud. Toutes les partitions de données doivent être de rechange.

2. Saisissez le niveau de privilège avancé :

```
set advanced
```

3. Pour chaque partition data1 détenue par le nœud qui sera le nœud passif, affectez-la au nœud actif :

```
storage disk assign -force -data1 -owner active_node_name -disk disk_name
```

Il n'est pas nécessaire d'inclure la partition dans le nom du disque

4. Pour chaque partition de données2 détenue par le nœud qui sera le nœud passif, affectez-le au nœud actif :

```
storage disk assign -force -data2 -owner active_node_name -disk disk_name
```

Il n'est pas nécessaire d'inclure la partition dans le nom du disque

5. Vérifiez que toutes les partitions sont affectées au nœud actif :

storage aggregate show-spare-disks

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
Pool0
Partitioned Spares

Local
Local
Data
Root Physical
Disk Type RPM Checksum Usable
Usable Size

1.0.0 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.1 BSAS 7200 block 753.8GB
73.89GB 828.0GB
1.0.2 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.3 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.4 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.5 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.6 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.7 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.8 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.9 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.10 BSAS 7200 block 753.8GB
0B 828.0GB
1.0.11 BSAS 7200 block 753.8GB
0B 828.0GB

Original Owner: cluster1-02
Pool0
Partitioned Spares
```

```

Local
Local
Data
Root Physical
Disk Type RPM Checksum Usable
Usable Size

1.0.8 BSAS 7200 block 0B
73.89GB 828.0GB
13 entries were displayed.

```

Notez que la cluster1-02 est toujours propriétaire d'une partition racine de rechange.

#### 6. Revenir au privilège administratif :

```
set admin
```

#### 7. Créer votre agrégat de données en laissant au moins une partition de données comme spare :

```
storage aggregate create new_aggr_name -diskcount number_of_partitions -node
active_node_name
```

L'agrégat de données est créé et appartient au nœud actif.

#### 8. Vous pouvez également utiliser la disposition des agrégats recommandée par ONTAP, qui inclut de bonnes pratiques pour la disposition des groupes RAID et le nombre de disques de rechange :

```
storage aggregate auto-provision
```

### Supprimer la propriété d'un disque

ONTAP écrit les informations de propriété du disque sur le disque. Avant de retirer un disque de spare ou son tiroir d'un nœud, vous devez supprimer ses informations de propriété de sorte qu'elles puissent être correctement intégrées à un autre nœud.



Si le disque est partitionné pour le partitionnement données-racines et que vous exécutez ONTAP 9.10.1 ou une version ultérieure, contactez le support technique NetApp pour obtenir de l'aide sur la suppression de la propriété. Pour plus d'informations, reportez-vous au ["Article de la base de connaissances : impossible de supprimer le propriétaire du disque"](#).

### Ce dont vous avez besoin

Le disque dont vous souhaitez supprimer la propriété doit respecter les exigences suivantes :

- Il doit être un disque de spare.

Vous ne pouvez pas supprimer la propriété d'un disque utilisé dans un niveau local (agrégat).

- Il ne peut pas être dans le centre de maintenance.

- Il ne peut pas être en cours de nettoyage.
- Elle ne peut pas avoir échoué.

Il n'est pas nécessaire de supprimer la propriété d'un disque défectueux.

### Description de la tâche

Si l'affectation automatique de disque est activée, ONTAP peut réaffecter automatiquement la propriété avant de supprimer le disque du nœud. C'est pour cette raison que vous désactivez l'affectation de propriété automatique jusqu'à ce que le disque soit supprimé, puis vous le réactivez.

### Étapes

1. Si l'affectation automatique de la propriété de disque est activée, utilisez l'interface de ligne de commandes pour la désactiver :

```
storage disk option modify -node node_name -autoassign off
```

2. Si nécessaire, répétez l'étape précédente pour le partenaire HA du nœud.
3. Supprimez les informations de propriété logicielle du disque :

```
storage disk removeowner disk_name
```

Pour supprimer les informations de propriété de plusieurs disques, utilisez une liste séparée par des virgules.

Exemple :

```
storage disk removeowner sys1:0a.23,sys1:0a.24,sys1:0a.25
```

4. Si le disque est partitionné pour le partitionnement données-racines et que vous exécutez ONTAP 9.9.1 ou une version antérieure, supprimez la propriété des partitions :

```
storage disk removeowner -disk disk_name -root true
```

```
storage disk removeowner -disk disk_name -data true
```

Les deux partitions ne sont plus la propriété d'aucun nœud.

5. Si vous avez précédemment désactivé l'affectation automatique de la propriété de disque, activez-la une fois que le disque a été supprimé ou réaffecté :

```
storage disk option modify -node node_name -autoassign on
```

6. Si nécessaire, répétez l'étape précédente pour le partenaire HA du nœud.

### Retirez un disque défectueux

Un disque en panne totale n'est plus compté par ONTAP en tant que disque utilisable, et vous pouvez immédiatement déconnecter le disque du tiroir disque. Cependant, vous devez laisser un disque partiellement défectueux connecté assez longtemps pour que le processus de restauration Rapid RAID s' termine.



## Description de la tâche

Si vous retirez un disque parce qu'il a échoué ou parce qu'il génère des messages d'erreur excessifs, vous ne devez pas réutiliser le disque dans ce système de stockage ou tout autre système.

## Étapes

1. Utilisez l'interface de ligne de commandes pour trouver l'ID de disque du disque défaillant :

```
storage disk show -broken
```

Si le disque n'apparaît pas dans la liste des disques défaillants, il peut en être partiellement défaillant, avec une restauration Rapid RAID en cours. Dans ce cas, attendez que le disque soit présent dans la liste des disques défaillants (ce qui signifie que le processus de restauration Rapid RAID est terminé) avant de retirer le disque.

2. Déterminez l'emplacement physique du disque à supprimer :

```
storage disk set-led -action on -disk disk_name 2
```

La LED de panne sur la face du disque est allumée.

3. Retirez le disque du tiroir disque en suivant les instructions du guide matériel correspondant à votre modèle de tiroir disque.

## Nettoyage de disque

### Présentation du nettoyage du disque

Le nettoyage de disque est le processus d'effacement physique des données en remplaçant les disques ou les disques SSD par des modèles d'octets spécifiés ou des données aléatoires afin que la restauration des données d'origine soit impossible. Le processus de nettoyage permet de garantir que personne ne peut restaurer les données présentes sur les disques.

Cette fonctionnalité est disponible via le nodeshell dans toutes les versions de ONTAP 9 et à partir de ONTAP 9.6 en mode de maintenance.

Le processus de nettoyage des disques utilise trois modèles de remplacement d'octets successifs par défaut ou spécifiés par l'utilisateur pour sept cycles maximum par opération. Le modèle d'écrasement aléatoire est répété pour chaque cycle.

Selon la capacité du disque, les modèles et le nombre de cycles, le processus peut prendre plusieurs heures. Le nettoyage s'exécute en arrière-plan. Vous pouvez démarrer, arrêter et afficher l'état du processus de nettoyage. Le processus de nettoyage contient deux phases : la phase de formatage et la phase de remplacement du motif.

### Phase de formatage

L'opération effectuée pour la phase de formatage dépend de la classe du disque désinfecté, comme indiqué dans le tableau suivant :

| Classe des disques           | Phase de formatage |
|------------------------------|--------------------|
| Disques durs grande capacité | Ignoré             |

|                          |                             |
|--------------------------|-----------------------------|
| Disques durs performants | Opération de format SCSI    |
| SSD                      | Opération de nettoyage SCSI |

### Phase d'écrasement du modèle

Les modèles d'écrasement spécifiés sont répétés pour le nombre de cycles spécifié.

Lorsque le processus de nettoyage est terminé, les disques spécifiés sont en état aseptisé. Ils ne sont pas renvoyés automatiquement à l'état de réserve. Vous devez remettre les disques aseptisés dans la réserve avant que les disques récemment aseptisés soient disponibles pour être ajoutés à un autre agrégat.

### Lorsqu'un nettoyage de disque ne peut pas être effectué

Le nettoyage de disque n'est pas pris en charge pour tous les types de disques. En outre, le nettoyage de disque ne peut pas être effectué dans certains cas.

- Elle n'est pas prise en charge par toutes les références des disques SSD.

Pour plus d'informations sur les références du disque SSD prenant en charge le nettoyage de disque, reportez-vous à la section "[Hardware Universe](#)".

- Il n'est pas pris en charge en mode basculement pour les systèmes situés dans une paire haute disponibilité.
- Il ne peut pas être exécuté sur des disques ayant échoué en raison de problèmes de lisibilité ou d'écriture.
- Elle n'effectue pas sa phase de formatage sur les disques ATA.
- Si vous utilisez le motif aléatoire, il ne peut pas être exécuté sur plus de 100 disques à la fois.
- Il n'est pas pris en charge sur les LUN de baies.
- Si vous procédez à la suppression simultanée de deux disques ses dans le même tiroir ESH, des erreurs s'affichent sur la console concernant l'accès à ce tiroir. Des avertissements concernant les tiroirs ne sont pas signalés pendant la durée du nettoyage.

Cependant, l'accès aux données à ce tiroir n'est pas interrompu.

### Que se passe-t-il si le nettoyage du disque est interrompu

Si le nettoyage des disques est interrompu par l'intervention de l'utilisateur ou un événement inattendu tel qu'une panne de courant, ONTAP prend les mesures nécessaires pour rétablir les disques aseptisés dans un état connu. Cependant, vous devez également prendre les mesures nécessaires pour que le processus de nettoyage puisse se terminer.

Le nettoyage de disque est une opération longue durée. Si le processus de nettoyage est interrompu par une panne de courant, une intervention panique du système ou manuelle, le processus de nettoyage doit être répété depuis le début. Le disque n'est pas désigné comme désinfecté.

Si la phase de formatage du nettoyage du disque est interrompue, ONTAP doit restaurer tout disque endommagé par l'interruption. Après un redémarrage du système et une fois toutes les heures, ONTAP vérifie s'il existe un disque cible de nettoyage qui n'a pas terminé la phase de formatage de son nettoyage. Si des disques de ce type sont trouvés, ONTAP les récupère. La méthode de restauration dépend du type de disque. Une fois qu'un disque a été restauré, vous pouvez réexécuter le processus de nettoyage sur ce disque. Pour

les disques durs, vous pouvez utiliser le `-s` option permettant de spécifier que la phase de formatage n'est pas répétée à nouveau.

#### **Conseils pour créer et sauvegarder des tiers locaux (agrégats) contenant des données à désinfecter**

Si vous créez ou sauvegardez des tiers locaux (agrégats) afin de contenir des données qui peuvent être désinfectées, la procédure suivante permet de limiter le temps nécessaire à la suppression de vos données.

- Veillez à ce que vos tiers locaux contenant des données sensibles ne soient pas plus volumineux qu'ils ne le souhaitent.

Si elles sont plus importantes que nécessaire, le nettoyage nécessite plus de temps, d'espace disque et de bande passante.

- Lorsque vous sauvegardez des tiers locaux contenant des données sensibles, évitez de les sauvegarder sur un niveau local contenant également d'importantes quantités de données non sensibles.

Cette opération réduit les ressources requises pour déplacer des données non sensibles avant le nettoyage des données sensibles.

#### **Procédez à la suppression d'un disque**

Le nettoyage d'un disque vous permet de supprimer les données d'un disque ou d'un ensemble de disques sur les systèmes déclassés ou non opérationnels, de sorte que les données ne puissent jamais être restaurées.

Deux méthodes sont disponibles pour désinfecter les disques à l'aide de l'interface de ligne de commande :

À partir de ONTAP 9.6, vous pouvez effectuer le nettoyage de disque en mode de maintenance.

### Avant de commencer

- Les disques ne peuvent pas être des disques à autochiffrement (SED).

Vous devez utiliser le `storage encryption disk sanitize` Commande permettant de désinfecter un SED.

["Cryptage des données au repos"](#)

### Étapes

1. Démarre en mode de maintenance.

- a. Quitter le shell en cours en saisissant `halt`.

L'invite DU CHARGEUR s'affiche.

- b. Passez en mode maintenance en saisissant `boot_ontap maint`.

Lorsque certaines informations s'affichent, l'invite du mode maintenance s'affiche.

2. Si les disques que vous souhaitez désinfecter sont partitionnés, départitionnez chaque disque :



La commande permettant de départitionner un disque est uniquement disponible au niveau diagnostic et ne doit être effectuée qu'avec NetApp support supervision. Nous vous recommandons vivement de contacter le support NetApp avant de continuer. Vous pouvez également vous reporter à l'article de la base de connaissances ["Comment départitionner un lecteur de réserve dans ONTAP"](#)

```
disk unpartition disk_name
```

3. Procédez à la nettoyage des disques spécifiés :

```
disk sanitize start [-p pattern1|-r [-p pattern2|-r [-p pattern3|-r]]] [-c cycle_count] disk_list
```



Ne mettez pas le nœud hors tension, arrêtez la connectivité du stockage et ne retirez pas les disques cibles pendant le nettoyage. Si le nettoyage est interrompu pendant la phase de formatage, la phase de formatage doit être redémarrée et autorisée à terminer avant que les disques soient nettoyés et prêts à être renvoyés dans le pool de réserve. Si vous devez abandonner le processus de nettoyage, vous pouvez le faire en utilisant le `disk sanitize abort` commande. Si la phase de nettoyage des disques spécifiés est en cours de formatage, l'abandon ne se produit qu'une fois la phase terminée.

``-p` `_pattern1_` `-p` `_pattern2_` `-p` `_pattern3_`` spécifie un cycle d'écrasement d'un à trois octets hexadécimaux définis par l'utilisateur qui peuvent être appliqués successivement aux disques en cours d'assainissement. Le motif par défaut est trois passes, en utilisant 0x55 pour le premier passage, 0xaa pour le second passage et 0x3c pour le troisième passage.

`-r` remplace un remplacement à répétition par un remplacement aléatoire pour une ou toutes les passes.

`-c cycle_count` spécifie le nombre de fois où les modèles d'écrasement spécifiés sont appliqués. La valeur par défaut est un cycle. La valeur maximale est de sept cycles.

`disk_list` Spécifie une liste séparée par des espaces des ID des disques de rechange à désinfecter.

4. Si vous le souhaitez, vérifiez l'état du processus de nettoyage de disque :

```
disk sanitize status [disk_list]
```

5. Une fois le processus de nettoyage terminé, retournez les disques à l'état de spare de chaque disque :

```
disk sanitize release disk_name
```

6. Quittez le mode maintenance.

## Nettoyage d'un disque avec "nodeshell" commandes (toutes les versions d'ONTAP 9)

Pour toutes les versions d'ONTAP 9, lorsque le nettoyage de disque est activé à l'aide des commandes du nodeshell, certaines commandes de ONTAP bas niveau sont désactivées. Une fois le nettoyage de disque activé sur un nœud, il ne peut pas être désactivé.

### Avant de commencer

- Les disques doivent être des disques de spare ; ils doivent être détenus par un nœud, mais pas utilisés dans un niveau local (agrégat).

Si les disques sont partitionnés, aucune partition ne peut être utilisée dans un niveau local (agrégat).

- Les disques ne peuvent pas être des disques à autochiffrement (SED).

Vous devez utiliser le `storage encryption disk sanitize` Commande permettant de désinfecter un SED.

### "Cryptage des données au repos"

- Les disques ne peuvent pas faire partie d'un pool de stockage.

### Étapes

1. Si les disques que vous souhaitez désinfecter sont partitionnés, départitionnez chaque disque :



La commande permettant de départitionner un disque est uniquement disponible au niveau diagnostic et ne doit être effectuée qu'avec NetApp support supervision. **Il est fortement recommandé de contacter le support NetApp avant de continuer.** vous pouvez également consulter l'article de la base de connaissances "[Comment départitionner un lecteur de réserve dans ONTAP](#)".

```
disk unpartition disk_name
```

2. Entrez le nodeshell pour le nœud qui possède les disques à désinfecter :

```
system node run -node node_name
```

3. Activation du nettoyage de disque :

```
options licensed_feature.disk_sanitization.enable on
```

Vous êtes invité à confirmer la commande car elle est irréversible.

4. Basculer vers le niveau de privilège avancé du nodeshell :

```
priv set advanced
```

5. Procédez à la nettoyage des disques spécifiés :

```
disk sanitize start [-p pattern1|-r [-p pattern2|-r [-p pattern3|-r]]] [-c
cycle_count] disk_list
```



Ne mettez pas le nœud hors tension, ne perturbent pas la connectivité du stockage et ne supprimez pas la cible disques lors du nettoyage. Si le nettoyage est interrompu pendant la phase de formatage, le formatage la phase doit être redémarrée et doit se terminer avant que les disques ne soient désinfectés et prêts à l'être nous sommes retournés au pool de réserve. Si vous devez abandonner le processus de nettoyage, vous pouvez l'utiliser en procédant au nettoyage de disque abandonner la commande. Si les disques spécifiés sont en phase de formatage du nettoyage, le l'abandon ne se produit pas tant que la phase n'est pas terminée.

`-p pattern1 -p pattern2 -p pattern3` spécifie un cycle de un à trois octets hexadécimaux définis par l'utilisateur remplacer les motifs qui peuvent être appliqués successivement aux disques en cours de nettoyage. La valeur par défaut le motif est constitué de trois passes, avec 0x55 pour le premier passage, 0xaa pour le second passage et 0x3c pour le troisième passe.

`-r` remplace un remplacement à répétition par un remplacement aléatoire pour une ou toutes les passes.

`-c cycle_count` spécifie le nombre de fois où les modèles d'écrasement spécifiés sont appliqués.

La valeur par défaut est un cycle. La valeur maximale est de sept cycles.

`disk_list` Spécifie une liste séparée par des espaces des ID des disques de rechange à désinfecter.

6. Pour vérifier l'état du processus de nettoyage de disque :

```
disk sanitize status [disk_list]
```

7. Une fois le processus de nettoyage terminé, retournez les disques à l'état spare :

```
disk sanitize release disk_name
```

8. Retour au niveau de privilège admin du nodeshell :

```
priv set admin
```

9. Revenir à l'interface de ligne de commandes ONTAP :

```
exit
```

10. Déterminer si tous les disques ont été renvoyés à l'état de réserve :

```
storage aggregate show-spare-disks
```

|       |          |
|-------|----------|
| Si... | Alors... |
|-------|----------|

|                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tous les disques aseptisés sont répertoriés comme pièces de rechange            | Vous avez terminé. Les disques sont aseptisés et en état de rechange.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Certains des disques aseptisés ne sont pas répertoriés comme pièces de rechange | <p>Procédez comme suit :</p> <p>a. Entrer en mode de privilège avancé :</p> <pre>set -privilege advanced</pre> <p>b. Affectez les disques aseptisés non affectés au nœud approprié pour chaque disque :</p> <pre>storage disk assign -disk <i>disk_name</i> -owner <i>node_name</i></pre> <p>c. Renvoyer les disques à l'état libre pour chaque disque :</p> <pre>storage disk unfail -disk <i>disk_name</i> -s -q</pre> <p>d. Revenir en mode administratif :</p> <pre>set -privilege admin</pre> |

## Résultat

Les disques spécifiés sont aseptisés et désignés comme des disques de rechange chauds. Les numéros de série des disques aseptisés sont écrits sur `/etc/log/sanitized_disks`.

Les journaux de nettoyage des disques spécifiés, qui indiquent ce qui a été terminé sur chaque disque, sont écrits dans `/mroot/etc/log/sanitization.log`.

## Commandes de gestion des disques

Vous pouvez utiliser le `storage disk` et `storage aggregate` commandes pour gérer vos disques.

| Les fonctions que vous recherchez...                                                                                                | Utilisez cette commande...                      |
|-------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| Affiche la liste des disques de rechange, y compris les disques partitionnés, par propriétaire                                      | <code>storage aggregate show-spare-disks</code> |
| Afficher le type de RAID disque, l'utilisation actuelle et le groupe RAID par agrégat                                               | <code>storage aggregate show-status</code>      |
| Afficher le type RAID, l'utilisation actuelle, l'agrégat et le groupe RAID, y compris les unités de rechange pour disques physiques | <code>storage disk show -raid</code>            |



|                                                                                    |                                                                                                  |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Affiche la liste des disques défaillants                                           | <code>storage disk show -broken</code>                                                           |
| Affiche le nom du disque pré-cluster (nodescope) pour un disque                    | <code>storage disk show -primary-paths</code> (avancé)                                           |
| Allume la LED d'un disque ou d'un tiroir en particulier                            | <code>storage disk set-led</code>                                                                |
| Affiche le type de somme de contrôle d'un disque spécifique                        | <code>storage disk show -fields checksum-compatibility</code>                                    |
| Afficher le type de checksum pour tous les disques de spare                        | <code>storage disk show -fields checksum-compatibility -container-type spare</code>              |
| Affichez les informations relatives à la connectivité et au placement des disques  | <code>storage disk show -fields disk,primary-port,secondary-name,secondary-port,shelf,bay</code> |
| Affiche les noms des disques de pré-cluster pour des disques spécifiques           | <code>storage disk show -disk diskname -fields diskpathnames</code>                              |
| Afficher la liste des disques dans le centre de maintenance                        | <code>storage disk show -maintenance</code>                                                      |
| Affiche la durée de vie des SSD                                                    | <code>storage disk show -ssd-wear</code>                                                         |
| Départitionner un disque partagé                                                   | <code>storage disk unpartition</code> (disponible au niveau de diagnostic)                       |
| Remettre à zéro tous les disques non nuls                                          | <code>storage disk zerospares</code>                                                             |
| Arrêtez un processus de nettoyage continu sur un ou plusieurs disques spécifiés    | <code>system node run -node nodename -command disk sanitize</code>                               |
| Affiche les informations sur le disque de chiffrement de stockage                  | <code>storage encryption disk show</code>                                                        |
| Récupère les clés d'authentification de tous les serveurs de gestion des clés liés | <code>security key-manager restore</code>                                                        |

#### Informations associées

- ["Référence de commande ONTAP"](#)

#### Commandes permettant d'afficher les informations d'utilisation de l'espace

Vous utilisez le `storage aggregate` et `volume` Commandes pour voir l'espace utilisé

dans vos agrégats et volumes et leurs copies Snapshot.

| Pour afficher des informations sur...                                                                                                                                                      | Utilisez cette commande...                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Agrégats, y compris des informations détaillées sur les pourcentages d'espace utilisés et disponibles, la taille de la réserve Snapshot et d'autres informations d'utilisation de l'espace | <code>storage aggregate show</code><br><code>storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve</code> |
| Mode d'utilisation des disques et des groupes RAID dans un agrégat et état RAID                                                                                                            | <code>storage aggregate show-status</code>                                                                                               |
| Quantité d'espace disque qui serait récupérée si vous avez supprimé une copie Snapshot spécifique                                                                                          | <code>volume snapshot compute-reclaimable</code>                                                                                         |
| Quantité d'espace utilisée par un volume                                                                                                                                                   | <code>volume show -fields size,used,available,percent-used</code><br><code>volume show-space</code>                                      |
| Quantité d'espace utilisé par un volume dans l'agrégat contenant                                                                                                                           | <code>volume show-footprint</code>                                                                                                       |

#### Informations associées

- ["Référence de commande ONTAP"](#)

#### Commandes permettant d'afficher des informations sur les tiroirs de stockage

Vous utilisez le `storage shelf show` commande permettant d'afficher les informations de configuration et d'erreur de vos tiroirs disques.

| Si vous voulez afficher...                                                                 | Utilisez cette commande...                    |
|--------------------------------------------------------------------------------------------|-----------------------------------------------|
| Informations générales sur la configuration des tiroirs et l'état du matériel              | <code>storage shelf show</code>               |
| Informations détaillées pour un tiroir spécifique, y compris l'ID de la pile               | <code>storage shelf show -shelf</code>        |
| Non résolu, exploitables par le client, erreurs par tiroir                                 | <code>storage shelf show -errors</code>       |
| Informations sur les baies                                                                 | <code>storage shelf show -bay</code>          |
| Informations sur la connectivité                                                           | <code>storage shelf show -connectivity</code> |
| Informations de refroidissement, y compris les capteurs de température et les ventilateurs | <code>storage shelf show -cooling</code>      |

| Si vous voulez afficher...                                                                                          | Utilisez cette commande...              |
|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| Informations sur les modules d'E/S.                                                                                 | <code>storage shelf show -module</code> |
| Informations sur les ports                                                                                          | <code>storage shelf show -port</code>   |
| Informations d'alimentation, y compris les blocs d'alimentation, les capteurs de courant et les capteurs de tension | <code>storage shelf show -power</code>  |

#### Informations associées

- ["Référence de commande ONTAP"](#)

## Gérer les configurations RAID

### Présentation de la gestion des configurations RAID

Vous pouvez effectuer diverses procédures pour gérer les configurations RAID de votre système.

- **Aspects de la gestion des configurations RAID :**
  - ["Règles RAID par défaut pour les niveaux locaux \(agrégats\)"](#)
  - ["Niveaux de protection RAID pour les disques"](#)
- **Informations sur les disques et les groupes RAID pour un niveau local (agrégat)**
  - ["Déterminer les informations sur les disques et les groupes RAID pour un niveau local \(agrégat\)"](#)
- **Conversions de configuration RAID**
  - ["Conversion de RAID-DP en RAID-TEC"](#)
  - ["Passez de RAID-TEC à RAID-DP"](#)
- **Dimensionnement du groupe RAID**
  - ["Considérations relatives au dimensionnement des groupes RAID"](#)
  - ["Personnalisez la taille de votre groupe RAID"](#)

### Règles RAID par défaut pour les niveaux locaux (agrégats)

RAID-DP ou RAID-TEC est la règle RAID par défaut pour tous les nouveaux niveaux locaux (agrégats). La règle RAID détermine la protection de parité dont vous disposez en cas de défaillance de disque.

La technologie RAID-DP offre une protection à double parité en cas de défaillance d'un disque unique ou double. RAID-DP est la règle RAID par défaut pour les types de niveau local (agrégat) suivants :

- Niveaux locaux 100 % Flash
- Niveaux locaux de Flash Pool
- Niveaux locaux de disque dur hautes performances

RAID-TEC est pris en charge sur tous les types de disques et sur toutes les plateformes, y compris AFF. Les niveaux locaux contenant des disques plus volumineux ont plus de risques de pannes de disques simultanées. RAID-TEC contribue à réduire ce risque en proposant une protection à triple parité afin que vos données puissent résister à trois pannes de disques simultanées. RAID-TEC est la stratégie RAID par défaut pour les niveaux locaux de disques durs haute capacité avec des disques d'au moins 6 To.

Chaque type de stratégie RAID nécessite un nombre minimal de disques :

- RAID-DP : 5 disques au minimum
- RAID-TEC : minimum de 7 disques

### Niveaux de protection RAID pour les disques

ONTAP prend en charge trois niveaux de protection RAID pour les niveaux locaux (agrégats). Le niveau de protection RAID détermine le nombre de disques de parité disponibles pour la restauration des données en cas de défaillance de disque.

Avec la protection RAID, en cas de panne de disque de données au sein d'un groupe RAID, ONTAP peut remplacer le disque défectueux par un disque de spare et utiliser les données de parité pour reconstruire les données du disque défaillant.

- \* RAID4\*

Avec la protection RAID4, ONTAP peut utiliser un disque de rechange pour remplacer et reconstruire les données à partir d'un disque défaillant au sein du groupe RAID.

- **RAID-DP**

Grâce à la protection RAID-DP, ONTAP peut utiliser jusqu'à deux disques de spare pour remplacer et reconstruire les données à partir d'un maximum de deux disques défectueux simultanément au sein du groupe RAID.

- **RAID-TEC**

Grâce à la protection RAID-TEC, ONTAP peut utiliser jusqu'à trois disques de spare pour remplacer et reconstruire les données à partir d'un maximum de trois disques défectueux simultanément au sein du groupe RAID.

### Informations sur les disques et groupes RAID pour un niveau local (agrégat)

Certaines tâches d'administration de niveau local (agrégat) nécessitent de savoir quels types de disques composent le niveau local, leur taille, leur checksum et leur état, qu'ils soient partagés avec d'autres niveaux locaux, ainsi que la taille et la composition des groupes RAID.

#### Étape

1. Afficher les disques de l'agrégat, par groupe RAID :

```
storage aggregate show-status aggr_name
```

Les disques sont affichés pour chaque groupe RAID de l'agrégat.

Vous pouvez afficher le type RAID du disque (données, parité, parité) dans le `Position` colonne. Si le `Position` s'affiche `shared`, Le lecteur est ensuite partagé : s'il s'agit d'un disque dur, il s'agit d'un disque partitionné ; s'il s'agit d'un disque SSD, il fait partie d'un pool de stockage.

```
cluster1::> storage aggregate show-status nodeA_fp_1
```

Owner Node: cluster1-a

Aggregate: nodeA\_fp\_1 (online, mixed RAID type, hybrid) (block checksums)

Plex: /nodeA\_fp\_1/plex0 (online, normal, active, pool0)

RAID Group /nodeA\_fp\_1/plex0/rg0 (normal, block checksums, RAID-DP)

| Position | Disk   | Pool | Type | RPM   | Usable Size | Physical Size | Status   |
|----------|--------|------|------|-------|-------------|---------------|----------|
| shared   | 2.0.1  | 0    | SAS  | 10000 | 472.9GB     | 547.1GB       | (normal) |
| shared   | 2.0.3  | 0    | SAS  | 10000 | 472.9GB     | 547.1GB       | (normal) |
| shared   | 2.0.5  | 0    | SAS  | 10000 | 472.9GB     | 547.1GB       | (normal) |
| shared   | 2.0.7  | 0    | SAS  | 10000 | 472.9GB     | 547.1GB       | (normal) |
| shared   | 2.0.9  | 0    | SAS  | 10000 | 472.9GB     | 547.1GB       | (normal) |
| shared   | 2.0.11 | 0    | SAS  | 10000 | 472.9GB     | 547.1GB       | (normal) |

RAID Group /nodeA\_flashpool\_1/plex0/rg1

(normal, block checksums, RAID4) (Storage Pool: SmallSP)

| Position | Disk   | Pool | Type | RPM | Usable Size | Physical Size | Status   |
|----------|--------|------|------|-----|-------------|---------------|----------|
| shared   | 2.0.13 | 0    | SSD  | -   | 186.2GB     | 745.2GB       | (normal) |
| shared   | 2.0.12 | 0    | SSD  | -   | 186.2GB     | 745.2GB       | (normal) |

8 entries were displayed.

## Conversion de RAID-DP en RAID-TEC

Si vous souhaitez bénéficier de la protection supplémentaire de la triple parité, vous pouvez passer de RAID-DP à RAID-TEC. RAID-TEC est recommandé si la taille des disques utilisés dans votre niveau local (agrégat) est supérieure à 4 To.

### Ce dont vous avez besoin

Le niveau local (agrégat) à convertir doit comporter au moins sept disques.

### Description de la tâche

- Les niveaux locaux de disque dur peuvent être convertis de RAID-DP à RAID-TEC. Cela inclut les niveaux de disques durs dans les niveaux locaux de Flash Pool.
- Pour comprendre les implications d'une conversion entre types RAID, reportez-vous à la section ["paramètres"](#) pour la `storage aggregate modify` commande.

## Étapes

1. Vérifier que l'agrégat est en ligne et dispose d'un minimum de six disques :

```
storage aggregate show-status -aggregate aggregate_name
```

2. Conversion de l'agrégat de RAID-DP en RAID-TEC :

```
storage aggregate modify -aggregate aggregate_name -raidtype raid_tec
```

3. Vérifier que la politique RAID de l'agrégat est RAID-TEC :

```
storage aggregate show aggregate_name
```

## Passez de RAID-TEC à RAID-DP

Si vous réduisez la taille de votre niveau local (agrégat) et n'avez plus besoin de la triple parité, vous pouvez convertir votre stratégie RAID RAID-TEC en RAID-DP et réduire le nombre de disques nécessaires pour la parité RAID.

### Ce dont vous avez besoin

La taille maximale du groupe RAID pour RAID-TEC est supérieure à la taille maximale du groupe RAID pour RAID-DP. Si la plus grande taille de groupe RAID-TEC ne se trouve pas dans les limites RAID-DP, vous ne pouvez pas convertir en RAID-DP.

### Description de la tâche

Pour comprendre les implications d'une conversion entre types RAID, reportez-vous à la section ["paramètres"](#) pour la `storage aggregate modify` commande.

## Étapes

1. Vérifier que l'agrégat est en ligne et dispose d'un minimum de six disques :

```
storage aggregate show-status -aggregate aggregate_name
```

2. Conversion de l'agrégat de RAID-TEC en RAID-DP :

```
storage aggregate modify -aggregate aggregate_name -raidtype raid_dp
```

3. Vérifier que la politique RAID de l'agrégat est RAID-DP :

```
storage aggregate show aggregate_name
```

## Considérations relatives au dimensionnement des groupes RAID

Pour configurer une taille de groupe RAID optimale, il faut faire une reprise des facteurs. Vous devez décider des facteurs (vitesse de reconstruction RAID, assurance contre le risque de perte de données en raison de défaillances de disque, optimisation des performances d'E/S et optimisation de l'espace de stockage) qui sont les plus importants pour l'agrégat (niveau local) que vous configurez.

Lorsque vous créez de plus grands groupes RAID, vous optimisez l'espace disponible pour le stockage des

données pour la même quantité de stockage utilisée pour la parité (également appelée « taxe de parité »). Par ailleurs, lorsqu'un disque tombe en panne au sein d'un groupe RAID plus important, le temps de reconstruction augmente et les performances sont affectées pendant une période plus longue. En outre, le fait d'avoir plus de disques dans un groupe RAID augmente la probabilité d'une défaillance de plusieurs disques au sein d'un même groupe RAID.

#### **Groupes RAID de disques durs ou de LUN de baies**

Lors du dimensionnement de vos groupes RAID composés de disques durs ou de LUN de baies, veuillez à respecter les consignes suivantes :

- Tous les RAID groupes d'un niveau local (agrégat) doivent avoir le même nombre de disques.

Même si le nombre de disques des différents groupes raid peut être inférieur ou égal à 50 % sur un niveau local, cela peut entraîner des goulets d'étranglement des performances dans certains cas, ce qui évite généralement d'avoir à utiliser cette méthode.

- La plage recommandée pour les disques des groupes RAID est comprise entre 12 et 20.

La fiabilité des disques hautes performances peut prendre en charge une taille de groupe RAID allant jusqu'à 28, si nécessaire.

- Si les deux premières directives sont conformes à plusieurs numéros de disques de groupe RAID, vous devez choisir le plus grand nombre de disques.

#### **Groupes RAID SSD dans les niveaux locaux de Flash Pool (agrégats)**

La taille du groupe RAID SSD peut être différente de la taille du groupe RAID pour les groupes RAID de disques durs dans un niveau local Flash Pool (agrégat). En règle générale, vous devez vous assurer que vous ne disposez que d'un seul groupe SSD RAID pour un niveau local Flash Pool, afin de réduire le nombre de disques SSD requis pour la parité.

#### **Groupes RAID SSD dans niveaux locaux SSD (agrégats)**

Lors du dimensionnement de vos groupes RAID composés de disques SSD, veuillez à respecter les consignes suivantes :

- Tous les RAID groupes d'un niveau local (agrégat) doivent disposer d'un nombre similaire de disques.

Il n'est pas nécessaire que les groupes RAID soient de la même taille, mais ne doivent pas avoir de groupe RAID de moins de la moitié de la taille des autres groupes RAID du même niveau local lorsque cela est possible.

- Pour RAID-DP, la plage recommandée pour la taille de groupe RAID est comprise entre 20 et 28.

#### **Personnalisez la taille de vos groupes RAID**

Vous pouvez personnaliser la taille de vos groupes RAID afin de vous assurer que les tailles de groupes RAID sont adaptées à la quantité de stockage que vous prévoyez d'inclure pour un niveau local (agrégat).

#### **Description de la tâche**

Pour les niveaux locaux standard (agrégats), vous modifiez séparément la taille des groupes RAID pour chaque niveau local. Pour les niveaux locaux de Flash Pool, vous pouvez modifier la taille du groupe RAID des groupes RAID SSD et des groupes RAID de disques durs de manière indépendante.

La liste suivante décrit quelques faits relatifs à la modification de la taille du groupe RAID :

- Par défaut, si le nombre de disques ou de LUN de baie du groupe RAID le plus récent est inférieur à la nouvelle taille de groupe RAID, des disques ou des LUN de baie sont ajoutés au groupe RAID le plus récent jusqu'à ce qu'il atteigne la nouvelle taille.
- Tous les autres groupes RAID existants de ce niveau local restent de la même taille, à moins d'ajouter explicitement des disques.
- Vous ne pouvez jamais augmenter la taille d'un groupe RAID par rapport à la taille maximale actuelle du groupe RAID pour le niveau local.
- Vous ne pouvez pas réduire la taille des groupes RAID déjà créés.
- La nouvelle taille s'applique à tous les groupes RAID du niveau local concerné (ou, dans le cas d'un niveau local Flash Pool, tous les groupes RAID du type de groupe RAID affecté (SSD ou HDD)).

## Étapes

1. Utilisez la commande applicable :

| Les fonctions que vous recherchez...                                                         | Saisissez la commande suivante...                                                      |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Modifiez la taille maximale du groupe RAID pour les groupes SSD RAID d'un agrégat Flash Pool | <code>storage aggregate modify -aggregate aggr_name -cache-raid-group-size size</code> |
| Modifier la taille maximale de tout autre groupe RAID                                        | <code>storage aggregate modify -aggregate aggr_name -maxraidsz size</code>             |

## Exemples

La commande suivante modifie la taille maximale du groupe RAID de l'agrégat n1\_a4 en 20 disques ou LUN de baie :

```
storage aggregate modify -aggregate n1_a4 -maxraidsz 20
```

La commande suivante modifie la taille maximale du groupe RAID des groupes RAID cache SSD de l'agrégat Flash Pool n1\_cache\_a2 en 24 :

```
storage aggregate modify -aggregate n1_cache_a2 -cache-raid-group-size 24
```

## Gestion des niveaux locaux Flash Pool (agrégats)

### Gestion des niveaux Flash Pool (agrégats)

Vous pouvez effectuer diverses procédures pour gérer les niveaux Flash Pool (agrégats) du système.

- **Stratégies de mise en cache**
  - ["Règles de mise en cache au niveau local Flash Pool \(agrégat\)"](#)
  - ["Gérer les règles de mise en cache Flash Pool"](#)
- **Partitionnement SSD**
  - ["Partitionnement SSD Flash Pool pour les niveaux locaux Flash Pool \(agrégats\) avec pools de](#)



stockage"

- **Candidature et taille du cache**

- "Déterminer la candidature de Flash Pool et la taille optimale du cache"

- **Création de pool Flash**

- "Créez un niveau local Flash Pool (agrégat) à l'aide de disques SSD physiques"
- "Créez un niveau local Flash Pool (agrégat) à l'aide de pools de stockage SSD"

### **Règles de mise en cache au niveau local Flash Pool (agrégat)**

Les règles de mise en cache des volumes au niveau local Flash Pool (agrégat) vous permettent de déployer la technologie Flash en tant que cache hautes performances pour votre jeu de données de travail tout en utilisant des disques durs à moindre coût pour les données auxquelles vous accédez moins. Si vous fournissez un cache à deux niveaux locaux Flash Pool ou plus, vous devez utiliser le partitionnement SSD Flash Pool pour partager les disques SSD entre les niveaux locaux de Flash Pool.

Les règles de mise en cache sont appliquées aux volumes résidant dans les niveaux locaux Flash Pool. Vous devez comprendre le fonctionnement des stratégies de mise en cache avant de les modifier.

Dans la plupart des cas, la politique de mise en cache par défaut de « auto » est la meilleure politique de mise en cache à utiliser. La règle de mise en cache ne doit être modifiée que si une autre règle améliore les performances de votre charge de travail. La configuration d'une règle de mise en cache incorrecte peut fortement dégrader les performances des volumes. La dégradation des performances peut augmenter progressivement au fil du temps.

Les règles de mise en cache combinent une règle de mise en cache de lecture et une règle de mise en cache d'écriture. Le nom de la règle concatène les noms de la règle de mise en cache des lectures et de la règle de mise en cache des écritures, séparés par un tiret. S'il n'y a pas de trait d'Union dans le nom de la politique, la politique de mise en cache des écritures est « aucune », à l'exception de la politique « auto ».

Les règles de mise en cache de lecture optimisent l'utilisation pour les performances de lecture futures en plaçant des copies des données dans le cache en plus des données stockées sur des disques durs. Pour les règles de mise en cache de lecture qui insèrent des données dans le cache pour les opérations d'écriture, le cache fonctionne comme un *cache-transfert*.

Les données insérées dans le cache en utilisant la règle de mise en cache d'écriture n'existent que dans le cache ; il n'y a pas de copie dans les disques durs. Le cache Flash Pool est protégé par RAID. L'activation de la mise en cache d'écriture permet aux données d'effectuer immédiatement des opérations d'écriture à partir du cache, puis de reporter l'écriture des données sur les disques durs jusqu'à ce qu'elles deviennent hors du cache.

Si vous déplacez un volume d'un niveau local Flash Pool vers un niveau local à un niveau unique, sa stratégie de mise en cache est perdue. Par la suite, vous la redéplacez sur un niveau local Flash Pool, elle se voit assignée à la stratégie de mise en cache par défaut de « auto ». Si vous déplacez un volume entre deux niveaux locaux Flash Pool, la règle de mise en cache est conservée.

### **Modifier une règle de mise en cache**

Vous pouvez utiliser l'interface de ligne de commandes pour modifier la règle de mise en cache d'un volume résidant sur un niveau local Flash Pool à l'aide de `-caching-policy` paramètre avec le `volume create` commande.

Lorsque vous créez un volume sur un niveau local Flash Pool, la règle de mise en cache « automatique » est attribuée par défaut au volume.

## Gérer les règles de mise en cache Flash Pool

### Présentation de la gestion des règles de mise en cache Flash Pool

L'utilisation de l'interface de ligne de commandes permet d'effectuer diverses procédures de gestion des règles de mise en cache Flash Pool sur votre système.

- **Préparation**

- "Déterminer si modifier la règle de mise en cache des niveaux locaux Flash Pool (agrégats)"

- **Modification des stratégies de mise en cache**

- "Modifier les règles de mise en cache des niveaux locaux Flash Pool (agrégats)"
- "Définir la règle de conservation du cache pour les niveaux locaux Flash Pool (agrégats)"

### Déterminer si modifier la règle de mise en cache des niveaux locaux Flash Pool (agrégats)

Vous pouvez attribuer des règles de conservation du cache aux volumes des niveaux locaux Flash Pool (agrégats) afin de déterminer la durée pendant laquelle les données du volume restent dans le cache Flash Pool. Toutefois, dans certains cas, la modification de la règle de conservation du cache peut n'avoir aucune incidence sur la durée pendant laquelle les données du volume sont conservées dans le cache.

### Description de la tâche

Si vos données répondent à l'une des conditions suivantes, la modification de la règle de conservation du cache peut n'avoir aucun impact :

- Votre charge de travail est séquentielle.
- Votre charge de travail ne relise pas les blocs aléatoires mis en cache dans les disques SSD.
- La taille du cache du volume est trop petite.

### Étapes

Les étapes suivantes permettent de vérifier les conditions devant être remplies par les données. La tâche doit être effectuée à l'aide de l'interface de ligne de commandes en mode de privilège avancé.

1. Utilisez l'interface de ligne de commande pour afficher le volume des workloads :

```
statistics start -object workload_volume
```

2. Déterminez le modèle de charge de travail du volume :

```
statistics show -object workload_volume -instance volume-workload -counter sequential_reads
```

3. Déterminez le taux d'impact du volume :

```
statistics show -object waf1_hya_vvol -instance volume -counter read_ops_replaced_pwercent|wc_write_blks_overwritten_percent
```

#### 4. Déterminez le `Cacheable Read` et `Project Cache Alloc` du volume :

```
system node run -node node_name wafl awa start aggr_name
```

#### 5. Afficher le résumé AWA :

```
system node run -node node_name wafl awa print aggr_name
```

#### 6. Comparez le taux de réussite du volume avec le `Cacheable Read`.

Si le taux de réussite du volume est supérieur à `Cacheable Read`, Votre charge de travail ne relise pas les blocs aléatoires mis en cache dans les disques SSD.

#### 7. Comparer la taille actuelle du cache au `Project Cache Alloc`.

Si la taille actuelle du cache du volume est supérieure à `Project Cache Alloc`, puis la taille de votre cache de volume est trop petite.

### Modifier les règles de mise en cache des niveaux locaux Flash Pool (agrégats)

Vous devez modifier la stratégie de mise en cache d'un volume uniquement si une règle de mise en cache différente est censée améliorer les performances. Vous pouvez modifier la politique de mise en cache d'un volume situé au niveau local Flash Pool (agrégat).

#### Ce dont vous avez besoin

Vous devez déterminer si vous souhaitez modifier votre stratégie de mise en cache.

#### Description de la tâche

Dans la plupart des cas, la politique de mise en cache par défaut de « auto » est la meilleure stratégie de mise en cache que vous pouvez utiliser. La règle de mise en cache ne doit être modifiée que si une autre règle améliore les performances de votre charge de travail. La configuration d'une règle de mise en cache incorrecte peut fortement dégrader les performances des volumes. La dégradation des performances peut augmenter progressivement au fil du temps. Vous devez être prudent lorsque vous modifiez les règles de mise en cache. Si vous rencontrez des problèmes de performances avec un volume pour lequel la stratégie de mise en cache a été modifiée, vous devez rétablir la règle de mise en cache sur « auto ».

#### Étape

1. Utiliser l'interface de ligne de commande pour modifier la règle de mise en cache du volume :

```
volume modify -volume volume_name -caching-policy policy_name
```

#### Exemple

L'exemple suivant modifie la politique de mise en cache d'un volume nommé `vol2` en politique `none`:

```
volume modify -volume vol2 -caching-policy none
```

### Définir la règle de conservation du cache pour les niveaux locaux Flash Pool (agrégats)

Vous pouvez attribuer des règles de conservation du cache aux volumes des niveaux locaux Flash Pool (agrégats). Les données des volumes dont la règle de conservation du

cache est élevée restent mises en cache plus longtemps et les données des volumes dont la règle de conservation du cache est faible sont supprimées plus rapidement. Vos workloads stratégiques sont ainsi plus performants en rendant les informations prioritaires accessibles plus rapidement et sur une période plus longue.

**Ce dont vous avez besoin**

Vous devez savoir si votre système présente des conditions qui peuvent empêcher la règle de rétention du cache d’avoir un impact sur la durée pendant laquelle vos données restent en cache.

**Étapes**

Utilisez l’interface de ligne de commandes en mode de privilège avancé pour effectuer les étapes suivantes :

- 1. Modifiez le paramètre de privilège sur avancé :

```
set -privilege advanced
```

- 2. Vérifiez la règle de conservation du cache du volume :

Par défaut, la politique de conservation du cache est « normale ».

- 3. Définissez la règle de rétention du cache :

| Version ONTAP                   | Commande                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ONTAP 9.0, 9.1                  | <pre>priority hybrid-cache set volume_name<br/>read-cache=read_cache_value write-<br/>cache=write_cache_value cache-<br/>retention-<br/>priority=cache_retention_policy</pre> <p>Réglez <code>cache_retention_policy</code> à <code>high</code> si vous souhaitez conserver les données dans le cache, Réglez <code>cache_retention_policy</code> à <code>low</code> permet de supprimer plus rapidement les données du cache.</p> |
| ONTAP 9.2 ou version ultérieure | <pre>volume modify -volume volume_name<br/>-vserver vsriver_name -caching-policy<br/>policy_name.</pre>                                                                                                                                                                                                                                                                                                                            |

- 4. Vérifiez que la règle de conservation du cache du volume est modifiée en fonction de l’option que vous avez sélectionnée.

- 5. Renvoyez le paramètre de privilège à admin :

```
set -privilege admin
```

**Partitionnement SSD Flash Pool pour les niveaux locaux Flash Pool (agrégats) avec pools de stockage**

Si vous fourni le cache à deux niveaux locaux (agrégats) Flash Pool ou plus, il est conseillé d’utiliser le partitionnement SSD Flash Pool. Le partitionnement SSD Flash Pool

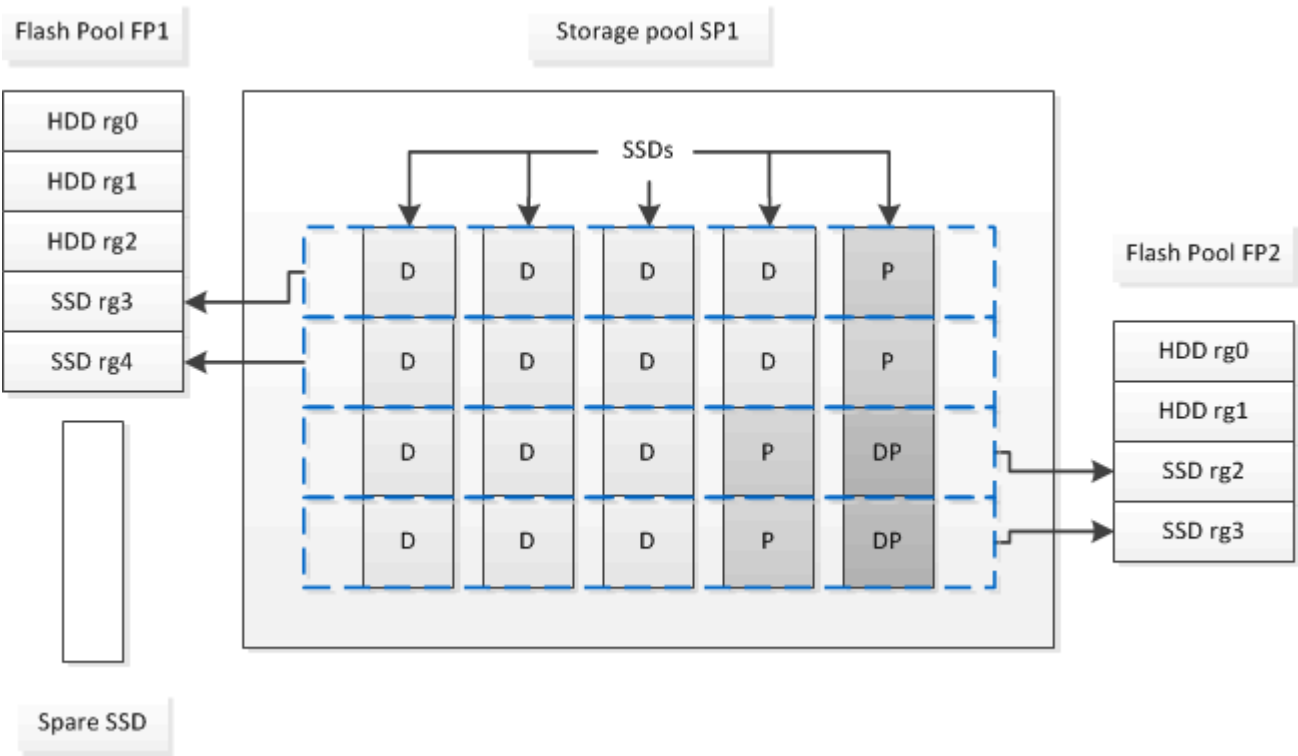
permet de partager les disques SSD entre tous les niveaux locaux qui utilisent Flash Pool. Le coût de la parité est ainsi bien supérieur à celui des tiers locaux, ce qui augmente la flexibilité de l'allocation du cache SSD et optimise les performances des SSD.

Pour qu'un disque SSD soit utilisé dans un niveau local Flash Pool, il doit être placé dans un pool de stockage. Vous ne pouvez pas utiliser des disques SSD partitionnés pour le partitionnement données-racines dans un pool de stockage. Une fois le disque SSD placé dans le pool de stockage, il ne peut plus être géré comme un disque autonome. Il ne peut plus être supprimé du pool de stockage, à moins que vous détruisiez les niveaux locaux associés à Flash Pool et détruisiez le pool de stockage.

Les pools de stockage SSD sont répartis en quatre unités d'allocation identiques. Les disques SSD ajoutés au pool de stockage sont répartis en quatre partitions et une partition est attribuée à chacune des quatre unités d'allocation. Les disques SSD du pool de stockage doivent être détenus par la même paire haute disponibilité. Par défaut, deux unités d'allocation sont attribuées à chaque nœud de la paire HA. Les unités d'allocation doivent être détenues par le nœud propriétaire du niveau local qu'elles servent. Si des niveaux locaux sont requis de Flash cache supplémentaires sur l'un des nœuds, le nombre d'unités d'allocation par défaut peut être modifié pour diminuer le nombre sur un nœud et augmenter le nombre sur le nœud partenaire.

Vous utilisez des disques SSD de rechange pour ajouter des disques à un pool de stockage SSD. Si le pool de stockage fournit des unités d'allocation aux niveaux locaux Flash Pool détenus par les deux nœuds de la paire haute disponibilité, les disques SSD de secours peuvent être la propriété de chaque nœud. Toutefois, si le pool de stockage fournit des unités d'allocation uniquement aux niveaux locaux Flash Pool détenus par l'un des nœuds de la paire haute disponibilité, les disques de secours SSD doivent être la propriété du même nœud.

L'illustration suivante est un exemple de partitionnement SSD Flash Pool. Le pool de stockage SSD fournit un cache à deux niveaux locaux Flash Pool :



Le pool de stockage SP1 se compose de cinq disques SSD et d'un disque SSD de secours. Deux unités d'allocation du pool de stockage sont allouées à Flash Pool FP1, et deux sont allouées à Flash Pool FP2. FP1 dispose d'un type RAID de cache du RAID4. Par conséquent, les unités d'allocation fournies à FP1 ne

contiennent qu'une seule partition désignée pour la parité. FP2 dispose d'un type RAID de cache de RAID-DP. Ainsi, les unités d'allocation fournies à FP2 incluent une partition de parité et une partition à double parité.

Dans cet exemple, deux unités d'allocation sont allouées à chaque niveau local Flash Pool. Toutefois, si un niveau local Flash Pool nécessitait un plus grand cache, vous pouvez allouer trois des unités d'allocation au niveau local Flash Pool, et l'une à l'autre.

## Déterminer la candidature de Flash Pool et la taille optimale du cache

Avant de convertir un niveau local (agrégat) en niveau local Flash Pool, vous pouvez déterminer si le niveau local est limité aux E/S et la taille de cache Flash Pool la plus adaptée à votre charge de travail et à votre budget. Vous pouvez également vérifier si le cache d'un niveau local Flash Pool existant est correctement dimensionné.

### Ce dont vous avez besoin

Vous devez savoir approximativement quand le niveau local que vous analysez subit son pic de charge.

### Étapes

1. Entrer en mode avancé :

```
set advanced
```

2. Si vous avez besoin de déterminer si un niveau local (agrégat) existant serait un bon candidat pour la conversion en un agrégat Flash Pool, déterminez quelle est la occupation des disques de l'agrégat pendant une période de pics de charge et comment cela affecte la latence :

```
statistics show-periodic -object disk:raid_group -instance raid_group_name
-counter disk_busy|user_read_latency -interval 1 -iterations 60
```

Vous pouvez décider si la réduction de la latence via l'ajout de cache Flash Pool convient à cet agrégat.

La commande suivante présente les statistiques du premier groupe RAID de l'agrégat « aggr1 » :

```
statistics show-periodic -object disk:raid_group -instance /aggr1/plex0/rg0
-counter disk_busy|user_read_latency -interval 1 -iterations 60
```

3. Démarrer l'analyseur de charge de travail automatisé (AWA) :

```
storage automated-working-set-analyzer start -node node_name -aggregate
aggr_name
```

AWA commence à collecter les données de charge de travail pour les volumes associés à l'agrégat spécifié.

4. Quitter le mode avancé :

```
set admin
```

Laisser l'AWA tourner jusqu'à ce qu'un ou plusieurs intervalles de charge de crête aient eu lieu. AWA collecte les statistiques de charge de travail pour les volumes associés à l'agrégat spécifié et analyse les données pour une durée d'une semaine de roulement maximum. L'utilisation de l'AWA pendant plus d'une semaine ne fera rapport que sur les données collectées au cours de la semaine la plus récente. Les estimations de la taille du cache sont basées sur les charges les plus élevées observées pendant la

période de collecte des données ; la charge n'a pas besoin d'être élevée pendant toute la période de collecte des données.

5. Entrer en mode avancé :

```
set advanced
```

6. Afficher l'analyse des charges de travail :

```
storage automated-working-set-analyzer show -node node_name -instance
```

7. Arrêt AWA :

```
storage automated-working-set-analyzer stop node_name
```

Toutes les données des charges de travail sont transférées et ne sont plus disponibles pour l'analyse.

8. Quitter le mode avancé :

```
set admin
```

## Créez un niveau local Flash Pool (agrégat) à l'aide de disques SSD physiques

Vous créez un niveau local Flash Pool (agrégat) en activant la fonctionnalité sur un niveau local existant composé de groupes RAID de disques durs, puis en ajoutant un ou plusieurs groupes RAID SSD à ce niveau local. Ce niveau local compte deux ensembles de groupes RAID pour ce niveau local : groupes RAID SSD (cache SSD) et groupes RAID de disques durs.

### Description de la tâche

Après avoir ajouté un cache SSD à un niveau local pour créer un niveau local Flash Pool, vous ne pouvez pas supprimer le cache SSD afin de reconvertir le niveau local en sa configuration d'origine.

Par défaut, le niveau RAID du cache SSD est le même que le niveau RAID des groupes RAID de disques durs. Vous pouvez remplacer cette sélection par défaut en spécifiant l'option « raidtype » lorsque vous ajoutez les premiers groupes RAID SSD.

### Avant de commencer

- Vous devez avoir identifié un niveau local valide composé de disques durs à convertir en niveau local Flash Pool.
- Vous devez avoir déterminé l'éligibilité à la mise en cache en écriture des volumes associés au niveau local et avoir effectué toutes les étapes requises pour résoudre les problèmes d'éligibilité.
- Vous devez avoir déterminé que les disques SSD que vous allez ajouter. Ces disques doivent appartenir au nœud sur lequel vous créez le niveau local Flash Pool.
- Vous devez avoir déterminé les types de checksum concernant les deux disques SSD que vous ajoutez et les disques durs déjà présents dans le Tier local.
- Vous devez avoir déterminé le nombre de disques SSD que vous ajoutez et la taille de groupe RAID optimale pour les groupes SSD RAID.

L'utilisation d'un moins grand nombre de groupes RAID dans le cache SSD réduit le nombre de disques de parité requis, mais les groupes RAID de taille supérieure requièrent RAID-DP.

- Vous devez avoir déterminé le niveau de RAID que vous souhaitez utiliser pour le cache SSD.
- Vous devez avoir déterminé la taille maximale du cache de votre système et déterminé que l'ajout de cache SSD au niveau local ne vous fera pas dépasser.
- Vous devez vous familiariser avec les conditions de configuration requises pour les niveaux locaux Flash Pool.


## Étapes

Vous pouvez créer un agrégat Flash Pool à l'aide de System Manager ou de l'interface de ligne de commande ONTAP.

### System Manager

Depuis ONTAP 9.12.1, vous pouvez utiliser System Manager pour créer un niveau local Flash Pool à l'aide de disques SSD physiques.

#### Étapes

1. Sélectionnez **stockage > niveaux**, puis sélectionnez un niveau de stockage de disque dur local existant.
2. Sélectionnez  puis **Ajouter Flash Pool cache**.
3. Sélectionnez **utiliser des disques SSD dédiés comme cache**.
4. Sélectionnez un type de disque et le nombre de disques.
5. Choisissez un type de RAID.
6. Sélectionnez **Enregistrer**.
7. Localisez le niveau de stockage, puis sélectionnez .
8. Sélectionnez **plus de détails**. Vérifiez que Flash Pool indique **activé**.

### CLI

#### Étapes

1. Marquer le niveau local (agrégat) comme éligible pour devenir un agrégat Flash Pool :

```
storage aggregate modify -aggregate aggr_name -hybrid-enabled true
```

Si cette étape ne réussisse pas, déterminez l'éligibilité à la mise en cache des écritures pour l'agrégat cible.

2. Ajouter les disques SSD à l'agrégat en utilisant le `storage aggregate add` commande.
  - Vous pouvez spécifier les disques SSD par ID ou à l'aide de `diskcount` et `disktype` paramètres.
  - Si les disques durs et les disques SSD ne disposent pas du même type de checksum, ou si l'agrégat est un checksum mixte, vous devez utiliser le `checksumstyle` paramètre pour spécifier le type de checksum des disques que vous ajoutez à l'agrégat.
  - Vous pouvez spécifier un autre type RAID pour le cache SSD à l'aide de la `raidtype` paramètre.
  - Si vous souhaitez que la taille du groupe RAID du cache soit différente de celle par défaut du type RAID que vous utilisez, vous devez le modifier maintenant à l'aide de `-cache-raid-group -size` paramètre.



## Créez un niveau local Flash Pool (agrégat) à l'aide de pools de stockage SSD

### Présentation de la création d'un niveau local Flash Pool (agrégat) à l'aide de pools de stockage SSD

Plusieurs procédures sont disponibles pour créer un niveau local Flash Pool (agrégat) à l'aide des pools de stockage SSD :

- **Préparation**
  - "Déterminez si un niveau local Flash Pool (agrégat) utilise un pool de stockage SSD"
- **Création du pool de stockage SSD**
  - "Créer un pool de stockage SSD"
  - "Ajoutez des disques SSD à un pool de stockage SSD"
- **Création de pool Flash à l'aide de pools de stockage SSD**
  - "Créez un niveau local Flash Pool (agrégat) en utilisant des unités d'allocation de pools de stockage SSD"
  - "Déterminez l'impact de l'ajout de disques SSD à un pool de stockage SSD sur la taille du cache"

### Déterminez si un niveau local Flash Pool (agrégat) utilise un pool de stockage SSD

Vous pouvez configurer un agrégat Flash Pool (niveau local) en ajoutant une ou plusieurs unités d'allocation d'un pool de stockage SSD à un niveau local HDD existant.

Les niveaux locaux Flash Pool sont gérés de façon différente lorsqu'ils utilisent des pools de stockage SSD pour fournir leur cache qu'ils utilisent des disques SSD distincts.

#### Étape

1. Afficher les disques de l'agrégat par groupe RAID :

```
storage aggregate show-status aggr_name
```

Si l'agrégat utilise un ou plusieurs pools de stockage SSD, la valeur pour le système `Position` La colonne des groupes SSD RAID s'affiche comme `Shared`, Et le nom du pool de stockage s'affiche en regard du nom du groupe RAID.

### Ajout de cache à un niveau local (agrégat) en créant un pool de stockage SSD

Pour provisionner le cache, il vous suffit de convertir un niveau local (agrégat) en agrégat (Flash Pool local Tier) en ajoutant des disques SSD.

Vous pouvez créer des pools de stockage SSD afin de fournir un cache SSD pour deux à quatre niveaux locaux Flash Pool (agrégats). Les agrégats Flash Pool vous permettent de déployer la technologie Flash comme cache haute performance pour vos données de travail tout en utilisant des disques durs à moindre coût pour les données moins fréquemment utilisées.

#### Description de la tâche

- Vous devez fournir une liste de disques lors de la création ou de l'ajout de disques à un pool de stockage.

Les pools de stockage ne prennent pas en charge un `diskcount` paramètre.

- Les disques SSD utilisés dans le pool de stockage doivent être de la même taille.

## System Manager

### Utilisez System Manager pour ajouter un cache SSD (ONTAP 9.12.1 et versions ultérieures)

Depuis ONTAP 9.12.1, vous pouvez utiliser System Manager pour ajouter un cache SSD.



Les options de pool de stockage ne sont pas disponibles sur les systèmes AFF.

#### Étapes

1. Cliquez sur **Cluster > disques**, puis sur **Afficher/Masquer**.
2. Sélectionnez **Type** et vérifiez que des disques SSD de rechange existent sur le cluster.
3. Cliquez sur **stockage > niveaux** et cliquez sur **Ajouter un pool de stockage**.
4. Sélectionnez le type de disque.
5. Entrez une taille de disque.
6. Sélectionnez le nombre de disques à ajouter au pool de stockage.
7. Vérifiez la taille estimée du cache.

### Utilisez System Manager pour ajouter un cache SSD (ONTAP 9.7 uniquement)



Utilisez la procédure de l'interface de ligne de commandes si vous utilisez une version ONTAP ultérieure à ONTAP 9.7 ou antérieure à ONTAP 9.12.1.

#### Étapes

1. Cliquez sur \* (revenir à la version classique)\*.
2. Cliquez sur **stockage > agrégats et disques > agrégats**.
3. Sélectionnez le niveau local (agrégat), puis cliquez sur **actions > Ajouter cache**.
4. Sélectionnez la source de cache comme « pools de stockage » ou « disques SSD dédiés ».
5. Cliquez sur **(passer à la nouvelle expérience)**.
6. Cliquez sur **stockage > niveaux** pour vérifier la taille du nouvel agrégat.

## CLI

### Utilisez l'interface de ligne de commande pour créer un pool de stockage SSD

#### Étapes

1. Déterminez le nom des disques SSD de spare disponibles :

```
storage aggregate show-spare-disks -disk-type SSD
```

Les disques SSD utilisés dans un pool de stockage peuvent être détenus par l'un ou l'autre nœud d'une paire haute disponibilité.

2. Créez le pool de stockage :

```
storage pool create -storage-pool sp_name -disk-list disk1,disk2,...
```

### 3. **Facultatif** : Vérifiez le pool de stockage nouvellement créé :

```
storage pool show -storage-pool sp_name
```

#### Résultats

Une fois les disques SSD placés dans le pool de stockage, ils n'apparaissent plus en tant que disques de rechange sur le cluster, même si le stockage fourni par le pool de stockage n'a pas encore été alloué à des caches Flash Pool. Vous ne pouvez pas ajouter de disques SSD à un groupe RAID en tant que disques discrets ; leur stockage peut être provisionné uniquement à l'aide des unités d'allocation du pool de stockage auquel ils appartiennent.

#### Créez un niveau local Flash Pool (agrégat) en utilisant des unités d'allocation de pools de stockage SSD

Vous pouvez configurer un niveau local Flash Pool (agrégat) en ajoutant une ou plusieurs unités d'allocation d'un pool de stockage SSD à un niveau local HDD existant.

À partir de ONTAP 9.12.1, vous pouvez utiliser System Manager redessiné pour créer un niveau local Flash Pool à partir d'unités d'allocation de pool de stockage.

#### Ce dont vous avez besoin

- Vous devez avoir identifié un niveau local valide composé de disques durs à convertir en niveau local Flash Pool.
- Vous devez avoir déterminé l'éligibilité à la mise en cache en écriture des volumes associés au niveau local et avoir effectué toutes les étapes requises pour résoudre les problèmes d'éligibilité.
- Vous devez avoir créé un pool de stockage SSD afin de fournir le cache SSD à ce niveau local Flash Pool.

Toute unité d'allocation du pool de stockage que vous souhaitez utiliser doit appartenir au même nœud qui possède le niveau local Flash Pool.

- Vous devez avoir déterminé la quantité de cache que vous souhaitez ajouter au niveau local.

Vous ajoutez de la mémoire cache au niveau local par unités d'allocation. Si de l'espace est nécessaire, vous pouvez augmenter la taille des unités d'allocation en ajoutant des disques SSD au pool de stockage.

- Vous devez avoir déterminé le type de RAID que vous souhaitez utiliser pour le cache SSD.

Une fois que vous avez ajouté un cache au niveau local à partir des pools de stockage SSD, vous ne pouvez pas modifier le type RAID des groupes RAID de cache.

- Vous devez avoir déterminé la taille maximale du cache de votre système et déterminé que l'ajout de cache SSD au niveau local ne vous fera pas dépasser.

Vous pouvez voir la quantité de cache qui sera ajoutée à la taille totale du cache en utilisant le `storage pool show` commande.

- Vous devez vous familiariser avec les conditions de configuration requises pour le niveau local Flash Pool.

#### Description de la tâche

Si vous souhaitez que le type RAID du cache soit différent de celui des groupes RAID de disques durs, vous devez spécifier le type RAID du cache lors de l'ajout de la capacité SSD. Une fois la capacité SSD ajoutée au niveau local, vous ne pouvez plus modifier le type RAID du cache.

Après avoir ajouté un cache SSD à un niveau local pour créer un niveau local Flash Pool, vous ne pouvez pas supprimer le cache SSD afin de reconvertir le niveau local en sa configuration d'origine.

## System Manager

Depuis ONTAP 9.12.1, vous pouvez utiliser System Manager pour ajouter des disques SSD à un pool de stockage SSD.

### Étapes

1. Cliquez sur **stockage > niveaux** et sélectionnez un niveau de stockage de disque dur local existant.
2. Cliquez sur  et sélectionnez **Ajouter Flash Pool cache**.
3. Sélectionnez **utiliser les pools de stockage**.
4. Sélectionnez un pool de stockage.
5. Sélectionnez une taille de cache et une configuration RAID.
6. Cliquez sur **Enregistrer**.
7. Localisez à nouveau le niveau de stockage et cliquez sur .
8. Sélectionnez **plus de détails** et vérifiez que Flash Pool indique **activé**.

## CLI

### Étapes

1. Marquer l'agrégat comme éligible pour devenir un agrégat Flash Pool :

```
storage aggregate modify -aggregate aggr_name -hybrid-enabled true
```

Si cette étape ne réussisse pas, déterminez l'éligibilité à la mise en cache des écritures pour l'agrégat cible.

2. Afficher les unités d'allocation de pool de stockage SSD disponibles :

```
storage pool show-available-capacity
```

3. Ajout de la capacité SSD à l'agrégat :

```
storage aggregate add aggr_name -storage-pool sp_name -allocation-units
number_of_units
```

Si vous souhaitez que le type RAID du cache soit différent de celui des groupes RAID de disques durs, vous devez le modifier lorsque vous saisissez cette commande en utilisant le `raidtype` paramètre.

Il n'est pas nécessaire de spécifier un nouveau groupe RAID ; ONTAP place automatiquement le cache SSD dans des groupes RAID distincts des groupes RAID de disques durs.

Vous ne pouvez pas définir la taille du groupe RAID du cache ; elle est déterminée par le nombre de disques SSD du pool de stockage.

Le cache est ajouté à l'agrégat et l'agrégat est désormais un agrégat Flash Pool. Chaque unité d'allocation ajoutée à l'agrégat devient son propre groupe RAID.

4. Confirmer la présence et la taille du cache SSD :

```
storage aggregate show aggregate_name
```

La taille du cache est indiquée sous Total Hybrid Cache Size.

## Informations associées

["Rapport technique NetApp 4070 : Guide de la conception et de l'implémentation Flash Pool"](#)

### Déterminez l'impact de l'ajout de disques SSD à un pool de stockage SSD sur la taille du cache

Si l'ajout de disques SSD à un pool de stockage entraîne le dépassement de la limite de cache fixée par votre modèle de plateforme, ONTAP n'alloue pas la capacité nouvellement ajoutée aux niveaux locaux Flash Pool (agrégats). Cela peut entraîner la mise hors service de la capacité supplémentaire en partie ou en totalité.

### Description de la tâche

Lorsque vous ajoutez des disques SSD à un pool de stockage SSD dont les unités d'allocation sont déjà allouées aux niveaux locaux Flash Pool (agrégats), vous augmentez la taille du cache de chacun de ces niveaux locaux, ainsi que le cache total du système. Si aucune unité d'allocation du pool de stockage n'a été allouée, l'ajout de disques SSD à ce pool n'affecte la taille du cache SSD que lorsqu'une ou plusieurs unités d'allocation sont allouées à la mise en cache.

### Étapes

1. Déterminez la taille utilisable des disques SSD que vous ajoutez au pool de stockage :

```
storage disk show disk_name -fields usable-size
```

2. Déterminez le nombre d'unités d'allocation qui restent non allouées au pool de stockage :

```
storage pool show-available-capacity sp_name
```

Toutes les unités d'allocation non allouées du pool de stockage sont affichées.

3. Calculez la quantité de cache qui sera ajoutée en appliquant la formule suivante :

$(4 - \text{nombre d'unités d'allocation non allouées}) \times 25 \% \times \text{taille utilisable} \times \text{nombre de disques SSD}$

### Ajoutez des disques SSD à un pool de stockage SSD

Lorsque vous ajoutez des disques SSD à un pool de stockage SSD, vous augmentez les tailles physiques et utilisables du pool de stockage et la taille de l'unité d'allocation. La taille d'unité d'allocation plus importante affecte également les unités d'allocation qui ont déjà été allouées à des niveaux locaux (agrégats).

### Ce dont vous avez besoin

Vous devez avoir déterminé que cette opération n'entraînera pas le dépassement de la limite de cache pour la paire haute disponibilité. Lorsque vous ajoutez des disques SSD à un pool de stockage SSD, ONTAP ne vous empêche pas de dépasser la limite du cache, et l'utilisation de la nouvelle capacité de stockage ajoutée sera indisponible.

### Description de la tâche

Lorsque vous ajoutez des disques SSD à un pool de stockage SSD existant, les disques SSD doivent appartenir à un nœud ou à l'autre de la même paire haute disponibilité qui possédait déjà les disques SSD


existants du pool de stockage. Vous pouvez ajouter des disques SSD qui sont détenus par l'un ou l'autre nœuds de la paire HA.

Le disque SSD que vous ajoutez au pool de stockage doit être de la même taille que le disque actuellement utilisé dans le pool de stockage.

**System Manager**

Depuis ONTAP 9.12.1, vous pouvez utiliser System Manager pour ajouter des disques SSD à un pool de stockage SSD.

**Étapes**

- 1. Cliquez sur **stockage > niveaux** et recherchez la section **pools de stockage**.
- 2. Localisez le pool de stockage, cliquez sur , puis sélectionnez **Ajouter des disques**.
- 3. Choisissez le type de disque et sélectionnez le nombre de disques.
- 4. Vérifiez l'estimation de la taille du cache.

**CLI**

**Étapes**

- 1. **Facultatif** : consultez la taille de l'unité d'allocation actuelle et le stockage disponible pour le pool de stockage :

```
storage pool show -instance sp_name
```

- 2. Recherchez les disques SSD disponibles :

```
storage disk show -container-type spare -type SSD
```

- 3. Ajoutez les disques SSD au pool de stockage :

```
storage pool add -storage-pool sp_name -disk-list disk1,disk2...
```

Le système affiche les agrégats Flash Pool dont la taille a augmenté via cette opération et la quantité, et vous invite à confirmer l'opération.

**Commandes de gestion des pools de stockage SSD**

ONTAP offre la solution `storage pool` Commande permettant de gérer les pools de stockage SSD.

| Les fonctions que vous recherchez...                                                                                                                  | Utilisez cette commande...               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| Afficher la quantité de stockage qu'un pool de stockage fournit à quels agrégats                                                                      | <code>storage pool show-aggregate</code> |
| Afficher la quantité de cache qui serait ajoutée à la capacité globale du cache pour les deux types RAID (taille des données de l'unité d'allocation) | <code>storage pool show -instance</code> |



|                                                                                                                    |                                                   |
|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| Afficher les disques dans un pool de stockage                                                                      | <code>storage pool show-disks</code>              |
| Affiche les unités d'allocation non allouées pour un pool de stockage                                              | <code>storage pool show-available-capacity</code> |
| Modifiez la propriété d'une ou de plusieurs unités d'allocation d'un pool de stockage d'un partenaire HA à l'autre | <code>storage pool reassign</code>                |

#### Informations associées

- ["Référence de commande ONTAP"](#)

## Gestion des niveaux FabricPool

### Présentation de la gestion des niveaux FabricPool

Vous pouvez utiliser FabricPool pour procéder au Tiering automatique des données, en fonction de la fréquence d'accès aux données.

FabricPool est une solution de stockage hybride qui, sur les systèmes AFF, utilise un agrégat 100 % Flash (100 % SSD), et sur les systèmes FAS, utilise un agrégat 100 % Flash (100 % SSD) ou un agrégat HDD comme Tier de performance et un magasin d'objets comme Tier cloud. L'utilisation d'un FabricPool vous permet de réduire les coûts de stockage sans compromettre les performances, l'efficacité ni la protection.

Le Tier cloud peut se trouver sous NetApp StorageGRID ou ONTAP S3 (à partir de ONTAP 9.8), ou l'un de ces fournisseurs :

- Cloud Alibaba
- Amazon S3
- Amazon commercial Cloud Services
- Google Cloud
- Cloud IBM
- Stockage Microsoft Azure Blob Storage



À partir de la version ONTAP 9.7, vous pouvez utiliser d'autres fournisseurs de magasins d'objets prenant en charge des API S3 génériques en sélectionnant le fournisseur de magasin d'objets compatible S3.

#### Informations associées

Voir aussi ["NetApp Cloud Tiering"](#) documentation :

### Avantages des niveaux de stockage à l'aide de FabricPool

La configuration d'un agrégat pour utiliser FabricPool permet d'utiliser des niveaux de stockage. Vous pouvez équilibrer efficacement les performances et le coût de votre système de stockage, surveiller et optimiser l'utilisation de l'espace, et effectuer le

déplacement des données basé sur des règles entre les tiers de stockage.

- Vous pouvez optimiser les performances de stockage et réduire les coûts de stockage en stockant les données dans un niveau basé sur la fréquence d'accès aux données.
  - Les données fréquemment utilisées (« actives ») sont stockées dans le *Tier de performance*.

Le niveau de performance utilise un stockage primaire haute performance, comme un agrégat 100 % Flash (100 % SSD) du système de stockage.

- Les données rarement utilisées (« inactives ») sont stockées dans le *Cloud Tier*, également appelé *Capacity Tier*.

Le Tier cloud utilise un magasin d'objets moins coûteux et ne requiert pas de hautes performances.

- Vous avez la possibilité de spécifier le niveau dans lequel les données doivent être stockées.

Vous pouvez spécifier l'une des options de règles de Tiering prises en charge au niveau du volume. Avec ces options, vous pouvez déplacer efficacement les données entre les tiers quand elles sont actives ou inactives.

#### "Types de règles de Tiering FabricPool"

- Vous pouvez choisir l'un des magasins d'objets pris en charge à utiliser comme Tier cloud pour FabricPool.
- Vous pouvez surveiller l'utilisation de l'espace dans un agrégat compatible FabricPool.
- Vous pouvez connaître la quantité de données inactives d'un volume grâce au reporting des données inactives.
- Vous pouvez réduire l'empreinte sur site du système de stockage.

Nous économisons de l'espace physique lorsque vous utilisez un magasin d'objets basé dans le cloud pour le Tier cloud.

## Considérations et configuration requise pour l'utilisation de FabricPool

Pour optimiser vos configurations FabricPool, nous vous recommandons de vous familiariser avec quelques considérations et exigences relatives à l'utilisation de FabricPool.

### Considérations générales et besoins

#### ONTAP 9.2

Vous devez exécuter ONTAP 9.2 ou une version ultérieure de FabricPool.

#### ONTAP 9.4

- Vous devez exécuter ONTAP 9.4 ou une version ultérieure pour prendre en compte les fonctionnalités FabricPool suivantes :
  - Le auto "[règle de hiérarchisation](#)"
  - Spécification de la période de refroidissement minimum du Tiering
  - Reporting des données inactives

- Utilisation de Microsoft Azure Blob Storage pour le cloud en tant que Tier cloud pour FabricPool
- Utilisation de FabricPool avec ONTAP Select

#### ONTAP 9.5

- Vous devez exécuter ONTAP 9.5 ou une version ultérieure pour les fonctionnalités FabricPool suivantes :
  - Spécification du seuil de remplissage de niveaux
  - Utilisation d'IBM Cloud Object Storage comme Tier cloud pour FabricPool
  - NetApp Volume Encryption (NVE) du Tier cloud, activé par défaut.

#### ONTAP 9.6

- Vous devez exécuter ONTAP 9.6 ou une version ultérieure pour les fonctionnalités FabricPool suivantes :
  - Le `all` règle de hiérarchisation
  - Reporting des données inactives activé manuellement sur les agrégats HDD
  - Le reporting de données inactives est activé automatiquement pour les agrégats SSD lorsque vous effectuez une mise à niveau vers ONTAP 9.6 ou lors de la création de l'agrégat, sauf sur les systèmes bas de gamme avec moins de 4 CPU, moins de 6 Go de RAM ou lorsque la taille du cache du tampon WAFL est inférieure à 3 Go.

ONTAP surveille la charge du système et, si la charge reste élevée pendant 4 minutes en continu, l'IDR est désactivé et n'est pas automatiquement activé. Vous pouvez réactiver l'IDR manuellement, mais l'IDR activé manuellement n'est pas automatiquement désactivé.

- Utilisation d'Alibaba Cloud Object Storage comme Tier cloud pour FabricPool
- Utilisation de Google Cloud Platform comme Tier cloud pour FabricPool
- Déplacement de volumes sans copie des données par Tier dans le cloud

#### ONTAP 9.7

- Vous devez exécuter ONTAP 9.7 ou une version ultérieure pour les fonctionnalités FabricPool suivantes :
  - Proxy HTTP et HTTPS non transparent permettant d'accéder uniquement aux points d'accès blanchis et de fournir des fonctionnalités d'audit et de création de rapports.
  - Mise en miroir FabricPool pour transférer simultanément les données inactives vers deux magasins d'objets
  - FabricPool est mis en miroir dans les configurations MetroCluster
  - NDMP dump and restore qui est activé par défaut sur les agrégats connectés à FabricPool.



Si l'application de sauvegarde utilise un protocole autre que NDMP, tel que NFS ou SMB, toutes les données sauvegardées dans le Tier de performance deviennent actives et peuvent affecter le Tiering des données vers le cloud. Les lectures non NDMP peuvent entraîner la migration des données du Tier cloud vers le Tier de performance.

"Prise en charge de la sauvegarde et de la restauration NDMP pour FabricPool"

## ONTAP 9.8

- Vous devez exécuter ONTAP 9.8 ou version ultérieure pour les fonctionnalités FabricPool suivantes :
  - Récupération dans le cloud
  - FabricPool avec SnapLock Enterprise. FabricPool avec SnapLock Enterprise requiert une demande FPVR (Feature Product variance Request). Pour créer une FPVR, contactez votre équipe commerciale.
  - Période de refroidissement minimum de 183 jours maximum
  - Balisage d'objets à l'aide de balises personnalisées créées par l'utilisateur
  - Agrégats FabricPool HDD

HDD FabricPools est pris en charge avec des disques SAS, FSA, BSA et MSATA uniquement sur les systèmes dotés de 6 cœurs de processeur ou plus.

Fait "[Hardware Universe](#)" pour les derniers modèles pris en charge.

## ONTAP 9.10.1

- Vous devez exécuter ONTAP 9.10.1 ou une version ultérieure pour les fonctionnalités FabricPool suivantes :
  - METTEZ la restriction
  - Efficacité de stockage sensible à la température (TSSE).

## ONTAP 9.12.1

- Vous devez exécuter ONTAP 9.12.1 ou une version ultérieure pour les fonctionnalités FabricPool suivantes :
  - SVM Migrate
  - Prise en charge combinée des systèmes FabricPool, FlexGroup et SVM-DR (Avant 9.12.1, deux de ces fonctions fonctionnaient ensemble, mais pas les trois en même temps.)

## ONTAP 9.14.1

- Vous devez exécuter ONTAP 9.14.1 ou une version ultérieure pour les fonctionnalités FabricPool suivantes :
  - Ecriture dans le cloud
  - Lecture anticipée agressive

## Plateformes

- FabricPool est pris en charge sur toutes les plateformes qui exécutent ONTAP 9.2, sauf dans les cas suivants :
  - FAS8020
  - FAS2554
  - FAS2552
  - FAS2520

## Tiers locaux (agrégats)

FabricPool prend en charge les types d'agrégats suivants :

- Sur les systèmes AFF, les agrégats SSD ne peuvent être utilisés que pour FabricPool.
- Sur les systèmes FAS, vous pouvez utiliser des agrégats de disques SSD ou HDD pour FabricPool.
- Sur les systèmes Cloud Volumes ONTAP et ONTAP Select, vous pouvez utiliser des agrégats SSD ou HDD pour FabricPool. L'utilisation d'agrégats SSD est recommandée.



Les agrégats Flash Pool, qui contiennent à la fois des disques SSD et des disques durs, ne sont pas pris en charge.

## Tiers cloud

FabricPool prend en charge l'utilisation de plusieurs magasins d'objets comme Tier cloud :

- Alibaba Cloud Object Storage Service (Standard, Infrequent Access)
- Amazon S3 (Standard, Standard-IA, One zone-IA, Intelligent-Tiering, Glacier Instant Retrieval)
- Amazon commercial Cloud Services (C2S)
- Google Cloud Storage (multirégional, régional, Nearline, Coldline, Archive)
- Stockage objet cloud IBM (Standard, Vault, Cold Vault, Flex)
- Microsoft Azure Blob Storage (chaud et froid)
- NetApp ONTAP S3 (ONTAP 9.8 et versions ultérieures)
- NetApp StorageGRID (StorageGRID 10.3 et versions ultérieures)



Glacier flexible Retrieval et Glacier Deep Archive ne sont pas pris en charge.

- Le magasin d'objets « compartiment » (conteneur) que vous envisagez d'utiliser doit avoir déjà été configuré, avoir au moins 10 Go d'espace de stockage et ne doit pas être renommé.
- Les paires HAUTE DISPONIBILITÉ qui utilisent FabricPool nécessitent que les LIF intercluster communiquent avec le magasin d'objets.
- Vous ne pouvez pas détacher un niveau de cloud d'un niveau local après qu'il est attaché ; vous pouvez cependant l'utiliser "[Miroir FabricPool](#)" pour associer un tier local à un autre tier de cloud.

## Fonctionnalités d'efficacité du stockage ONTAP

Les fonctionnalités d'efficacité du stockage, telles que la compression, la déduplication et la compaction, sont conservées lors du déplacement des données vers le Tier cloud, ce qui réduit la capacité de stockage objet requise et les coûts de transport.



Depuis ONTAP 9.15.1, FabricPool prend en charge la technologie Intel QuickAssist (QAT4), qui permet des économies plus agressives et plus performantes en termes d'efficacité du stockage.

La déduplication à la volée dans l'agrégat est prise en charge au niveau local, mais les fonctionnalités d'efficacité du stockage associées ne sont pas reportées aux objets stockés sur le Tier cloud.

Lorsque la règle de Tiering sur tous les volumes est utilisée, les fonctionnalités d'efficacité du stockage associées aux processus de déduplication en arrière-plan peuvent être réduites, car les données sont

susceptibles d'être hiérarchisées avant de pouvoir appliquer les fonctionnalités d'efficacité du stockage supplémentaires.

## Licence de Tiering BlueXP

Pour les systèmes AFF et FAS, FabricPool requiert une licence basée sur la capacité lorsque vous connectez des fournisseurs de stockage objet tiers (comme Amazon S3) à des tiers cloud. Aucune licence BlueXP Tiering n'est requise lors de l'utilisation de StorageGRID ou ONTAP S3 en tant que Tier cloud ou du Tiering avec Cloud Volumes ONTAP, Amazon FSX pour NetApp ONTAP ou Azure NetApp Files.

Les licences BlueXP (y compris les extensions ou les extensions des licences FabricPool préexistantes) sont activées dans le ["Portefeuille digital BlueXP"](#).

## Contrôles de cohérence StorageGRID

Les contrôles de cohérence de StorageGRID affectent la façon dont se trouvent les métadonnées utilisées par StorageGRID pour le suivi des objets distribué entre les nœuds et la disponibilité des objets pour les requêtes des clients. NetApp recommande l'utilisation de Contrôle de cohérence par défaut, lecture après nouvelle écriture, pour les compartiments utilisés comme cibles FabricPool.



N'utilisez pas le contrôle de cohérence disponible pour les compartiments utilisés comme cibles FabricPool.

## Considérations supplémentaires relatives au Tiering des données accessibles par les protocoles SAN

Lors du Tiering des données accessibles par les protocoles SAN, NetApp recommande l'utilisation de clouds privés tels qu'ONTAP S3 ou StorageGRID, pour des raisons de connectivité.



Lorsque vous utilisez FabricPool dans un environnement SAN avec un hôte Windows, si le stockage objet devient indisponible pendant une période prolongée lors du Tiering des données dans le cloud, les fichiers du LUN NetApp de l'hôte Windows peuvent devenir inaccessibles ou disparaître. Consultez l'article de la base de connaissances ["Pendant l'indisponibilité du magasin d'objets FabricPool S3, l'hôte SAN Windows a signalé une corruption du système de fichiers"](#).

## Qualité de service

- Si vous utilisez le débit au sol (QoS min), la règle de Tiering sur les volumes doit être définie sur `none` Avant que l'agrégat ne puisse être relié à FabricPool.

D'autres règles de hiérarchisation empêchent la connexion de l'agrégat à FabricPool. Une règle de qualité de service n'applique pas de niveaux de débit lorsque FabricPool est activé.

## Fonctionnalité ou fonctionnalités non prises en charge par FabricPool

- Magasins d'objets avec WORM activé et gestion des versions d'objets activée.
- Les règles de gestion du cycle de vie des informations (ILM) appliquées aux compartiments de magasin d'objets

FabricPool prend en charge les règles de gestion du cycle de vie des informations de StorageGRID uniquement pour la réplication des données et le code d'effacement afin de protéger les données de Tier

cloud en cas de défaillance. Cependant, FabricPool ne prend pas en charge les règles ILM avancées, telles que le filtrage basé sur les balises ou les métadonnées de l'utilisateur. La gestion du cycle de vie des informations inclut généralement plusieurs règles de déplacement et de suppression. Ces règles peuvent être perturbateurs pour les données stockées dans le niveau cloud de FabricPool. L'utilisation de FabricPool avec des règles ILM configurées sur des magasins d'objets peut entraîner la perte de données.

- Transition des données 7-mode à l'aide des commandes CLI ONTAP ou de l'outil 7-mode transition Tool
- Virtualisation FlexArray
- RAID SyncMirror, sauf dans une configuration MetroCluster
- Les volumes SnapLock sont utilisés avec ONTAP 9.7 et les versions antérieures
- Sauvegarde sur bande utilisant SMTape pour les agrégats compatibles FabricPool
- La fonction de balance automatique
- Volumes utilisant une garantie d'espace autre que `none`

À l'exception des volumes des SVM racines et des volumes d'audit intermédiaire CIFS, FabricPool ne prend pas en charge la connexion d'un Tier cloud à un agrégat contenant des volumes dotés d'une garantie d'espace autre que `none`. Par exemple, un volume utilisant une garantie d'espace de `volume (-space-guarantee volume)` n'est pas pris en charge.

- Avec "[Licence DP\\_Optimized](#)"
- Les agrégats Flash Pool

## À propos des règles de hiérarchisation FabricPool

Les règles de Tiering de FabricPool vous permettent de déplacer efficacement les données entre les tiers à mesure que les données sont actives ou inactives. Le respect des règles de hiérarchisation vous permet de choisir la règle la plus adaptée à vos besoins en matière de gestion du stockage.

### Types de règles de Tiering FabricPool

Les règles de Tiering FabricPool déterminent quand ou si les blocs de données utilisateur d'un volume d'FabricPool sont déplacés vers le Tier cloud, en fonction de la « température » du volume « actif » ou froid (inactif). Le volume « température » augmente lorsqu'il est fréquemment utilisé et diminue lorsqu'il n'est pas utilisé. Certaines règles de Tiering ont associé une période de refroidissement minimale de Tiering, qui définit le temps pendant lequel les données utilisateur d'un volume FabricPool doivent rester inactives pour que les données soient considérées comme « inactives » et déplacées vers le Tier cloud.

Une fois qu'un bloc a été identifié comme froid, il est marqué comme éligible pour être hiérarchisé. Une analyse quotidienne de la hiérarchisation en arrière-plan recherche les blocs inactifs. Lorsque suffisamment de blocs de 4 Ko provenant du même volume ont été collectés, ils sont concaténés dans un objet de 4 Mo et déplacés au niveau cloud en fonction de la règle de Tiering des volumes.



Données dans des volumes utilisant `all` la règle de tiering est immédiatement marquée comme inactives et commence le tiering vers le tier cloud dès que possible. Inutile d'attendre l'exécution de l'analyse de Tiering quotidienne.

Vous pouvez utiliser le volume `object-store tiering show` Pour afficher l'état de la hiérarchisation d'un volume FabricPool. Pour plus d'informations, reportez-vous à la section "[Référence de commande](#)".

La règle de Tiering FabricPool est spécifiée au niveau du volume. Quatre options sont disponibles :

- Le `snapshot-only` La règle de Tiering (par défaut) déplace les blocs de données utilisateur des copies Snapshot de volume non associées au système de fichiers actif vers le niveau cloud.

La période de refroidissement minimum par niveaux est de 2 jours. Vous pouvez modifier le paramètre par défaut de la période de refroidissement minimum par niveaux avec l' `-tiering-minimum-cooling-days` paramètre au niveau de privilège avancé de l' `volume create` et `volume modify` commandes. Les valeurs valides sont comprises entre 2 et 183 jours avec ONTAP 9.8 et version ultérieure. Si vous utilisez une version de ONTAP antérieure à 9.8, les valeurs valides sont comprises entre 2 et 63 jours.

- Le `auto` La règle de Tiering, prise en charge uniquement sur ONTAP 9.4 et les versions ultérieures, déplace les blocs de données inactives dans les copies Snapshot et le système de fichiers actif vers le Tier cloud.

La période de refroidissement minimale par défaut du Tiering est de 31 jours. Elle s'applique à tout le volume, pour le système de fichiers actif et les copies Snapshot.

Vous pouvez modifier le paramètre par défaut de la période de refroidissement minimum par niveaux avec l' `-tiering-minimum-cooling-days` paramètre au niveau de privilège avancé de l' `volume create` et `volume modify` commandes. Les valeurs valides sont de 2 à 183 jours.

- Le `all` La règle de Tiering, prise en charge uniquement avec ONTAP 9.6 et versions ultérieures, déplace tous les blocs de données utilisateur du système de fichiers actif et des copies Snapshot vers le Tier cloud. Elle remplace le `backup` règle de hiérarchisation.

Le `all` la règle de tiering des volumes ne doit pas être utilisée sur les volumes en lecture/écriture présentant un trafic client normal.

La période de refroidissement minimale du Tiering ne s'applique pas, car les données sont déplacées vers le Tier cloud dès l'exécution de l'analyse du Tiering. Vous ne pouvez pas modifier ce paramètre.

- Le `none` la règle de tiering conserve les données d'un volume dans le tier de performance et ne les déplace pas à froid vers le tier cloud.

Définition de la règle de hiérarchisation sur `none` empêche le nouveau tiering. Les données de volume qui ont déjà été déplacées vers le Tier cloud restent dans le Tier cloud jusqu'à ce qu'elles deviennent actives, et sont automatiquement déplacées vers le Tier local.

Le Tiering n'applique pas la période de refroidissement minimale, car les données ne sont jamais déplacées vers le Tier cloud et vous ne pouvez pas modifier le paramètre.

En cas de blocs inactifs dans un volume dont la règle de Tiering est définie sur `none` ils sont lus, ils sont brûlants et écrits sur le niveau local.

Le `volume show` la sortie de la commande affiche la politique de tiering d'un volume. Un volume qui n'a encore jamais été utilisé avec FabricPool présente la `none` règle de hiérarchisation dans la sortie.

### Que se passe-t-il lorsque vous modifiez la règle de Tiering d'un volume dans FabricPool

Vous pouvez modifier la règle de hiérarchisation d'un volume en effectuant une `volume modify` fonctionnement. Vous devez savoir en quoi la modification de la règle de Tiering peut affecter le temps nécessaire aux données inactives et déplacées vers le Tier cloud.



- Modification de la règle de hiérarchisation à partir de `snapshot-only` ou `none` à `auto` Dans ce cas, ONTAP envoie des blocs de données utilisateur dans le système de fichiers actif qui sont déjà inactifs vers le Tier cloud, même si ces blocs de données ne sont pas encore éligibles pour le Tier cloud.
- Modification de la règle de hiérarchisation en `all` D'autre part, ONTAP déplace dès que possible tous les blocs utilisateurs du système de fichiers actif et des copies Snapshot dans le cloud. Avant ONTAP 9.8, les blocs devaient attendre l'analyse de hiérarchisation suivante.

Le déplacement des blocs vers le Tier de performance n'est pas autorisé.

- Modification de la règle de hiérarchisation à partir de `auto` à `snapshot-only` ou `none` n'entraîne pas la migration vers le tier de performance des blocs de système de fichiers actifs qui sont déjà déplacés vers le tier cloud.

Les lectures de volume sont nécessaires pour que les données puissent être retransférées vers le Tier de performance.

- Chaque fois que vous modifiez la règle de Tiering sur un volume, la période de refroidissement minimum de Tiering est redéfinie sur la valeur par défaut de la règle.

### Que arrive-t-il à la règle de Tiering lorsque vous déplacez un volume

- Sauf si vous spécifiez explicitement une règle de Tiering, un volume conserve sa règle de Tiering d'origine lorsqu'il est déplacé dans un agrégat compatible FabricPool ou en dehors.

Toutefois, la règle de Tiering s'applique uniquement lorsque le volume se trouve dans un agrégat compatible FabricPool.

- Valeur existante du `-tiering-minimum-cooling-days` paramètre d'un volume déplacé avec le volume sauf si vous spécifiez une règle de tiering différente pour la destination.

Si vous spécifiez une autre règle de Tiering, le volume utilise la période de refroidissement minimale par défaut de Tiering pour cette règle. C'est le cas si la destination est FabricPool ou non.

- Vous pouvez déplacer un volume entre agrégats et modifier simultanément la règle de Tiering.
- Vous devez accorder une attention particulière lorsqu'un `volume move` l'opération implique le `auto` règle de hiérarchisation.

Si la source et la destination sont des agrégats compatibles FabricPool, le tableau suivant résume le résultat d'un `volume move` opération qui implique des changements de stratégie liés à `auto`:

| Lorsque vous déplacez un volume doté d'une règle de Tiering : | Et vous modifiez la règle de Tiering en effectuant la transition vers : | Puis, après le déplacement du volume...                          |
|---------------------------------------------------------------|-------------------------------------------------------------------------|------------------------------------------------------------------|
| <code>all</code>                                              | <code>auto</code>                                                       | Toutes les données sont transférées vers le Tier de performance. |

|                              |               |                                                                                                                    |
|------------------------------|---------------|--------------------------------------------------------------------------------------------------------------------|
| snapshot-only, none, ou auto | auto          | Les blocs de données sont déplacés vers le même niveau de destination que ceux précédemment stockés sur la source. |
| auto ou all                  | snapshot-only | Toutes les données sont transférées vers le Tier de performance.                                                   |
| auto                         | all           | Toutes les données utilisateur sont déplacées vers le niveau cloud.                                                |
| snapshot-only,auto ou all    | none          | Toutes les données sont conservées sur le Tier de performance.                                                     |

### Que arrive-t-il à la règle de Tiering lorsque vous clonez un volume

- Depuis ONTAP 9.8, le volume clone hérite toujours de la règle de Tiering et de la politique d'extraction du cloud du volume parent.

Dans les versions antérieures à ONTAP 9.8, un clone hérite de la règle de Tiering du parent, sauf lorsque le clone possède le `all` règle de hiérarchisation.

- Si le volume parent a le `never` la politique de récupération du cloud, son volume clone doit avoir l'une ou l'autre `never` récupération cloud ou `all` la règle de tiering et la politique de récupération de cloud correspondante `default`.
- La politique de récupération du cloud du volume parent ne peut pas être changée en `never` à moins que tous ses volumes de clones ne disposent d'une politique de récupération cloud `never`.

Lors du clonage de volumes, tenez compte des bonnes pratiques suivantes :

- Le `-tiering-policy option` et `tiering-minimum-cooling-days` l'option de clonage contrôle uniquement le comportement de hiérarchisation des blocs uniques au clone. Par conséquent, nous recommandons d'utiliser les paramètres de Tiering sur la FlexVol parent qui déplacent la même quantité de données ou déplacent moins de données que n'importe quel clone
- La politique de récupération cloud de l'FlexVol parent doit déplacer la même quantité de données ou déplacer plus de données que la politique de récupération de l'un des clones

### Fonctionnement des règles de Tiering avec la migration vers le cloud

La récupération des données dans le cloud FabricPool est contrôlée par des règles de Tiering qui déterminent la récupération des données depuis le Tier cloud vers le Tier de performance selon le modèle de lecture. Les modèles de lecture peuvent être séquentiels ou aléatoires.

Le tableau ci-dessous répertorie les politiques de Tiering ainsi que les règles de récupération des données cloud pour chaque règle.

| Règle de hiérarchisation | Comportement de récupération         |
|--------------------------|--------------------------------------|
| Aucune                   | Lectures séquentielles et aléatoires |
| snapshot uniquement      | Lectures séquentielles et aléatoires |
| automatique              | Lectures aléatoires                  |
| tous                     | Aucune récupération des données      |

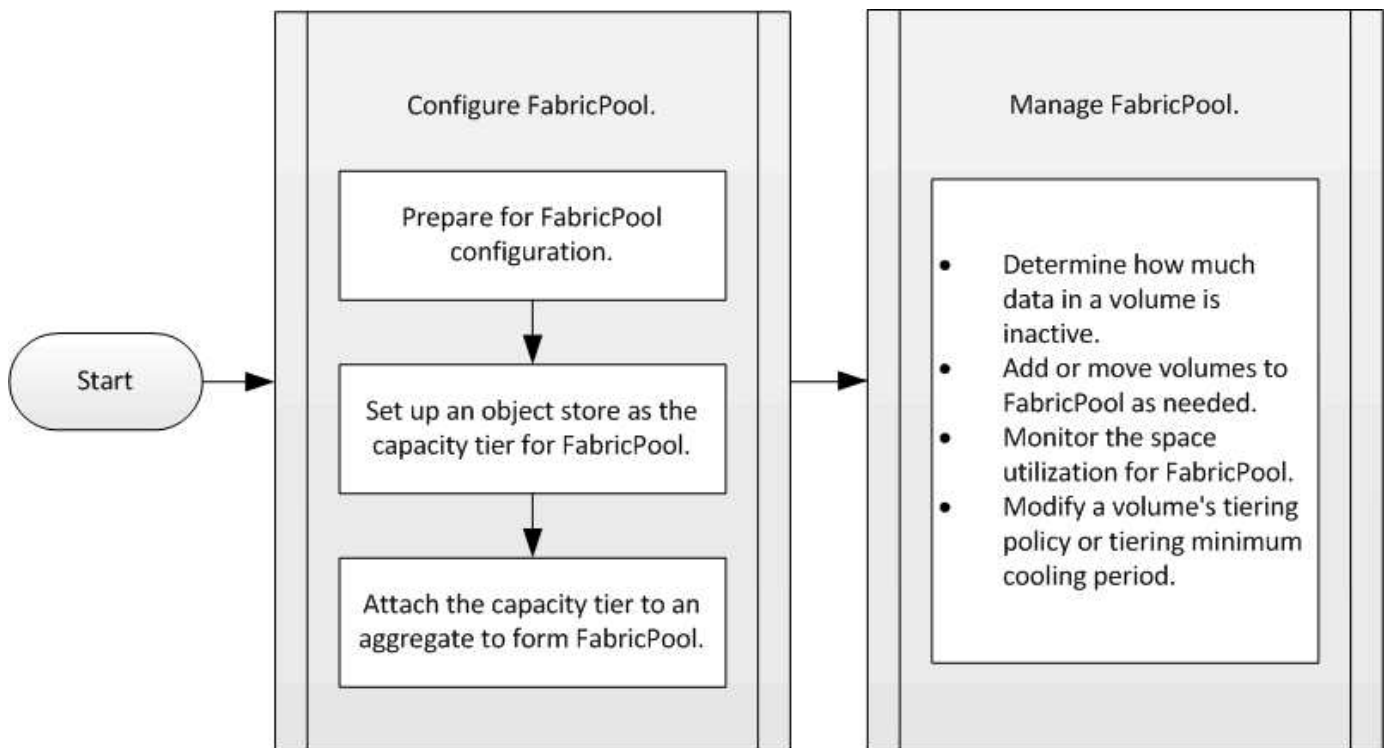
Depuis ONTAP 9.8, vous gardez le contrôle de la migration vers le cloud `cloud-retrieval-policy` l'option remplace le comportement par défaut de migration ou de récupération dans le cloud contrôlé par la règle de tiering.

Le tableau suivant répertorie les politiques de récupération du cloud prises en charge et leur comportement de récupération.

| Politique de récupération cloud | Comportement de récupération                                                                                                                                                                                                                                        |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| valeur par défaut               | La règle de Tiering décide des données à récupérer et ne modifie pas la récupération des données cloud par « deDefault », " `cloud-retrieval-policy. Cette règle correspond à la valeur par défaut de tout volume, quel que soit le type d'agrégat hébergé.         |
| en lecture                      | Toutes les données client lues sont extraites du Tier cloud au Tier de performance.                                                                                                                                                                                 |
| jamais                          | Aucune donnée client n'est tirée du Tier cloud vers le Tier de performance                                                                                                                                                                                          |
| promouvoir                      | <ul style="list-style-type: none"> <li>• Pour la règle de Tiering « aucune », toutes les données cloud sont transférées du Tier cloud vers le Tier de performance</li> <li>• Pour la règle de Tiering « snapshot-only », les données AFS sont extraites.</li> </ul> |

## Workflow de gestion FabricPool

Vous pouvez utiliser le diagramme des flux de travail de FabricPool pour planifier les tâches de configuration et de gestion.



## Configurez FabricPool

### Préparation à la configuration FabricPool

#### Préparer la configuration FabricPool

La configuration d'FabricPool vous aide à gérer le Tier de stockage (Tier de performance local ou Tier cloud) à stocker vos données selon que celles-ci sont fréquemment utilisées.

La préparation requise pour la configuration FabricPool dépend du magasin d'objets que vous utilisez comme Tier cloud.

#### Installez une licence FabricPool

La licence FabricPool que vous avez peut-être utilisée auparavant est en train de changer et ne sera conservée que pour les configurations qui ne sont pas prises en charge dans BlueXP. À partir du 21 août 2021, les licences Cloud Tiering BYOL ont été introduites pour les configurations de Tiering prises en charge dans BlueXP via le service Cloud Tiering.

["En savoir plus sur les nouvelles licences BYOL de NetApp Cloud Tiering".](#)

Les configurations prises en charge par BlueXP doivent utiliser la page du portefeuille numérique dans BlueXP pour le Tiering des licences des clusters ONTAP. Pour cela, vous devez configurer un compte BlueXP et configurer le Tiering pour le fournisseur de stockage objet que vous prévoyez d'utiliser. BlueXP prend actuellement en charge le Tiering vers le stockage objet suivant : Amazon S3, Azure Blob Storage, Google Cloud Storage, un stockage objet compatible S3 et StorageGRID.

["En savoir plus sur le service de Tiering dans le cloud".](#)

Vous pouvez télécharger et activer une licence FabricPool à l'aide de System Manager si vous disposez d'une des configurations non prises en charge dans BlueXP :

- Installations de ONTAP dans les sites sombres
- Clusters ONTAP qui permettent de Tiering des données vers une solution de stockage objet cloud IBM ou encore vers une solution de stockage objet cloud Alibaba

La licence FabricPool est une licence pour l'ensemble du cluster. Elle inclut une limite d'utilisation autorisée que vous achetez pour le stockage objet associé à FabricPool dans le cluster. L'utilisation au sein du cluster ne doit pas dépasser la capacité de la limite d'utilisation autorisée. Si vous devez augmenter la limite d'utilisation de la licence, contactez votre représentant commercial.

Les licences FabricPool sont disponibles en versions perpétuelles ou basées sur les contrats, 1 ou 3 ans.

Une licence FabricPool à durée déterminée avec 10 To de capacité disponible est disponible pour la première commande FabricPool pour les configurations de clusters existantes non prises en charge par BlueXP. La capacité libre n'est pas disponible avec les licences permanentes.

Aucune licence n'est requise si vous utilisez NetApp StorageGRID ou ONTAP S3 pour le Tier cloud. Cloud Volumes ONTAP ne requiert pas de licence FabricPool, quel que soit le fournisseur que vous utilisez.

Cette tâche est uniquement prise en charge en téléchargeant le fichier de licence sur le cluster à l'aide de System Manager.

### Étapes

1. Téléchargez le fichier de licence NetApp (NLF) pour la licence FabricPool sur le ["Site de support NetApp"](#).
2. Effectuez les actions suivantes avec System Manager pour charger la licence FabricPool sur le cluster :
  - a. Dans le volet **Cluster > Paramètres**, sur la carte **Licenses**, cliquez sur ➔.
  - b. Sur la page **Licence**, cliquez sur **+ Add**.
  - c. Dans la boîte de dialogue **Ajouter une licence**, cliquez sur **Parcourir** pour sélectionner le fichier NLF que vous avez téléchargé, puis cliquez sur **Ajouter** pour télécharger le fichier sur le cluster.

### Informations associées

["Présentation des licences ONTAP FabricPool \(FP\)"](#)

["Recherche de licences logicielles NetApp"](#)

["NetApp TechComm TV : liste de lecture FabricPool"](#)

### Installez un certificat d'autorité de certification si vous utilisez StorageGRID

Sauf si vous prévoyez de désactiver la vérification du certificat pour StorageGRID, vous devez installer un certificat d'autorité de certification StorageGRID sur le cluster de manière à ce que ONTAP puisse s'authentifier auprès de StorageGRID comme magasin d'objets pour FabricPool.

### Description de la tâche

Les versions ONTAP 9.4 et ultérieures vous permettent de désactiver la vérification des certificats pour StorageGRID.

### Étapes

1. Contactez votre administrateur StorageGRID pour obtenir le certificat d'autorité de certification du système

StorageGRID.

2. Utilisez le `security certificate install` commande avec `-type server-ca` Paramètre permettant d'installer le certificat d'autorité de certification StorageGRID sur le cluster.

Le nom de domaine complet (FQDN) que vous saisissez doit correspondre au nom commun personnalisé du certificat de l'autorité de certification StorageGRID.

### **Mettre à jour un certificat expiré**

Pour mettre à jour un certificat expiré, il est recommandé d'utiliser une autorité de certification approuvée pour générer le nouveau certificat de serveur. Par ailleurs, vous devez vous assurer que le certificat est mis à jour simultanément sur le serveur StorageGRID et sur le cluster ONTAP afin de limiter au maximum le temps d'interruption.

#### **Informations associées**

["Ressources StorageGRID"](#)

#### **Installez un certificat d'autorité de certification si vous utilisez ONTAP S3**

Sauf si vous prévoyez de désactiver la vérification du certificat pour ONTAP S3, vous devez installer un certificat d'autorité de certification ONTAP S3 sur le cluster afin que ONTAP puisse s'authentifier auprès d'ONTAP S3 en tant que magasin d'objets pour FabricPool.

#### **Étapes**

1. Obtenir le certificat de l'autorité de certification du système ONTAP S3
2. Utilisez le `security certificate install` commande avec `-type server-ca` Paramètre permettant d'installer le certificat d'autorité de certification ONTAP S3 sur le cluster.

Le nom de domaine complet que vous entrez doit correspondre au nom commun personnalisé du certificat de l'autorité de certification ONTAP S3.

### **Mettre à jour un certificat expiré**

Pour mettre à jour un certificat expiré, il est recommandé d'utiliser une autorité de certification approuvée pour générer le nouveau certificat de serveur. Par ailleurs, assurez-vous que le certificat est mis à jour simultanément sur le serveur ONTAP S3 et sur le cluster ONTAP afin de limiter au maximum le temps d'indisponibilité.

#### **Informations associées**

["Configuration de S3"](#)

#### **Configurez un magasin d'objets comme Tier cloud pour FabricPool**

#### **Configurez un magasin d'objets en tant que Tier cloud pour la présentation d'FabricPool**

La configuration de FabricPool implique de spécifier les informations de configuration du magasin d'objets (StorageGRID, ONTAP S3, Alibaba Cloud Object Storage, Amazon S3, Google Cloud Storage, IBM Cloud Object Storage ou Microsoft Azure Blob Storage pour le cloud) que vous prévoyez d'utiliser en tant que Tier cloud pour FabricPool.

## Configurez StorageGRID comme Tier cloud

Si vous exécutez ONTAP 9.2 ou une version ultérieure, vous pouvez configurer StorageGRID en tant que Tier cloud pour FabricPool. Lorsque le Tiering des données accessibles par les protocoles SAN, NetApp recommande l'utilisation de clouds privés tels que StorageGRID, en raison des problèmes de connectivité.

### Considérations relatives à l'utilisation de StorageGRID avec FabricPool

- Vous devez installer un certificat d'autorité de certification pour StorageGRID, à moins que vous ne désactiviez explicitement la vérification des certificats.
- Vous ne devez pas activer la gestion des versions d'objets StorageGRID sur le compartiment de magasin d'objets.
- Aucune licence FabricPool n'est requise.
- Si un nœud StorageGRID est déployé dans une machine virtuelle dont le stockage est affecté à un système NetApp AFF, vérifiez que cette FabricPool règle n'est pas activée pour le volume.

La désactivation du Tiering FabricPool pour les volumes utilisés avec des nœuds StorageGRID simplifie la résolution des problèmes et les opérations de stockage.



N'utilisez jamais FabricPool pour transférer automatiquement toutes les données liées à StorageGRID vers StorageGRID. Le Tiering des données StorageGRID vers StorageGRID augmente la complexité opérationnelle et la résolution des problèmes.

### Description de la tâche

L'équilibrage de charge est activé pour StorageGRID dans ONTAP 9.8 et versions ultérieures. Lorsque le nom d'hôte du serveur résout plusieurs adresses IP, ONTAP établit des connexions client avec toutes les adresses IP renvoyées (jusqu'à 16 adresses IP maximum). Les adresses IP sont récupérées dans une méthode de séquence périodique lors de l'établissement des connexions.

### Procédures

Vous pouvez configurer StorageGRID en tant que Tier cloud pour FabricPool avec ONTAP System Manager ou l'interface de ligne de commande ONTAP.

## System Manager

1. Cliquez sur **stockage > tiers > Ajouter un niveau de cloud** et sélectionnez StorageGRID comme fournisseur de magasin d'objets.
2. Complétez les informations demandées.
3. Si vous souhaitez créer un miroir de nuage, cliquez sur **Ajouter en tant que miroir FabricPool**.

Un miroir FabricPool vous permet de remplacer un datastore en toute transparence et de garantir la disponibilité de vos données en cas d'incident.

## CLI

1. Spécifier les informations de configuration de StorageGRID à l'aide de `storage aggregate object-store config create` commande avec `-provider-type SGWS` paramètre.
  - Le `storage aggregate object-store config create` La commande échoue si ONTAP ne peut pas accéder à StorageGRID avec les informations fournies.
  - Vous utilisez le `-access-key` Paramètre permettant de spécifier la clé d'accès pour autoriser les requêtes vers le magasin d'objets StorageGRID.
  - Vous utilisez le `-secret-password` Paramètre pour spécifier le mot de passe (clé d'accès secrète) pour l'authentification des requêtes vers le magasin d'objets StorageGRID.
  - Si le mot de passe StorageGRID est modifié, vous devez mettre à jour immédiatement le mot de passe correspondant stocké dans ONTAP.

ONTAP peut ainsi accéder aux données dans StorageGRID sans interruption.

- Réglage du `-is-certificate-validation-enabled` paramètre à `false` Désactive la vérification de certificat pour StorageGRID.

```
cluster1::> storage aggregate object-store config create
-object-store-name mySGWS -provider-type SGWS -server mySGWSserver
-container-name mySGWScontainer -access-key mySGWSkey
-secret-password mySGWSpass
```

2. Afficher et vérifier les informations de configuration StorageGRID à l'aide du `storage aggregate object-store config show` commande.

Le `storage aggregate object-store config modify` Commande vous permet de modifier les informations de configuration des StorageGRID pour FabricPool.

## Configuration d'ONTAP S3 en tant que Tier cloud

Si vous exécutez ONTAP 9.8 ou une version ultérieure, vous pouvez configurer ONTAP S3 en tant que Tier cloud pour FabricPool.

### Ce dont vous avez besoin

Vous devez disposer du nom du serveur ONTAP S3 et de l'adresse IP des LIFs associées sur le cluster distant.



Il faut que des LIF intercluster se trouvent sur le cluster local.

### "Création des LIFs intercluster pour le Tiering des FabricPool distants"

#### **Description de la tâche**

L'équilibrage de charge est activé pour les serveurs ONTAP S3 dans ONTAP 9.8 et versions ultérieures. Lorsque le nom d'hôte du serveur résout plusieurs adresses IP, ONTAP établit des connexions client avec toutes les adresses IP renvoyées (jusqu'à 16 adresses IP maximum). Les adresses IP sont récupérées dans une méthode de séquence périodique lors de l'établissement des connexions.

#### **Procédures**

Vous pouvez configurer ONTAP S3 en tant que Tier cloud pour FabricPool avec ONTAP System Manager ou l'interface de ligne de commande ONTAP.

## System Manager

1. Cliquez sur **stockage > tiers > Ajouter un niveau de cloud** et sélectionnez ONTAP S3 comme fournisseur de magasin d'objets.
2. Complétez les informations demandées.
3. Si vous souhaitez créer un miroir de nuage, cliquez sur **Ajouter en tant que miroir FabricPool**.

Un miroir FabricPool vous permet de remplacer un datastore en toute transparence et de garantir la disponibilité de vos données en cas d'incident.

## CLI

1. Ajoutez des entrées pour le serveur S3 et les LIF à votre serveur DNS.

| Option                                                            | Description                                                                                                                               |
|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Si vous utilisez un serveur DNS externe</b>                    | Attribuez le nom du serveur S3 et les adresses IP à l'administrateur des serveurs DNS.                                                    |
| <b>Si vous utilisez la table hôtes DNS de votre système local</b> | Saisissez la commande suivante :<br><br><pre>dns host create -vserver svm_name<br/>-address ip_address -hostname<br/>s3_server_name</pre> |

2. Spécifiez les informations de configuration ONTAP S3 à l'aide du `storage aggregate object-store config create` commande avec `-provider-type ONTAP_S3` paramètre.
  - Le `storage aggregate object-store config create` Échec de la commande si le système ONTAP local ne peut pas accéder au serveur ONTAP S3 avec les informations fournies.
  - Vous utilisez le `-access-key` Paramètre permettant de spécifier la clé d'accès pour autoriser les requêtes vers le serveur ONTAP S3.
  - Vous utilisez le `-secret-password` Paramètre pour spécifier le mot de passe (clé d'accès secrète) pour l'authentification des requêtes vers le serveur ONTAP S3.
  - Si le mot de passe du serveur ONTAP S3 est modifié, vous devez immédiatement mettre à jour le mot de passe correspondant stocké dans le système ONTAP local.

L'accès aux données du magasin d'objets ONTAP S3 est donc possible sans interruption.

- Réglage du `-is-certificate-validation-enabled` paramètre à `false` Désactive la vérification du certificat pour ONTAP S3.

```
cluster1::> storage aggregate object-store config create
-object-store-name myS3 -provider-type ONTAP_S3 -server myS3server
-container-name myS3container -access-key myS3key
-secret-password myS3pass
```

3. Affichez et vérifiez les informations de configuration ONTAP\_S3 à l'aide de `storage aggregate object-store config show` commande.

Le `storage aggregate object-store config modify` vous permet de modifier le `ONTAP_S3` Informations de configuration pour FabricPool.

## Configurez Alibaba Cloud Object Storage en tant que Tier cloud

Si vous exécutez ONTAP 9.6 ou version ultérieure, vous pouvez configurer Alibaba Cloud Object Storage en tant que Tier cloud pour FabricPool.

### Considérations relatives à l'utilisation du stockage objet cloud d'Alibaba avec FabricPool

- Vous aurez peut-être besoin d'une licence FabricPool.

Les systèmes AFF nouvellement commandés disposent d'une capacité libre de 10 To pour l'utilisation de FabricPool. Si vous avez besoin de capacité supplémentaire sur un système AFF, si vous utilisez Alibaba Cloud Object Storage sur un système non-AFF ou si vous effectuez une mise à niveau à partir d'un cluster existant, vous avez besoin d'un "[Licence FabricPool](#)".

- Sur les systèmes AFF et FAS et ONTAP Select, FabricPool prend en charge les classes de services de stockage objet Alibaba suivantes :
  - Service de stockage objet Alibaba Standard
  - Alibaba Object Storage Service Infrequent Access

["Alibaba Cloud : introduction aux classes de stockage"](#)

Contactez votre ingénieur commercial NetApp pour obtenir des informations sur les classes de stockage qui ne figurent pas dans cette liste.

### Étapes

1. Spécifiez les informations de configuration du stockage objet Cloud Alibaba à l'aide de `storage aggregate object-store config create` commande avec `-provider-type AliCloud` paramètre.
  - Le `storage aggregate object-store config create` La commande échoue si ONTAP ne parvient pas à accéder au stockage objet cloud Alibaba avec les informations fournies.
  - Vous utilisez le `-access-key` Paramètre pour spécifier la clé d'accès pour autoriser les requêtes vers le magasin d'objets Cloud Alibaba.
  - Si le mot de passe du stockage objet Cloud Alibaba change, vous devez mettre à jour immédiatement le mot de passe correspondant stocké dans ONTAP.

ONTAP peut ainsi accéder sans interruption aux données dans le stockage objet cloud Alibaba.

```
storage aggregate object-store config create my_ali_oss_store_1
-provider-type AliCloud -server oss-us-east-1.aliyuncs.com
-container-name my-ali-oss-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Affichez et vérifiez les informations de configuration du stockage objet Cloud Alibaba à l'aide de `storage aggregate object-store config show` commande.

Le `storage aggregate object-store config modify` Permet de modifier les informations de configuration du stockage objet dans le cloud Alibaba pour FabricPool.

## Configuration d'Amazon S3 en tant que Tier cloud

Si vous exécutez ONTAP 9.2 ou une version ultérieure, vous pouvez configurer Amazon S3 en tant que Tier cloud pour FabricPool. Si vous utilisez ONTAP 9.5 ou une version ultérieure, vous pouvez configurer Amazon commercial Cloud Services (C2S) pour FabricPool.

### Remarques concernant l'utilisation d'Amazon S3 avec FabricPool

- Vous aurez peut-être besoin d'une licence FabricPool.
  - Les systèmes AFF nouvellement commandés disposent d'une capacité libre de 10 To pour l'utilisation de FabricPool.

Si vous avez besoin de capacité supplémentaire sur un système AFF, si vous utilisez Amazon S3 sur un système non AFF ou si vous effectuez une mise à niveau à partir d'un cluster existant, vous avez besoin d'"[Licence FabricPool](#)"un .

Si vous commandez FabricPool pour la première fois pour un cluster existant, une licence FabricPool avec 10 To de capacité libre est disponible.

- Il est recommandé que la LIF utilisée par ONTAP pour se connecter au serveur objet Amazon S3 se trouve sur un port 10 Gbit/s.
- Sur les systèmes AFF et FAS, ainsi que sur ONTAP Select, FabricPool prend en charge les classes de stockage Amazon S3 suivantes :
  - Amazon S3 Standard
  - Amazon S3 Standard – Infrequent Access (Standard – IA)
  - Amazon S3 One zone – Infrequent Access (One zone – IA)
  - Tiering intelligent Amazon S3
  - Amazon commercial Cloud Services
  - Depuis ONTAP 9.11.1, Amazon S3 Glacier Instant Retrieval (FabricPool ne prend pas en charge Glacier flexible Retrieval ni Glacier Deep Archive)

["Documentation Amazon Web Services : classes de stockage Amazon S3"](#)

Contactez votre ingénieur commercial pour plus d'informations sur les classes de stockage non répertoriées.

- Sur Cloud Volumes ONTAP, FabricPool prend en charge le Tiering à partir de disques SSD à usage générique (gp2) et de volumes HDD à optimisation du débit d'Amazon Elastic Block Store (EBS).

## Étapes

1. Spécifiez les informations de configuration d'Amazon S3 à l'aide du `storage aggregate object-store config create` commande avec `-provider-type AWS_S3` paramètre.
  - Vous utilisez le `-auth-type CAP` Paramètre permettant d'obtenir des informations d'identification pour l'accès au C2S.

Lorsque vous utilisez le `-auth-type CAP` vous devez utiliser le paramètre `-cap-url` Paramètre permettant de spécifier l'URL complète pour demander des informations d'identification temporaires pour l'accès à C2S.

- Le `storage aggregate object-store config create` Si ONTAP ne peut pas accéder à Amazon S3 avec les informations fournies, la commande échoue.
- Vous utilisez le `-access-key` Paramètre permettant de spécifier la clé d'accès pour autoriser les requêtes vers le magasin d'objets Amazon S3.
- Vous utilisez le `-secret-password` Paramètre permettant de spécifier le mot de passe (clé d'accès secrète) pour l'authentification des requêtes vers le magasin d'objets Amazon S3.
- En cas de modification du mot de passe Amazon S3, vous devez immédiatement mettre à jour le mot de passe correspondant stocké dans ONTAP.

ONTAP accède ainsi aux données dans Amazon S3 sans interruption.

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

+

```
cluster1::> storage aggregate object-store config create -object-store
-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&role
=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-bucket
```

2. Affichez et vérifiez les informations de configuration d'Amazon S3 à l'aide du `storage aggregate object-store config show` commande.

Le `storage aggregate object-store config modify` Permet de modifier les informations de configuration d'Amazon S3 pour FabricPool.

## Configuration de Google Cloud Storage en tant que Tier cloud

Si vous exécutez ONTAP 9.6 ou une version ultérieure, vous pouvez configurer Google Cloud Storage en tant que Tier cloud pour FabricPool.

## Considérations supplémentaires sur l'utilisation de Google Cloud Storage avec FabricPool

- Vous aurez peut-être besoin d'une licence FabricPool.

Les systèmes AFF nouvellement commandés disposent d'une capacité libre de 10 To pour l'utilisation de FabricPool. Si vous avez besoin de capacité supplémentaire sur un système AFF, si vous utilisez Google Cloud Storage sur un système non AFF ou si vous effectuez une mise à niveau à partir d'un cluster existant, vous avez besoin d'un "[Licence FabricPool](#)".

- Il est recommandé que le LIF utilisé par ONTAP pour se connecter au serveur objet Google Cloud Storage soit sur un port 10 Gbit/s.
- Sur les systèmes AFF et FAS, ainsi que sur ONTAP Select, FabricPool prend en charge plusieurs classes de stockage objet Google Cloud :
  - Google Cloud Multi-régional
  - Google Cloud régional
  - Google Cloud Nearline
  - Google Cloud Coldline

["Google Cloud : classes de stockage"](#)

## Étapes

1. Spécifiez les informations de configuration de Google Cloud Storage à l'aide du `storage aggregate object-store config create` commande avec `-provider-type GoogleCloud` paramètre.
  - Le `storage aggregate object-store config create` Échec de la commande si ONTAP ne peut pas accéder à Google Cloud Storage avec les informations fournies.
  - Vous utilisez le `-access-key` Paramètre permettant de spécifier la clé d'accès pour autoriser les requêtes vers le magasin d'objets Google Cloud Storage.
  - Si le mot de passe Google Cloud Storage est modifié, vous devez immédiatement mettre à jour le mot de passe correspondant stocké dans ONTAP.

ONTAP peut ainsi accéder sans interruption aux données dans Google Cloud Storage.

```
storage aggregate object-store config create my_gcp_store_1 -provider
-type GoogleCloud -container-name my-gcp-bucket1 -access-key
GOOGAUZZUV2USCFGHGQ511I8
```

2. Affichez et vérifiez les informations de configuration de Google Cloud Storage à l'aide du `storage aggregate object-store config show` commande.

Le `storage aggregate object-store config modify` Vous permet de modifier les informations de configuration de Google Cloud Storage pour FabricPool.

## Configuration d'IBM Cloud Object Storage en tant que Tier cloud

Si vous exécutez ONTAP 9.5 ou version ultérieure, vous pouvez configurer IBM Cloud Object Storage en tant que Tier cloud pour FabricPool.

### Considérations relatives à l'utilisation du stockage objet cloud IBM avec FabricPool

- Vous aurez peut-être besoin d'une licence FabricPool.

Les systèmes AFF nouvellement commandés disposent d'une capacité libre de 10 To pour l'utilisation de FabricPool. Si vous avez besoin de capacité supplémentaire sur un système AFF, si vous utilisez IBM Cloud Object Storage sur un système non AFF ou si vous effectuez une mise à niveau à partir d'un cluster existant, vous avez besoin d'un ["Licence FabricPool"](#).

Si vous commandez FabricPool pour la première fois pour un cluster existant, une licence FabricPool avec 10 To de capacité libre est disponible.

- Il est recommandé que le LIF utilisé par ONTAP pour se connecter avec le serveur d'objets IBM Cloud soit sur un port 10 Gbit/s.

## Étapes

1. Spécifiez les informations de configuration du stockage objet IBM Cloud à l'aide de `storage aggregate object-store config create` commande avec `-provider-type IBM_COS` paramètre.

- Le `storage aggregate object-store config create` Échec de la commande si ONTAP ne peut pas accéder au stockage objet cloud IBM avec les informations fournies.
- Vous utilisez le `-access-key` Paramètre permettant de spécifier la clé d'accès pour autoriser les requêtes vers le magasin d'objets IBM Cloud Object Storage.
- Vous utilisez le `-secret-password` Paramètre pour spécifier le mot de passe (clé d'accès secrète) pour l'authentification des requêtes vers le magasin d'objets IBM Cloud Object Storage.
- Si le mot de passe du stockage objet IBM Cloud a été modifié, vous devez immédiatement mettre à jour le mot de passe correspondant stocké dans ONTAP.

ONTAP peut ainsi accéder sans interruption aux données du stockage objet dans le cloud IBM.

```
storage aggregate object-store config create
-object-store-name MyIBM -provider-type IBM_COS
-server s3.us-east.objectstorage.softlayer.net
-container-name my-ibm-cos-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Affichez et vérifiez les informations de configuration du stockage objet IBM Cloud à l'aide du `storage aggregate object-store config show` commande.

Le `storage aggregate object-store config modify` Permet de modifier les informations de configuration du stockage objet dans le cloud IBM pour FabricPool.

## Configurez Azure Blob Storage pour le cloud en tant que Tier cloud

Si vous exécutez ONTAP 9.4 ou une version ultérieure, vous pouvez configurer Azure Blob Storage pour le cloud en tant que Tier cloud pour FabricPool.

### Considérations relatives à l'utilisation du stockage Microsoft Azure Blob avec FabricPool

- Vous aurez peut-être besoin d'une licence FabricPool.

Les systèmes AFF nouvellement commandés disposent d'une capacité libre de 10 To pour l'utilisation de FabricPool. Si vous avez besoin de capacité supplémentaire sur un système AFF, si vous utilisez Azure Blob Storage sur un système non AFF ou si vous effectuez une mise à niveau à partir d'un cluster existant, vous avez besoin d'"[Licence FabricPool](#)"un .

Si vous commandez FabricPool pour la première fois pour un cluster existant, une licence FabricPool avec 10 To de capacité libre est disponible.

- Une licence FabricPool n'est pas requise si vous utilisez Azure Blob Storage avec Cloud Volumes ONTAP.

- Il est recommandé que le LIF utilisé par ONTAP pour se connecter avec le serveur d'objets Azure Blob Storage soit sur un port 10 Gbit/s.
- FabricPool ne prend pas encore en charge Azure Stack, qui est actuellement disponible dans les services Azure sur site.
- Au niveau du compte dans Microsoft Azure Blob Storage, FabricPool ne prend en charge que les tiers de stockage à chaud et froid.

FabricPool ne prend pas en charge le Tiering au niveau des objets blob. Il ne prend pas également en charge le Tiering vers le Tier de stockage d'archivage d'Azure.

### Description de la tâche

FabricPool ne prend pas encore en charge Azure Stack, qui est actuellement disponible dans les services Azure sur site.

### Étapes

1. Spécifiez les informations de configuration du stockage Azure Blob Storage à l'aide du `storage aggregate object-store config create` commande avec `-provider-type Azure_Cloud` paramètre.
  - Le `storage aggregate object-store config create` Échec de la commande si ONTAP ne peut pas accéder au stockage Azure Blob Storage avec les informations fournies.
  - Vous utilisez le `-azure-account` Paramètre permettant de spécifier le compte Azure Blob Storage.
  - Vous utilisez le `-azure-private-key` Paramètre pour spécifier la clé d'accès pour l'authentification des requêtes vers Azure Blob Storage.
  - Si le mot de passe du stockage Azure Blob Storage est modifié, vous devez immédiatement mettre à jour le mot de passe correspondant stocké dans ONTAP.

ONTAP peut ainsi accéder sans interruption aux données dans le stockage Azure Blob Storage.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyAzure -provider-type Azure_Cloud
-server blob.core.windows.net -container-name myAzureContainer
-azure-account myAzureAcct -azure-private-key myAzureKey
```

2. Affichez et vérifiez les informations de configuration d'Azure Blob Storage à l'aide du `storage aggregate object-store config show` commande.

Le `storage aggregate object-store config modify` Vous permet de modifier les informations de configuration du stockage Azure Blob pour FabricPool.

### Configurez les magasins d'objets pour FabricPool dans une configuration MetroCluster

Si vous exécutez ONTAP 9.7 ou une version ultérieure, vous pouvez configurer une FabricPool en miroir sur une configuration MetroCluster pour transférer les données inactives vers des magasins d'objets dans deux zones de défaillance différentes.

### Description de la tâche



- FabricPool dans MetroCluster nécessite que l'agrégat en miroir sous-jacent et la configuration de magasin d'objets associée soient la même configuration MetroCluster.
- Vous ne pouvez pas associer un agrégat à un magasin d'objets créé sur le site MetroCluster distant.
- Vous devez créer des configurations de magasin d'objets dans la configuration MetroCluster qui est propriétaire de l'agrégat.

#### Avant de commencer

- La configuration MetroCluster est configurée et correctement configurée.
- Deux magasins d'objets sont configurés sur les sites MetroCluster appropriés.
- Les conteneurs sont configurés sur chaque magasin d'objets.
- Des espaces IP sont créés ou identifiés sur les deux configurations MetroCluster, dont le nom correspond.

#### Étape

1. Spécifiez les informations de configuration du magasin d'objets sur chaque site MetroCluster à l'aide du `storage object-store config create` commande.

Dans cet exemple, FabricPool est requis sur un seul cluster de la configuration MetroCluster. Deux configurations de magasin d'objets sont créées pour ce cluster, une pour chaque compartiment de magasin d'objets.

```
storage aggregate
 object-store config create -object-store-name mccl-ostore-config-s1
 -provider-type SGWS -server
 <SGWS-server-1> -container-name <SGWS-bucket-1> -access-key <key>
 -secret-password <password> -encrypt
 <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
 ipspace
 <IPSpace>
```

```
storage aggregate object-store config create -object-store-name mccl-
ostore-config-s2
 -provider-type SGWS -server <SGWS-server-2> -container-name <SGWS-
bucket-2> -access-key <key> -secret-password <password> -encrypt
 <true|false> -provider <provider-type>
 -is-ssl-enabled <true|false> ipspace <IPSpace>
```

Cet exemple illustre la configuration FabricPool sur le second cluster de la MetroCluster.

```
storage aggregate
 object-store config create -object-store-name mcc2-ostore-config-s1
-provider-type SGWS -server
 <SGWS-server-1> -container-name <SGWS-bucket-3> -access-key <key>
-secret-password <password> -encrypt
 <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
 <IPSpace>
```

```
storage aggregate
 object-store config create -object-store-name mcc2-ostore-config-s2
-provider-type SGWS -server
 <SGWS-server-2> -container-name <SGWS-bucket-4> -access-key <key>
-secret-password <password> -encrypt
 <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
 <IPSpace>
```

#### Testez les performances de débit du magasin d'objets avant de vous connecter à un Tier local

Avant de rattacher un magasin d'objets à un Tier local, vous pouvez tester la latence et les performances de débit du magasin d'objets à l'aide de l'éditeur de profil du magasin d'objets.

#### Avant d'être

- Vous devez ajouter le Tier de cloud à ONTAP avant de pouvoir l'utiliser avec l'éditeur de profil de magasin d'objets.
- Vous devez utiliser le mode de privilèges avancé de l'interface de ligne de commandes ONTAP.

#### Étapes

1. Démarrez l'éditeur de profil du magasin d'objets :

```
storage aggregate object-store profiler start -object-store-name <name> -node
<name>
```

2. Afficher les résultats :

```
storage aggregate object-store profiler show
```

#### Association du Tier cloud à un niveau local (agrégat)

Une fois que vous avez configuré un magasin d'objets comme Tier cloud, vous devez spécifier le Tier local (agrégat) à utiliser en le connectant à FabricPool. Dans ONTAP 9.5 et les versions ultérieures, vous pouvez également associer des niveaux locaux (agrégats) contenant des composants de volume FlexGroup qualifiés.

## Description de la tâche

L'association d'un niveau de cloud à un niveau local est une action permanente. Un Tier cloud ne peut pas être dissocié d'un Tier local après avoir été associé. Cependant, vous pouvez utiliser "[Miroir FabricPool](#)" pour relier un Tier local à un autre Tier cloud.

## Avant de commencer

Lorsque vous utilisez l'interface de ligne de commandes de ONTAP pour configurer un agrégat pour FabricPool, cet agrégat doit déjà exister.




Lorsque vous utilisez System Manager pour configurer un niveau local pour FabricPool, vous pouvez créer le niveau local et le configurer pour FabricPool en même temps.

## Étapes

Vous pouvez associer un niveau local (agrégat) à un magasin d'objets FabricPool avec ONTAP System Manager ou l'interface de ligne de commande de ONTAP.

## System Manager

1. Accédez à **Storage > tiers**, sélectionnez un niveau de cloud, puis cliquez sur .
2. Sélectionnez **attacher des niveaux locaux**.
3. Sous **Ajouter en tant que primaire**, vérifiez que les volumes peuvent être attachés.
4. Si nécessaire, sélectionnez **convertir les volumes en provisionnement fin**.
5. Cliquez sur **Enregistrer**.

## CLI

Pour attacher un magasin d'objets à un agrégat avec l'interface de ligne de commandes :

1. **Facultatif** : pour voir le volume de données inactives d'un volume, suivez les étapes de la section ["Détermination de la quantité de données inactives d'un volume grâce au reporting des données inactives"](#).

Vous pouvez identifier l'agrégat à utiliser pour FabricPool en raison de la quantité de données inactives d'un volume.

2. Reliez le magasin d'objets à un agrégat à l'aide de `storage aggregate object-store attach` commande.

Si jamais l'agrégat n'a été utilisé avec FabricPool et qu'il contient des volumes existants, les volumes se voient attribuer la valeur par défaut `snapshot-only` règle de hiérarchisation.

```
cluster1::> storage aggregate object-store attach -aggregate myaggr
-object-store-name Amazon01B1
```

Vous pouvez utiliser le `allow-flexgroup true` Possibilité de connecter des agrégats contenant des composants de volume FlexGroup

3. Affichez les informations du magasin d'objets et vérifiez que le magasin d'objets attaché est disponible à l'aide de `storage aggregate object-store show` commande.

```
cluster1::> storage aggregate object-store show
```

| Aggregate | Object Store Name | Availability State |
|-----------|-------------------|--------------------|
| -----     | -----             | -----              |
| myaggr    | Amazon01B1        | available          |

## Tiering des données vers le compartiment local


À partir de ONTAP 9.8, vous pouvez transférer les données vers un stockage objet local à l'aide de ONTAP S3.

Le Tiering des données dans un compartiment local constitue une alternative simple au déplacement des données vers un niveau local différent. Cette procédure utilise un compartiment existant sur le cluster local ou permet à ONTAP de créer automatiquement une machine virtuelle de stockage et un nouveau compartiment.

N'oubliez pas qu'une fois connecté à un Tier local (agrégat), le Tier cloud ne peut pas être déassocié.

Une licence S3 est requise pour ce workflow qui crée un nouveau serveur S3 et un nouveau compartiment, ou utilise les stockages existants. Cette licence est incluse dans "ONTAP One". Aucune licence FabricPool n'est requise pour ce flux de travail.

### Étape

1. Transférer les données vers un compartiment local : cliquez sur **tiers**, sélectionnez un niveau, puis cliquez sur .
2. Si nécessaire, activez le provisionnement fin.
3. Choisissez un niveau existant ou créez-en un nouveau.
4. Si nécessaire, modifiez la stratégie de hiérarchisation existante.

## Gérer FabricPool

### Présentation de Manage FabricPool

Pour vous aider à faire le Tiering du stockage, ONTAP vous permet d'afficher la quantité de données inactives d'un volume, d'ajouter ou de déplacer des volumes vers FabricPool, de surveiller l'utilisation de l'espace pour FabricPool, ou de modifier la règle de Tiering d'un volume ou une période de refroidissement minimale appliquée par le Tiering.

### Déterminez la quantité de données inactives d'un volume grâce au reporting des données inactives

Une vue la quantité de données inactives d'un volume, vous permet d'utiliser correctement les tiers de stockage. Les informations contenues dans le reporting de données inactives vous aident à décider de l'agrégat à utiliser pour FabricPool, qu'il s'agisse de déplacer un volume vers ou hors FabricPool, ou de modifier la règle de Tiering d'un volume.

### Ce dont vous avez besoin

Vous devez exécuter ONTAP 9.4 ou version ultérieure pour utiliser la fonctionnalité de reporting des données inactives.

### Description de la tâche

- Le reporting de données inactives n'est pas pris en charge sur certains agrégats.

Lorsque FabricPool ne peut pas être activé, vous ne pouvez pas activer le reporting des données inactives, y compris les instances suivantes :

- Agrégats racine
- Agrégats MetroCluster exécutant des versions ONTAP antérieures à 9.7
- Flash Pool (agrégats hybrides ou agrégats SnapLock)
- Le reporting sur les données inactives est activé par défaut sur les agrégats sur lesquels la compression adaptative est activée pour tous les volumes.
- Le reporting sur les données inactives est activé par défaut sur tous les agrégats SSD dans ONTAP 9.6.
- Le reporting des données inactives est activé par défaut sur les agrégats FabricPool dans les environnements ONTAP 9.4 et ONTAP 9.5.

- Vous pouvez activer le reporting des données inactives sur des agrégats non FabricPool à l'aide de l'interface de ligne de commande ONTAP, y compris les agrégats HDD, à partir de ONTAP 9.6.

#### **Procédure**

Déterminez la quantité de données inactives avec ONTAP System Manager ou l'interface de ligne de commandes ONTAP.

## System Manager

### 1. Choisissez l'une des options suivantes :

- Lorsque vous disposez d'agrégats de disques durs existants, accédez à **Storage > tiers** et cliquez sur l'agrégat sur lequel vous souhaitez activer le reporting des données inactives.
- Lorsqu'aucun niveau de Cloud n'est configuré, accédez à **Dashboard** et cliquez sur le lien **Activer le reporting des données inactives** sous **Capacity**.

## CLI

### Pour activer le reporting des données inactives avec l'interface de ligne de commandes :

1. Si l'agrégat pour lequel vous souhaitez voir le reporting de données inactives n'est pas utilisé dans FabricPool, activez le reporting de données inactives de l'agrégat à l'aide de `storage aggregate modify` avec `-is-inactive-data-reporting-enabled true` paramètre.

```
cluster1::> storage aggregate modify -aggregate aggr1 -is-inactive
-data-reporting-enabled true
```

Vous devez activer de manière explicite la fonctionnalité de reporting de données inactives sur un agrégat non utilisé pour FabricPool.

Il n'est pas nécessaire d'activer le reporting des données inactives sur un agrégat compatible FabricPool, car l'agrégat est déjà inclus dans le reporting des données inactives. Le `-is-inactive-data-reporting-enabled` paramètre ne fonctionne pas sur les agrégats compatibles avec FabricPool.

Le `-fields is-inactive-data-reporting-enabled` paramètre du `storage aggregate show` commande indique si le reporting de données inactives est activé sur un agrégat.

2. Pour afficher la quantité de données inactives sur un volume, utilisez le `volume show` commande avec `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` paramètre.

```
cluster1::> volume show -fields performance-tier-inactive-user-
data,performance-tier-inactive-user-data-percent

vserver volume performance-tier-inactive-user-data performance-tier-
inactive-user-data-percent

vsim1 vol0 0B 0%
vs1 vs1rv1 0B 0%
vs1 vv1 10.34MB 0%
vs1 vv2 10.38MB 0%
4 entries were displayed.
```

- Le `performance-tier-inactive-user-data` affiche la quantité de données utilisateur stockées dans l'agrégat inactives.

- Le `performance-tier-inactive-user-data-percent` Indique quel pourcentage des données inactives sur le système de fichiers actif et les copies Snapshot.
- Dans le cas d'un agrégat qui n'est pas utilisé pour FabricPool, le reporting des données inactives utilise la règle de Tiering afin de déterminer la quantité de données à signaler comme inactives.
  - Pour le `none` règle de tiering, 31 jours sont utilisés.
  - Pour le `snapshot-only` et `auto`, utilisation de rapports de données inactives `tiering-minimum-cooling-days`.
  - Pour le `ALL` la génération de rapports de données inactives suppose que les données seront stockées sur un tier d'ici une journée.

Jusqu'à ce que la période soit atteinte, la production indique "-" pour la quantité de données inactives au lieu d'une valeur.
- Sur un volume faisant partie d'FabricPool, le rapport ONTAP inactif dépend de la règle de Tiering définie sur un volume.
  - Pour le `none` Règle de Tiering, ONTAP indique le volume entier inactif pendant au moins 31 jours. Vous ne pouvez pas utiliser `-tiering-minimum-cooling-days` paramètre avec le `none` règle de hiérarchisation.
  - Pour le `ALL`, `snapshot-only`, et `auto` les règles de tiering, le reporting des données inactives n'est pas pris en charge.

## Gestion des volumes pour FabricPool

### Créer un volume pour FabricPool

Vous pouvez ajouter des volumes dans FabricPool en créant de nouveaux volumes directement dans l'agrégat compatible FabricPool ou en déplaçant des volumes existants d'un autre agrégat vers l'agrégat compatible FabricPool.

Lorsque vous créez un volume pour FabricPool, vous pouvez spécifier une règle de Tiering. Si aucune règle de Tiering n'est spécifiée, le volume créé utilise la valeur par défaut `snapshot-only` règle de hiérarchisation. Pour un volume avec `snapshot-only` ou `auto` vous pouvez également spécifier la période de tiering minimum de refroidissement.

### Ce dont vous avez besoin

- Réglage d'un volume pour utiliser le `auto` Le Tiering ou la définition de la période de refroidissement minimale de Tiering requiert la version ONTAP 9.4 ou ultérieure.
- L'utilisation des volumes FlexGroup requiert ONTAP 9.5 ou version ultérieure.
- Réglage d'un volume pour utiliser le `all` La règle de Tiering nécessite ONTAP 9.6 ou une version ultérieure.
- Réglage d'un volume pour utiliser le `-cloud-retrieval-policy` Paramètre nécessite ONTAP 9.8 ou version ultérieure.

### Étapes

1. Créez un volume pour FabricPool en utilisant le `volume create` commande.
  - Le `-tiering-policy` le paramètre facultatif vous permet de spécifier la règle de tiering du volume.



Vous pouvez spécifier l'une des règles de hiérarchisation suivantes :

- `snapshot-only` (valeur par défaut)
- `auto`
- `all`
- `backup` (obsolète)
- `none`

#### "Types de règles de Tiering FabricPool"

- Le `-cloud-retrieval-policy` paramètre facultatif permet aux administrateurs du cluster disposant du niveau de privilège avancé de remplacer le comportement de migration ou de récupération du cloud par défaut contrôlé par la règle de tiering.

Vous pouvez définir l'une des règles de récupération cloud suivantes :

- `default`

La règle de Tiering détermine les données qui sont récupérées, donc aucune modification n'est apportée à la récupération des données du cloud `default` stratégie de récupération cloud. Le comportement est donc identique à celui des versions antérieures à ONTAP 9.8 :

- Si la règle de hiérarchisation est `none` ou `snapshot-only`, « par conséquent » signifie que toutes les données lues par les clients sont extraites du tier cloud vers le tier de performance.
- Si la règle de hiérarchisation est `auto`, les lectures aléatoires basées sur le client sont alors extraites, mais pas les lectures séquentielles.
- Si la règle de hiérarchisation est `all` alors, aucune donnée axée sur les clients n'est extraite du tier cloud.

- `on-read`

Toutes les lectures de données basées sur client sont transférées du Tier cloud vers le Tier de performance.

- `never`

Aucune donnée client n'est tirée du Tier cloud vers le Tier de performance

- `promote`

- De la règle de Tiering `none`, toutes les données du cloud sont extraites du tier cloud jusqu'au tier de performance
- De la règle de Tiering `snapshot-only`, toutes les données de système de fichiers actives sont extraites du tier cloud vers le tier de performance.

- Le `-tiering-minimum-cooling-days` le paramètre facultatif du niveau de privilège avancé vous permet de spécifier la période de refroidissement minimum du tiering pour un volume qui utilise le `snapshot-only` ou `auto` règle de hiérarchisation.

Depuis la version ONTAP 9.8, vous pouvez spécifier une valeur entre 2 et 183 pour les jours de refroidissement minimum par Tiering. Si vous utilisez une version de ONTAP antérieure à la version

9.8, vous pouvez indiquer une valeur comprise entre 2 et 63 pour les jours de refroidissement minimum par Tiering.

### Exemple de création de volume pour FabricPool

L'exemple suivant crée un volume appelé « myvol1 » dans l'agrégat doté de FabricPool « myFabricPool ». La règle de Tiering est définie sur `auto` la période de tiering minimale de refroidissement est définie sur 45 jours :

```
cluster1::*> volume create -vserver myVS -aggregate myFabricPool
-volume myvol1 -tiering-policy auto -tiering-minimum-cooling-days 45
```

### Informations associées

["Gestion des volumes FlexGroup"](#)

### Déplacer un volume vers FabricPool

Lorsque vous déplacez un volume vers FabricPool, vous avez la possibilité d' spécifier ou de modifier la règle de Tiering du volume déplacé. Depuis ONTAP 9.8, lorsque vous déplacez un volume non FabricPool avec les fonctions de reporting des données inactives activées, FabricPool utilise une carte des points chauds pour lire les blocs tiabiles et déplace les données inactives vers le Tier de capacité sur la destination FabricPool.

### Ce dont vous avez besoin

Vous devez savoir en quoi la modification de la règle de Tiering peut affecter le temps nécessaire aux données inactives et déplacées vers le Tier cloud.

["Que arrive-t-il à la règle de Tiering lorsque vous déplacez un volume"](#)

### Description de la tâche

Si le reporting des données inactives est activé pour un volume non FabricPool, lorsque vous déplacez un volume avec une règle de Tiering `auto` ou `snapshot-only` Dans un FabricPool, FabricPool lit les blocs de température tibles d'un fichier de carte des chaleur et utilise cette température pour déplacer les données inactives directement vers le Tier de capacité sur le système de destination FabricPool.

Vous ne devez pas utiliser le `-tiering-policy` Option de déplacement des volumes avec ONTAP 9.8.1, avec FabricPool, vous pouvez utiliser les informations de reporting des données inactives afin de déplacer directement les données vers le Tier de capacité. Avec cette option, FabricPool ignore les données de température et suit à la place le comportement de déplacement des versions antérieures à ONTAP 9.8.

### Étape

1. Utilisez le `volume move start` Commande de déplacement d'un volume vers FabricPool.

Le `-tiering-policy` le paramètre facultatif vous permet de spécifier la règle de tiering du volume.

Vous pouvez spécifier l'une des règles de hiérarchisation suivantes :

- `snapshot-only` (valeur par défaut)
- `auto`

- all
- none

### "Types de règles de Tiering FabricPool"

#### Exemple de déplacement d'un volume vers FabricPool

L'exemple suivant déplace un volume nommé « myvol2 » de la SVM « vs1 » vers l'agrégat « dest\_FabricPool » activé par FabricPool. Le volume est explicitement défini pour utiliser le `none` règle de hiérarchisation :

```
cluster1::> volume move start -vserver vs1 -volume myvol2
-destination-aggregate dest_FabricPool -tiering-policy none
```

#### Activez et désactivez les volumes pour écrire directement dans le cloud

Depuis ONTAP 9.14.1, vous pouvez activer et désactiver l'écriture directement dans le cloud sur un volume nouveau ou existant d'un FabricPool. Les clients NFS peuvent ainsi écrire des données directement dans le cloud sans attendre les analyses de Tiering. Les clients SMB écrivent toujours dans le Tier de performance dans un volume cloud compatible avec l'écriture. Le mode d'écriture dans le cloud est désactivé par défaut.

La possibilité d'écrire directement dans le cloud s'avère utile pour des cas tels que les migrations, par exemple lorsqu'un grand volume de données est transféré vers un cluster que le cluster ne peut prendre en charge sur le niveau local. Sans mode d'écriture dans le cloud, lors d'une migration, de petites quantités de données sont transférées, puis hiérarchisées, puis retransférées et hiérarchisées jusqu'à la fin de la migration. Avec le mode d'écriture dans le cloud, ce type de gestion n'est plus nécessaire, car les données ne sont jamais transférées vers le Tier local.

#### Avant de commencer

- Vous devez être administrateur de cluster ou SVM.
- Vous devez avoir le niveau de privilège avancé.
- Le volume doit être de type lecture-écriture.
- Le volume doit disposer de la règle de hiérarchisation TOTALE.

#### Activez l'écriture directement dans le cloud lors de la création du volume

##### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Créer un volume et activer le mode d'écriture cloud :

```
volume create -volume <volume name> -is-cloud-write-enabled <true|false>
-aggregate <local tier name>
```

L'exemple suivant illustre la création d'un volume nommé vol1 avec l'écriture cloud activée sur le Tier local FabricPool (aggr1) :

```
volume create -volume vol1 -is-cloud-write-enabled true -aggregate aggr1
```

## Activez l'écriture directement dans le cloud sur un volume existant

### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Modifier un volume pour activer le mode d'écriture sur le cloud :

```
volume modify -volume <volume name> -is-cloud-write-enabled <true|false>
-aggregate <local tier name>
```

L'exemple suivant modifie un volume nommé vol1 avec l'écriture cloud activée sur le niveau local FabricPool (aggr1) :

```
volume modify -volume vol1 -is-cloud-write-enabled true -aggregate aggr1
```

## Désactivez l'écriture directement dans le cloud sur un volume

### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Désactiver le mode d'écriture dans le cloud :

```
volume modify -volume <volume name> -is-cloud-write-enabled <true|false>
-aggregate <aggregate name>
```

L'exemple suivant illustre la création d'un volume nommé vol1 avec l'écriture dans le cloud activée :

```
volume modify -volume vol1 -is-cloud-write-enabled false -aggregate
aggr1
```

## Activer et désactiver le mode de lecture anticipée agressif

À partir de ONTAP 9.14.1, vous pouvez activer et désactiver le mode lecture anticipée agressif sur les volumes de FabricPools qui prennent en charge les médias et le divertissement, tels que les workloads de streaming de films. Un mode de lecture anticipée agressif est disponible dans ONTAP 9.14.1 sur toutes les plateformes sur site qui prennent en charge FabricPool. La fonction est désactivée par défaut.

### Description de la tâche

Le `aggressive-readahead-mode` la commande a deux options :

- `none`: la lecture anticipée est désactivée.
- `file_prefetch`: le système lit l'intégralité du fichier en mémoire avant l'application client.

### Avant de commencer

- Vous devez être administrateur de cluster ou SVM.
- Vous devez avoir le niveau de privilège avancé.

## Activer le mode de lecture anticipée agressif pendant la création du volume

### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Créer un volume et activer un mode de lecture anticipée agressif :

```
volume create -volume <volume name> -aggressive-readahead-mode
<none|file_prefetch>
```

L'exemple suivant crée un volume nommé `vol1` avec la lecture anticipée aggressive activée avec l'option `file_prefetch` :

```
volume create -volume vol1 -aggressive-readahead-mode file_prefetch
```

## Désactiver le mode de lecture anticipée agressif

### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Désactiver le mode de lecture anticipée agressif :

```
volume modify -volume <volume name> -aggressive-readahead-mode none
```

L'exemple suivant modifie un volume nommé vol1 pour désactiver le mode de lecture anticipée agressif :

```
volume modify -volume vol1 -aggressive-readahead-mode none
```

## Affichez un mode de lecture anticipée agressif sur un volume

### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Afficher le mode de lecture anticipée agressif :

```
volume show -fields aggressive-readahead-mode
```

## Balises d'objets à l'aide de balises personnalisées créées par l'utilisateur

### Présentation du balisage d'objets à l'aide de balises personnalisées créées par l'utilisateur

Depuis ONTAP 9.8, FabricPool prend en charge le balisage d'objets à l'aide de balises personnalisées créées par l'utilisateur pour classer et trier les objets pour une gestion simplifiée. Si vous êtes un utilisateur avec le niveau de privilège admin, vous pouvez créer de nouvelles balises d'objet, modifier, supprimer et afficher des balises existantes.

### Attribuez une nouvelle balise lors de la création du volume

Vous pouvez créer une nouvelle balise d'objet lorsque vous souhaitez affecter une ou plusieurs balises à de nouveaux objets qui sont placés à un niveau à partir d'un nouveau volume que vous créez. Les balises permettent de classer et de trier les objets de hiérarchisation pour plus de facilité la gestion des données. À partir de ONTAP 9.8, vous pouvez utiliser System Manager pour créer des balises d'objet.

### Description de la tâche

Vous pouvez définir des balises uniquement sur les volumes FabricPool reliés à StorageGRID. Ces balises sont conservées lors du déplacement de volume.

- Un maximum de 4 balises par volume est autorisé.
- Dans l'interface de ligne de commande, chaque balise d'objet doit être une paire clé-valeur séparée par un signe égal ("").
- Dans l'interface de ligne de commande, plusieurs balises doivent être séparées par une virgule (",").

- Chaque valeur de balise peut contenir un maximum de 127 caractères.
- Chaque touche de balise doit commencer par un caractère alphabétique ou un trait de soulignement.

Les touches ne doivent contenir que des caractères alphanumériques et des traits de soulignement, et le nombre maximum de caractères autorisé est de 127.

## Procédure

Vous pouvez attribuer des balises d'objet à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes de ONTAP.

### System Manager

1. Accédez à **stockage > niveaux**.
2. Localisez un niveau de stockage contenant les volumes à marquer.
3. Cliquez sur l'onglet **volumes**.
4. Localisez le volume que vous souhaitez marquer et dans la colonne **balises d'objet**, sélectionnez **cliquez pour entrer des balises**.
5. Entrez une clé et une valeur.
6. Cliquez sur **appliquer**.

### CLI

1. Utilisez le `volume create` commande avec `-tiering-object-tags` option permettant de créer un nouveau volume avec les balises spécifiées. Vous pouvez spécifier plusieurs balises dans des paires séparées par des virgules :

```
volume create [-vserver <vserver name>] -volume <volume_name>
-tiering-object-tags <key1=value1> [
 ,<key2=value2>,<key3=value3>,<key4=value4>]
```

L'exemple suivant illustre la création d'un volume nommé `fp_Volume 1` avec trois balises d'objet.

```
vol create -volume fp_volumel -vserver vs0 -tiering-object-tags
project=fabricpool,type=abc,content=data
```

### Modifier une balise existante

Vous pouvez modifier le nom d'une balise, remplacer des balises sur des objets existants dans le magasin d'objets ou ajouter une balise différente aux nouveaux objets que vous prévoyez d'ajouter ultérieurement.

### Description de la tâche

À l'aide du `volume modify` commande avec `-tiering-object-tags` option remplace les étiquettes existantes par la nouvelle valeur que vous avez apportée.

## Procédure

### System Manager

1. Accédez à **stockage > niveaux**.
2. Recherchez un Tier de stockage contenant des volumes contenant des balises à modifier.
3. Cliquez sur l'onglet **volumes**.
4. Localisez le volume avec les balises que vous souhaitez modifier et dans la colonne **balises d'objet**, cliquez sur le nom de la balise.
5. Modifier la balise.
6. Cliquez sur **appliquer**.

### CLI

1. Utilisez le `volume modify` commande avec `-tiering-object-tags` option permettant de modifier une balise existante.

```
volume modify [-vserver <vserver name>] -volume <volume_name>
-tiering-object-tags <key1=value1> [,<key2=value2>,
<key3=value3>,<key4=value4>]
```

L'exemple suivant modifie le nom du type de balise existant=abc en type=xyz.

```
vol create -volume fp_volumel -vserver vs0 -tiering-object-tags
project=fabricpool,type=xyz,content=data
```

### Supprimer une balise

Vous pouvez supprimer des balises d'objet lorsque vous ne souhaitez plus les définir sur un volume ou sur des objets du magasin d'objets.

## Procédure

Vous pouvez supprimer les balises d'objet avec ONTAP System Manager ou l'interface de ligne de commandes de ONTAP.



## System Manager

1. Accédez à **stockage > niveaux**.
2. Localisez un niveau de stockage contenant des volumes contenant des balises à supprimer.
3. Cliquez sur l'onglet **volumes**.
4. Localisez le volume avec les balises que vous souhaitez supprimer et dans la colonne **balises d'objet**, cliquez sur le nom de la balise.
5. Pour supprimer la balise, cliquez sur l'icône de corbeille.
6. Cliquez sur **appliquer**.

## CLI

1. Utilisez le `volume modify` commande avec `-tiering-object-tags` suivi d'une valeur vide ("" ) pour supprimer une balise existante.

L'exemple suivant supprime les balises existantes sur `fp_Volume 1`.

```
vol modify -volume fp_volumel -vserver vs0 -tiering-object-tags ""
```

## Afficher les balises existantes sur un volume

Vous pouvez afficher les balises existantes sur un volume pour voir les balises disponibles avant d'ajouter de nouvelles balises dans la liste.

### Étape

1. Utilisez le `volume show` commande avec `-tiering-object-tags` option pour afficher les balises existantes sur un volume.

```
volume show [-vserver <vserver name>] -volume <volume_name> -fields
-tiering-object-tags
```

## Vérifier l'état du balisage d'objets sur les volumes FabricPool

Vous pouvez vérifier si l'étiquetage est terminé sur un ou plusieurs volumes FabricPool.

### Étape

1. Utilisez le `vol show` commande avec `-fieldsneeds-object-retagging` option permettant de vérifier si le marquage est en cours, s'il est terminé ou si le marquage n'est pas défini.

```
vol show -fields needs-object-retagging [-instance | -volume <volume
name>]
```

L'une des valeurs suivantes s'affiche :

- `true` — le scanner de marquage d'objet n'a pas encore été exécuté ou doit être de nouveau exécuté pour ce volume
- `false` — le scanneur de marquage d'objet a terminé le balisage de ce volume
- `<->` — le scanner de marquage d'objet n'est pas applicable pour ce volume. Cela se produit pour les volumes qui ne résident pas sur FabricPool.

## Surveiller l'utilisation de l'espace pour FabricPool

Vous devez connaître la quantité de données stockées dans les tiers de performance et de cloud pour FabricPool. Ces informations vous permettent de déterminer si vous devez modifier la règle de Tiering d'un volume, d'augmenter la limite d'utilisation sous licence d'FabricPool ou d'augmenter l'espace de stockage du Tier cloud.

### Étapes

1. Contrôlez l'utilisation de l'espace pour les agrégats compatibles FabricPool à l'aide de l'une des commandes suivantes pour afficher les informations :

| Si vous voulez afficher...                                                                                      | Ensuite, utilisez cette commande :                                                 |
|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Taille utilisée du Tier cloud dans un agrégat                                                                   | <code>storage aggregate show</code> avec le <code>-instance</code> paramètre       |
| Détails de l'utilisation de l'espace au sein d'un agrégat, y compris la capacité référencée du magasin d'objets | <code>storage aggregate show-space</code> avec le <code>-instance</code> paramètre |
| Utilisation de l'espace des magasins d'objets connectés aux agrégats, y compris l'espace de licence utilisé     | <code>storage aggregate object-store show-space</code>                             |
| Liste des volumes d'un agrégat et de leurs données et métadonnées sans leur empreinte                           | <code>volume show-footprint</code>                                                 |

En plus d'utiliser les commandes de l'interface de ligne de commandes, vous pouvez utiliser Active IQ Unified Manager (anciennement OnCommand Unified Manager) avec FabricPool Advisor, qui est pris en charge sur les clusters ONTAP 9.4 et versions ultérieures, ou System Manager pour contrôler l'utilisation de l'espace.

L'exemple suivant montre des moyens d'afficher l'utilisation de l'espace et les informations associées pour FabricPool :

```
cluster1::> storage aggregate show-space -instance
```

```
Aggregate: MyFabricPool
...
Aggregate Display Name:
MyFabricPool
...
Total Object Store Logical Referenced
Capacity: -
Object Store Logical Referenced Capacity
Percentage: -
...
Object Store
Size: -
Object Store Space Saved by Storage
Efficiency: -
Object Store Space Saved by Storage Efficiency
Percentage: -
Total Logical Used
Size: -
Logical Used
Percentage: -
Logical Unreferenced
Capacity: -
Logical Unreferenced
Percentage: -
```

```
cluster1::> storage aggregate show -instance
```

```
Aggregate: MyFabricPool
...
Composite: true
Capacity Tier Used Size:
...
```

```
cluster1::> volume show-footprint
```

```
Vserver : vs1
```

```
Volume : rootvol
```

| Feature                  | Used | Used% |
|--------------------------|------|-------|
| Volume Footprint         | KB   | %     |
| Volume Guarantee         | MB   | %     |
| Flexible Volume Metadata | KB   | %     |
| Delayed Frees            | KB   | %     |
| Total Footprint          | MB   | %     |

```
Vserver : vs1
```

```
Volume : vol
```

| Feature                       | Used | Used% |
|-------------------------------|------|-------|
| Volume Footprint              | KB   | %     |
| Footprint in Performance Tier | KB   | %     |
| Footprint in Amazon01         | KB   | %     |
| Flexible Volume Metadata      | MB   | %     |
| Delayed Frees                 | KB   | %     |
| Total Footprint               | MB   | %     |
| ...                           |      |       |

## 2. Procédez de l'une des manières suivantes :

| Les fonctions que vous recherchez...                       | Alors...                                                                                                                                                                             |
|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modification de la règle de Tiering d'un volume            | Suivre la procédure de la section " <a href="#">Gestion du Tiering du stockage en modifiant la règle de hiérarchisation ou la période de refroidissement minimale d'un volume</a> ". |
| Augmentez la limite d'utilisation de la licence FabricPool | Contactez votre ingénieur commercial NetApp ou partenaire.<br><br><a href="#">"Support NetApp"</a>                                                                                   |
| Augmentez l'espace de stockage du Tier cloud               | Contactez le fournisseur du magasin d'objets que vous utilisez pour le Tier cloud.                                                                                                   |

## Gérez le Tiering du stockage en modifiant la règle de hiérarchisation d'un volume ou une période de refroidissement minimale de hiérarchisation

Vous pouvez modifier la règle de Tiering d'un volume afin de déterminer si les données sont déplacées vers le Tier cloud lorsqu'elles deviennent inactives (*Cold*). Pour un volume avec `snapshot-only` ou `auto` la règle de tiering permet également de définir la période de refroidissement minimale de tiering à laquelle les données utilisateur doivent rester inactives avant leur transfert vers le tier cloud.

### Ce dont vous avez besoin

Modification d'un volume sur le `auto` La règle de Tiering ou la modification de la période de refroidissement minimum de Tiering nécessite ONTAP 9.4 ou une version ultérieure.

### Description de la tâche

La modification de la règle de Tiering d'un volume modifie uniquement le comportement de Tiering ultérieur du volume. Elle ne déplace pas de façon rétroactive les données vers le Tier cloud.

La modification de la règle de Tiering peut affecter le temps nécessaire aux données inactives et déplacées vers le Tier cloud.

"Que se passe-t-il lorsque vous modifiez la règle de Tiering d'un volume dans FabricPool"

### Étapes

1. Modifiez la règle de hiérarchisation pour un volume existant à l'aide de la `volume modify` commande avec `-tiering-policy` paramètre :

Vous pouvez spécifier l'une des règles de hiérarchisation suivantes :

- `snapshot-only` (valeur par défaut)
- `auto`
- `all`
- `none`

"Types de règles de Tiering FabricPool"

2. Si le volume utilise le `snapshot-only` ou `auto` et que vous souhaitez modifier la période de tiering minimum de refroidissement, utilisez le `volume modify` commande avec `-tiering-minimum-cooling-days` paramètre facultatif au niveau de privilège avancé.

Vous pouvez spécifier une valeur comprise entre 2 et 183 pour les jours de refroidissement minimum par niveaux. Si vous utilisez une version de ONTAP antérieure à la version 9.8, vous pouvez indiquer une valeur comprise entre 2 et 63 pour les jours de refroidissement minimum par Tiering.

### Exemple de modification de la règle de Tiering et de la période de refroidissement minimale d'un volume

L'exemple suivant modifie la politique de hiérarchisation du volume « myvol » dans la SVM « vs1 » en `auto` et la période de refroidissement minimale par tiering à 45 jours :

```
cluster1::> volume modify -vserver vs1 -volume myvol
-tiering-policy auto -tiering-minimum-cooling-days 45
```

### Archiver des volumes avec FabricPool (vidéo)

Cette vidéo présente l'utilisation de System Manager pour archiver un volume dans un Tier cloud avec FabricPool.

["Vidéo NetApp : archivage de volumes avec FabricPool \(sauvegarde + déplacement de volume\)"](#)

### Informations associées

["NetApp TechComm TV : liste de lecture FabricPool"](#)

### Utilisez les contrôles de migration cloud pour remplacer la règle de Tiering par défaut d'un volume

Vous pouvez modifier la règle de Tiering par défaut d'un volume pour contrôler la récupération des données utilisateur depuis le Tier cloud vers le Tier de performance à l'aide de `-cloud-retrieval-policy` Option introduite dans ONTAP 9.8.

### Ce dont vous avez besoin

- Modification d'un volume à l'aide du `-cloud-retrieval-policy` Option requise : ONTAP 9.8 ou version ultérieure.
- Vous devez disposer du niveau de privilège avancé pour effectuer cette opération.
- Vous devez comprendre le comportement des règles de hiérarchisation avec `-cloud-retrieval-policy`.

["Fonctionnement des règles de Tiering avec la migration vers le cloud"](#)

### Étape

1. Modifiez le comportement de la règle de hiérarchisation pour un volume existant à l'aide de la `volume modify` commande avec `-cloud-retrieval-policy` option :

```
volume create -volume <volume_name> -vserver <vserver_name> - tiering-
policy <policy_name> -cloud-retrieval-policy
```

```
vol modify -volume fp_volume4 -vserver vs0 -cloud-retrieval-policy
promote
```

### Promouvoir les données vers le Tier de performance

#### Promouvoir les données auprès des niveaux de performance

Depuis ONTAP 9.8, si vous êtes administrateur de cluster au niveau de privilège avancé, vous pouvez promouvoir les données de manière proactive à partir du Tier de

performance à partir du cloud, à l'aide d'une combinaison de la `tiering-policy` et le `cloud-retrieval-policy` réglage.

### Description de la tâche

Cette opération peut être nécessaire si vous souhaitez arrêter l'utilisation d'FabricPool sur un volume ou si vous disposez d'un `snapshot-only` La règle de Tiering et vous voulez renvoyer les données de copie Snapshot restaurées vers le Tier de performance.

#### Promotion de toutes les données d'un volume FabricPool vers le Tier de performance

Vous pouvez récupérer toutes les données de manière proactive sur un volume FabricPool dans le cloud et les promouvoir dans le Tier de performance.

#### Étape

1. Utilisez le `volume modify` commande à définir `tiering-policy` à `none` et `cloud-retrieval-policy` à `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy none -cloud-retrieval-policy promote
```

#### Promotion des données du système de fichiers sur le Tier de performances

Vous pouvez récupérer de manière proactive les données du système de fichiers actif à partir d'une copie Snapshot restaurée dans le Tier cloud et les promouvoir dans le Tier de performance.

#### Étape

1. Utilisez le `volume modify` commande à définir `tiering-policy` à `snapshot-only` et `cloud-retrieval-policy` à `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy snapshot-only cloud-retrieval-policy promote
```

#### Vérifier le statut de la promotion du niveau de performances

Vous pouvez vérifier l'état de la promotion du niveau de performances pour déterminer une fois l'opération terminée.

#### Étape

1. Utiliser le `volume object-store` commande avec `tiering` option permettant de vérifier le statut de la promotion du niveau de performance.

```

volume object-store tiering show [-instance | -fields <fieldname>, ...
] [-vserver <vserver name>] *Vserver
[[-volume] <volume name>] *Volume [-node <nodename>] *Node Name [-vol
-dsid <integer>] *Volume DSID
[-aggregate <aggregate name>] *Aggregate Name

```

```

volume object-store tiering show v1 -instance

 Vserver: vs1
 Volume: v1
 Node Name: node1
 Volume DSID: 1023
 Aggregate Name: a1
 State: ready
 Previous Run Status: completed
 Aborted Exception Status: -
 Time Scanner Last Finished: Mon Jan 13 20:27:30 2020
 Scanner Percent Complete: -
 Scanner Current VBN: -
 Scanner Max VBNs: -
 Time Waiting Scan will be scheduled: -
 Tiering Policy: snapshot-only
 Estimated Space Needed for Promotion: -
 Time Scan Started: -
 Estimated Time Remaining for scan to complete: -
 Cloud Retrieve Policy: promote

```

#### Déclenchement de la migration planifiée et de la hiérarchisation

Depuis ONTAP 9.8, vous pouvez déclencher une demande de scan de Tiering à tout moment si vous ne souhaitez pas attendre le scan de Tiering par défaut.

#### Étape

1. Utilisez le `volume object-store` commande avec `trigger` possibilité de demander la migration et le tiering.

```

volume object-store tiering trigger [-vserver <vserver name>] *VServer
Name [-volume] <volume name> *Volume Name

```

## Gérer les miroirs FabricPool



## Présentation de la gestion des miroirs FabricPool

Pour garantir l'accès aux données dans les data stores en cas d'incident et pour vous permettre de remplacer un datastore, vous pouvez configurer un miroir FabricPool en ajoutant un second datastore afin de hiérarchiser de manière synchrone les données sur deux datastores . Vous pouvez ajouter un second magasin de données à des configurations FabricPool nouvelles ou existantes, surveiller l'état du miroir, afficher les détails du miroir FabricPool, promouvoir un miroir et supprimer un miroir. Vous devez exécuter ONTAP 9.7 ou une version ultérieure.

### Créer un miroir FabricPool

Pour créer un miroir FabricPool, vous devez associer deux magasins d'objets à une seule FabricPool. Vous pouvez créer un miroir FabricPool en reliant un second magasin d'objets à une configuration FabricPool existante de magasin d'objets unique, ou créer une nouvelle configuration FabricPool de magasin d'objets unique, puis y rattacher un second magasin d'objets. Vous pouvez également créer des miroirs FabricPool sur les configurations MetroCluster.

#### Ce dont vous avez besoin

- Vous devez avoir déjà créé les deux magasins d'objets à l'aide de `storage aggregate object-store config` commande.
- Si vous créez des miroirs FabricPool sur les configurations MetroCluster :
  - Vous devez avoir déjà configuré et configuré MetroCluster
  - Vous devez avoir créé les configurations de magasin d'objets sur le cluster sélectionné.

Si vous créez des miroirs FabricPool sur les deux clusters dans une configuration MetroCluster, vous devez avoir créé des configurations de magasin d'objets sur les deux clusters.

- Si vous n'utilisez pas de magasins d'objets sur site pour les configurations MetroCluster, vous devez vous assurer que l'un des scénarios suivants existe :
  - Les magasins d'objets se trouvent dans différentes zones de disponibilité
  - Les magasins d'objets sont configurés pour conserver des copies d'objets dans plusieurs zones de disponibilité

["Configuration des magasins d'objets pour FabricPool dans une configuration MetroCluster"](#)

#### Description de la tâche

Le magasin d'objets que vous utilisez pour le miroir FabricPool doit être différent du magasin d'objets primaire.

La procédure de création d'un miroir FabricPool est la même pour les configurations MetroCluster et non-MetroCluster.

#### Étapes

1. Si vous n'utilisez pas de configuration FabricPool existante, créez-en une nouvelle en connectant un magasin d'objets à un agrégat à l'aide de `storage aggregate object-store attach` commande.

Dans cet exemple, une nouvelle FabricPool est créée en connectant un magasin d'objets à un agrégat.

```
cluster1::> storage aggregate object-store attach -aggregate aggr1 -name my-store-1
```

2. Reliez un second magasin d'objets à l'agrégat à l'aide de `storage aggregate object-store mirror` commande.

Cet exemple attache un second magasin d'objets à un agrégat pour créer un miroir FabricPool.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name my-store-2
```

### Surveillez l'état des synchronisations du miroir FabricPool

Lorsque vous remplacez un magasin d'objets primaire par un miroir, vous devrez peut-être attendre que le miroir puisse resynchroniser avec le magasin de données primaire.

#### Description de la tâche

Si le miroir FabricPool est en mode synchrone, aucune entrée n'est affichée.

#### Étape

1. Surveillez l'état des synchronisations des miroirs à l'aide de `storage aggregate object-store show-resync-status` commande.

```
aggregate1::> storage aggregate object-store show-resync-status -aggregate aggr1
```

| Aggregate | Primary    | Mirror     | Complete Percentage |
|-----------|------------|------------|---------------------|
| -----     | -----      | -----      | -----               |
| aggr1     | my-store-1 | my-store-2 | 40%                 |

### Afficher les détails du miroir FabricPool

Vous pouvez afficher des détails sur un miroir FabricPool pour voir quels magasins d'objets sont dans la configuration et si le miroir du magasin d'objets est synchronisé avec le magasin d'objets principal.

#### Étape

1. Affiche des informations sur un miroir FabricPool à l'aide du `storage aggregate object-store show` commande.

Cet exemple affiche les détails des magasins d'objets principal et miroir dans un miroir FabricPool.

```
cluster1::> storage aggregate object-store show
```

| Aggregate | Object Store Name | Availability | Mirror Type |
|-----------|-------------------|--------------|-------------|
| -----     | -----             | -----        | -----       |
| aggr1     | my-store-1        | available    | primary     |
|           | my-store-2        | available    | mirror      |

Cet exemple affiche des informations détaillées sur le miroir FabricPool, notamment si le miroir est dégradé en raison d'une opération de resynchronisation.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-mirror-degraded
```

| aggregate | object-store-name | mirror-type | is-mirror-degraded |
|-----------|-------------------|-------------|--------------------|
| -----     | -----             | -----       | -----              |
| aggr1     | my-store-1        | primary     | -                  |
|           | my-store-2        | mirror      | false              |

## Promouvoir un miroir FabricPool

Vous pouvez réattribuer le miroir du magasin d'objets en tant que magasin d'objets principal en le promouvant. Lorsque le miroir du magasin d'objets devient le miroir principal, le miroir d'origine devient automatiquement le miroir.

### Ce dont vous avez besoin

- Le miroir FabricPool doit être synchronisé
- Le magasin d'objets doit être opérationnel

### Description de la tâche

Vous pouvez remplacer le magasin d'objets d'origine par un magasin d'objets d'un autre fournisseur cloud. Par exemple, le miroir d'origine peut être un magasin d'objets AWS, mais vous pouvez le remplacer par un magasin d'objets Azure.

### Étape

1. Promouvoir un miroir de magasin d'objets à l'aide du `storage aggregate object-store modify -aggregate` commande.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name my-store-2 -mirror-type primary
```

## Déposer un miroir FabricPool

Si vous n'avez plus besoin de répliquer un magasin d'objets, vous pouvez supprimer un miroir FabricPool.

### Ce dont vous avez besoin

Le magasin d'objets principal doit être opérationnel ; sinon, la commande échoue.

### Étape

1. Supprimez un miroir de magasin d'objets dans un FabricPool à l'aide de `storage aggregate object-store unmirror -aggregate commande`.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

## Remplacer un magasin d'objets existant à l'aide d'un miroir FabricPool

Vous pouvez utiliser la technologie FabricPool mirror pour remplacer un magasin d'objets par un autre. Le nouveau magasin d'objets n'a pas besoin d'utiliser le même fournisseur cloud que le magasin d'objets d'origine.

### Description de la tâche

Vous pouvez remplacer le magasin d'objets d'origine par un magasin d'objets qui utilise un autre fournisseur cloud. Par exemple, votre magasin d'objets d'origine peut utiliser AWS en tant que fournisseur cloud, mais vous pouvez le remplacer par un magasin d'objets qui utilise Azure comme fournisseur cloud, et inversement. Toutefois, le nouveau magasin d'objets doit conserver la même taille d'objet que l'original.

### Étapes

1. Créez un miroir FabricPool en ajoutant un nouveau magasin d'objets à un FabricPool existant à l'aide de `storage aggregate object-store mirror -aggregate commande`.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1
-object-store-name my-AZURE-store
```

2. Surveillez l'état de resynchronisation du miroir à l'aide du `storage aggregate object-store show-resync-status commande`.

```
cluster1::> storage aggregate object-store show-resync-status -aggregate
aggr1
```

| Aggregate | Primary      | Mirror         | Complete<br>Percentage |
|-----------|--------------|----------------|------------------------|
| -----     | -----        | -----          | -----                  |
| aggr1     | my-AWS-store | my-AZURE-store | 40%                    |

3. Vérifiez que le miroir est en mode synchrone à l'aide du `storage aggregate object-store> show -fields mirror-type,is-mirror-degraded` commande.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

| aggregate | object-store-name | mirror-type | is-mirror-degraded |
|-----------|-------------------|-------------|--------------------|
| aggr1     | my-AWS-store      | primary     | -                  |
|           | my-AZURE-store    | mirror      | false              |

4. Remplacez le magasin d'objets principal par le magasin d'objets symétriques à l'aide du `storage aggregate object-store modify` commande.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1
-object-store-name my-AZURE-store -mirror-type primary
```

5. Affiche des détails sur le miroir FabricPool à l'aide du `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` commande.

Cet exemple affiche les informations relatives au miroir FabricPool, y compris si le miroir est dégradé (hors synchronisation).

```
cluster1::> storage aggregate object-store show -fields mirror-type, is-
mirror-degraded
```

| aggregate | object-store-name | mirror-type | is-mirror-degraded |
|-----------|-------------------|-------------|--------------------|
| aggr1     | my-AZURE-store    | primary     | -                  |
|           | my-AWS-store      | mirror      | false              |

6. Déposer le rétroviseur FabricPool à l'aide de l'outil `storage aggregate object-store unmirror` commande.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

7. Vérifiez que FabricPool est de nouveau dans une configuration de magasin d'objets unique à l'aide du `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` commande.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-mirror-degraded
```

| aggregate | object-store-name | mirror-type | is-mirror-degraded |
|-----------|-------------------|-------------|--------------------|
| aggr1     | my-AZURE-store    | primary     | -                  |

## Remplacement d'un miroir FabricPool sur une configuration MetroCluster

Si l'un des magasins d'objets d'un miroir FabricPool est détruit ou devient définitivement indisponible dans une configuration MetroCluster, vous pouvez faire du magasin d'objets le miroir s'il ne s'agit pas déjà du miroir, supprimer le magasin d'objets endommagé du miroir FabricPool, Puis ajoutez un nouveau miroir de magasin d'objets à FabricPool.

### Étapes

1. Si le magasin d'objets endommagés n'est pas déjà le miroir, faites stocker l'objet avec le `storage aggregate object-store modify` commande.

```
storage aggregate object-store modify -aggregate -aggregate fp_aggr1_A01
-name mccl_ostore1 -mirror-type mirror
```

2. Retirez le miroir du magasin d'objets de l'FabricPool à l'aide du `storage aggregate object-store unmirror` commande.

```
storage aggregate object-store unmirror -aggregate <aggregate name>
-name mccl_ostore1
```

3. Vous pouvez forcer la hiérarchisation pour reprendre le magasin de données primaire après la suppression du magasin de données en miroir à l'aide de `storage aggregate object-store modify` avec le `-force-tiering-on-metrocluster true` option.

L'absence de miroir interfère sur les exigences de réplication d'une configuration MetroCluster.

```
storage aggregate object-store modify -aggregate <aggregate name> -name
mccl_ostore1 -force-tiering-on-metrocluster true
```

4. Créez un magasin d'objets de remplacement à l'aide du `storage aggregate object-store config create` commande.

```
storage aggregate object-store config create -object-store-name
mcc1_ostore3 -cluster clusterA -provider-type SGWS -server <SGWS-server-
1> -container-name <SGWS-bucket-1> -access-key <key> -secret-password
<password> -encrypt <true|false> -provider <provider-type> -is-ssl
-enabled <true|false> ipspace <IPSpace>
```

5. Ajoutez le miroir du magasin d'objets au miroir FabricPool à l'aide de `storage aggregate object-store mirror` commande.

```
storage aggregate object-store mirror -aggregate aggr1 -name
mcc1_ostore3-mc
```

6. Afficher les informations du magasin d'objets à l'aide du `storage aggregate object-store show` commande.

```
storage aggregate object-store show -fields mirror-type,is-mirror-
degraded
```

| aggregate | object-store-name | mirror-type | is-mirror-degraded |
|-----------|-------------------|-------------|--------------------|
| aggr1     | mcc1_ostore1-mc   | primary     | -                  |
|           | mcc1_ostore3-mc   | mirror      | true               |

7. Surveillez l'état de resynchronisation du miroir à l'aide du `storage aggregate object-store show-resync-status` commande.

```
storage aggregate object-store show-resync-status -aggregate aggr1
```

| Aggregate | Primary         | Mirror          | Complete Percentage |
|-----------|-----------------|-----------------|---------------------|
| aggr1     | mcc1_ostore1-mc | mcc1_ostore3-mc | 40%                 |

## Commandes pour la gestion des agrégats avec FabricPool

Vous utilisez le `storage aggregate object-store` Commandes permettant de gérer les magasins d'objets pour FabricPool. Vous utilisez le `storage aggregate` Commandes pour gérer les agrégats pour FabricPool. Vous utilisez le `volume` Commandes permettant de gérer les volumes pour FabricPool.

| Les fonctions que vous recherchez...                                                                                          | Utilisez cette commande :                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Définissez la configuration d'un magasin d'objets afin que ONTAP puisse y accéder                                             | <code>storage aggregate object-store config create</code>                                                                                                        |
| Modifier les attributs de configuration du magasin d'objets                                                                   | <code>storage aggregate object-store config modify</code>                                                                                                        |
| Renommer une configuration de magasin d'objets existante                                                                      | <code>storage aggregate object-store config rename</code>                                                                                                        |
| Supprimer la configuration d'un magasin d'objets                                                                              | <code>storage aggregate object-store config delete</code>                                                                                                        |
| Affiche une liste de configurations de magasin d'objets                                                                       | <code>storage aggregate object-store config show</code>                                                                                                          |
| Reliez un second magasin d'objets à un FabricPool nouveau ou existant en tant que miroir                                      | <code>storage aggregate object-store mirror</code> avec le <code>-aggregate</code> et <code>-name</code> paramètre au niveau de privilège admin                  |
| Supprime un miroir de magasin d'objets d'un miroir FabricPool existant                                                        | <code>storage aggregate object-store unmirror</code> avec le <code>-aggregate</code> et <code>-name</code> paramètre au niveau de privilège admin                |
| Surveillez l'état des synchronisations du miroir FabricPool                                                                   | <code>storage aggregate object-store show-resync-status</code>                                                                                                   |
| Afficher les détails du miroir FabricPool                                                                                     | <code>storage aggregate object-store show</code>                                                                                                                 |
| Promouvoir un miroir de magasin d'objets pour remplacer un magasin d'objets primaire dans une configuration FabricPool miroir | <code>storage aggregate object-store modify</code> avec le <code>-aggregate</code> paramètre au niveau de privilège admin                                        |
| Testez les performances et la latence d'un magasin d'objets sans relier le magasin d'objets à un agrégat                      | <code>storage aggregate object-store profiler start</code> avec le <code>-object-store-name</code> et <code>-node</code> paramètre au niveau de privilège avancé |
| Contrôler l'état du profileur du magasin d'objets                                                                             | <code>storage aggregate object-store profiler show</code> avec le <code>-object-store-name</code> et <code>-node</code> paramètre au niveau de privilège avancé  |
| Abandonner le profileur du magasin d'objets lorsqu'il est en cours d'exécution                                                | <code>storage aggregate object-store profiler abort</code> avec le <code>-object-store-name</code> et <code>-node</code> paramètre au niveau de privilège avancé |



|                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reliez un magasin d'objets à un agrégat pour utiliser FabricPool                                                                                                                                                                                                                                                      | <code>storage aggregate object-store attach</code>                                                                                                                                                                                                                                                                                                                            |
| Reliez un magasin d'objets à un agrégat qui contient un volume FlexGroup pour l'utilisation de FabricPool                                                                                                                                                                                                             | <code>storage aggregate object-store attach</code> avec le <code>allow-flexgroup true</code>                                                                                                                                                                                                                                                                                  |
| Affiche les détails des magasins d'objets associés à des agrégats compatibles avec FabricPool                                                                                                                                                                                                                         | <code>storage aggregate object-store show</code>                                                                                                                                                                                                                                                                                                                              |
| Afficher le seuil de plénitude d'agrégat utilisé par le scan à niveaux                                                                                                                                                                                                                                                | <code>storage aggregate object-store show</code> avec le <code>-fields tiering-fullness-threshold</code> paramètre au niveau de privilège avancé                                                                                                                                                                                                                              |
| Affichage de l'utilisation de l'espace des magasins d'objets rattachés à des agrégats compatibles avec FabricPool                                                                                                                                                                                                     | <code>storage aggregate object-store show-space</code>                                                                                                                                                                                                                                                                                                                        |
| Activez le reporting sur les données inactives sur un agrégat non utilisé pour FabricPool                                                                                                                                                                                                                             | <code>storage aggregate modify</code> avec le <code>-is -inactive-data-reporting-enabled true</code> paramètre                                                                                                                                                                                                                                                                |
| Indique si le reporting de données inactives est activé sur un agrégat                                                                                                                                                                                                                                                | <code>storage aggregate show</code> avec le <code>-fields is-inactive-data-reporting-enabled</code> paramètre                                                                                                                                                                                                                                                                 |
| Afficher des informations sur la quantité de données utilisateur inactives dans un agrégat                                                                                                                                                                                                                            | <code>storage aggregate show-space</code> avec le <code>-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent</code> paramètre                                                                                                                                                                                                              |
| Création d'un volume pour FabricPool, notamment en spécifiant les éléments suivants : <ul style="list-style-type: none"> <li>• La règle de hiérarchisation</li> <li>• La période de refroidissement minimum par niveaux (pour le <code>snapshot-only</code> ou <code>auto</code> règle de hiérarchisation)</li> </ul> | <code>volume create</code> <ul style="list-style-type: none"> <li>• Vous utilisez le <code>-tiering-policy</code> paramètre permettant de spécifier la règle de hiérarchisation.</li> <li>• Vous utilisez le <code>-tiering-minimum-cooling -days</code> paramètre du niveau de privilège avancé pour spécifier la période de refroidissement minimale de tiering.</li> </ul> |
| Modifiez un volume pour FabricPool, y compris en modifiant : <ul style="list-style-type: none"> <li>• La règle de hiérarchisation</li> <li>• La période de refroidissement minimum par niveaux (pour le <code>snapshot-only</code> ou <code>auto</code> règle de hiérarchisation)</li> </ul>                          | <code>volume modify</code> <ul style="list-style-type: none"> <li>• Vous utilisez le <code>-tiering-policy</code> paramètre permettant de spécifier la règle de hiérarchisation.</li> <li>• Vous utilisez le <code>-tiering-minimum-cooling -days</code> paramètre du niveau de privilège avancé pour spécifier la période de refroidissement minimale de tiering.</li> </ul> |

|                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Afficher les informations FabricPool relatives à un volume, notamment les suivantes :</p> <ul style="list-style-type: none"> <li>• La période de refroidissement minimum par niveaux</li> <li>• Quantité de données utilisateur inactives</li> </ul>                                     | <p><code>volume show</code></p> <ul style="list-style-type: none"> <li>• Vous utilisez le <code>-fields tiering-minimum-cooling-days</code> paramètre du niveau de privilège avancé pour afficher la période de refroidissement minimale de tiering.</li> <li>• Vous utilisez le <code>-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent</code> paramètre pour afficher la quantité de données utilisateur inactives.</li> </ul> |
| <p>Déplacer un volume vers ou depuis FabricPool</p>                                                                                                                                                                                                                                         | <p><code>volume move start</code> Vous utilisez le <code>-tiering -policy</code> paramètre facultatif permettant de spécifier la policy de tiering pour le volume.</p>                                                                                                                                                                                                                                                                                                 |
| <p>Modifiez le seuil de récupération de l'espace non référencé (seuil de défragmentation) pour FabricPool</p>                                                                                                                                                                               | <p><code>storage aggregate object-store modify</code> avec le <code>-unreclaimed-space-threshold</code> paramètre au niveau de privilège avancé</p>                                                                                                                                                                                                                                                                                                                    |
| <p>Modifiez le seuil du pourcentage de saturation de l'agrégat avant que le scan de Tiering ne commence le Tiering des données pour FabricPool</p> <p>FabricPool continue à transférer les données inactives vers un Tier cloud jusqu'à ce que le Tier local atteigne 98 % de capacité.</p> | <p><code>storage aggregate object-store modify</code> avec le <code>-tiering-fullness-threshold</code> paramètre au niveau de privilège avancé</p>                                                                                                                                                                                                                                                                                                                     |
| <p>Affiche le seuil de récupération de l'espace non référencé pour FabricPool</p>                                                                                                                                                                                                           | <p><code>storage aggregate object-store show</code> ou <code>storage aggregate object-store show-space</code> commande avec <code>-unreclaimed-space -threshold</code> paramètre au niveau de privilège avancé</p>                                                                                                                                                                                                                                                     |

## Mobilité des données des SVM

### Présentation de la mobilité des données des SVM

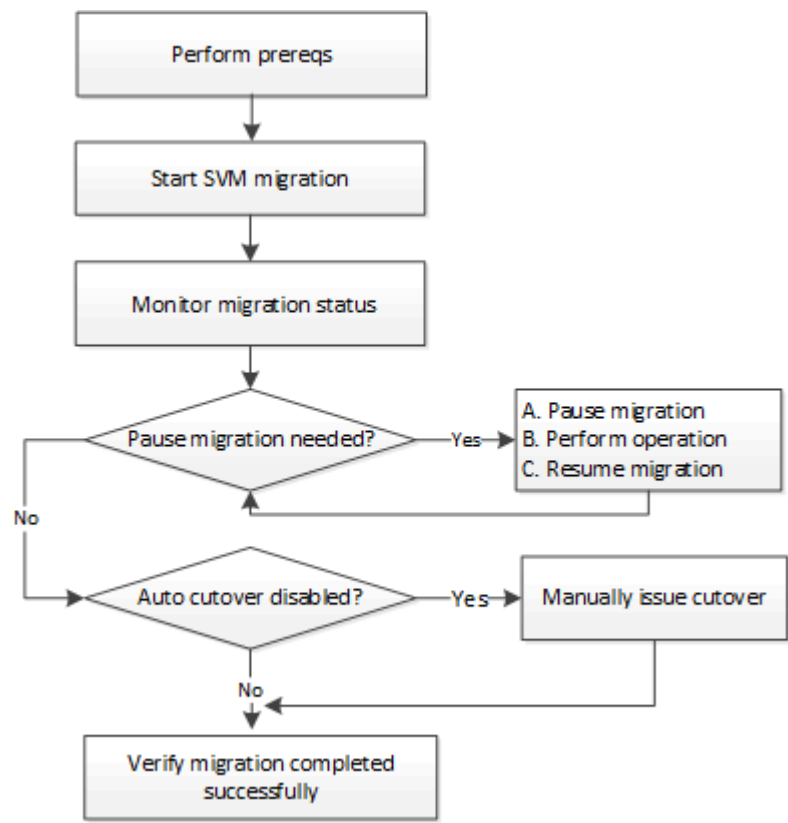
Depuis la version ONTAP 9.10.1, les administrateurs de cluster peuvent déplacer un SVM d'un cluster source vers un cluster de destination sans interruption. Ils peuvent ainsi gérer l'équilibrage de la capacité et de la charge, ou encore procéder à des mises à niveau d'équipement ou à des consolidations de data Center via l'interface de ligne de commande ONTAP.

Cette fonctionnalité de déplacement de SVM sans interruption est prise en charge sur les plateformes AFF dans ONTAP 9.10.1 et 9.11.1. Depuis la version ONTAP 9.12.1, cette fonctionnalité est prise en charge à la fois sur les plateformes FAS et AFF et sur les agrégats hybrides.

Le nom et l'UUID du SVM restent inchangés après la migration, ainsi que le nom de la LIF de données, l'adresse IP et les noms d'objet, comme le nom du volume. L'UUID des objets du SVM sera différent.

Flux de production de la migration SVM

Le schéma représente le workflow standard d'une migration de SVM. Démarrer une migration SVM depuis le cluster destination. Vous pouvez contrôler la migration depuis la source ou la destination. Vous pouvez effectuer une mise en service manuelle ou automatique. La mise en service automatique est effectuée par défaut.



Prise en charge de la plateforme de migration SVM

| Famille de contrôleurs | Versions de ONTAP prises en charge    |
|------------------------|---------------------------------------|
| AFF A-Series           | ONTAP 9.10.1 et versions ultérieures  |
| AFF série C.           | ONTAP 9.12.1 correctif 4 et ultérieur |
| FAS                    | ONTAP 9.12.1 et versions ultérieures  |



Lors de la migration d'un cluster AFF vers un cluster FAS avec des agrégats hybrides, le placement automatique de volumes tente d'effectuer une correspondance d'agrégat similaire à celle-ci. Par exemple, si le cluster source compte 60 volumes, le placement du volume tente de trouver un agrégat AFF sur la destination pour placer les volumes. Lorsqu'il n'y a pas suffisamment d'espace sur les agrégats AFF, les volumes sont placés sur des agrégats avec des disques non Flash.

## Prise en charge de l'évolutivité par version ONTAP

| Version ONTAP | Paires HAUTE DISPONIBILITÉ dans la source et la destination |
|---------------|-------------------------------------------------------------|
| ONTAP 9.14.1  | 12                                                          |
| ONTAP 9.13.1  | 6                                                           |
| ONTAP 9.11.1  | 3                                                           |
| ONTAP 9.10.1  | 1                                                           |

## Exigences de performances de l'infrastructure réseau pour le temps de réponse aller-retour TCP (RTT) entre le cluster source et le cluster de destination

En fonction de la version ONTAP installée sur le cluster, le réseau qui connecte les clusters source et destination doit avoir un temps d'aller-retour maximal, comme indiqué :

| Version ONTAP                        | RTT maximum |
|--------------------------------------|-------------|
| ONTAP 9.12.1 et versions ultérieures | 10 ms.      |
| ONTAP 9.11.1 et versions antérieures | 2 ms.       |

## Nombre maximal de volumes pris en charge par SVM

| Source | Destination | ONTAP 9.14.1 | ONTAP 9.13.1 | ONTAP 9.12.1 | ONTAP 9.11.1 et versions antérieures |
|--------|-------------|--------------|--------------|--------------|--------------------------------------|
| AFF    | AFF         | 400          | 200          | 100          | 100                                  |
| FAS    | FAS         | 80           | 80           | 80           | S/O                                  |
| FAS    | AFF         | 80           | 80           | 80           | S/O                                  |
| AFF    | FAS         | 80           | 80           | 80           | S/O                                  |

## Prérequis

Avant de lancer une migration d'un SVM, vous devez réunir les conditions préalables suivantes :

- Vous devez être un administrateur de cluster.
- ["Les clusters source et destination doivent être mis en cluster par groupes"](#).
- SnapMirror doit être synchrone sur les clusters source et destination ["licence installée"](#). Cette licence est incluse avec ["ONTAP One"](#).
- Tous les nœuds du cluster source doivent exécuter ONTAP 9.10.1 ou une version ultérieure. Pour connaître la prise en charge spécifique du contrôleur de baie ONTAP, reportez-vous à la section ["Hardware Universe"](#).
- Tous les nœuds du cluster source doivent exécuter la même version de ONTAP.
- Tous les nœuds du cluster destination doivent exécuter la même version de ONTAP.
- Le cluster de destination doit être au même niveau ou pas plus de deux versions de cluster effectif (ECV) majeures plus récentes que le cluster source.

- Les clusters source et destination doivent prendre en charge le même sous-réseau IP pour l'accès aux LIF de données.
- La SVM source doit contenir moins de [nombre maximal de volumes de données pris en charge pour la version](#).
- Un espace suffisant pour le placement des volumes doit être disponible sur la destination
- Onboard Key Manager doit être configuré sur le site de destination si le SVM source possède des volumes chiffrés

## Et des meilleures pratiques

Lors d'une migration d'un SVM, il est recommandé de laisser une marge de 30 % sur le cluster source et le cluster de destination pour permettre l'exécution de la charge de travail du processeur.

## Opérations SVM

Vous devez vérifier si les opérations peuvent entrer en conflit avec une migration SVM :

- Aucune opération de basculement n'est en cours
- WAFLIRON ne peut pas être en cours d'exécution
- L'empreinte digitale n'est pas en cours
- Le déplacement de volumes, le réhébergement, le clonage, la création, la conversion ou l'analytique ne sont pas en cours d'exécution


## Fonctionnalités prises en charge et non prises en charge


Le tableau présente les fonctionnalités ONTAP prises en charge par la mobilité des données des SVM et les versions ONTAP dans lesquelles la prise en charge est disponible.

Pour plus d'informations sur l'interopérabilité de la version ONTAP entre une source et une destination dans une migration SVM, voir ["Compatibilité des versions ONTAP pour les relations SnapMirror"](#).

| Fonction                                   | Version d'abord prise en charge | Commentaires                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protection autonome contre les ransomwares | ONTAP 9.12.1                    |                                                                                                                                                                                                                                                                                                                   |
| Cloud Volumes ONTAP                        | Non pris en charge              |                                                                                                                                                                                                                                                                                                                   |
| Gestionnaire de clés externe               | ONTAP 9.11.1                    |                                                                                                                                                                                                                                                                                                                   |
| FabricPool                                 | ONTAP 9.11.1                    | <p>La migration SVM est prise en charge avec des volumes sur FabricPools pour les plateformes suivantes :</p> <ul style="list-style-type: none"> <li>• Plate-forme Azure NetApp Files. Toutes les règles de hiérarchisation sont prises en charge (copie Snapshot uniquement, auto, toutes et aucune).</li> </ul> |

|                                                                                                                      |                    |                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Relation de type « fanout » (la source de migration possède un volume source SnapMirror avec plusieurs destinations) | ONTAP 9.11.1       |                                                                                                                                                                                                                                                                                                                                                                              |
| SAN FC                                                                                                               | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                              |
| Flash Pool                                                                                                           | ONTAP 9.12.1       |                                                                                                                                                                                                                                                                                                                                                                              |
| Volumes FlexCache                                                                                                    | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                              |
| FlexGroup                                                                                                            | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                              |
| Stratégies IPsec                                                                                                     | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                              |
| LIF IPv6                                                                                                             | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                              |
| San iSCSI                                                                                                            | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                              |
| Réplication de la planification des tâches                                                                           | ONTAP 9.11.1       | Dans ONTAP 9.10.1, les planifications de tâches ne sont pas répliquées au cours de la migration et doivent être créées manuellement sur le volume de destination. Depuis ONTAP 9.11.1, les planifications des tâches utilisées par la source sont automatiquement répliquées au cours de la migration.                                                                       |
| Miroirs de partage de charge                                                                                         | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                              |
| SVM MetroCluster                                                                                                     | Non pris en charge | Bien que la migration des SVM ne prenne pas en charge la migration des SVM MetroCluster, vous pouvez utiliser la réplication asynchrone de SnapMirror vers <a href="#">"Migrer un SVM dans une configuration MetroCluster"</a> . Sachez que le processus décrit pour la migration d'un SVM dans une configuration MetroCluster est <i>not</i> une méthode sans perturbation. |
| Chiffrement d'agrégat NetApp (NAE)                                                                                   | Non pris en charge | La migration n'est pas prise en charge à partir d'une source non chiffrée vers une destination chiffrée.                                                                                                                                                                                                                                                                     |
| Configurations NDMP                                                                                                  | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                              |
| NVE (NetApp Volume Encryption)                                                                                       | ONTAP 9.10.1       |                                                                                                                                                                                                                                                                                                                                                                              |

|                                                                                                                   |                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Journaux d'audit NFS et SMB                                                                                       | ONTAP 9.13.1       |  <p>La redirection du journal des audits n'est disponible qu'en mode cloud. Pour la migration SVM sur site avec audit activé, vous devez désactiver l'audit sur le SVM source, puis effectuer la migration.</p> <p>Avant la migration des SVM :</p> <ul style="list-style-type: none"> <li>• "La redirection du journal d'audit doit être activée sur le cluster de destination".</li> <li>• "Le chemin de destination du journal d'audit depuis la SVM source doit être créé sur le cluster destination".</li> </ul> |
| NFS v3, NFS v4.1 et NFS v4.2                                                                                      | ONTAP 9.10.1       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| NFS v4.0                                                                                                          | ONTAP 9.12.1       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| NFSv4.1 avec pNFS                                                                                                 | ONTAP 9.14.1       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| NVMe over Fabric                                                                                                  | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Gestionnaire de clés intégré OKM (Onboard Key Manager) avec le mode critères communs activé sur le cluster source | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Qtrees                                                                                                            | ONTAP 9.14.1       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Quotas                                                                                                            | ONTAP 9.14.1       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| S3                                                                                                                | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Protocole SMB                                                                                                     | ONTAP 9.12.1       | Les migrations SMB sont perturbatrices et qui nécessitent une mise à jour du client après la migration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Relations cloud SnapMirror                                                                                        | ONTAP 9.12.1       | À partir de ONTAP 9.12.1, lorsque vous migrez un SVM avec des relations cloud SnapMirror, le cluster de destination doit être " <a href="#">Licence cloud SnapMirror</a> " installé et la capacité disponible doit être suffisante pour prendre en charge le déplacement de la capacité des volumes mis en miroir vers le cloud.                                                                                                                                                                                                                                                                       |
| Destination asynchrone SnapMirror                                                                                 | ONTAP 9.12.1       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                                                     |                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source asynchrone SnapMirror                        | ONTAP 9.11.1       | <ul style="list-style-type: none"> <li>• Les transferts peuvent se poursuivre normalement sur les relations FlexVol SnapMirror pendant la majeure partie de la migration.</li> <li>• Tout transfert en cours est annulé pendant la mise en service et les nouveaux transferts échouent pendant la mise en service et ils ne peuvent pas être redémarrés tant que la migration n'est pas terminée.</li> <li>• Les transferts planifiés annulés ou manqués pendant la migration ne sont pas automatiquement démarrés une fois la migration terminée.</li> </ul> <div>  <p>Lors de la migration d'une source SnapMirror, ONTAP n'empêche pas la suppression du volume après la migration tant que la mise à jour SnapMirror n'a pas lieu. Cela se produit car les informations relatives à SnapMirror pour les volumes source SnapMirror migrés sont disponibles uniquement une fois la migration terminée et après la première mise à jour.</p> </div> |
| Paramètres SMTape                                   | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SnapLock                                            | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Synchronisation active SnapMirror                   | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Relations entre les pairs SVM SnapMirror            | ONTAP 9.12.1       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Reprise d'activité de SVM SnapMirror                | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SnapMirror synchrone                                | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| La copie Snapshot                                   | ONTAP 9.10.1       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Verrouillage inviolable des copies Snapshot         | ONTAP 9.14.1       | Le verrouillage inviolable des copies Snapshot n'est pas équivalent à SnapLock. SnapLock reste non pris en charge.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| LIF/BGP IP virtuelles                               | Non pris en charge |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Virtual Storage Console 7.0 et versions ultérieures | Non pris en charge | VSC fait partie du <a href="#">"Appliance virtuelle ONTAP Tools pour VMware vSphere"</a> À partir de VSC 7.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



|                   |                    |  |
|-------------------|--------------------|--|
| Clones de volumes | Non pris en charge |  |
| VStorage          | Non pris en charge |  |

## Opérations prises en charge pendant la migration

Le tableau suivant indique les opérations de volume prises en charge au sein du SVM de migration en fonction de l'état de migration :

| Opération de volume                                             | État de la migration SVM |          |                    |
|-----------------------------------------------------------------|--------------------------|----------|--------------------|
|                                                                 | En cours                 | Pause    | Mise en service    |
| Création                                                        | Non autorisé             | Autorisé | Non pris en charge |
| Supprimer                                                       | Non autorisé             | Autorisé | Non pris en charge |
| Désactivation de l'analyse du système de fichiers               | Autorisé                 | Autorisé | Non pris en charge |
| Activation de l'analyse du système de fichiers                  | Non autorisé             | Autorisé | Non pris en charge |
| Modifier                                                        | Autorisé                 | Autorisé | Non pris en charge |
| Hors ligne/en ligne                                             | Non autorisé             | Autorisé | Non pris en charge |
| Déplacer/réhéberger                                             | Non autorisé             | Autorisé | Non pris en charge |
| Création/modification qtree                                     | Non autorisé             | Autorisé | Non pris en charge |
| Création/modification de quotas                                 | Non autorisé             | Autorisé | Non pris en charge |
| Renommer                                                        | Non autorisé             | Autorisé | Non pris en charge |
| Redimensionner                                                  | Autorisé                 | Autorisé | Non pris en charge |
| Limiter                                                         | Non autorisé             | Autorisé | Non pris en charge |
| Les attributs de copie Snapshot sont modifiés                   | Autorisé                 | Autorisé | Non pris en charge |
| Modification de la suppression automatique de la copie Snapshot | Autorisé                 | Autorisé | Non pris en charge |
| Création d'une copie Snapshot                                   | Autorisé                 | Autorisé | Non pris en charge |
| Suppression de la copie Snapshot                                | Autorisé                 | Autorisé | Non pris en charge |
| Restaurer le fichier à partir de la copie Snapshot              | Autorisé                 | Autorisé | Non pris en charge |

## Migrer un SVM

Une fois la migration SVM terminée, les clients sont automatiquement mis en service sur le cluster de destination et le SVM inutile est retiré du cluster source. La mise en service automatique et le nettoyage automatique des sources sont activés par défaut. Si nécessaire, vous pouvez désactiver la mise en service automatique des clients pour

suspendre la migration avant la mise en service et désactiver le nettoyage automatique des SVM source.

- Vous pouvez utiliser le `-auto-cutover false` option permettant de suspendre la migration lors de la mise en service client automatique, puis d'effectuer la mise en service manuellement ultérieurement.

#### [Mise en service manuelle des clients après la migration de SVM](#)

- Vous pouvez utiliser le privilège d'avance `-auto-source-cleanup false` Option permettant de désactiver la suppression du SVM source après la mise en service, puis de déclencher le nettoyage source manuellement ultérieurement, après la mise en service.

#### [Supprimer manuellement le SVM source après la mise en service](#)

### **Migrer un SVM avec la mise en service automatique activée**

Par défaut, les clients sont automatiquement mis en service sur le cluster de destination une fois la migration terminée et le SVM inutile est retiré du cluster source.

#### **Étapes**

1. Depuis le cluster destination, exécutez les contrôles préalables de migration :

```
dest_cluster> vservers migrate start -vservers SVM_name -source-cluster
cluster_name -check-only true
```

2. Depuis le cluster destination, démarrer la migration SVM :

```
dest_cluster> vservers migrate start -vservers SVM_name -source-cluster
cluster_name
```

3. Vérifier l'état de la migration :

```
dest_cluster> vservers migrate show
```

L'état affiche « migrate-Complete » lorsque la migration de SVM est terminée.

### **Migrer un SVM avec la mise en service client automatique désactivée**

Vous pouvez utiliser l'option `-auto-mise en service false` pour suspendre la migration lors de la mise en service automatique du client, puis effectuer la mise en service manuellement ultérieurement. Voir [Mise en service manuelle des clients après la migration de SVM](#).

#### **Étapes**

1. Depuis le cluster destination, exécutez les contrôles préalables de migration :

```
dest_cluster> vservers migrate start -vservers SVM_name -source-cluster
cluster_name -check-only true
```

2. Depuis le cluster destination, démarrer la migration SVM :

```
dest_cluster> vservers migrate start -vservers SVM_name -source-cluster
cluster_name -auto-cutover false
```

### 3. Vérifier l'état de la migration :

```
dest_cluster> vserver migrate show
```

L'état affiche « prêt à la mise en service » lorsque la migration des SVM termine les transferts de données asynchrones et est prête pour la mise en service.

## Migrer un SVM avec le nettoyage source désactivé

Vous pouvez utiliser l'option faux privilèges `-auto-source-cleanup` pour désactiver la suppression du SVM source après la mise en service, puis déclencher le nettoyage source manuellement après la mise en service. Voir [Supprimer manuellement la SVM source](#).

### Étapes

1. Depuis le cluster destination, exécutez les contrôles préalables de migration :

```
dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster
cluster_name -check-only true
```

2. Depuis le cluster destination, démarrer la migration SVM :

```
dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster
cluster_name -auto-source-cleanup false
```

3. Vérifier l'état de la migration :

```
dest_cluster*> vserver migrate show
```

L'état affiche `Ready-for-source-cleanup` lorsque la mise en service de la migration des SVM est terminée, et est prêt à supprimer le SVM sur le cluster source.

## Surveiller la migration de volume

Outre le contrôle de la migration globale du SVM avec `vserver migrate show` Commande, vous pouvez surveiller l'état de migration des volumes que le SVM contient.

### Étapes

1. Vérifier l'état de la migration du volume :

```
dest_clust> vserver migrate show-volume
```

## Mettre en pause et reprendre la migration du SVM

Vous pouvez interrompre une migration SVM avant le démarrage de la mise en service. Vous pouvez interrompre une migration SVM à l'aide de `vserver migrate pause` commande.

### Interrompre la migration

Vous pouvez interrompre une migration SVM avant le démarrage de la mise en service client à l'aide de `vserver migrate pause` commande.

Certaines modifications de configuration sont restreintes lorsqu'une opération de migration est en cours ; cependant, à partir de ONTAP 9.12.1, vous pouvez interrompre une migration pour corriger certaines configurations restreintes et pour certains États défaillants afin de résoudre les problèmes de configuration susceptibles d'avoir causé la défaillance. Voici quelques-uns des États défaillants que vous pouvez corriger lorsque vous interrompez la migration des SVM :

- échec-configuration-configuration
- échec de la migration

### Étapes

1. Depuis le cluster destination, suspendre la migration :

```
dest_cluster> vserver migrate pause -vserver <vserver name>
```

### Reprendre les migrations

Lorsque vous êtes prêt à reprendre une migration SVM en pause ou en cas d'échec d'une migration SVM, vous pouvez utiliser `vserver migrate resume` commande.

### Étape

1. Reprise de la migration SVM :

```
dest_cluster> vserver migrate resume
```

2. Vérifier que la migration SVM a repris et contrôler la progression :

```
dest_cluster> vserver migrate show
```

### Annuler une migration SVM

Si vous devez annuler une migration SVM avant sa fin, vous pouvez utiliser le `vserver migrate abort` commande. Vous pouvez annuler une migration SVM uniquement lorsque l'opération est à l'état mis en pause ou échoué. Vous ne pouvez pas annuler une migration SVM lorsque l'état est « mise en service démarrée » ou lorsque la mise en service est terminée. Vous ne pouvez pas utiliser `abort` Option lorsqu'une migration SVM est en cours.

### Étapes

1. Vérifier l'état de la migration :

```
dest_cluster> vserver migrate show -vserver <vserver name>
```

2. Annuler la migration :

```
dest_cluster> vserver migrate abort -vserver <vserver name>
```

3. Vérifier la progression de l'opération d'annulation :

```
dest_cluster> vserver migrate show
```

L'état de la migration indique l'abandon de la migration lorsque l'opération d'annulation est en cours. Lorsque l'opération d'annulation est terminée, l'état de la migration n'indique rien.

## Couper manuellement les clients

Par défaut, la mise en service du client vers le cluster de destination est effectuée automatiquement une fois la migration du SVM arrivée à l'état « prêt pour la mise en service ». Si vous désactivez la mise en service client automatique, vous devez effectuer la mise en service client manuellement.

### Étapes

1. Exécuter manuellement la mise en service des clients :

```
dest_cluster> vserver migrate cutover -vserver <vserver name>
```

2. Vérifier l'état de l'opération de mise en service :

```
dest_cluster> vserver migrate show
```

## Supprimer manuellement la SVM source après la mise en service du client

Si vous avez effectué la migration SVM avec le nettoyage source désactivé, vous pouvez supprimer le SVM source manuellement une fois la mise en service client terminée.

### Étapes

1. Vérifiez qu'ils sont prêts pour le nettoyage de la source :

```
dest_cluster> vserver migrate show
```

2. Nettoyez la source :

```
dest_cluster> vserver migrate source-cleanup -vserver <vserver_name>
```

# Gestion des paires HAUTE DISPONIBILITÉ

## Présentation de la gestion des paires HAUTE DISPONIBILITÉ

Les nœuds de cluster sont configurés en paires haute disponibilité pour la tolérance aux pannes et la continuité de l'activité. Si un nœud tombe en panne ou si vous devez mettre un nœud hors service pour des opérations de maintenance de routine, son partenaire peut prendre le contrôle de son stockage tout en continuant de transmettre les données de celui-ci. Le partenaire fournit du stockage de retour lorsque le nœud est revenu en ligne.

La configuration de contrôleurs de paires haute disponibilité consiste à faire correspondre une paire de contrôleurs de stockage FAS/AFF (nœud local et nœud partenaire). Chacun de ces nœuds est connecté aux tiroirs disques de l'autre. Lorsqu'un nœud d'une paire HA rencontre une erreur et arrête le traitement des données, son partenaire détecte l'état en panne du partenaire et prend en charge l'ensemble du traitement de

données à partir de ce contrôleur.

*Takeover* est le processus où un nœud assume le contrôle du stockage de son partenaire.

*Giveback* est le processus dans lequel le stockage est retourné au partenaire.

Par défaut, les prises de contrôle se produisent automatiquement dans l'une des situations suivantes :

- Une défaillance logicielle ou système se produit sur un nœud qui entraîne un incident de type « panic ». Les contrôleurs de paire haute disponibilité basculent automatiquement vers le nœud partenaire. Une fois que le partenaire a récupéré son incident et démarré, le nœud exécute automatiquement un retour et fonctionne normalement.
- Une panne système se produit sur un nœud et ce dernier ne peut pas redémarrer. Par exemple, lorsqu'un nœud tombe en panne en raison d'une panne de courant, les contrôleurs de paire haute disponibilité basculent automatiquement vers le nœud partenaire et font passer les données du contrôleur de stockage restant.



Si le stockage d'un nœud perd également de l'alimentation en même temps, un basculement standard n'est pas possible.

- Les messages de pulsation ne sont pas reçus du partenaire du nœud. Cela peut se produire si le partenaire a subi une défaillance matérielle ou logicielle (par exemple, une défaillance d'interconnexion) qui n'a pas produit de panique, mais qui l'a toujours empêchée de fonctionner correctement.
- Vous arrêtez l'un des nœuds sans utiliser le `-f` ou `-inhibit-takeover true` paramètre.



Dans un cluster à deux nœuds avec haute disponibilité de cluster activée, arrêt ou redémarrage d'un nœud à l'aide du système `-inhibit-takeover true` Provoque l'arrêt du service des données sur les deux nœuds, sauf si vous désactivez d'abord le cluster HA, puis affectez epsilon au nœud que vous souhaitez rester en ligne.

- Vous redémarrez l'un des nœuds sans utiliser le `-inhibit-takeover true` paramètre. (Le `-onboot` paramètre du `storage failover` la commande est activée par défaut.)
- Le périphérique de gestion à distance (processeur de service) détecte une défaillance du nœud partenaire. Ceci n'est pas applicable si vous désactivez le basculement assisté par matériel.

Vous pouvez également lancer des prises de contrôle manuellement avec le `storage failover takeover` commande.

## Amélioration de la résilience du cluster et des diagnostics

Depuis ONTAP 9.9.1, les ajouts de résilience et de diagnostic suivants améliorent le fonctionnement du cluster :

- **Surveillance et évitement des ports** : dans les configurations de cluster sans commutateur à deux nœuds, le système évite les ports qui subissent une perte totale de paquets (perte de connectivité). Dans ONTAP 9.8.1 et les versions antérieures, cette fonctionnalité n'était disponible que dans les configurations commutées.
- **Basculement automatique de nœud** : si un nœud ne peut pas transmettre de données sur son réseau de cluster, ce nœud ne doit pas posséder de disques. Au lieu de cela, son partenaire de haute disponibilité devrait prendre le relais, si ce dernier est en bonne santé.
- **Commandes pour analyser les problèmes de connectivité** : utilisez la commande suivante pour afficher

les chemins de grappe qui subissent une perte de paquets : `network interface check cluster-connectivity show`

## Fonctionnement du basculement assisté par matériel

Activée par défaut, la fonctionnalité hardware-Assisted Takeover permet d'accélérer le processus de Takeover à l'aide d'un périphérique de gestion à distance (Service Processor) d'un nœud.

Lorsque le périphérique de gestion distant détecte une défaillance, il lance rapidement le basculement au lieu d'attendre que ONTAP reconnaisse que la pulsation du partenaire s'est arrêtée. En cas de défaillance sans cette fonctionnalité activée, le partenaire attend jusqu'à ce qu'il remarque que le nœud ne fournit plus de signal de détection, confirme la perte de signal de détection, puis lance le basculement.

La fonctionnalité hardware-Assisted Takeover utilise le processus suivant pour éviter cette attente :

1. Le périphérique de gestion à distance surveille le système local pour détecter certains types de défaillances.
2. Si une défaillance est détectée, le périphérique de gestion à distance envoie immédiatement une alerte au nœud partenaire.
3. Le partenaire commence le basculement dès réception de l'alerte.

### Événements système qui déclenchent un basculement assisté par matériel

Le nœud partenaire peut générer un basculement en fonction du type d'alerte qu'il reçoit du périphérique de gestion à distance (Service Processor).

| Alerte              | Prise de contrôle lancée à réception ? | Description                                                                                                                                                                                                                                                                                              |
|---------------------|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| redémarrage anormal | Non                                    | Un redémarrage anormal du nœud s'est produit.                                                                                                                                                                                                                                                            |
| l2_watchdog_reset   | Oui.                                   | Le matériel de surveillance du système a détecté une réinitialisation L2.<br>Le périphérique de gestion à distance a détecté un manque de réponse de la CPU du système et réinitialisé le système.                                                                                                       |
| perte_de_pulsation  | Non                                    | Le périphérique de gestion à distance ne reçoit plus le message de pulsation du nœud.<br>Cette alerte ne fait pas référence aux messages de signal de détection entre les nœuds de la paire HA ; il fait référence au signal de détection entre le nœud et son périphérique de gestion à distance local. |
| message_périodique  | Non                                    | Un message périodique est envoyé lors d'une opération normale de basculement assisté par matériel.                                                                                                                                                                                                       |
| power_cycle_via_sp  | Oui.                                   | Le périphérique de gestion à distance a mis le système hors tension et sous tension.                                                                                                                                                                                                                     |

|                    |      |                                                                                                                                                                                                                                                                                 |
|--------------------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| perte_de_puissance | Oui. | Une panne d'alimentation s'est produite sur le nœud. Le périphérique de gestion à distance est doté d'une alimentation qui maintient l'alimentation pendant une courte période après une coupure de courant, ce qui lui permet de signaler la perte de puissance au partenaire. |
| power_off_via_sp   | Oui. | Le périphérique de gestion à distance a mis hors tension le système.                                                                                                                                                                                                            |
| reset_via_sp       | Oui. | Le périphérique de gestion à distance réinitialise le système.                                                                                                                                                                                                                  |
| testez             | Non  | Un message de test est envoyé pour vérifier une opération de basculement assistée par matériel.                                                                                                                                                                                 |

### Informations associées

["Basculement assisté par matériel \(HWAssist\) - Guide de résolution"](#)

## Fonctionnement du Takeover et Giveback automatique

Les opérations de Takeover automatique et giveback peuvent fonctionner ensemble pour réduire et éviter les pannes client.

Par défaut, si un nœud de la paire haute disponibilité fonctionne de façon incohérente, redémarre ou s'arrête, le nœud partenaire prend automatiquement le relais, puis renvoie le stockage lors du redémarrage du nœud affecté. La paire HA reprend son état de fonctionnement normal.

Des prises de contrôle automatiques peuvent également se produire si l'un des nœuds ne répond plus.

Le rétablissement automatique est effectué par défaut. Si vous préférez contrôler l'impact du rétablissement sur les clients, vous pouvez désactiver le rétablissement automatique et utiliser le `storage failover modify -auto-giveback false -node <node>` commande. Avant d'effectuer un retour automatique (quel que soit l'origine de l'opération), le nœud partenaire attend une durée fixe, telle que contrôlée par le `-delay- seconds` paramètre du `storage failover modify` commande. Le délai par défaut est de 600 secondes. Avec le report du rétablissement, ce processus provoque deux brèves pannes : une lors du basculement et une lors du rétablissement.

Ce processus permet d'éviter une seule panne prolongée qui inclut le temps nécessaire pour :

- Opération de basculement
- Le nœud pris-le pour démarrer jusqu'à l'instant où il est prêt pour le rétablissement
- L'opération de rétablissement

Si le rétablissement automatique échoue pour l'un des agrégats non racines, le système effectue automatiquement deux tentatives supplémentaires pour terminer le rétablissement.



Lors du processus de basculement, le processus de rétablissement automatique démarre avant que le nœud partenaire soit prêt pour le rétablissement. Lorsque la limite de temps du processus de rétablissement automatique expire et que le nœud partenaire n'est pas encore prêt, le compteur redémarre. Par conséquent, le temps entre le nœud partenaire et le rétablissement proprement dit peut être plus court que le délai de rétablissement automatique.



## Ce qui se passe pendant le basculement

Lorsqu'un nœud prend le relais, il continue à transmettre et à mettre à jour les données dans les agrégats et les volumes du partenaire.

Les étapes suivantes se produisent durant le processus de basculement :

1. Si le basculement négocié est initié par l'utilisateur, les données agrégées sont déplacées du nœud partenaire vers le nœud qui effectue le basculement. Une brève panne se produit en tant que le propriétaire actuel de chaque agrégat (à l'exception de l'agrégat root) est remplacé par le nœud Takeover. Cette panne est plus qu'un problème survient lors d'un basculement sans déplacement d'agrégats.



Un takeover négocié pendant la panique ne peut pas se produire en cas de panique. Le basculement peut résulter d'un échec non associé à un problème de panique. Une défaillance survient lorsque la communication est perdue entre un nœud et son partenaire, également appelée perte de pulsation. Si un basculement a lieu à cause d'une défaillance, la panne peut être plus longue, car le nœud partenaire a besoin de temps pour détecter la perte d'impulsion.

- Vous pouvez contrôler la progression à l'aide de l' `storage failover show-takeover` commande.
- Vous pouvez éviter le transfert d'agrégat pendant cette instance de basculement en utilisant le `-bypass-optimization` paramètre avec le `storage failover takeover` commande.

Les agrégats sont transférés en série lors des opérations de basculement planifiées afin de réduire l'interruption des activités du client. Si le transfert d'agrégats est contourné, une panne client plus longue se produit lors d'événements de basculement planifiés.

2. Si le basculement initié par l'utilisateur est un basculement négocié, le nœud cible s'arrête normalement, suivi du basculement de l'agrégat racine du nœud cible et des agrégats qui n'ont pas été déplacés au cours de la première étape.
3. Les LIF de données (interfaces logiques) migrent du nœud cible vers le nœud Takeover, ou vers tout autre nœud du cluster basé sur les règles de failover LIF. Vous pouvez éviter la migration de LIF à l'aide de `-skip-lif-migration` paramètre avec le `storage failover takeover` commande. Dans le cas d'un basculement initié par l'utilisateur, les LIF de données sont migrées avant le début du basculement du stockage. En cas de panique ou de défaillance, selon votre configuration, les LIF de données peuvent être migrées avec le stockage ou une fois le basculement terminé.
4. Les sessions SMB existantes sont déconnectées lors du basculement.



En raison de la nature du protocole SMB, toutes les sessions SMB sont interrompues (à l'exception des sessions SMB 3.0 connectées à des partages avec la propriété Continuous Availability set). Les sessions SMB 1.0 et SMB 2.x ne peuvent pas reconnecter les descripteurs de fichier ouvert après un événement de basculement. Le basculement est donc disruptif et pourrait entraîner une perte de données.

5. Les sessions SMB 3.0 établies pour des partages avec la propriété Continuous Availability activée peuvent se reconnecter aux partages déconnectés après un événement de basculement. Si votre site utilise des connexions SMB 3.0 vers Microsoft Hyper-V et que la propriété Continuous Availability est activée sur les partages associés, les prises de contrôle ne sont pas perturbatrices pour ces sessions.

## Que se passe-t-il si un nœud exécute un basculement de façon incohérente

Si le nœud exécutant le basculement fonctionne de façon incohérente dans les 60 secondes suivant le

lancement du basculement, les événements suivants se produisent :

- Le nœud qui s'est paniqué redémarre.
- Après le redémarrage, le nœud effectue des opérations de reprise automatique et n'est plus en mode basculement.
- Le basculement est désactivé.
- Si le nœud possède toujours certains agrégats du partenaire, après activation du basculement de stockage, retournez ces agrégats au partenaire à l'aide du `storage failover giveback` commande.

### Ce qui se passe pendant le retour

Le nœud local revient à la propriété sur le nœud partenaire lorsque les problèmes sont résolus, lors du démarrage du nœud partenaire ou lors du lancement du retour.

Le processus suivant a lieu dans une opération de rétablissement normale. Dans cette discussion, le nœud A a pris le relais du nœud B. Tout problème sur le nœud B a été résolu et il est prêt à reprendre le service des données.

1. Tout problème sur le nœud B est résolu et le message suivant s'affiche : `Waiting for giveback`
2. Le rétablissement est initié par le `storage failover giveback` commande ou par rétablissement automatique si le système est configuré pour celui-ci. Cette opération démarre le processus de retour à la propriété des agrégats et volumes du nœud B, à partir du nœud A, vers le nœud B.
3. Le nœud A renvoie en premier le contrôle de l'agrégat racine.
4. Le nœud B termine le processus de démarrage jusqu'à son état de fonctionnement normal.
5. Dès que le nœud B atteint le point de démarrage où il peut accepter les agrégats non racines, le nœud A renvoie la propriété des autres agrégats, un par un, jusqu'à ce que le rétablissement soit terminé. Vous pouvez surveiller la progression du rétablissement à l'aide de `storage failover show-giveback` commande.



Le `storage failover show-giveback` la commande ne renvoie pas (ni n'est destinée) affiche les informations relatives à toutes les opérations qui se produisent durant l'opération de rétablissement du basculement du stockage. Vous pouvez utiliser le `storage failover show` commande permettant d'afficher des informations supplémentaires sur l'état de basculement actuel du nœud, par exemple si ce dernier est entièrement fonctionnel, si un basculement est possible et si un retour est terminé.

Les E/S sont reprises pour chaque agrégat après le rétablissement de cet agrégat, ce qui réduit la fenêtre de l'interruption globale.

### LA politique DE HAUTE DISPONIBILITÉ et ses effets sur le basculement et le rétablissement

ONTAP attribue automatiquement une stratégie de haute disponibilité de CFO (basculement du contrôleur) et de SFO (basculement du stockage) à un agrégat. Cette règle détermine la façon dont des opérations de basculement du stockage se déroulent pour l'agrégat et ses volumes.

Les deux options, CFO et SFO, déterminent la séquence de contrôle de l'agrégat que ONTAP utilise lors des opérations de basculement et de rétablissement du stockage.

Bien que les termes CFO et SFO sont parfois utilisés de manière informelle pour les opérations de basculement de stockage (basculement et rétablissement), ils représentent réellement la politique de haute

disponibilité attribuée aux agrégats. Par exemple, les termes agrégat SFO ou agrégat CFO font simplement référence à l'affectation des règles haute disponibilité de l'agrégat.

Les règles HAUTE DISPONIBILITÉ affectent les opérations de basculement et de rétablissement :

- Les agrégats créés sur les systèmes ONTAP (à l'exception de l'agrégat racine qui contient le volume racine) disposent d'une règle de haute disponibilité SFO. Le basculement initié manuellement est optimisé pour les performances en déplaçant des agrégats SFO (non racine) en série vers le partenaire avant le basculement. Lors du processus de rétablissement, les agrégats sont remis en série après le démarrage du système de basculement et les applications de gestion sont en ligne, ce qui permet au nœud de recevoir ses agrégats.
- Étant donné que les opérations de transfert d'agrégats impliquent la réaffectation de la propriété des disques dans l'agrégat et le transfert du contrôle d'un nœud vers son partenaire, seuls les agrégats disposant d'une politique de haute disponibilité du SFO sont éligibles pour le transfert de ces agrégats.
- L'agrégat root dispose toujours d'une politique de CFO de haute disponibilité et est redonné au début de l'opération de rétablissement. Ceci est nécessaire pour permettre au système de reprise de démarrer. Tous les autres agrégats sont remis en série une fois le processus de démarrage terminé et les applications de gestion sont en ligne, ce qui permet au nœud de recevoir ses agrégats.



La modification de la politique HA d'un agrégat de SFO vers le CFO est une opération en mode maintenance. Ne modifiez pas ce paramètre à moins d'être invité par un représentant du service clientèle.

### Comment les mises à jour d'arrière-plan affectent le basculement et le rétablissement

Les mises à jour en arrière-plan du firmware du disque affectent les opérations de basculement, de rétablissement et de transfert d'agrégats HA différemment, selon le mode de lancement de ces opérations.

La liste ci-dessous décrit la manière dont les mises à jour du firmware des disques en arrière-plan affectent le basculement, le rétablissement et le transfert d'agrégats :

- Si la mise à jour du firmware d'un disque en arrière-plan se produit sur un des nœuds, les opérations de basculement lancées manuellement sont retardées jusqu'à ce que la mise à jour du firmware du disque soit terminée sur ce disque. Si la mise à jour du firmware du disque en arrière-plan prend plus de 120 secondes, les opérations de basculement sont abandonnées et doivent être redémarrées manuellement après la fin de la mise à jour du firmware des disques. Si le basculement a été initié par le `-bypass -optimization` paramètre du `storage failover takeover` commande définie sur `true`, la mise à jour du micrologiciel du disque en arrière-plan effectuée sur le nœud de destination n'affecte pas le basculement.
- Si une mise à jour du firmware du disque en arrière-plan est effectuée sur un disque du nœud source (ou basculement), et l'acquisition a été lancée manuellement avec le `-options` paramètre du `storage failover takeover` commande définie sur `immediate`, les opérations de basculement commencent immédiatement.
- Si la mise à jour du firmware d'un disque en arrière-plan se produit sur un nœud et qu'elle fonctionne de façon incohérente, le basculement du nœud mis à niveau commence immédiatement.
- Si une mise à jour du firmware du disque en arrière-plan est effectuée sur un disque sur un des nœuds, le rétablissement d'agrégats de données est retardé jusqu'à ce que la mise à jour du firmware du disque soit terminée sur ce disque.
- Si la mise à jour du firmware du disque en arrière-plan prend plus de 120 secondes, les opérations de rétablissement sont abandonnées et doivent être redémarrées manuellement une fois la mise à jour du firmware du disque terminée.

- Si une mise à jour du firmware du disque en arrière-plan se produit sur un disque de l'un des nœuds, les opérations de transfert des agrégats sont retardées jusqu'à ce que la mise à jour du firmware du disque soit terminée sur ce disque. Si la mise à jour du firmware du disque en arrière-plan prend plus de 120 secondes, les opérations de transfert d'agrégats sont abandonnées et doivent être redémarrées manuellement après la fin de la mise à jour du firmware des disques. Si le transfert d'agrégats a été initié avec le `-override-destination-checks` du `storage aggregate relocation` commande définie sur `true`, la mise à jour du firmware du disque en arrière-plan effectuée sur le nœud de destination n'affecte pas le transfert d'agrégats.

## Commandes de basculement automatique

Le basculement automatique est activé par défaut sur toutes les plateformes NetApp FAS, AFF et ASA prises en charge. Vous devrez peut-être modifier le comportement et le contrôle par défaut lorsque des prises de contrôle automatiques se produisent lorsque le nœud partenaire redémarre, fonctionne de façon incohérente ou s'arrête.

| Si vous souhaitez que le basculement se produise automatiquement lorsque le nœud partenaire... | Utilisez cette commande...                                         |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Redémarre ou s'arrête                                                                          | <code>storage failover modify -node nodename -onreboot true</code> |
| Les paniques                                                                                   | <code>storage failover modify -node nodename -onpanic true</code>  |

### Activez la notification par e-mail si l'option de basculement est désactivée

Pour recevoir une notification rapide en cas de désactivation de la fonctionnalité de basculement, vous devez configurer votre système de manière à activer une notification automatique par e-mail pour les messages EMS « basculement impossible » :

- `ha.takeoverImpVersion`
- `ha.takeoverImpLowMem`
- `ha.takeoverImpDegraded`
- `ha.takeoverImpUnsync`
- `ha.takeoverImpIC`
- `ha.takeoverImpHotShelf`
- `ha.takeoverImpNotDef`

## Commandes de rétablissement automatique

Par défaut, le nœud partenaire de reprise renvoie automatiquement le stockage lorsque le nœud hors ligne est rétabli en ligne, ce qui permet de restaurer la relation de paire haute disponibilité. Dans la plupart des cas, il s'agit du comportement souhaité. Si vous devez désactiver le retour automatique, par exemple pour rechercher la cause du basculement avant de le renvoyer, vous devez connaître l'interaction avec des paramètres non par défaut.

| Les fonctions que vous recherchez...                                                                                                                                                                                                                                                                                                                                                             | Utilisez cette commande...                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <p>Activez le rétablissement automatique afin que le rétablissement se produise dès le démarrage du nœud de basculement, atteint l'état en attente de rétablissement et le délai avant que la période de rétablissement automatique ait expiré.</p> <p>Le paramètre par défaut est vrai.</p>                                                                                                     | <pre>storage failover modify -node <i>nodename</i> -auto-giveback true</pre>              |
| <p>Désactiver le rétablissement automatique. Le paramètre par défaut est vrai.</p> <p><b>Note:</b> le fait de définir ce paramètre sur <i>false</i> ne désactive pas le retour automatique après basculement sur incident panic ; le retour automatique après basculement sur incident ("panic") doit être désactivé en définissant le <i>-auto-giveback-after-panic</i> paramètre sur faux.</p> | <pre>storage failover modify -node <i>nodename</i> -auto-giveback false</pre>             |
| <p>Désactiver le retour automatique après le basculement sur incident « panic » (ce paramètre est activé par défaut).</p>                                                                                                                                                                                                                                                                        | <pre>storage failover modify -node <i>nodename</i> -auto-giveback-after-panic false</pre> |
| <p>Retarder le rétablissement automatique pendant un nombre spécifié de secondes (la valeur par défaut est 600). Cette option détermine la durée minimale pendant laquelle un nœud reste en basculement avant d'effectuer un retour automatique.</p>                                                                                                                                             | <pre>storage failover modify -node <i>nodename</i> -delay-seconds <i>seconds</i></pre>    |

### Le mode d'incidence des variations de la commande **Storage failover modify** sur le giveback automatique

Le fonctionnement du retour automatique dépend de la façon dont vous configurez les paramètres de la commande **Storage failover modify**.

Le tableau suivant répertorie les paramètres par défaut du `storage failover modify` les paramètres de commande qui s'appliquent aux événements de basculement n'ont pas été causés par un problème.

| Paramètre                        | Paramètre par défaut                          |
|----------------------------------|-----------------------------------------------|
| <code>-auto-giveback true</code> | <code>false</code>                            |
| <code>true</code>                | <code>-delay-seconds integer (seconds)</code> |
| 600                              | <code>-onreboot true</code>                   |
| <code>false</code>               | <code>true</code>                             |

Le tableau suivant décrit comment les combinaisons de `-onreboot` et `-auto-giveback` les paramètres

affectent le rétablissement automatique pour des événements de basculement non provoqués par un incident de type panique.

| storage failover modify paramètres utilisés                                                    | Cause du basculement                                                                           | Le rétablissement automatique s'effectue-t-il ?                                                |
|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| -onreboot <i>true</i><br><br>-auto-giveback <i>true</i>                                        | commande reboot                                                                                | Oui.                                                                                           |
| Commande arrêtez ou opération de cycle d'alimentation exécutée depuis le processeur de service | Oui.                                                                                           | -onreboot <i>true</i><br><br>-auto-giveback <i>false</i>                                       |
| commande reboot                                                                                | Oui.                                                                                           | Commande arrêtez ou opération de cycle d'alimentation exécutée depuis le processeur de service |
| Non                                                                                            | -onreboot <i>false</i><br><br>-auto-giveback <i>true</i>                                       | commande reboot                                                                                |
| S/O<br>Dans ce cas, le basculement n'a pas lieu                                                | Commande arrêtez ou opération de cycle d'alimentation exécutée depuis le processeur de service | Oui.                                                                                           |
| -onreboot <i>false</i><br><br>-auto-giveback <i>false</i>                                      | commande reboot                                                                                | Non                                                                                            |

Le -auto-giveback les paramètres contrôlent le rétablissement après panique et tous les autres takovers automatiques. Si le -onreboot le paramètre est défini sur *true* de plus, un basculement a lieu suite à un redémarrage, puis un retour automatique est toujours effectué, que le soit -auto-giveback le paramètre est défini sur *true*.

Le -onreboot Le paramètre s'applique aux redémarrages et aux commandes d'arrêt générées par ONTAP. Lorsque le -onreboot le paramètre est défini sur *false*, un basculement ne se produit pas dans le cas d'un redémarrage de nœud. Par conséquent, le rétablissement automatique ne peut pas avoir lieu, que le ait ou non -auto-giveback le paramètre est défini sur *vrai*. Une interruption du client se produit.

### Les effets des combinaisons de paramètres de rétablissement automatique qui s'appliquent aux situations extrêmes.

Le tableau suivant répertorie la storage failover modify paramètres de commande qui s'appliquent aux situations d'urgence :

| Paramètre             | Paramètre par défaut |
|-----------------------|----------------------|
| -onpanic <i>_true</i> | false <i>_`</i>      |

|                                              |                                                |
|----------------------------------------------|------------------------------------------------|
| <code>true</code>                            | <code>`-auto-giveback-after-panic _true</code> |
| <code>false_`</code><br>(Privilège : avancé) | <code>true</code>                              |
| <code>`-auto-giveback _true</code>           | <code>false_`</code>                           |

Le tableau suivant explique comment les combinaisons de paramètres de l'`storage failover modify` la commande affecte le retour automatique dans les situations de panique.

| storage failover paramètres utilisés                                                                                                                                                                                                               | Le rétablissement automatique se produit-il après une panique ? |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| <code>-onpanic true</code><br><code>-auto-giveback true</code><br><code>-auto-giveback-after-panic true</code>                                                                                                                                     | Oui.                                                            |
| <code>-onpanic true</code><br><code>-auto-giveback true</code><br><code>-auto-giveback-after-panic false</code>                                                                                                                                    | Oui.                                                            |
| <code>-onpanic true</code><br><code>-auto-giveback false</code><br><code>-auto-giveback-after-panic true</code>                                                                                                                                    | Oui.                                                            |
| <code>-onpanic true</code><br><code>-auto-giveback false</code><br><code>-auto-giveback-after-panic false</code>                                                                                                                                   | Non                                                             |
| <code>-onpanic false</code><br>Si <code>-onpanic</code> est défini sur <code>false</code> , le basculement/retour ne se produit pas, quelle que soit la valeur définie pour <code>-auto-giveback</code> ou <code>-auto-giveback-after-panic</code> | Non                                                             |



Le basculement peut résulter d'un échec non associé à un problème de panique. Un *échec* se produit lorsque la communication est perdue entre un nœud et son partenaire, également appelée *heartbeat loss*. En cas de basculement à cause d'une défaillance, le rétablissement est contrôlé par le `-onfailure` paramètre au lieu du `-auto-giveback-after-panic` parameter.



Lorsqu'un nœud fonctionne de façon incohérente, il envoie un paquet de type `panic` à son nœud partenaire. Si, pour une raison quelconque, le paquet `panic` n'est pas reçu par le nœud partenaire, le problème peut être interprété incorrectement comme une défaillance. Sans réception du paquet `panic`, le nœud partenaire sait uniquement que la communication a été perdue et ne sait pas qu'un problème s'est produit. Dans ce cas, le nœud partenaire traite la perte de communication en tant que défaillance au lieu d'une panique, et le rétablissement est contrôlé par le `-onfailure` paramètre (et non pas par `-auto-giveback-after-panic` parameter).

Pour plus de détails sur tous `storage failover modify` paramètres, voir ["Pages de manuel ONTAP"](#).

## Commandes de basculement manuel

Vous pouvez effectuer un basculement manuellement lorsque des opérations de maintenance sont requises sur le partenaire et dans d'autres cas similaires. En fonction de l'état du partenaire, la commande que vous utilisez pour effectuer le basculement varie.

| Les fonctions que vous recherchez...                                                                                                                                                                                   | Utilisez cette commande...                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Reprendre le nœud partenaire                                                                                                                                                                                           | <code>storage failover takeover</code>                                           |
| Surveillez la progression du basculement lorsque les agrégats du partenaire sont déplacés vers le nœud qui prend le relais                                                                                             | <code>storage failover show-takeover</code>                                      |
| Afficher l'état du basculement de stockage pour tous les nœuds du cluster                                                                                                                                              | <code>storage failover show</code>                                               |
| Reprendre le nœud partenaire sans migrer les LIF                                                                                                                                                                       | <code>storage failover takeover -skip-lif -migration-before-takeover true</code> |
| Reprendre le nœud partenaire même en cas de non-concordance de disque                                                                                                                                                  | <code>storage failover takeover -skip-lif -migration-before-takeover true</code> |
| Prendre le contrôle du nœud partenaire même en cas de non-concordance de version de ONTAP<br><br><b>Remarque :</b> cette option est uniquement utilisée pendant le processus de mise à niveau ONTAP sans interruption. | <code>storage failover takeover -option allow-version-mismatch</code>            |
| Reprendre le nœud partenaire sans effectuer de transfert d'agrégats                                                                                                                                                    | <code>storage failover takeover -bypass -optimization true</code>                |
| Prenez le relais avant que le partenaire n'ait le temps de fermer ses ressources de stockage en toute élégance                                                                                                         | <code>storage failover takeover -option immediate</code>                         |



Avant d'exécuter la commande Storage Failover avec l'option immédiate, vous devez migrer les LIFs de données vers un autre nœud à l'aide de la commande suivante : `network interface migrate-all -node node`

Si vous spécifiez le `storage failover takeover -option immediate` Commande sans migrer au préalable les LIFs de données, la migration de LIF de données depuis le nœud est considérablement retardée, même si le `skip-lif-migration-before-takeover` option non spécifiée.

De même, si vous spécifiez l'option immédiate, l'optimisation du basculement négocié est contournée même si l'option Bypass-optimisation est définie sur *false*.

## Déplacement d'épsilon pour certaines prises de contrôle initiées manuellement

Vous devez déplacer epsilon si vous prévoyez que les transferts initiés manuellement peuvent entraîner une panne de nœud inattendue du système de stockage à l'écart d'une perte du quorum au niveau du cluster.



Description de la tâche

Pour effectuer la maintenance planifiée, vous devez prendre le relais d'un des nœuds d'une paire haute disponibilité. Le quorum à l'échelle du cluster doit être maintenu afin d'éviter les interruptions non planifiées des données client pour les nœuds restants. Dans certains cas, l'exécution du basculement peut entraîner une panne inattendue d'un nœud en dehors de la perte du quorum au niveau du cluster.

Cela peut se produire si le nœud pris sur epsilon ou si le nœud avec epsilon n'est pas sain. Pour maintenir un cluster plus résilient, vous pouvez transférer epsilon vers un nœud sain qui n'est pas pris en charge. Il s'agit généralement du partenaire de haute disponibilité.

Seuls les noeuds sains et admissibles participent au vote du quorum. Pour maintenir le quorum à l'échelle du cluster, plus de votes  $N/2$  sont nécessaires (où  $N$  représente la somme des nœuds en ligne sains et admissibles). Dans les clusters avec un nombre pair de nœuds en ligne, epsilon ajoute un poids supplémentaire aux votes afin de maintenir le quorum pour le nœud auquel il est attribué.



Bien que le vote de formation de groupe puisse être modifié à l'aide du `cluster modify -eligibility false` sauf dans le cas contraire, vous devez restaurer la configuration du nœud ou procéder à une maintenance prolongée du nœud. Si vous définissez un nœud comme non éligible, il cesse de transmettre les données SAN jusqu'à ce que le nœud soit réinitialisé à sa valeur éligible et à son redémarrage. L'accès aux données NAS au nœud peut également être affecté lorsque ce dernier n'est pas éligible.

Étapes

- 1. Vérifier l'état du cluster et confirmer qu'epsilon est maintenu par un nœud sain qui n'est pas pris en charge :
  - a. Passer au niveau de privilège avancé, en confirmant que vous souhaitez continuer lorsque l'invite du mode avancé s'affiche (\*>) :

```
set -privilege advanced
```

- b. Déterminer quel nœud contient epsilon :

```
cluster show
```

Dans l'exemple suivant, Node1 possède epsilon :

| Nœud   | Santé | Éligibilité | Epsilon |
|--------|-------|-------------|---------|
| Nœud 1 | vrai  | vrai        | vrai    |
| Nœud 2 | vrai  | vrai        | faux    |

+  
Si le nœud que vous souhaitez prendre le relais ne contient pas epsilon, passer à l'étape 4.

- 2. Supprimer epsilon du nœud que vous souhaitez prendre le contrôle :

```
cluster modify -node Node1 -epsilon false
```

- 3. Assigner epsilon au nœud partenaire (dans cet exemple, Node4) :

```
cluster modify -node Node2 -epsilon true
```

4. Effectuez l'opération de basculement :

```
storage failover takeover -ofnode node_name
```

5. Retour au niveau de privilège admin :

```
set -privilege admin
```

## Commandes de rétablissement manuel

Vous pouvez effectuer un retour normal, un retour dans lequel vous interrompez les processus sur un nœud partenaire ou un rétablissement forcé.



Avant d'effectuer un retour, vous devez supprimer les disques défectueux dans le système de mise en service, comme décrit dans la ["Gestion des disques et des agrégats"](#).

### Si le retour est interrompu

En cas de défaillance ou de panne d'alimentation au cours du processus de rétablissement, ce processus s'arrête et le nœud de basculement revient en mode basculement jusqu'à ce que la panne soit réparée ou que l'alimentation soit restaurée.

Toutefois, cela dépend du stade de rétablissement dans lequel l'échec s'est produit. Si le nœud a rencontré une panne ou une panne de courant lors de l'état de rétablissement partiel (après qu'il a été renvoyé l'agrégat racine), celui-ci ne sera pas renvoyé en mode basculement. À la place, le nœud revient en mode de retour partiel. Dans ce cas, terminez le processus en répétant l'opération de rétablissement.

### Si le retour est refusé

Si le retour est vetoté, vous devez vérifier les messages EMS pour en déterminer la cause. En fonction de la ou des raisons, vous pouvez décider si vous pouvez ignorer les vetos en toute sécurité.

Le `storage failover show-giveback` la commande affiche la progression du rétablissement et affiche le sous-système qui a veto au rétablissement, le cas échéant. Les vetos souples peuvent être remplacés, alors que les vetos durs ne peuvent pas être, même si forcé. Les tableaux suivants résument les vetos logiciels qui ne doivent pas être remplacés, ainsi que les solutions de contournement recommandées.

Vous pouvez vérifier les détails EMS de tout giveback en utilisant la commande suivante:

```
event log show -node * -event gb*
```

### Rétablissement de l'agrégat racine

Ces vetos ne s'appliquent pas aux opérations de transfert d'agrégats :

| Vetoing sous-module | Solution de contournement |
|---------------------|---------------------------|
|---------------------|---------------------------|

|                        |                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vfiler_bas_niveau      | <p>Mettez fin aux sessions SMB à l'origine du veto, ou arrêtez l'application SMB qui a établi les sessions ouvertes.</p> <p>Le fait de ne pas accorder ce droit de veto peut entraîner la déconnexion soudaine de l'application utilisant SMB et la perte de données.</p>                                                                                                                      |
| Vérification du disque | <p>Tous les disques défectueux ou contournés doivent être supprimés avant de tenter le rétablissement. Si un disque est en cours de nettoyage, vous devez patienter jusqu'à la fin de l'opération.</p> <p>Le fait d'ignorer ce droit de veto peut entraîner une panne causée par des agrégats ou des volumes déconnectés en raison de conflits de réservation ou de disques inaccessibles.</p> |

## Rétablissement des agrégats SFO

Ces vetos ne s'appliquent pas aux opérations de transfert d'agrégats :

| Vetoing sous-module                      | Solution de contournement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gestionnaire de verrous                  | <p>Arrêtez aisément les applications SMB qui disposent de fichiers ouverts ou déplacez ces volumes vers un autre agrégat.</p> <p>Le fait de ne pas accorder ce droit de veto entraîne une perte de l'état de verrouillage SMB, ce qui entraîne une interruption et une perte de données.</p>                                                                                                                                                                                                                                                                                                                                     |
| CONTINUITÉ de l'activité de Lock Manager | <p>Attendez que les verrous soient mis en miroir.</p> <p>Le fait de ne pas accorder ce droit de veto entraîne des perturbations sur les machines virtuelles Microsoft Hyper-V.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| RAID                                     | <p>Vérifiez les messages EMS pour déterminer la cause du droit de veto :</p> <p>Si le veto est dû au fichier nvfile, mettez les volumes et les agrégats hors ligne en ligne.</p> <p>Si des opérations d'ajout de disque ou de réaffectation de propriété des disques sont en cours, attendez qu'elles soient terminées.</p> <p>Si le veto est dû à un conflit de nom d'agrégat ou d'UUID, dépannez et résolvez le problème.</p> <p>Si le veto est dû à une resynchronisation du miroir, à une vérification du miroir ou à des disques hors ligne, le veto peut être annulé et l'opération redémarre après le rétablissement.</p> |

|                                    |                                                                                                                                                                                                                                                                                                    |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inventaire des disques             | <p>Dépanner pour identifier et résoudre la cause du problème.</p> <p>Le nœud de destination peut ne pas voir les disques appartenant à un agrégat en cours de migration.</p> <p>Les disques inaccessibles peuvent entraîner des agrégats ou des volumes inaccessibles.</p>                         |
| Opération de déplacement de volume | <p>Dépanner pour identifier et résoudre la cause du problème.</p> <p>Ce veto empêche l'opération de déplacement du volume de passer outre lors de la phase importante de la mise en service. Si le travail est abandonné au cours de la mise en service, le volume risque d'être inaccessible.</p> |

### Commandes pour effectuer un rétablissement manuel

Vous pouvez lancer manuellement un rétablissement sur un nœud d'une paire HA pour le renvoyer au propriétaire d'origine après les opérations de maintenance ou de résolution tous les problèmes qui ont provoqué le basculement.

| Les fonctions que vous recherchez...                                                                            | Utilisez cette commande...                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Renvoyer le stockage à un nœud partenaire                                                                       | <code>storage failover giveback -ofnode <i>nodename</i></code>                                                                                                                                                                                                                           |
| Remettre le stockage de retour même si le partenaire n'est pas en mode d'attente de rétablissement              | <code>storage failover giveback -ofnode <i>nodename</i></code><br><code>-require-partner-waiting false</code><br><br><p>N'utilisez pas cette option à moins qu'une interruption de service client plus longue ne soit acceptable.</p>                                                    |
| Remettre le stockage en arrière même si les processus sont vetoting the giveback opération (forcer le giveback) | <code>storage failover giveback -ofnode <i>nodename</i></code><br><code>-override-vetoes true</code><br><br><p>L'utilisation de cette option peut potentiellement entraîner une panne du client plus longue ou des agrégats et des volumes non mis en ligne après le rétablissement.</p> |
| Renvoyer uniquement les agrégats CFO (l'agrégat racine)                                                         | <code>storage failover giveback -ofnode <i>nodename</i></code><br><br><code>-only-cfo-aggregates true</code>                                                                                                                                                                             |
| Surveiller la progression du retour après l'exécution de la commande giveback                                   | <code>storage failover show-giveback</code>                                                                                                                                                                                                                                              |

## Test de basculement et de rétablissement

Une fois que vous avez configuré tous les aspects de votre paire haute disponibilité, vérifiez qu'elle fonctionne comme prévu afin de maintenir un accès ininterrompu au stockage des deux nœuds lors des opérations de basculement et de rétablissement. Tout au long du processus de basculement, le nœud local (ou le basculement) doit continuer à transmettre les données normalement fournies par le nœud partenaire. Lors du rétablissement, le contrôle et la livraison du stockage du partenaire doivent revenir sur le nœud partenaire.

### Étapes

1. Vérifiez le câblage des câbles d'interconnexion haute disponibilité pour vous assurer qu'ils sont bien fixés.
2. Vérifiez que vous pouvez créer et récupérer des fichiers sur les deux nœuds pour chaque protocole sous licence.
3. Saisissez la commande suivante :

```
storage failover takeover -ofnode partnernode
```

Consultez la page man pour plus de détails sur la commande.

4. Entrez l'une ou l'autre des commandes suivantes pour confirmer que le basculement a eu lieu :

```
storage failover show-takeover
```

```
storage failover show
```

Si vous avez le `storage failover` commandes `-auto-giveback` option activée :

| Nœud   | En tant que partenaire | Basculement possible | Description de l'état                                                                 |
|--------|------------------------|----------------------|---------------------------------------------------------------------------------------|
| nœud 1 | nœud 2                 | -                    | Attente du retour                                                                     |
| nœud 2 | nœud 1                 | faux                 | En cas de basculement, le rétablissement automatique sera initié en quelques secondes |

Si vous avez le `storage failover` commandes `-auto-giveback` option désactivée :

| Nœud   | En tant que partenaire | Basculement possible | Description de l'état |
|--------|------------------------|----------------------|-----------------------|
| nœud 1 | nœud 2                 | -                    | Attente du retour     |
| nœud 2 | nœud 1                 | faux                 | En prise de contrôle  |

5. Afficher tous les disques qui appartiennent au nœud partenaire (Node4) que le nœud Takeover (Node1) peut détecter :

```
storage disk show -home node2 -ownership
```

La commande suivante affiche tous les disques appartenant au nœud 2 que le nœud 1 peut détecter :

```
cluster::> storage disk show -home node2 -ownership
```

| Disque | Agrégat | Accueil | Propriétaire | Accueil de la reprise après incident | ID domicile | ID propriétaire | ID domicile DR | Réservation | Piscine |
|--------|---------|---------|--------------|--------------------------------------|-------------|-----------------|----------------|-------------|---------|
| 1.0.2  | -       | nœud 2  | nœud 2       | -                                    | 4078312453  | 4078312453      | -              | 4078312452  | Pool0   |
| 1.0.3  | -       | nœud 2  | nœud 2       | -                                    | 4078312453  | 4078312453      | -              | 4078312452  | Pool0   |

6. Confirmer que le nœud du basculement (Node1) contrôle les agrégats du nœud partenaire (Node2) :

```
aggr show -fields home-id,home-name,is-home
```

| agrégat | id-domicile | maison-nameh | chez soi |
|---------|-------------|--------------|----------|
| aggr0_1 | 2014942045  | nœud 1       | vrai     |
| aggr0_2 | 4078312453  | nœud 2       | faux     |
| aggr1_1 | 2014942045  | nœud 1       | vrai     |
| aggr1_2 | 4078312453  | nœud 2       | faux     |

Pendant l'acquisition, la valeur « is-home » des agrégats du nœud partenaire est fausse.

7. Remettre le service de données du nœud partenaire après avoir affiché le message « en attente de rétablissement » :

```
storage failover giveback -ofnode partnernode
```

8. Entrez l'une ou l'autre des commandes suivantes pour observer la progression de l'opération de rétablissement :

```
storage failover show-giveback
```

```
storage failover show
```

9. Continuer, selon que vous avez vu le message que le rétablissement a été effectué correctement :

| Si le basculement et le rétablissement... | Alors...                                                                            |
|-------------------------------------------|-------------------------------------------------------------------------------------|
| Sont terminées avec succès                | Répétez les étapes 2 à 8 sur le nœud partenaire.                                    |
| Echec                                     | Corrigez l'échec de basculement ou de rétablissement, puis répétez cette procédure. |

## Commandes permettant de contrôler une paire HA

Vous pouvez utiliser des commandes ONTAP pour contrôler l'état de la paire HA. En cas

de basculement, vous pouvez également déterminer l'origine du basculement.

| Si vous voulez vérifier                                                                                                                                                                                                                      | Utilisez cette commande                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Si le basculement est activé ou s'est produit, ou si la raison pour laquelle le basculement n'est pas possible pour le moment                                                                                                                | <code>storage failover show</code>                                                |
| Afficher les nœuds sur lesquels le paramètre HA-mode de basculement du stockage est activé<br>Vous devez définir la valeur sur <code>ha</code> pour que le nœud puisse participer à une configuration de basculement du stockage (paire HA). | <code>storage failover show -fields mode</code>                                   |
| Indique si le basculement assisté par matériel est activé                                                                                                                                                                                    | <code>storage failover hwassist show</code>                                       |
| Historique des événements de basculement assisté par matériel qui se sont produits                                                                                                                                                           | <code>storage failover hwassist stats show</code>                                 |
| La progression d'une opération de basculement lorsque les agrégats du partenaire sont déplacés vers le nœud faisant le basculement                                                                                                           | <code>storage failover show-takeover</code>                                       |
| Progression d'une opération de rétablissement visant à renvoyer les agrégats au nœud partenaire                                                                                                                                              | <code>storage failover show-giveback</code>                                       |
| Qu'un agrégat soit en hébergement lors des opérations de basculement ou de rétablissement                                                                                                                                                    | <code>aggregate show -fields home-id,owner-id,home-name,owner-name,is-home</code> |
| Si la haute disponibilité du cluster est activée (s'applique uniquement aux clusters à deux nœuds)                                                                                                                                           | <code>cluster ha show</code>                                                      |
| L'état de haute disponibilité des composants d'une paire haute disponibilité (sur les systèmes qui utilisent l'état HA)                                                                                                                      | <code>ha-config show</code><br>Il s'agit d'une commande du mode maintenance.      |

### État du nœud affiché par les commandes `Storage failover show-type`

La liste suivante décrit l'état du nœud `storage failover show` affichage des commandes.

| État du nœud                                                              | Description                                                                                                                                                 |
|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connecté à <code>Partner_name</code> , basculement automatique désactivé. | L'interconnexion haute disponibilité est active et peut transmettre des données au nœud partenaire. Le basculement automatique du partenaire est désactivé. |

|                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| En attente de Partner_name, Giveback des disques de spare du partenaire en attente.                                                                                                                      | <p>Le nœud local ne peut pas échanger d'informations avec le nœud partenaire via l'interconnexion haute disponibilité. Le rétablissement des agrégats SFO vers le partenaire s'effectue, mais les disques de spare du partenaire sont toujours la propriété du nœud local.</p> <ul style="list-style-type: none"> <li>• Exécutez le <code>storage failover show-giveback</code> commande pour plus d'informations.</li> </ul> |
| En attente de Partner_name. En attente de synchronisation du verrouillage partenaire.                                                                                                                    | Le nœud local ne peut pas échanger d'informations avec le nœud partenaire via l'interconnexion haute disponibilité et attend que la synchronisation de verrouillage partenaire se produise.                                                                                                                                                                                                                                   |
| En attente de Partner_name. Attente de la mise en ligne des applications de cluster sur le nœud local.                                                                                                   | Le nœud local ne peut pas échanger d'informations avec le nœud partenaire via l'interconnexion haute disponibilité, et attend que les applications de cluster soient en ligne.                                                                                                                                                                                                                                                |
| Basculement planifié. Le nœud cible replace ses agrégats SFO en préparation du basculement.                                                                                                              | Le traitement de basculement a commencé. Le nœud cible délocalise la propriété de ses agrégats SFO en préparation au basculement.                                                                                                                                                                                                                                                                                             |
| Basculement planifié. Le nœud cible a déplacé ses agrégats SFO en préparation du basculement.                                                                                                            | Le traitement de basculement a commencé. Le nœud cible a déplacé la propriété de ses agrégats SFO en préparation pour le basculement.                                                                                                                                                                                                                                                                                         |
| Basculement planifié. Attente de désactivation des mises à jour du firmware du disque en arrière-plan sur le nœud local. Une mise à jour du firmware est en cours sur le nœud.                           | Le traitement de basculement a commencé. Le système attend que les opérations de mise à jour du firmware du disque en arrière-plan soient terminées sur le nœud local.                                                                                                                                                                                                                                                        |
| Déplacement des agrégats SFO vers le transfert du nœud en préparation du basculement.                                                                                                                    | Le nœud local réinstalle la propriété de ses agrégats SFO vers le nœud « pré-basculement » pour la préparation du basculement.                                                                                                                                                                                                                                                                                                |
| Transfert des agrégats SFO vers le basculement du nœud. Attente du basculement du nœud.                                                                                                                  | Le déplacement de la propriété des agrégats SFO du nœud local vers le nœud de prise en charge est terminé. Le système attend le basculement par le nœud de prise de contrôle.                                                                                                                                                                                                                                                 |
| Déplacement des agrégats SFO vers Partner_name. En attente de désactiver les mises à jour du firmware du disque en arrière-plan sur le nœud local. Une mise à jour du firmware est en cours sur le nœud. | La relocalisation de la propriété des agrégats SFO du nœud local vers le nœud de prise en charge est en cours. Le système attend que les opérations de mise à jour du firmware du disque en arrière-plan soient terminées sur le nœud local.                                                                                                                                                                                  |



|                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Déplacement des agrégats SFO vers Partner_name. Attente de désactivation des mises à jour du firmware du disque en arrière-plan sur Partner_name. Une mise à jour du firmware est en cours sur le nœud.</p>                                                                                                                                                                                                                   | <p>La relocalisation de la propriété des agrégats SFO du nœud local vers le nœud de prise en charge est en cours. Le système attend que les opérations de mise à jour du firmware du disque en arrière-plan soient effectuées sur le nœud partenaire.</p>                                                                                                                                                                                                                                                                                                                                                                                    |
| <p>Connecté à Partner_name. La tentative précédente de basculement a été abandonnée en raison de cette raison. Le nœud local possède certains agrégats SFO du partenaire.<br/>Réémettez un basculement du partenaire avec le <code>-bypass-optimization</code> paramètre défini sur <code>true</code> pour le basculement des agrégats restants ou du rétablissement d'un partenaire pour le retour des agrégats transférés.</p> | <p>L'interconnexion haute disponibilité est active et peut transmettre des données au nœud partenaire. La tentative de basculement précédente a été abandonnée en raison de la raison affichée sous Reason. Le nœud local possède certains agrégats SFO de son partenaire.</p> <ul style="list-style-type: none"> <li>• Vous pouvez soit réémettre un basculement du nœud partenaire, en définissant le paramètre d'optimisation <code>-sur</code> la valeur <code>true</code> pour le basculement des agrégats SFO restants ou procéder à un rétablissement du partenaire pour renvoyer les agrégats transférés.</li> </ul>                 |
| <p>Connecté à Partner_name. La tentative précédente de basculement a été abandonnée. Le nœud local possède certains agrégats SFO du partenaire.<br/>Réémettez un basculement du partenaire avec le <code>-bypass-optimization</code> paramètre défini sur <code>true</code> pour le basculement des agrégats restants ou du rétablissement d'un partenaire pour le retour des agrégats transférés.</p>                           | <p>L'interconnexion haute disponibilité est active et peut transmettre des données au nœud partenaire. La tentative de basculement précédente a été abandonnée. Le nœud local possède certains agrégats SFO de son partenaire.</p> <ul style="list-style-type: none"> <li>• Vous pouvez soit réémettre un basculement du nœud partenaire, en définissant le paramètre d'optimisation <code>-sur</code> la valeur <code>true</code> pour le basculement des agrégats SFO restants ou procéder à un rétablissement du partenaire pour renvoyer les agrégats transférés.</li> </ul>                                                             |
| <p>En attente de Partner_name. La tentative précédente de basculement a été abandonnée en raison de cette raison. Le nœud local possède certains agrégats SFO du partenaire.<br/>Refaites le basculement du partenaire avec le paramètre « contournement-optimisation » défini sur « <code>true</code> » pour le basculement d'agrégats restants ou exécutez un retour du partenaire pour renvoyer les agrégats transférés.</p>  | <p>Le nœud local ne peut pas échanger d'informations avec le nœud partenaire via l'interconnexion haute disponibilité. La tentative de basculement précédente a été abandonnée en raison de la raison affichée sous Reason. Le nœud local possède certains agrégats SFO de son partenaire.</p> <ul style="list-style-type: none"> <li>• Vous pouvez soit réémettre un basculement du nœud partenaire, en définissant le paramètre d'optimisation <code>-sur</code> la valeur <code>true</code> pour le basculement des agrégats SFO restants ou procéder à un rétablissement du partenaire pour renvoyer les agrégats transférés.</li> </ul> |

|                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| En attente de Partner_name. La tentative précédente de basculement a été abandonnée. Le nœud local possède certains agrégats SFO du partenaire. Refaites le basculement du partenaire avec le paramètre « contournement-optimisation » défini sur « true » pour le basculement d'agrégats restants ou exécutez un retour du partenaire pour renvoyer les agrégats transférés. | <p>Le nœud local ne peut pas échanger d'informations avec le nœud partenaire via l'interconnexion haute disponibilité. La tentative de basculement précédente a été abandonnée. Le nœud local possède certains agrégats SFO de son partenaire.</p> <ul style="list-style-type: none"> <li>• Vous pouvez soit réémettre un basculement du nœud partenaire, en définissant le paramètre d'optimisation -sur la valeur true pour le basculement des agrégats SFO restants ou procéder à un rétablissement du partenaire pour renvoyer les agrégats transférés.</li> </ul> |
| Connecté à Partner_name. La tentative de basculement précédente a été abandonnée car la mise à jour du micrologiciel du disque en arrière-plan (BDFU) sur le nœud local a échoué.                                                                                                                                                                                             | L'interconnexion haute disponibilité est active et peut transmettre des données au nœud partenaire. La tentative de basculement précédente a été abandonnée car la mise à jour du firmware du disque en arrière-plan sur le nœud local n'a pas été désactivée.                                                                                                                                                                                                                                                                                                         |
| Connecté à Partner_name. La tentative précédente de basculement a été abandonnée en raison de cette raison.                                                                                                                                                                                                                                                                   | L'interconnexion haute disponibilité est active et peut transmettre des données au nœud partenaire. La tentative de basculement précédente a été abandonnée en raison de la raison affichée sous Reason.                                                                                                                                                                                                                                                                                                                                                               |
| En attente de Partner_name. La tentative précédente de basculement a été abandonnée en raison de cette raison.                                                                                                                                                                                                                                                                | Le nœud local ne peut pas échanger d'informations avec le nœud partenaire via l'interconnexion haute disponibilité. La tentative de basculement précédente a été abandonnée en raison de la raison affichée sous Reason.                                                                                                                                                                                                                                                                                                                                               |
| Connecté à Partner_name. La tentative précédente de basculement par Partner_name a été abandonnée car elle a été interrompue.                                                                                                                                                                                                                                                 | L'interconnexion haute disponibilité est active et peut transmettre des données au nœud partenaire. La tentative de basculement précédente par le nœud partenaire a été abandonnée en raison de la raison affichée sous Reason.                                                                                                                                                                                                                                                                                                                                        |
| Connecté à Partner_name. La tentative précédente de basculement par Partner_name a été abandonnée.                                                                                                                                                                                                                                                                            | L'interconnexion haute disponibilité est active et peut transmettre des données au nœud partenaire. La précédente tentative de basculement par le nœud partenaire a été abandonnée.                                                                                                                                                                                                                                                                                                                                                                                    |
| En attente de Partner_name. La tentative précédente de basculement par Partner_name a été abandonnée car elle a été interrompue.                                                                                                                                                                                                                                              | Le nœud local ne peut pas échanger d'informations avec le nœud partenaire via l'interconnexion haute disponibilité. La tentative de basculement précédente par le nœud partenaire a été abandonnée en raison de la raison affichée sous Reason.                                                                                                                                                                                                                                                                                                                        |

|                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Échec du retour précédent dans le module : nom du module. Le rétablissement automatique est lancé en quelques secondes.             | <p>La tentative de retour précédente a échoué dans le module nom_module. Le rétablissement automatique sera lancé en quelques secondes.</p> <ul style="list-style-type: none"> <li>• Exécutez le <code>storage failover show-giveback</code> commande pour plus d'informations.</li> </ul>                                                                  |
| Le nœud est propriétaire des agrégats du partenaire dans le cadre de la procédure de mise à niveau du contrôleur sans interruption. | Le nœud possède les agrégats de ses partenaires, car la procédure de mise à niveau du contrôleur sans interruption est en cours d'exécution.                                                                                                                                                                                                                |
| Connecté à Partner_name. Le nœud est propriétaire d'agrégats appartenant à un autre nœud du cluster.                                | L'interconnexion haute disponibilité est active et peut transmettre des données au nœud partenaire. Le nœud possède des agrégats appartenant à un autre nœud du cluster.                                                                                                                                                                                    |
| Connecté à Partner_name. En attente de synchronisation du verrouillage partenaire.                                                  | L'interconnexion haute disponibilité est active et peut transmettre des données au nœud partenaire. Le système attend la fin de la synchronisation du verrouillage partenaire.                                                                                                                                                                              |
| Connecté à Partner_name. Attente de la mise en ligne des applications de cluster sur le nœud local.                                 | L'interconnexion haute disponibilité est active et peut transmettre des données au nœud partenaire. Le système attend que les applications de cluster soient mises en ligne sur le nœud local.                                                                                                                                                              |
| En mode non HA, redémarrez le système pour utiliser la mémoire NVRAM complète.                                                      | <p>Le basculement du stockage n'est pas possible. L'option mode HA est configurée en tant que non_ha.</p> <ul style="list-style-type: none"> <li>• Vous devez redémarrer le nœud pour utiliser l'ensemble de sa mémoire NVRAM.</li> </ul>                                                                                                                   |
| Mode non HA. Redémarrez le nœud pour activer la haute disponibilité.                                                                | <p>Le basculement du stockage n'est pas possible.</p> <ul style="list-style-type: none"> <li>• Le nœud doit être redémarré pour activer la fonctionnalité haute disponibilité.</li> </ul>                                                                                                                                                                   |
| Mode non HA.                                                                                                                        | <p>Le basculement du stockage n'est pas possible. L'option mode HA est configurée en tant que non_ha.</p> <ul style="list-style-type: none"> <li>• Vous devez exécuter le <code>storage failover modify -mode ha -node nodename</code> Commande sur les deux nœuds de la paire HA, puis redémarrage des nœuds pour activer la fonctionnalité HA.</li> </ul> |

## Commandes d'activation et de désactivation du basculement du stockage

Utiliser les commandes suivantes pour activer et désactiver la fonctionnalité de

## basculement du stockage.

| Les fonctions que vous recherchez... | Utilisez cette commande...                                                |
|--------------------------------------|---------------------------------------------------------------------------|
| Activation du basculement            | <code>storage failover modify -enabled true -node <i>nodename</i></code>  |
| Désactiver le basculement            | <code>storage failover modify -enabled false -node <i>nodename</i></code> |



Vous ne devez désactiver le basculement du stockage que si nécessaire dans le cadre d'une procédure de maintenance.

## Arrêtez ou redémarrez un nœud sans initier le basculement dans un cluster à deux nœuds

Vous arrêtez ou redémarrez un nœud dans un cluster à deux nœuds sans passer par le basculement lorsque vous effectuez certaines opérations de maintenance matérielle sur un nœud ou un tiroir. Vous pouvez également limiter les temps d'indisponibilité en maintenant le nœud partenaire en fonctionnement, en cas de problème empêchant un basculement manuel, vous devez également maintenir les agrégats du nœud partenaire et assurer le service des données. De plus, si le support technique vous aide à résoudre les problèmes, il se peut que vous deviez effectuer cette procédure dans le cadre de ces efforts.

### Description de la tâche

- Avant de désactiver le basculement (à l'aide du `-inhibit-takeover true` Paramètre), vous désactivez le cluster HA.



- Dans un cluster à deux nœuds, la haute disponibilité du cluster permet de s'assurer que la défaillance d'un nœud ne désactive pas le cluster. Toutefois, si vous ne désactivez pas la haute disponibilité du cluster avant d'utiliser `-inhibit-takeover true` paramètre, le service des données n'est plus servi sur les deux nœuds.
- Si vous tentez d'arrêter ou de redémarrer un nœud avant de désactiver la haute disponibilité du cluster, ONTAP émet un avertissement et vous indique de désactiver la haute disponibilité du cluster.

- Vous migrez les LIF (interfaces logiques) vers le nœud partenaire que vous souhaitez conserver en ligne.
- Si sur le nœud que vous arrête ou redémarrez, des agrégats doivent être conservés, vous les déplacez vers le nœud que vous souhaitez conserver en ligne.

### Étapes

1. Vérifiez que les deux nœuds fonctionnent correctement :  
`cluster show`

Pour les deux nœuds, `true` s'affiche dans le `Health` colonne.

```
cluster::> cluster show
Node Health Eligibility

node1 true true
node2 true true
```

2. Migrer toutes les LIFs du nœud qui vont s'arrêter ou redémarrer vers le nœud partenaire :  
`network interface migrate-all -node node_name`
3. Si vous arrêtez ou redémarrez le nœud, vous voulez garder les agrégats en ligne lorsque le nœud n'est pas en panne, puis les transférer vers le nœud partenaire ; sinon, passez à l'étape suivante.

- a. Afficher les agrégats du nœud vous arrêtez ou redémarrez :

`storage aggregates show -node node_name`

Par exemple, le nœud 1 est le nœud qui sera arrêté ou redémarré :

```
cluster::> storage aggregates show -node node1
Aggregate Size Available Used% State #Vols Nodes RAID
Status

aggr0_node_1_0
 744.9GB 32.68GB 96% online 2 node1 raid_dp,
normal
aggr1 2.91TB 2.62TB 10% online 8 node1 raid_dp,
normal
aggr2 4.36TB 3.74TB 14% online 12 node1 raid_dp,
normal
test2_aggr 2.18TB 2.18TB 0% online 7 node1 raid_dp,
normal
4 entries were displayed.
```

- b. Déplacez les agrégats vers le nœud partenaire :

`storage aggregate relocation start -node node_name -destination node_name  
 -aggregate-list aggregate_name`

Par exemple, les agrégats aggr1, aggr2 et test2\_aggr sont déplacés du nœud 1 vers le nœud 2 :

```
storage aggregate relocation start -node node1 -destination node2 -aggregate

-list aggr1,aggr2,test2_aggr
```

4. Désactivation du cluster HA :

```
cluster ha modify -configured false
```

La sortie de retour confirme que la HA est désactivée : Notice: HA is disabled



Cette opération ne désactive pas le basculement du stockage.

5. Arrêtez ou redémarrez et inhiber le basculement du nœud cible, en utilisant la commande appropriée :

- ° `system node halt -node node_name -inhibit-takeover true`
- ° `system node reboot -node node_name -inhibit-takeover true`



Dans le résultat de la commande, un avertissement s'affiche vous demandant si vous souhaitez continuer, entrez `y`.

6. Vérifiez que le nœud qui est toujours en ligne est en état de santé (alors que le partenaire n'est pas en panne) :

```
cluster show
```

Pour le nœud en ligne, `true` s'affiche dans le Health colonne.



Dans le résultat de la commande, un avertissement s'affiche indiquant que le cluster HA n'est pas configuré. Vous pouvez ignorer l'avertissement pour le moment.

7. Exécutez les actions qui vous permettent d'arrêter ou de redémarrer le nœud.

8. Démarrage du nœud de mise hors ligne à partir de l'invite DU CHARGEUR :

```
boot_ontap
```

9. Vérifiez que les deux nœuds fonctionnent correctement :

```
cluster show
```

Pour les deux nœuds, `true` s'affiche dans le Health colonne.



Dans le résultat de la commande, un avertissement s'affiche indiquant que le cluster HA n'est pas configuré. Vous pouvez ignorer l'avertissement pour le moment.

10. Réactiver la haute disponibilité du cluster :

```
cluster ha modify -configured true
```

11. Si vous avez précédemment transféré des agrégats vers le nœud partenaire, déplacez-les vers le nœud de rattachement ; sinon, passez à l'étape suivante :

```
storage aggregate relocation start -node node_name -destination node_name
-aggregate-list aggregate_name
```

Par exemple, les agrégats `aggr1`, `aggr2` et `test2_aggr` sont déplacés du nœud `node2` vers le nœud `node1` :

```
storage aggregate relocation start -node node2 -destination node1 -aggregate
-list aggr1,aggr2,test2_aggr
```

12. Rerestaurer les LIF sur leurs home ports :

a. Affichez les LIF qui ne sont pas à la maison :

```
network interface show -is-home false
```

- b. Si certaines LIF ne se trouvent pas chez soi et n'ont pas été migrées depuis le nœud défaillant, vérifiez qu'il est sûr de les déplacer avant le rétablissement.
- c. Si vous êtes sûr de le faire, re restaurez toutes les LIF à la maison.  
`network interface revert *`

## Gestion des API REST avec System Manager

### Gestion des API REST avec System Manager

Le journal de l'API REST capture les appels API que System Manager envoie à ONTAP. Vous pouvez utiliser le journal pour comprendre la nature et la séquence des appels nécessaires à l'exécution des diverses tâches administratives ONTAP.

#### Comment System Manager utilise l'API REST et le journal d'API

Il existe plusieurs façons d'émettre les appels d'API REST vers ONTAP par System Manager.

#### Quand System Manager émet-il des appels d'API

Voici les exemples les plus importants lorsque System Manager émet des appels d'API REST ONTAP.

#### Actualisation automatique de la page

System Manager envoie automatiquement des appels d'API en arrière-plan pour actualiser les informations affichées, par exemple sur la page du tableau de bord.

#### Afficher l'action par l'utilisateur

Un ou plusieurs appels d'API sont émis lorsque vous affichez une ressource de stockage spécifique ou un ensemble de ressources dans l'interface utilisateur de System Manager.

#### Action de mise à jour par utilisateur

Un appel d'API est émis lorsque vous ajoutez, modifiez ou supprimez une ressource ONTAP dans l'interface utilisateur de System Manager.

#### Réémission d'un appel API

Vous pouvez également réémettre manuellement un appel API en cliquant sur une entrée de journal. La sortie JSON brute s'affiche alors dans l'appel.

#### Plus d'informations

- ["Documentation sur l'automatisation ONTAP 9"](#)

### Accès au journal de l'API REST

Vous pouvez accéder au journal contenant un enregistrement des appels de l'API REST ONTAP effectués par System Manager. Lors de l'affichage du journal, vous pouvez également réémettre des appels API et vérifier la sortie.

## Étapes

1. En haut de la page, cliquez sur  pour afficher le journal de l'API REST.

Les entrées les plus récentes s'affichent en bas de la page.

2. Sur la gauche, cliquez sur **DASHBOARD** et observez les nouvelles entrées créées pour les appels API émis pour actualiser la page.
3. Cliquez sur **STORAGE**, puis sur **Qtrees**.

Dans ce cas, System Manager génère un appel d'API spécifique pour récupérer la liste des qtrees.

4. Recherchez l'entrée du journal décrivant l'appel API qui a le formulaire :

```
GET /api/storage/qtrees
```

Vous verrez des paramètres de requête HTTP supplémentaires inclus avec l'entrée, tels que `max_records`.

5. Cliquez sur l'entrée du journal pour réémettre l'appel DE L'API GET et afficher la sortie JSON brute.

## Exemple

```
{
 "records": [
 {
 "svm": {
 "uuid": "19507946-e801-11e9-b984-00a0986ab770",
 "name": "SMQA",
 "_links": {
 "self": {
 "href": "/api/svm/svms/19507946-e801-11e9-b984-00a0986ab770"
 }
 }
 },
 "volume": {
 "uuid": "1e173258-f98b-11e9-8f05-00a0986abd71",
 "name": "vol_vol_test2_dest_dest",
 "_links": {
 "self": {
 "href": "/api/storage/volumes/1e173258-f98b-11e9-8f05-00a0986abd71"
 }
 }
 },
 "id": 1,
 "name": "test2",
 "security_style": "mixed",
 "unix_permissions": 777,
 }
]
}
```



```

 "export_policy": {
 "name": "default",
 "id": 12884901889,
 "_links": {
 "self": {
 "href": "/api/protocols/nfs/export-policies/12884901889"
 }
 }
 },
 "path": "/vol_vol_test2_dest_dest/test2",
 "_links": {
 "self": {
 "href": "/api/storage/qtrees/1e173258-f98b-11e9-8f05-00a0986abd71/1"
 }
 }
 },
],
"num_records": 1,
"_links": {
 "self": {
 "href":
"/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"
 }
}
}

```

# L'administration des volumes

## Gestion des volumes et des LUN avec System Manager

### Présentation de l'administration des volumes avec System Manager

Depuis ONTAP 9.7, System Manager peut être utilisé pour gérer le stockage logique, tel que les volumes FlexVol et les LUN, les qtrees, l'efficacité du stockage et les quotas.

Si vous utilisez le Gestionnaire système classique (disponible uniquement dans ONTAP 9.7 et versions antérieures), reportez-vous à la section "[La gestion du stockage logique](#)"

### Gérer les volumes

#### Présentation de la gestion des volumes





Une fois que vous avez affiché une liste de volumes dans System Manager, vous pouvez effectuer différentes actions pour gérer les volumes.



#### Étapes

1. Dans System Manager, cliquez sur **stockage > volumes**.

La liste des volumes s'affiche.

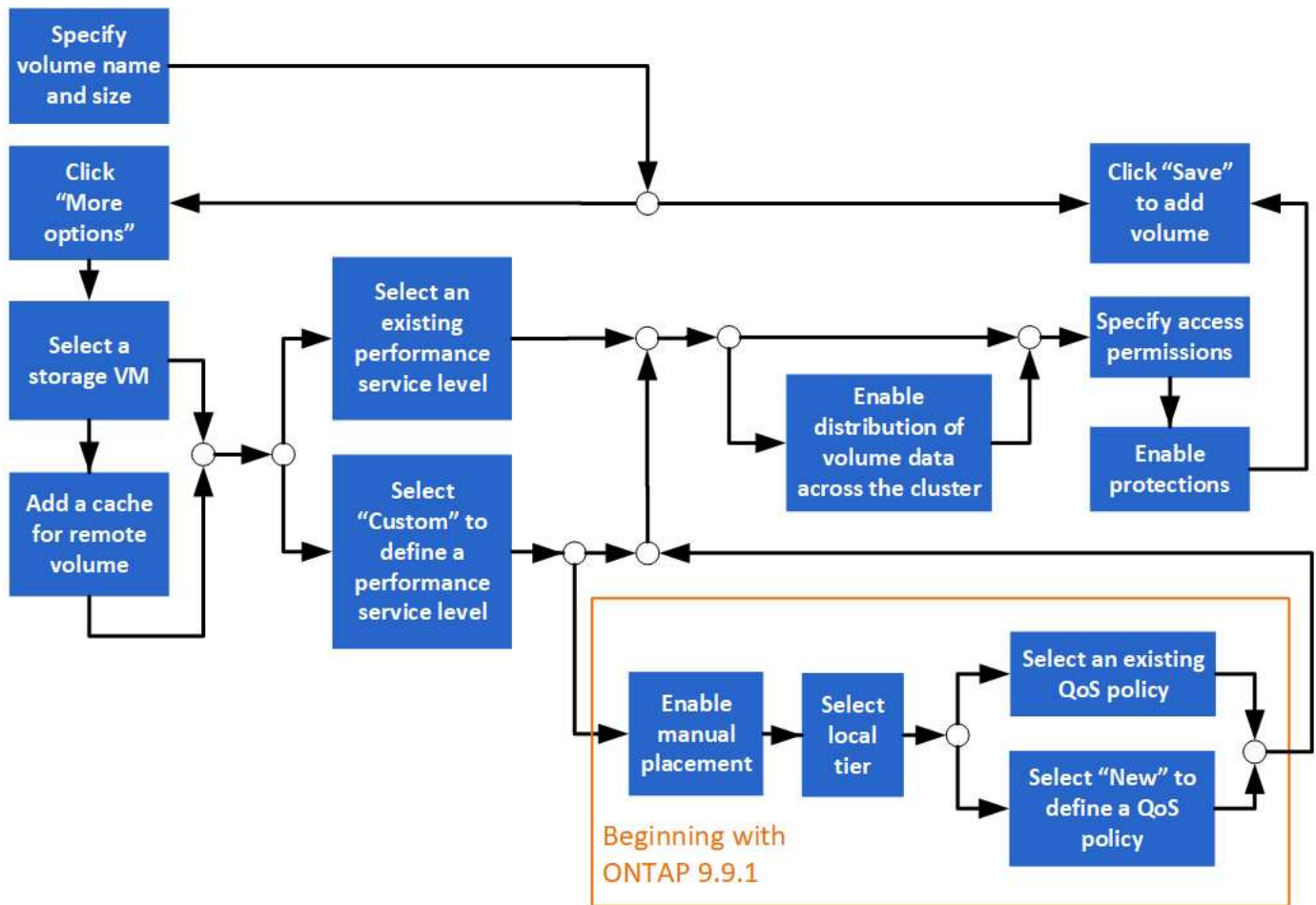
2. Vous pouvez effectuer les opérations suivantes :

| Pour effectuer cette tâche... | Prenez ces mesures...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ajouter un volume             | Cliquez sur  <b>Add</b> . Voir " <a href="#">Ajouter un volume</a> ".                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Gestion de plusieurs volumes  | <p>Cochez les cases en regard des volumes.</p> <ul style="list-style-type: none"><li>• Cliquez sur  <b>Delete</b> pour supprimer les volumes sélectionnés.</li><li>• Cliquez sur  <b>Protect</b> pour affecter une règle de protection aux volumes sélectionnés.</li><li>• Cliquez sur  <b>More</b> pour sélectionner l'une des actions suivantes à effectuer pour tous les volumes sélectionnés :<ul style="list-style-type: none"><li>◦ Activer un quota</li><li>◦ Mettez-le hors ligne</li><li>◦ Déplacer</li><li>◦ Afficher les volumes supprimés</li></ul></li></ul> |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gérer un seul volume | <p>En regard du volume, cliquez sur , puis sélectionnez l'une des actions suivantes à effectuer :</p> <ul style="list-style-type: none"> <li>• Modifier</li> <li>• Redimensionner (à partir de ONTAP 9.10.1, et uniquement pour les volumes en ligne et les volumes DP FlexVol)</li> <li>• Supprimer</li> <li>• Clonage</li> <li>• Mise hors ligne (ou mise en ligne)</li> <li>• Activer un quota (ou désactiver un quota)</li> <li>• Modifier la politique d'exportation</li> <li>• Modifier le chemin de montage</li> <li>• Déplacer</li> <li>• Modifier les paramètres de Tier cloud</li> <li>• Protéger</li> </ul> |
| Renommer un volume   | <p>Vous pouvez renommer un volume à partir de la page de présentation.</p> <p>Cliquez sur  en regard du nom du volume, puis modifiez le nom du volume.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

### Ajouter un volume

Vous pouvez créer un volume et l'ajouter à une VM de stockage existante configurée pour le service NFS ou SMB.



### Avant de commencer

- Une machine virtuelle de stockage configurée pour le service NFS ou SMB doit exister dans le cluster.
- À partir de ONTAP 9.13.1, vous pouvez activer l'analyse de la capacité et le suivi des activités par défaut sur les nouveaux volumes. Dans System Manager, vous pouvez gérer les paramètres par défaut au niveau du cluster ou de la VM de stockage. Pour plus d'informations, voir ["Activez l'analyse du système de fichiers"](#).

### Étapes

1. Accédez à **Storage > volumes**.
2. Sélectionnez **+ Add**.
3. Spécifiez un nom et une taille pour le volume.
4. Effectuez l'une des opérations suivantes :

| Sélectionnez ce bouton... | Pour effectuer cette action...                                                                                      |
|---------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Enregistrer</b>        | Le volume est créé et ajouté à l'aide des valeurs par défaut du système. Aucune étape supplémentaire n'est requise. |
| <b>Plus d'options</b>     | Passez à la section <a href="#">étape 5</a> pour définir les spécifications du volume.                              |

5. le nom et la taille du volume s'affichent si vous les avez préalablement spécifiés. Sinon, entrez le nom et la taille.

6. Sélectionnez une machine virtuelle de stockage dans la liste déroulante.

Seules les machines virtuelles de stockage configurées avec le protocole NFS sont répertoriées. Si une seule machine virtuelle de stockage configurée avec le protocole NFS est disponible, le champ **Storage VM** n'est pas affiché.

7. Pour ajouter un cache pour le volume distant, sélectionnez **Ajouter un cache pour le volume distant** et spécifiez les valeurs suivantes :

- Sélectionnez un cluster.
- Sélectionnez une VM de stockage.
- Sélectionnez le volume que vous souhaitez être un volume de cache.

8. Dans la section **stockage et optimisation**, spécifiez les valeurs suivantes :

- a. La capacité du volume est déjà affichée, mais vous pouvez la modifier.
- b. Dans le champ **Performance Service Level**, sélectionnez un niveau de service :

| Lorsque vous sélectionnez ce niveau de service...                                                                                                                                            | Cela se produit...                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Un niveau de service existant, tel que « Extreme », « Performance » ou « Value ».<br><br>Seuls les niveaux de service valides pour la plateforme système (AFF, FAS ou autres) sont affichés. | Un ou plusieurs niveaux locaux sont automatiquement choisis. Passez à la section <a href="#">Etape 9</a> . |
| Personnalisées                                                                                                                                                                               | Passez à la section <a href="#">étape 8c</a> pour définir un nouveau niveau de service.                    |

- c. ] à partir de ONTAP 9.9.1, vous pouvez utiliser System Manager pour sélectionner manuellement le niveau local sur lequel vous souhaitez placer le volume que vous créez (si vous avez sélectionné le niveau de service « personnalisé »).



Cette option n'est pas disponible si vous sélectionnez **Ajouter comme cache pour un volume distant** ou **distribuer les données de volume sur le cluster** (voir ci-dessous).

| Quand vous faites ce choix... | Procédez comme suit...                                                                                                                                                                                              |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Placement manuel</b>       | Le positionnement manuel est activé. La sélection <b>distribuer les données de volume sur le cluster</b> est désactivée (voir ci-dessous). Passez à la section <a href="#">Etape 8d</a> pour terminer le processus. |
| Pas de sélection              | Le positionnement manuel n'est pas activé. Le niveau local est automatiquement sélectionné. Passez à la section <a href="#">Etape 9</a> .                                                                           |

- a. sélectionnez un niveau local dans le menu déroulant.
- b. Sélectionnez une règle QoS.

Sélectionnez « existant » pour choisir une liste de stratégies existantes ou sélectionnez « Nouveau » pour entrer les spécifications d'une nouvelle police.

9. dans la section **Options d'optimisation**, déterminez si vous souhaitez distribuer les données de volume à travers le cluster :

| Quand vous faites ce choix...                                | Cela se produit...                                                                                                                                        |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Distribuer les données de volume à travers le cluster</b> | Le volume que vous ajoutez devient un volume FlexGroup. Cette option n'est pas disponible si vous avez précédemment sélectionné <b>placement manuel</b> . |
| Pas de sélection                                             | Le volume que vous ajoutez devient par défaut un volume FlexVol.                                                                                          |

10. Dans la section **autorisations d'accès**, spécifiez les autorisations d'accès pour les protocoles pour lesquels le volume est configuré.

Depuis ONTAP 9.11.1, le nouveau volume ne peut pas être partagé par défaut. Vous pouvez spécifier les autorisations d'accès par défaut en vous assurant que les cases à cocher suivantes sont cochées :

- **Exporter via NGS**: Crée le volume avec la politique d'exportation "par défaut" qui accorde aux utilisateurs un accès complet aux données.
- **Partager via SMB/CIFS** : crée un partage avec un nom généré automatiquement, que vous pouvez modifier. L'accès est accordé à « tout le monde ». Vous pouvez également spécifier le niveau d'autorisation.

11. Dans la section **protection**, spécifiez les protections du volume.

- Depuis ONTAP 9.12.1, vous pouvez sélectionner **Activer les copies Snapshot (local)** et choisir une règle de copie Snapshot plutôt que d'utiliser la valeur par défaut.
- Si vous sélectionnez **Activer SnapMirror (local ou distant)**, spécifiez la stratégie de protection et les paramètres du cluster de destination dans les listes déroulantes.

12. Sélectionnez **Enregistrer**.

Le volume est créé et ajouté au cluster et à la machine virtuelle de stockage.



Vous pouvez également enregistrer les spécifications de ce volume dans un PlayBook Ansible. Pour plus d'informations, consultez la page ["Utilisez les manuels de vente Ansible pour ajouter ou modifier des volumes ou des LUN"](#).

## Attribuez des balises aux volumes

Depuis ONTAP 9.14.1, System Manager permet d'attribuer des balises aux volumes pour identifier les objets appartenant à une catégorie, tels que des projets ou des centres de coûts.

### Description de la tâche

Vous pouvez attribuer une balise à un volume. Tout d'abord, vous devez définir et ajouter la balise. Vous pouvez ensuite modifier ou supprimer la balise.

Des balises peuvent être ajoutées lorsque vous créez un volume ou ultérieurement.

Vous définissez une balise en spécifiant une clé et en lui associant une valeur au format « `key:value` ». Par exemple : « `dept:engineering` » ou « `location:san-jose` ».

Les éléments suivants doivent être pris en compte lors de la création de balises :

- Les clés ont une longueur minimale d'un caractère et ne peuvent pas être nulles. Les valeurs peuvent être nulles.
- Une clé peut être associée à plusieurs valeurs en séparant les valeurs par une virgule, par exemple, « emplacement:san-jose,toronto ».
- Les balises peuvent être utilisées pour plusieurs ressources.
- Les touches doivent commencer par une lettre minuscule.
- Les balises attribuées aux volumes seront supprimées lors de la suppression du volume.
- Les balises ne sont pas restaurées si un volume est récupéré de la file d'attente de restauration.
- Les balises sont conservées si le volume est déplacé ou cloné.
- Les balises attribuées aux VM de stockage dans une relation de reprise sur incident sont répliquées sur le volume du site partenaire.

Étapes


Pour gérer les balises, procédez comme suit :

1. Dans System Manager, cliquez sur **volumes**, puis sélectionnez le volume auquel vous souhaitez ajouter une balise.

Les balises sont répertoriées dans la section **Tags**.

2. Cliquez sur **gérer les balises** pour modifier les balises existantes ou en ajouter de nouvelles.

Vous pouvez ajouter, modifier ou supprimer les balises.

| Pour effectuer cette action... | Procédez comme suit...                                                                                                                                                                          |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ajouter une balise             | <div>a. Cliquez sur <b>Ajouter une balise</b>.</div> <div>b. Spécifiez une clé et sa ou ses valeurs (séparez les valeurs par des virgules).</div> <div>c. Cliquez sur <b>Enregistrer</b>.</div> |
| Modifier une balise            | <div>a. Modifiez le contenu dans les champs <b>Key</b> et <b>Values (facultatif)</b>.</div> <div>b. Cliquez sur <b>Enregistrer</b>.</div>                                                       |
| Supprimer une balise           | <div>a. Cliquez sur  en regard de l'étiquette que vous souhaitez supprimer.</div>                            |

Restaurer les volumes supprimés

Si vous avez supprimé par erreur un ou plusieurs volumes FlexVol, vous pouvez utiliser System Manager pour restaurer ces volumes. Depuis ONTAP 9.8, vous pouvez également utiliser System Manager pour restaurer des volumes FlexGroup. Vous pouvez également supprimer les volumes de manière permanente en les purgeant.

La durée de conservation des volumes peut être définie au niveau des VM de stockage. Par défaut, la durée

de rétention du volume est définie sur 12 heures.

### Sélection de volumes supprimés

#### Étapes

1. Cliquez sur **Storage > volumes**.
2. Cliquez sur **plus > Afficher les volumes supprimés**.
3. Sélectionnez les volumes et cliquez sur l'action souhaitée pour récupérer ou supprimer définitivement les volumes.

### Réinitialisation des configurations de volume

La suppression d'un volume supprime les configurations associées du volume. La récupération d'un volume ne réinitialise pas toutes les configurations. Effectuez les tâches suivantes manuellement après la restauration d'un volume pour rétablir son état d'origine :

#### Étapes

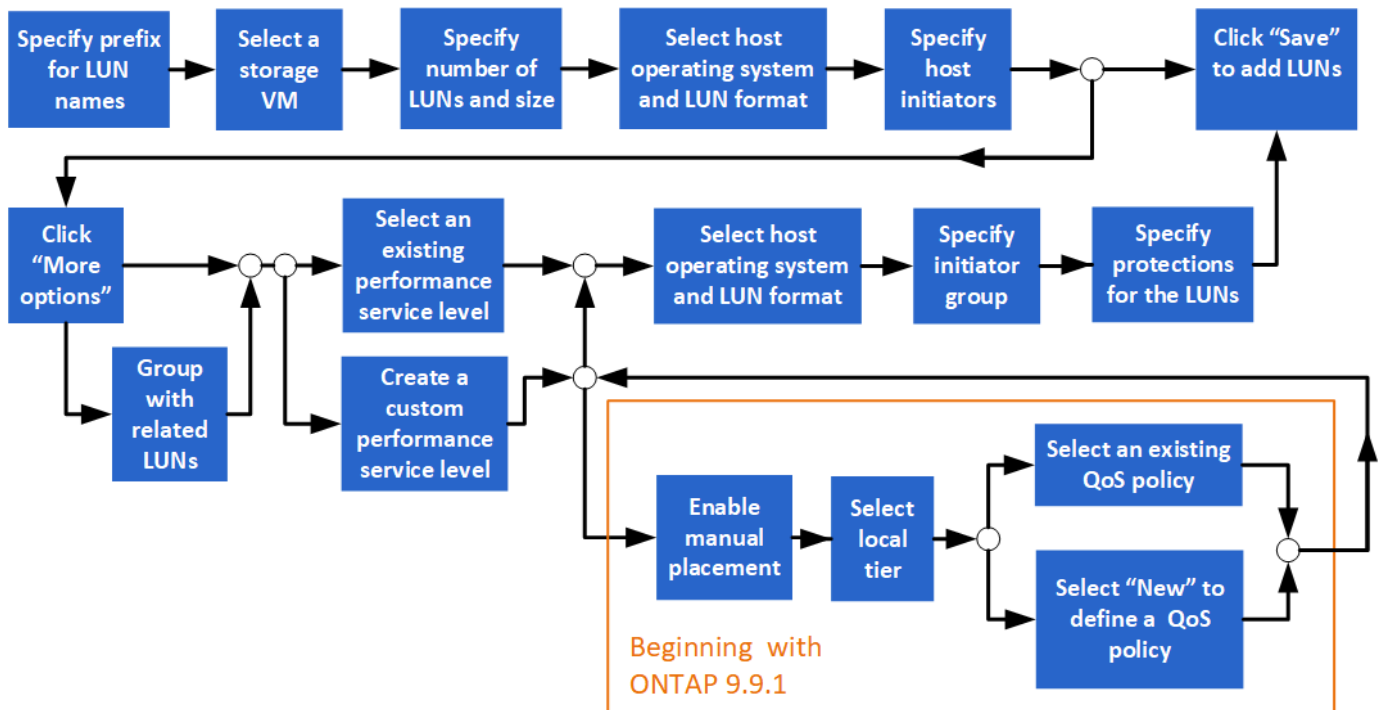
1. Renommez le volume.
2. Configurez un chemin de jonction (NAS).
3. Créez des mappages pour les LUN dans le volume (SAN).
4. Associer une policy Snapshot et export policy avec le volume.
5. Ajouter de nouvelles règles de politique de quotas pour le volume.
6. Ajoutez une règle QoS pour le volume.

## Gérer les LUN

Vous pouvez créer des LUN et les ajouter à une VM de stockage existante configurée avec le protocole SAN. Vous pouvez également grouper des LUN ou les renommer.

### Ajouter des LUN





## Avant de commencer

Une machine virtuelle de stockage configurée pour le service SAN doit exister dans le cluster.

## Étapes

1. Accédez à **stockage > LUN**.
2. Cliquez sur **+ Add**.
3. Spécifiez un préfixe qui sera utilisé au début de chaque nom de LUN. (Si vous créez une seule LUN, entrez le nom de la LUN.)
4. Sélectionnez une machine virtuelle de stockage dans la liste déroulante.

Seules les machines virtuelles de stockage configurées pour le protocole SAN sont répertoriées. Si une seule machine virtuelle de stockage configurée pour le protocole SAN est disponible, le champ **Storage VM** n'est pas affiché.

5. Indiquez le nombre de LUN à créer et la taille de chaque LUN.
6. Sélectionnez le système d'exploitation hôte et le format de LUN dans les listes déroulantes.
7. Entrez les initiateurs hôtes et séparez-les par des virgules.
8. Effectuez l'une des opérations suivantes :

| Cliquez sur ce bouton... | Pour effectuer cette action...                                                                                                                                                               |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enregistrer</b>       | Les LUN sont créées avec les spécifications que vous avez saisies. Les valeurs par défaut du système sont utilisées pour d'autres spécifications. Aucune étape supplémentaire n'est requise. |
| <b>Plus d'options</b>    | Passez à la section <a href="#">étape 9</a> Pour définir des spécifications supplémentaires pour les LUN.                                                                                    |

9. le préfixe de LUN est déjà affiché si vous le saisissez précédemment, mais vous pouvez le modifier. Sinon, entrez le préfixe.

10. Sélectionnez une machine virtuelle de stockage dans la liste déroulante.

Seules les machines virtuelles de stockage configurées pour le protocole SAN sont répertoriées. Si une seule machine virtuelle de stockage configurée pour le protocole SAN est disponible, le champ **Storage VM** n'est pas affiché.

11. Déterminez le mode de regroupement des LUN :

| Quand vous faites ce choix...   | Cela se produit...                                                                         |
|---------------------------------|--------------------------------------------------------------------------------------------|
| <b>Groupe avec LUN connexes</b> | Les LUN seront regroupées avec les LUN associées sur un volume existant du VM de stockage. |
| Pas de sélection                | Les LUN seront regroupées sur un volume appelé « conteneur ».                              |

12. Dans la section **stockage et optimisation**, spécifiez les valeurs suivantes :

a. Le nombre et la capacité des LUN sont déjà affichés si vous les avez précédemment saisies, mais vous pouvez les modifier. Sinon, saisissez les valeurs.

b. Dans le champ **Performance Service Level**, sélectionnez un niveau de service :

| Lorsque vous sélectionnez ce niveau de service...                                                                                                                                            | Cela se produit...                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Un niveau de service existant, tel que « Extreme », « Performance » ou « Value ».<br><br>Seuls les niveaux de service valides pour la plateforme système (AFF, FAS ou autres) sont affichés. | Un niveau local est automatiquement choisi. Passez à la section <a href="#">Etape 13</a> . |
| Personnalisées                                                                                                                                                                               | Passez à la section <a href="#">[step12c]</a> pour définir un nouveau niveau de service.   |

c. ] en commençant par ONTAP 9.9.1, vous pouvez utiliser System Manager pour sélectionner manuellement le niveau local sur lequel vous souhaitez placer les LUN que vous créez (si vous avez sélectionné le niveau de service « personnalisé »).

| Quand vous faites ce choix... | Procédez comme suit...                                                                                                                   |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Placement manuel</b>       | Le positionnement manuel est activé. Passez à la section <a href="#">Etape 12d</a> pour terminer le processus.                           |
| Pas de sélection              | La sélection manuelle n'est pas activée. Le niveau local est automatiquement sélectionné. Passez à la section <a href="#">Etape 13</a> . |

d. sélectionnez un niveau local dans le menu déroulant.

e. Sélectionnez une règle QoS.

Sélectionnez « existant » pour choisir une liste de stratégies existantes ou sélectionnez « Nouveau » pour entrer les spécifications d'une nouvelle police.

13. dans la section **Host information**, le système d'exploitation hôte et le format LUN sont déjà affichés, mais vous pouvez les modifier.

14. Sous **Host Mapping**, sélectionnez le type d'initiateurs pour les LUN :

- **Groupe initiateur existant** : sélectionnez un groupe initiateur pour la liste qui s'affiche.
- **Nouveau groupe initiateur utilisant des groupes initiateurs existants** : spécifiez le nom du nouveau groupe et sélectionnez le ou les groupes que vous souhaitez utiliser pour créer le nouveau groupe.
- **Initiateurs hôtes** : spécifiez un nom dans le nouveau groupe initiateur, puis cliquez sur **+Ajouter initiateur** pour ajouter des initiateurs au groupe.

15. Dans la section **protection**, spécifiez les protections pour les LUN.

Si vous sélectionnez **Activer SnapMirror (local ou distant)**, spécifiez la stratégie de protection et les paramètres du cluster de destination dans les listes déroulantes.

16. Cliquez sur **Enregistrer**.

Les LUN sont créées et ajoutées au cluster et à la machine virtuelle de stockage.




Vous pouvez également enregistrer les spécifications de ces LUN dans un PlayBook Ansible. Pour plus d'informations, consultez la page ["Utilisez les manuels de vente Ansible pour ajouter ou modifier des volumes ou des LUN"](#).

## Renommer une LUN

Vous pouvez renommer une LUN à partir de la page de présentation.

### Étapes

1. Dans System Manager, cliquez sur **LUN**.
2. Cliquez sur  en regard du nom de la LUN à renommer, puis modifiez le nom de cette LUN.
3. Cliquez sur **Enregistrer**.

## Extension du stockage

À l'aide de System Manager, vous pouvez augmenter la taille de votre volume ou de votre LUN afin d'augmenter l'espace disponible pour votre hôte. La taille d'une LUN ne peut pas dépasser la taille du volume contenant.

Depuis ONTAP 9.12.1, lorsque vous saisissez la nouvelle capacité d'un volume, la fenêtre **Resize Volume** affiche l'impact que le redimensionnement du volume aura sur l'espace de données et la réserve de copies Snapshot.

- [Augmenter la taille d'un volume](#)
- [Augmentez la taille d'une LUN](#)

Vous pouvez également ajouter une LUN à un volume existant. Les processus sont différents lors de l'utilisation de System Manager avec ONTAP 9.7 ou 9.8


- [Ajout d'une LUN à un volume existant \(ONTAP 9.7\)](#)
- [Ajout d'une LUN à un volume existant \(ONTAP 9.8\)](#)

Depuis ONTAP 9.8, vous pouvez également utiliser System Manager pour ajouter une LUN à un volume

existant.


## Augmenter la taille d'un volume

### Étapes

1. Cliquez sur **Storage > volumes**.
2. Placez le pointeur de la souris sur le nom du volume que vous souhaitez augmenter.
3. Cliquez sur .
4. Sélectionnez **Modifier**.
5. Augmentez la valeur de capacité.
6. Consultez les détails de l'espace de données **existant** et **Nouveau** et de la réserve d'instantanés.

## Augmentez la taille d'une LUN

### Étapes

1. Cliquez sur **stockage > LUN**.
2. Placez le pointeur de la souris sur le nom de la LUN que vous souhaitez augmenter.
3. Cliquez sur .
4. Sélectionnez **Modifier**.
5. Augmentez la valeur de capacité.

## Ajout d'une LUN à un volume existant (ONTAP 9.7)

Pour utiliser System Manager avec ONTAP 9.7 pour ajouter une LUN à un volume existant, vous devez d'abord passer à la vue classique.

### Étapes

1. Connectez-vous à System Manager dans ONTAP 9.7.
2. Cliquez sur **vue classique**.
3. Sélectionnez **stockage > LUN > Créer**
4. Spécifiez les détails de la création de la LUN.
5. Spécifiez à quel volume ou qtree la LUN doit être ajoutée.

## Ajout d'une LUN à un volume existant (ONTAP 9.8)

Depuis ONTAP 9.8, vous pouvez utiliser System Manager pour ajouter une LUN à un volume existant qui dispose déjà d'une LUN au moins.

### Étapes

1. Cliquez sur **stockage > LUN**.
2. Cliquez sur **Ajouter+**.
3. Renseignez les champs de la fenêtre **Ajouter des LUN**.
4. Sélectionnez **plus d'options**.
5. Cochez la case **Group avec LUN associées**.
6. Dans le champ déroulant, sélectionnez une LUN qui existe sur le volume auquel vous souhaitez ajouter

une autre LUN.

7. Complétez les autres champs. Pour **Host Mapping**, cliquez sur l'un des boutons radio suivants :
  - **Groupe d'initiateurs existant** vous permet de sélectionner un groupe existant dans une liste.
  - **Nouveau groupe initiateur** permet d'entrer un nouveau groupe dans le champ.

## Utilisez la compression, la compaction et la déduplication pour économiser de l'espace de stockage

Pour les volumes de clusters non AFF, vous pouvez exécuter la déduplication, la compression et la compaction des données, ensemble ou de manière indépendante, afin d'optimiser le gain d'espace.

- La déduplication permet d'éliminer les blocs de données dupliqués.
- La compression des données compresse les blocs de données afin de réduire la quantité d'espace de stockage physique nécessaire.
- Efficacité du stockage accrue grâce à la compaction des données qui stocke plus de données dans moins d'espace.



Ces tâches sont prises en charge pour les volumes des clusters non AFF. Depuis ONTAP 9.2, toutes les fonctionnalités d'efficacité du stockage à la volée, telles que la déduplication et la compression à la volée, sont activées par défaut sur les volumes AFF.

### Étapes

1. Cliquez sur **Storage > volumes**.
2. En regard du nom du volume pour lequel vous souhaitez enregistrer le stockage, cliquez sur
3. Cliquez sur **Modifier** et faites défiler jusqu'à **efficacité du stockage**.
4. *Facultatif* : si vous souhaitez activer la déduplication en arrière-plan, cochez la case.
5. *Facultatif* : si vous souhaitez activer la compression en arrière-plan, spécifiez la stratégie d'efficacité du stockage et cochez la case.
6. *Facultatif* : Si vous souhaitez activer la compression en ligne, assurez-vous que la case est cochée.

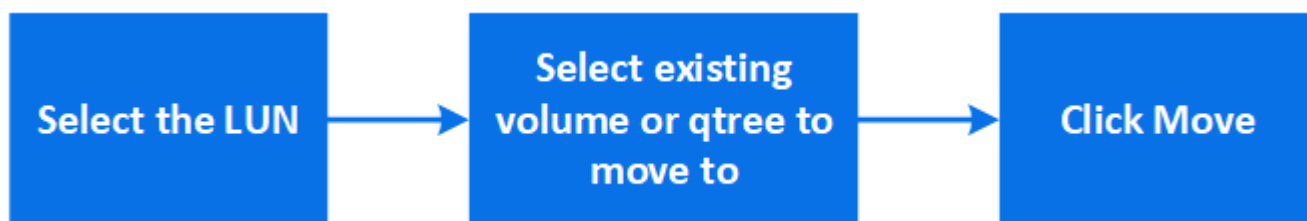
## Équilibrez les charges en déplaçant des LUN

Vous pouvez déplacer une LUN vers un autre volume de la machine virtuelle de stockage pour équilibrer la charge, ou la déplacer vers un volume offrant un niveau de service plus performant pour améliorer les performances.

### Restrictions de déplacement

- Une LUN ne peut pas être déplacée vers un qtree au sein d'un même volume.
- Une LUN créée à partir d'un fichier utilisant l'interface de ligne de commandes ne peut pas être déplacée avec System Manager.
- Les LUN en ligne et servant les données ne peuvent pas être déplacées.
- Les LUN ne peuvent pas être déplacés si l'espace alloué dans le volume de destination ne peut pas contenir la LUN (même si la croissance automatique est activée sur le volume).

- Les LUN des volumes SnapLock ne peuvent pas être déplacées avec System Manager.



### Étapes

1. Cliquez sur **stockage > LUN**.
2. Sélectionnez le LUN à déplacer et cliquez sur **Move**.
3. Sélectionnez un volume existant vers lequel vous souhaitez déplacer la LUN. Si le volume contient des qtrees, sélectionnez le qtree.



Lorsque l'opération de déplacement est en cours, la LUN s'affiche à la fois sur le volume d'origine et sur le volume de destination.

## Équilibrage des charges en déplaçant des volumes vers un autre niveau

Depuis ONTAP 9.8, il est possible d'utiliser System Manager pour déplacer un volume vers un autre niveau afin d'équilibrer la charge.

Depuis ONTAP 9.9.1, vous pouvez également déplacer des volumes sur la base d'une analyse du stockage de données actif et inactif. Pour plus d'informations, voir "[Présentation de l'analytique du système de fichiers](#)".

### Étapes

1. Cliquez sur **Storage > volumes**.
2. Sélectionnez le ou les volumes que vous souhaitez déplacer, puis cliquez sur **Move**.
3. Sélectionnez un niveau (agrégat) existant vers lequel vous souhaitez déplacer le ou les volumes.

## Utilisez les manuels de vente Ansible pour ajouter ou modifier des volumes ou des LUN

Depuis la version ONTAP 9.9.1, vous pouvez utiliser les manuels Ansible pour ajouter ou modifier des volumes ou des LUN avec System Manager.

Cette fonctionnalité vous permet d'utiliser la même configuration plusieurs fois ou d'utiliser la même configuration avec de légères modifications lorsque vous ajoutez ou modifiez des volumes ou des LUN.

### Activer ou désactiver les manuels de vente Ansible

Vous pouvez activer ou désactiver l'utilisation des manuels de vente Ansible dans System Manager.

### Étapes

1. Dans System Manager, accédez aux paramètres de l'interface utilisateur sur la page des paramètres du cluster :

**Cluster > Paramètres**

2. Sous **UI Settings**, réglez le curseur sur "Enabled" ou "Disabled".

## Enregistrez une configuration de volume dans un PlayBook Ansible

Lorsque vous créez ou modifiez la configuration d'un volume, vous pouvez enregistrer cette configuration en tant que fichiers Ansible PlayBook.

### Étapes

1. Ajouter ou modifier le volume :

**Volume > Ajouter** (ou **Volume > Modifier**)

2. Spécifiez ou modifiez les valeurs de configuration du volume.
3. Sélectionnez **Save to Ansible PlayBook** pour enregistrer la configuration dans les fichiers Ansible PlayBook.

Un fichier zip téléchargé contient les fichiers suivants :

- **variable.yaml**: Les valeurs que vous avez saisies ou modifiées pour ajouter ou modifier le volume.
- **volumeAdd.yaml** (ou **volumeEdit.yaml**) : Les cas de test requis pour créer ou modifier les valeurs lors de la lecture des entrées à partir du `variable.yaml` fichier.

## Enregistrez une configuration LUN dans un PlayBook Ansible

Lorsque vous créez ou modifiez la configuration d'une LUN, vous pouvez enregistrer la configuration en tant que fichiers Ansible PlayBook.

### Étapes

1. Ajouter ou modifier la LUN :

**LUN > Ajouter** (ou **LUN > Modifier**)

2. Spécifiez ou modifiez les valeurs de configuration de la LUN.
3. Sélectionnez **Save to Ansible PlayBook** pour enregistrer la configuration dans les fichiers Ansible PlayBook :

Un fichier zip téléchargé contient les fichiers suivants :

- **variable.yaml**: Les valeurs que vous avez saisies ou modifiées pour ajouter ou modifier la LUN.
- **lunAdd.yaml** (ou **lunEdit.yaml**) : Les cas de test requis pour créer ou modifier les valeurs lors de la lecture des entrées à partir du `variable.yaml` fichier.

## Téléchargez les fichiers Ansible PlayBook à partir des résultats de recherche globale

Vous pouvez télécharger les fichiers Ansible PlayBook lorsque vous effectuez une recherche globale.

### Étapes

1. Dans le champ de recherche, entrez "volume", "LUN" ou "manuel".
2. Recherchez le résultat de la recherche, soit « Volume Management (Ansible PlayBook) », soit « LUN Management (Ansible PlayBook) ».
- 3.

Cliquez sur  pour télécharger les fichiers Ansible Playbook.

## Consultez les fichiers Ansible PlayBook

Vous pouvez modifier et exécuter les fichiers Ansible PlayBook pour spécifier les configurations des volumes et des LUN.

### Description de la tâche

Vous utilisez deux fichiers pour effectuer une opération (soit un "ajout" ou une "modification") :

| Les fonctions que vous recherchez... | Utiliser ce fichier de variable... | Et utilisez ce fichier d'exécution... |
|--------------------------------------|------------------------------------|---------------------------------------|
| Ajouter un volume                    | volumeAdd-variable.yaml            | valueAdd.yaml                         |
| Modifier un volume                   | volumeEdit-variable.yaml           | volumeEdit.yaml                       |
| Ajouter une LUN                      | lunAdd-variable.yaml               | lunAdd.yaml                           |
| Modifier une LUN                     | lunEdit-variable.yaml              | lunEdit.yaml                          |

### Étapes

1. Modifiez le fichier de variables.

Le fichier contient les différentes valeurs que vous utilisez pour configurer le volume ou la LUN.

- Si vous ne modifiez pas les valeurs, laissez-les commenter.
- Si vous modifiez les valeurs, supprimez le commentaire.

2. Exécutez le fichier d'exécution associé.

Le fichier RUN contient les cas de test requis pour créer ou modifier les valeurs lors de la lecture des entrées à partir du fichier de variables.

3. Saisissez vos informations de connexion utilisateur.

## Gérez les règles d'efficacité du stockage

Depuis ONTAP 9.8, vous pouvez utiliser System Manager pour activer, désactiver, ajouter, modifier ou supprimer des stratégies d'efficacité pour les machines virtuelles de stockage sur les systèmes FAS.





Cette fonction n'est pas disponible sur les systèmes AFF.

### Étapes

1. Sélectionnez **stockage > machines virtuelles de stockage**
2. Sélectionnez la VM de stockage pour laquelle vous souhaitez gérer les règles d'efficacité.
3. Dans l'onglet **Paramètres**, sélectionnez  dans la section **politique d'efficacité**. Les règles d'efficacité pour cette machine virtuelle de stockage sont affichées.

Vous pouvez effectuer les tâches suivantes :



- **Activer ou désactiver** une stratégie d'efficacité en cliquant sur le bouton bascule dans la colonne État.
- **Ajouter** une stratégie d'efficacité en cliquant sur **Ajouter+**.
- **Modifier** une politique d'efficacité en cliquant sur  à droite du nom de la politique et en sélectionnant **Modifier**.
- **Supprimer** une politique d'efficacité en cliquant sur  à droite du nom de la politique et en sélectionnant **Supprimer**.

## Liste des règles d'efficacité

### • Auto

Spécifie que la déduplication est constamment exécutée en arrière-plan. Cette règle est définie pour tous les volumes nouvellement créés et pour tous les volumes mis à niveau qui n'ont pas été configurés manuellement pour la déduplication en arrière-plan. Si vous changez la politique en "par défaut" ou toute autre politique, la politique "auto" est désactivée.

Lorsqu'un volume est déplacé d'un système non AFF vers un système AFF, la règle « automatique » est activée par défaut sur le nœud de destination. Lorsqu'un volume est déplacé d'un nœud AFF vers un nœud non AFF, la règle « auto » sur le nœud de destination est remplacée par la règle « à la volée uniquement » par défaut.

### • Politique

Spécifie le nom d'une règle d'efficacité.

### • Statut

Spécifie le statut d'une règle d'efficacité. La liste ci-dessous répertorie les différents États de haute disponibilité :

#### ◦ Activé

Spécifie que la politique d'efficacité peut être attribuée à une opération de déduplication.

#### ◦ Désactivé

Spécifie que la stratégie d'efficacité est désactivée. Vous pouvez activer la règle en utilisant le menu déroulant Status et l'attribuer ultérieurement à une opération de déduplication.

### • Exécuter par

Indique si la stratégie d'efficacité du stockage est exécutée selon un planning ou en fonction d'une valeur seuil (seuil du journal des modifications).

### • Politique de qualité de service

Spécifie le type de QoS pour la règle d'efficacité du stockage. La liste ci-dessous répertorie les différents types de QoS :

#### ◦ Contexte

Spécifie que la règle de QoS s'exécute en arrière-plan, ce qui réduit l'impact potentiel sur les performances des opérations client.

- Meilleur effort

Spécifie que la règle de qualité de service s'exécute sur une base meilleur effort, ce qui vous permet d'optimiser l'utilisation des ressources système.

- **Durée maximale**

Spécifie la durée d'exécution maximale d'une règle d'efficacité. Si cette valeur n'est pas spécifiée, la règle d'efficacité est exécutée jusqu'à ce que l'opération soit terminée.

## **Zone de détails**

La zone située sous la liste des stratégies d'efficacité affiche des informations supplémentaires sur la stratégie d'efficacité sélectionnée, notamment le nom du programme et les détails de la planification d'une stratégie basée sur un planning, ainsi que la valeur du seuil d'une stratégie basée sur des seuils.

## **Gérez les ressources à l'aide de quotas**

Depuis ONTAP 9.7, vous pouvez configurer et gérer les quotas d'utilisation avec System Manager.

Si vous utilisez l'interface de ligne de commandes de ONTAP pour configurer et gérer les quotas d'utilisation, reportez-vous à ["Gestion du stockage logique"](#).

Si vous utilisez OnCommand System Manager pour ONTAP 9.7 et les versions antérieures pour configurer et gérer les quotas d'utilisation, reportez-vous à la section suivante pour votre version :

- ["Documentation ONTAP 9.6 et 9.7"](#)
- ["Documentation ONTAP 9.5"](#)
- ["Documentation ONTAP 9.4"](#)
- ["Documentation ONTAP 9.3"](#)
- ["Documentation archivée de ONTAP 9.2"](#)
- ["Documentation archivée de ONTAP 9.0"](#)

## **Présentation des quotas**

Les quotas permettent de limiter ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree. Les quotas group sont appliqués à un volume ou qtree spécifique.

Vous pouvez utiliser les quotas pour suivre et limiter l'utilisation des ressources dans les volumes, et fournir des notifications lorsque l'utilisation des ressources atteint des niveaux spécifiques.

Les quotas peuvent être conditionnels ou inconditionnels. Lors du dépassement de limites définies, les quotas conditionnels entraînent l'envoi d'une notification par ONTAP, tandis que les quotas inconditionnels empêcheront toute opération d'écriture.

## **Définissez des quotas pour limiter l'utilisation des ressources**

Ajoutez des quotas pour limiter la quantité d'espace disque que la cible de quota peut utiliser.

Vous pouvez définir une limite stricte et une limite souple pour un quota.

Les quotas matériels imposent une limite stricte aux ressources système, toute opération qui entraînerait un dépassement de la limite. Les quotas conditionnels envoient un message d'avertissement lorsque l'utilisation des ressources atteint un certain niveau, mais n'affectent pas les opérations d'accès aux données. Vous pouvez ainsi prendre l'action appropriée avant le dépassement du quota.

### Étapes

1. Cliquez sur **stockage > quotas**.
2. Cliquez sur **Ajouter**.

## Cloner des volumes et des LUN à des fins de test

Vous pouvez cloner des volumes et des LUN pour créer des copies temporaires inscriptibles à des fins de test. Les clones reflètent l'état actuel des données à un point dans le temps. Vous pouvez aussi utiliser des clones pour donner aux utilisateurs un accès aux données sans leur donner accès aux données de production.




La licence FlexClone doit être de "installé" sur le système de stockage.

### Clonage d'un volume

Créer un clone d'un volume, comme suit :

#### Étapes


1. Cliquez sur **Storage > volumes**.
2. Cliquez sur  en regard du nom du volume à cloner.
3. Sélectionnez **Clone** dans la liste.
4. Indiquez un nom pour le clone et effectuez les autres sélections.
5. Cliquez sur **Clone** et vérifiez que le clone de volume apparaît dans la liste des volumes.

Vous pouvez également cloner un volume à partir de **Overview** qui s'affiche lorsque vous affichez les détails du volume.

### Clonage d'une LUN

Créer un clone de LUN, comme suit :

#### Étapes

1. Cliquez sur **stockage > LUN**.
2. Cliquez sur  en regard du nom de la LUN à cloner.
3. Sélectionnez **Clone** dans la liste.
4. Indiquez un nom pour le clone et effectuez les autres sélections.
5. Cliquez sur **Clone** et vérifiez que le clone de LUN apparaît dans la liste des LUN.

Vous pouvez également cloner une LUN à partir de la **Présentation** qui s'affiche lorsque vous affichez les détails de la LUN.

Lorsque vous créez un clone de LUN, System Manager active automatiquement la suppression du clone lorsque de l'espace est nécessaire.

## Rechercher, filtrer et trier les informations dans System Manager

Vous pouvez rechercher différentes actions, objets et informations dans System Manager. Vous pouvez également rechercher des entrées spécifiques dans les données de la table.

System Manager propose deux types de recherche :

- [Recherche globale](#)

Lorsque vous saisissez un argument de recherche dans le champ en haut de chaque page, System Manager effectue une recherche dans l'interface pour trouver des correspondances. Vous pouvez ensuite trier et filtrer les résultats.


Depuis la version ONTAP 9.12.1, System Manager fournit également les résultats de recherche du site de support NetApp afin de fournir des liens vers les informations de support pertinentes.

- [Recherche par table-grid](#)

À partir de ONTAP 9.8, lorsque vous saisissez un argument de recherche dans le champ en haut d'une grille de table, System Manager recherche uniquement les colonnes et les lignes de cette table pour trouver les correspondances.

### Recherche globale

En haut de chaque page de System Manager, vous pouvez utiliser un champ de recherche globale pour rechercher divers objets et actions dans l'interface. Par exemple, vous pouvez rechercher différents objets par nom, pages disponibles dans la colonne du navigateur (à gauche), diverses actions, telles que « Ajouter un volume » ou « Ajouter une licence », et des liens vers des rubriques d'aide externes. Vous pouvez également filtrer et trier les résultats.



Pour de meilleurs résultats, effectuez une recherche, un filtrage et un tri une minute après la connexion et cinq minutes après la création, la modification ou la suppression d'un objet.

### Obtention des résultats de la recherche

La recherche n'est pas sensible à la casse. Vous pouvez entrer diverses chaînes de texte pour trouver la page, les actions ou les rubriques d'information dont vous avez besoin. Jusqu'à 20 résultats sont répertoriés. Si d'autres résultats sont trouvés, vous pouvez cliquer sur **Afficher plus** pour afficher tous les résultats. Les exemples suivants décrivent les recherches types :

| Type de recherche | Exemple de chaîne de recherche | Exemple de résultats de recherche                                                                                                                                                              |
|-------------------|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Par nom d'objet   | vol._                          | Vol_lun_dest sur la machine virtuelle de stockage : svm0 (volume)<br>/Vol/vol...est1/lun sur la machine virtuelle de stockage : svm0 (LUN)<br>Svm0:vol_lun_dest1 rôle : destination (relation) |

|                                  |            |                                                                                                                                  |
|----------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------|
| Par emplacement dans l'interface | volumétrie | Ajouter un volume (action)<br>Protection – Présentation (page)<br>Récupérer le volume supprimé (aide)                            |
| Par actions                      | autres     | Ajouter un volume (action)<br>Réseau – Présentation (page)<br>Extension de volumes et de LUN (aide)                              |
| Par contenu d'aide               | san        | Stockage – Présentation (page)<br>Présentation DU SAN (aide)<br>Provisionnement du stockage SAN pour les bases de données (aide) |

### Résultats de la recherche globale sur le site de support NetApp



Depuis ONTAP 9.12.1, System Active IQ Manager affiche une autre colonne de résultats contenant des liens vers le site de support NetApp, notamment les informations sur les produits System Manager.

Les résultats de la recherche contiennent les informations suivantes :

- **Titre** de l'information qui est un lien vers le document en format HTML, PDF, EPUB ou autre.
- **Type de contenu**, qui indique s'il s'agit d'un sujet de documentation produit, d'un article de la base de connaissances ou d'un autre type d'information.
- **Description sommaire** du contenu.
- **Créé** date de sa première publication.
- **Mis à jour** date à laquelle il a été mis à jour pour la dernière fois.

Vous pouvez effectuer les opérations suivantes :

| Action                                                                                        | Résultat                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cliquez sur <b>ONTAP System Manager</b> , puis saisissez du texte dans le champ de recherche. | Les résultats de recherche incluent des informations sur le site de support NetApp relatives à System Manager.                                                                                                                                                      |
| Cliquez sur <b>tous les produits</b> , puis entrez du texte dans le champ de recherche.       | Les résultats de recherche incluent des informations sur le site de support NetApp pour tous les produits NetApp, et pas seulement pour System Manager.                                                                                                             |
| Cliquez sur un résultat de recherche.                                                         | Les informations provenant du site de support NetApp sont affichées dans une fenêtre de navigateur ou un onglet distinct.                                                                                                                                           |
| Cliquez sur <b>Voir plus de résultats</b> .                                                   | S'il y a plus de dix résultats, vous pouvez cliquer sur <b>Voir plus de résultats</b> après le dixième résultat pour afficher plus de résultats. Chaque fois que vous cliquez sur <b>Voir plus de résultats</b> , dix autres résultats s'affichent, le cas échéant. |


|                                                                                                 |                                                                                                                                           |
|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Copiez le lien.                                                                                 | Le lien est copié dans le presse-papiers. Vous pouvez coller le lien dans un fichier ou dans une fenêtre de navigateur.                   |
| Cliquez sur  . | Le panneau sur lequel les résultats sont affichés est épinglé de sorte qu'il reste affiché lorsque vous travaillez dans un autre panneau. |
| Cliquez sur  . | Le panneau de résultats n'est plus épinglé et est fermé.                                                                                  |

### Filtrage des résultats de recherche

Vous pouvez affiner les résultats à l'aide de filtres, comme illustré dans les exemples suivants :

| Filtre                 | Syntaxe                                        | Exemple de chaîne de recherche |
|------------------------|------------------------------------------------|--------------------------------|
| Par type d'objet       | <type> :<nom de l'objet>                       | volume:vol_2                   |
| Par taille d'objet     | <type><symbole de taille><numéro><unités>      | lun < 500 mo                   |
| Par des disques cassés | « disque défectueux » ou « disque défectueux » | disque défectueux              |
| Par interface réseau   | <adresse IP>                                   | 172.22.108.21                  |

### Tri des résultats de la recherche

Lorsque vous affichez tous les résultats de recherche, ils sont triés par ordre alphabétique. Vous pouvez trier les résultats en cliquant sur et en  **Filter** sélectionnant le mode de tri des résultats.

### Recherche par table-grid

Depuis ONTAP 9.8, chaque fois que System Manager affiche les informations au format tableau, un bouton de recherche s'affiche en haut du tableau.

Lorsque vous cliquez sur **Rechercher**, un champ de texte apparaît dans lequel vous pouvez entrer un argument de recherche. System Manager recherche la table entière et affiche uniquement les lignes qui contiennent du texte correspondant à votre argument de recherche.

Vous pouvez utiliser un astérisque ( \* ) comme caractère générique pour remplacer les caractères. Par exemple, recherche de vol\* peut fournir des lignes qui contiennent les éléments suivants :

- Vol\_122\_D9
- vol\_lun\_des1
- vol2866
- volspec1
- vol\_dest\_765
- volumétrie
- volume\_new4
- volume

## Mesures de la capacité dans System Manager

La capacité du système peut être mesurée soit en tant qu'espace physique, soit en tant qu'espace logique. Depuis ONTAP 9.7, System Manager mesure la capacité physique et logique.

Les différences entre les deux mesures sont expliquées dans les descriptions suivantes :

- **Capacité physique** : l'espace physique fait référence aux blocs physiques de stockage utilisés dans le volume ou le niveau local. La valeur de la capacité physique utilisée est généralement inférieure à la valeur de la capacité logique utilisée grâce à la réduction des données provenant des fonctionnalités d'efficacité du stockage (telles que la déduplication et la compression).
- **Capacité logique** : l'espace logique fait référence à l'espace utilisable (les blocs logiques) dans un volume ou un niveau local. L'espace logique désigne la manière dont l'espace théorique peut être utilisé, sans tenir compte des résultats obtenus grâce à la déduplication ou à la compression. La valeur de l'espace logique utilisé est issue de la quantité d'espace physique utilisé, plus les économies réalisées grâce aux fonctionnalités d'efficacité du stockage (telles que la déduplication et la compression) qui ont été configurées. Cette mesure est souvent supérieure à la capacité physique utilisée, car elle inclut des copies Snapshot, des clones et d'autres composants, et ne reflète pas la compression des données et autres réductions de l'espace physique. La capacité logique totale peut donc être supérieure à l'espace provisionné.



Dans System Manager, les représentations de capacité ne prennent pas en compte les capacités du niveau de stockage racine (agrégat).

## Mesures de la capacité utilisée

Les mesures de la capacité utilisée s'affichent différemment en fonction de la version de System Manager que vous utilisez, comme expliqué dans le tableau ci-dessous :

| Version de System Manager     | Terme utilisé pour la capacité | Type de capacité visé                                                                  |
|-------------------------------|--------------------------------|----------------------------------------------------------------------------------------|
| 9.9.1 et versions ultérieures | Utilisation logique            | Espace logique utilisé<br>(si les paramètres d'efficacité du stockage ont été activés) |
| 9.7 et 9.8                    | Utilisé                        | Espace logique utilisé<br>(si les paramètres d'efficacité du stockage ont été activés) |
| 9.5 et 9.6<br>(Vue classique) | Utilisé                        | Espace physique utilisé                                                                |

## Termes de mesure de la capacité

Les termes suivants sont utilisés pour décrire la capacité :

- **Capacité allouée** : quantité d'espace allouée aux volumes d'une machine virtuelle de stockage.
- **Disponible** : quantité d'espace physique disponible pour stocker des données ou provisionner des volumes dans une machine virtuelle de stockage ou sur un niveau local.

- **Capacité sur les volumes** : somme du stockage utilisé et du stockage disponible de tous les volumes sur une machine virtuelle de stockage.
- **Données client** : quantité d'espace utilisée par les données client (physique ou logique).
  - Depuis ONTAP 9.13.1, la capacité utilisée par les données client est appelée **logique utilisée** et la capacité utilisée par les copies Snapshot est affichée séparément.
  - Dans ONTAP 9.12.1 et versions antérieures, la capacité utilisée par les données client ajoutées à la capacité utilisée par les copies Snapshot est appelée **logique utilisée**.
- **Validé** : le montant de la capacité engagée pour un niveau local.
- **Réduction des données** :
  - À partir de ONTAP 9.13.1, les taux de réduction des données sont affichés comme suit :
    - La valeur de réduction des données affichée sur le panneau **capacité** correspond au rapport entre l'espace logique utilisé et l'espace physique utilisé, sans tenir compte des réductions significatives obtenues lors de l'utilisation de fonctionnalités d'efficacité du stockage, telles que les copies Snapshot.
    - Lorsque vous affichez le panneau de détails, vous voyez à la fois le ratio affiché sur le panneau de vue d'ensemble et le ratio global de tout l'espace utilisé logique par rapport à l'espace physique utilisé. Appelé **avec les copies Snapshot**, cette valeur inclut les avantages découlant de l'utilisation des copies Snapshot et d'autres fonctionnalités d'efficacité du stockage.
  - Dans la ONTAP 9.12.1 et les versions antérieures, les taux de réduction des données sont affichés comme suit :
    - La valeur de réduction des données affichée sur le panneau **capacité** correspond au rapport global de tout l'espace logique utilisé par rapport à l'espace physique utilisé, et elle inclut les avantages découlant de l'utilisation des copies Snapshot et d'autres fonctionnalités d'efficacité du stockage.
    - Lorsque vous affichez le panneau de détails, vous voyez à la fois le ratio **global** qui était affiché sur le panneau de vue d'ensemble et le rapport de l'espace logique utilisé uniquement par les données client par rapport à l'espace physique utilisé uniquement par les données client, appelé **sans copies Snapshot et clones**.
- **Logique utilisée** :
  - Depuis ONTAP 9.13.1, la capacité utilisée par les données client est appelée **logique utilisée** et la capacité utilisée par les copies Snapshot est affichée séparément.
  - Dans ONTAP 9.12.1 et versions antérieures, la capacité utilisée par les données client ajoutées à la capacité utilisée par les copies Snapshot est appelée **logique utilisée**.
- **Logical Used %** : pourcentage de la capacité logique utilisée actuelle par rapport à la taille provisionnée, à l'exclusion des réserves snapshot. Cette valeur peut être supérieure à 100 %, grâce aux économies en termes d'efficacité réalisées dans le volume.
- **Capacité maximale** : quantité maximale d'espace allouée aux volumes sur une machine virtuelle de stockage.
- **Physical Used**: La capacité utilisée dans les blocs physiques d'un volume ou d'un niveau local.
- **Physical Used %** : pourcentage de capacité utilisée dans les blocs physiques d'un volume par rapport à la taille provisionnée.
- **Capacité provisionnée** : un système de fichiers (volume) qui a été alloué à partir d'un système Cloud Volumes ONTAP et est prêt à stocker les données des utilisateurs ou des applications.
- **Réservé** : espace réservé pour les volumes déjà provisionnés dans un niveau local.
- **Utilisé**: La quantité d'espace qui contient des données.



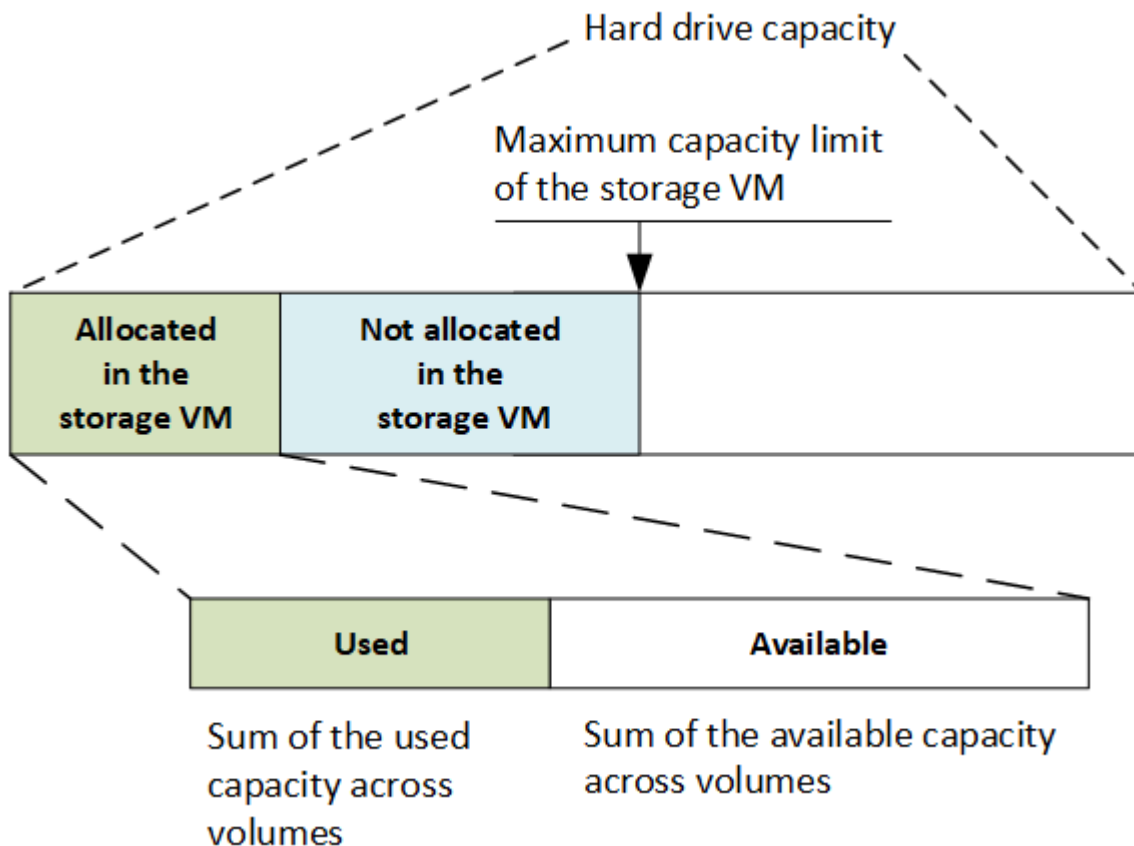
- **Utilisé et réservé** : somme de l'espace physique utilisé et réservé.

## Capacité d'une VM de stockage

La capacité maximale d'une machine virtuelle de stockage est déterminée par l'espace total alloué aux volumes plus l'espace restant non alloué.

- L'espace alloué aux volumes correspond à la somme de la capacité utilisée et de la capacité disponible des volumes FlexVol, des volumes FlexGroup et des volumes FlexCache.
- La capacité des volumes est incluse dans les sommes, même lorsqu'elles sont restreintes, hors ligne ou dans la file d'attente de restauration après suppression.
- Si les volumes sont configurés avec l'extension automatique, la valeur de taille automatique maximale du volume est utilisée dans les sommes. Sans croissance automatique, la capacité réelle du volume est utilisée dans les sommes.

Le tableau suivant explique comment la mesure de la capacité sur l'ensemble des volumes est liée à la limite de capacité maximale.



À partir de ONTAP 9.13.1, les administrateurs du cluster peuvent "[Limiter la capacité maximale pour une VM de stockage](#)". Toutefois, il est impossible de définir des limites de stockage pour une VM de stockage qui contient des volumes destinés à la protection des données, dans une relation SnapMirror ou dans une configuration MetroCluster. De même, les quotas ne peuvent pas être configurés pour dépasser la capacité maximale d'une machine virtuelle de stockage.


Une fois la limite de capacité maximale définie, elle ne peut pas être modifiée pour obtenir une taille inférieure à la capacité actuellement allouée.

Lorsqu’une machine virtuelle de stockage atteint sa capacité maximale, certaines opérations ne peuvent pas être effectuées. System Manager fournit des suggestions pour les étapes suivantes de "Aperçus ".

Unités de mesure de la capacité

System Manager calcule la capacité de stockage en fonction des unités binaires de 1024 (2<sup>10</sup>) octets.

- À partir de la version ONTAP 9.10.1, les unités de capacité de stockage sont affichées dans System Manager sous la forme KiB, MiB, GiB, TiB et PiB.
- Dans ONTAP 9.10.0 et les versions antérieures, ces unités sont affichées dans System Manager sous la forme de Ko, Mo, Go, To et po.



Les unités utilisées dans System Manager pour le débit continuent à être les Ko/s, Mo/s, Go/s, To/s et po/s pour toutes les versions des systèmes ONTAP.

| Unité de capacité affichée dans System Manager pour ONTAP 9.10.0 et versions antérieures | Unité de capacité affichée dans System Manager pour ONTAP 9.10.1 et versions ultérieures | Calcul                           | Valeur en octets             |
|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|----------------------------------|------------------------------|
| KO                                                                                       | Kio                                                                                      | 1024                             | 1024 octets                  |
| MO                                                                                       | Mio                                                                                      | 1024 * 1024                      | 1,048,576 octets             |
| GO                                                                                       | Gio                                                                                      | 1024 * 1024 * 1024               | 1,073,741,824 octets         |
| TO                                                                                       | Tio                                                                                      | 1024 * 1024 * 1024 * 1024        | 1,099,511,627,776 octets     |
| PO                                                                                       | Pio                                                                                      | 1024 * 1024 * 1024 * 1024 * 1024 | 1,125,899,906,842,624 octets |

Informations associées

- "Contrôle de la capacité dans System Manager"
- "Création de rapports sur l'espace logique et application des volumes"

Gestion du stockage logique avec l’interface de ligne de commandes

Présentation de la gestion du stockage logique avec l’interface de ligne de commande

L’interface de ligne de commande ONTAP vous permet de créer et de gérer des volumes FlexVol, d’utiliser la technologie FlexClone pour créer des copies efficaces de volumes, de fichiers et de LUN, de créer des qtrees et des quotas, et de gérer des fonctionnalités d’efficacité comme la déduplication et la compression.

Vous devez utiliser ces procédures dans les circonstances suivantes :

- Vous souhaitez connaître la gamme de fonctionnalités de volumes ONTAP FlexVol et de fonctionnalités d'efficacité du stockage ?
- Vous souhaitez utiliser l'interface de ligne de commande et non System Manager, ni un outil de création de scripts automatisé.

## Création et gestion des volumes

### Créer un volume

Vous pouvez créer un volume et spécifier son point de jonction et d'autres propriétés en utilisant le `volume create` commande.

#### Description de la tâche

Un volume doit inclure une *Junction path* pour que ses données soient mises à disposition des clients. Vous pouvez spécifier le chemin de jonction lorsque vous créez un nouveau volume. Si vous créez un volume sans spécifier un chemin de jonction, vous devez *mount* le volume du namespace du SVM à l'aide de `volume mount` commande.

#### Avant de commencer

- Le SVM pour le nouveau volume et l'agrégat qui fournira le stockage au volume doivent déjà exister.
- Si le SVM possède une liste d'agrégats associés, l'agrégat doit figurer dans la liste.
- À partir de ONTAP 9.13.1, vous pouvez créer des volumes dont l'analyse de la capacité et le suivi des activités sont activés. Pour activer le suivi de la capacité ou des activités, exécutez le `volume create` commande avec `-analytics-state` ou `-activity-tracking-state` réglés sur `on`.

Pour en savoir plus sur l'analyse de la capacité et le suivi des activités, reportez-vous à la section ["Activez l'analyse du système de fichiers"](#).

### Étapes

#### 1. Créer un volume :

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -user
user_name_or_number -group group_name_or_number -junction-path junction_path
[-policy export_policy_name]
```

Le `-security style`, `-user`, `-group`, `-junction-path`, et `-policy` Les options ne s'applique qu'aux espaces de noms NAS.

Les choix pour `-junction-path` sont les suivants :

- Directement sous la racine, par exemple, `/new_vol`

Vous pouvez créer un nouveau volume et préciser qu'il peut être monté directement sur le volume root du SVM.

- Sous un répertoire existant, par exemple, `/existing_dir/new_vol`

Vous pouvez créer un nouveau volume et spécifier qu'il doit être monté sur un volume existant (dans

une hiérarchie existante), exprimé en tant que répertoire.

Si vous souhaitez créer un volume dans un nouveau répertoire (dans une nouvelle hiérarchie sous un nouveau volume), par exemple, /new\_dir/new\_vol, Ensuite, vous devez d'abord créer un nouveau volume parent qui est relié par une jonction au volume racine de la SVM. Vous devez ensuite créer le nouveau volume enfant dans la Junction path du nouveau volume parent (nouveau répertoire).

2. Vérifier que le volume a été créé avec le point de jonction souhaité :

```
volume show -vserver svm_name -volume volume_name -junction
```

## Exemples

La commande suivante crée un volume nommé users1 sur le SVM vs1.example.com et l'agrégat aggr1. Le nouveau volume est disponible sur le site /users. Le volume a une taille de 750 Go et sa garantie de volume est de type volume (par défaut).

```
cluster1::> volume create -vserver vs1.example.com -volume users1
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users1 -junction
```

|                 |        | Junction |               | Junction    |
|-----------------|--------|----------|---------------|-------------|
| Vserver         | Volume | Active   | Junction Path | Path Source |
| vs1.example.com | users1 | true     | /users        | RW_volume   |

La commande suivante crée un nouveau volume nommé « maison 4 » sur la SVM « vs1.example.com » et l'agrégat « aggr1 ». Le répertoire /eng/ Existe déjà dans l'espace de nommage de la SVM vs1, et le nouveau volume est mis à disposition à /eng/home, qui devient le répertoire de base de l' /eng/ espace de noms. Le volume a une taille de 750 Go et sa garantie de volume est de type volume (par défaut).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
```

|                 |        | Junction |               | Junction    |
|-----------------|--------|----------|---------------|-------------|
| Vserver         | Volume | Active   | Junction Path | Path Source |
| vs1.example.com | home4  | true     | /eng/home     | RW_volume   |

## Prise en charge de volumes importants et de fichiers volumineux

Depuis la version ONTAP 9.12.1 P2, vous pouvez créer un nouveau volume ou modifier un volume existant pour prendre en charge une taille de volume maximale de 300 To et une taille de fichier (LUN) maximale de 128 To.

## Avant de commencer

- ONTAP 9.12.1 P2 ou version ultérieure est installé sur le cluster.
- Si vous activez la prise en charge de grands volumes sur le cluster source dans une relation SnapMirror, ONTAP 9.12.1 P2 ou version ultérieure doit être installé sur le cluster hébergeant le volume source ainsi que sur le cluster hébergeant le volume de destination.
- Vous êtes administrateur de cluster ou SVM.

## Créez un nouveau volume

### Étape

1. Créer un volume avec la prise en charge de gros volumes et fichiers activée :

```
volume create -vserver <svm_name> -volume <volume_name> -aggregate
<aggregate_name> -is-large-size-enabled true
```

### Exemple

L'exemple suivant crée un nouveau volume avec la prise en charge de grands volumes et de fichiers activée.

```
volume create -vserver vs1 -volume big_vol1 -aggregate aggr1 -is-large
-size-enabled true
```

## Modifier un volume existant

### Étape

1. Modifiez un volume pour activer la prise en charge de gros volumes et fichiers :

```
volume modify -vserver <svm_name> -volume <volume_name> -is-large-size
-enabled true
```

### Exemple

L'exemple suivant modifie un volume existant pour prendre en charge un volume et une taille de fichier importants.

```
volume modify -vserver vs2 -volume data_vol -is-large-size-enabled true
```

## Informations associées

- ["Créer un volume"](#)
- ["Référence de commande"](#)

## Volumes SAN

ONTAP propose plusieurs options de base pour le provisionnement des volumes SAN. Chaque option utilise une méthode différente pour gérer les besoins en espace et en volume des technologies de partage de blocs ONTAP. Vous devez comprendre le fonctionnement de chaque option de provisionnement afin de pouvoir choisir celle qui convient le mieux à votre environnement.



Il n'est pas recommandé de placer des LUN SAN et des partages NAS sur le même FlexVol volume. À la place, vous devez provisionner des volumes FlexVol distincts pour vos LUN SAN et vos partages NAS. Cela simplifie la gestion et les déploiements de réplication. Elle est également parallèle à la prise en charge des volumes FlexVol dans Active IQ Unified Manager (anciennement OnCommand Unified Manager).

### Provisionnement fin pour les volumes

Lors de la création d'un volume à provisionnement fin, ONTAP ne réserve aucun espace supplémentaire lors de la création du volume. Au fur et à mesure de l'écriture des données sur le volume, le volume demande le stockage dont il a besoin depuis l'agrégat pour prendre en charge l'opération d'écriture. L'utilisation de volumes à provisionnement fin vous permet d'effectuer un surengagement de votre agrégat. Ce dernier risque donc de ne pas pouvoir sécuriser l'espace requis lorsqu'il vient à manquer d'espace.

Vous créez un volume FlexVol à provisionnement fin en paramétrant son unité `-space-guarantee` option à `none`.

### Provisionnement lourd pour les volumes

Lorsqu'un volume à provisionnement lourd est créé, la mémoire ONTAP réserve suffisamment de stockage de l'agrégat pour garantir l'écriture à tout moment de n'importe quel bloc du volume. Lorsque vous configurez un volume pour utiliser le provisionnement lourd, vous pouvez utiliser n'importe quelle fonction d'efficacité du stockage ONTAP, comme la compression et la déduplication, pour ainsi compenser les plus importantes besoins en stockage initial.

Vous créez un volume FlexVol à provisionnement lourd en définissant sa valeur `-space-slo` (objectif de niveau de service) à `thick`.

### Provisionnement semi-lourd pour les volumes

Lorsqu'un volume utilisant un provisionnement semi-lourd est créé, ONTAP met de côté l'espace de stockage de l'agrégat pour tenir compte de la taille du volume. Si le volume manque d'espace disponible parce que les blocs sont utilisés par les technologies de partage de blocs, ONTAP supprime un effort de suppression des objets de protection (copies Snapshot et fichiers FlexClone et LUN) afin de libérer l'espace qu'ils conservent. Tant que la ONTAP peut supprimer les objets de données de protection assez rapidement pour prendre en charge l'espace requis pour les écrasements, les opérations d'écriture sont continues. Il s'agit là d'une garantie d'écriture « meilleur effort ».



Vous ne pouvez pas utiliser de technologies d'efficacité du stockage, comme la déduplication, la compression et la compaction, sur un volume qui utilise un provisionnement semi-lourd.

Vous créez un volume FlexVol à provisionnement semi-lourd en paramétrant son option `-space-slo` (objectif de niveau de service) à `semi-thick`.

## À utiliser avec des fichiers et des LUN réservés en espace

Une LUN ou un fichier réservé à l'espace est un fichier pour lequel le stockage est alloué lors de sa création. Par le passé, NetApp a utilisé le terme « LUN à provisionnement fin » pour désigner une LUN dont la réservation d'espace est désactivée (LUN non réservée d'espace).



Les fichiers non réservés à l'espace ne sont généralement pas appelés « fichiers à provisionnement fin ».

Le tableau suivant récapitule les principales différences de manière à utiliser les trois options de provisionnement de volumes avec des fichiers et des LUN réservés à l'espace :

| Provisionnement de volume | Réservation d'espace LUN/fichier | Écrasements                  | Données de protection <sup>2</sup> | Efficacité du stockage <sup>3</sup> |
|---------------------------|----------------------------------|------------------------------|------------------------------------|-------------------------------------|
| Épais                     | Pris en charge                   | Garanti <sup>1</sup>         | Résultats garantis                 | Pris en charge                      |
| Fin                       | Aucun effet                      | Aucune                       | Résultats garantis                 | Pris en charge                      |
| Semi-épais                | Pris en charge                   | Meilleur effort <sup>1</sup> | Meilleur effort                    | Non pris en charge                  |

### Notes

1. Pour garantir le remplacement ou fournir une garantie de remplacement sans effort, la réservation d'espace est activée sur la LUN ou le fichier.
2. Les données de protection incluent des copies Snapshot, ainsi que les fichiers FlexClone et les LUN marqués pour la suppression automatique (clones de sauvegarde).
3. L'efficacité du stockage inclut la déduplication, la compression, tous les fichiers FlexClone et LUN non marqués pour la suppression automatique (clones actifs) et les sous-fichiers FlexClone (utilisés pour le déchargement des copies).

### Prise en charge des LUN SCSI à provisionnement fin

ONTAP prend en charge les LUN T10 SCSI à provisionnement fin ainsi que les LUN NetApp à provisionnement fin. Le provisionnement fin SCSI T10 permet aux applications hôtes de prendre en charge les fonctionnalités SCSI, notamment la récupération d'espace LUN et la surveillance de l'espace LUN pour les environnements en blocs. Le provisionnement fin SCSI T10 doit être pris en charge par votre logiciel hôte SCSI.

Vous utilisez ONTAP `space-allocation` Paramètre permettant d'activer/de désactiver la prise en charge du provisionnement fin T10 sur une LUN. Vous utilisez ONTAP `space-allocation enable` Paramètre permettant d'activer le provisionnement fin SCSI T10 sur une LUN.

Le `[-space-allocation {enabled|disabled}]` Commande dans le manuel de référence des commandes ONTAP contient plus d'informations pour activer/désactiver la prise en charge du provisionnement fin T10 et activer le provisionnement fin SCSI T10 sur un LUN.

### Informations associées

- ["Référence de commande ONTAP"](#)

## Configurer les options de provisionnement de volumes

Vous pouvez configurer un volume pour le provisionnement fin, le provisionnement non fin ou le provisionnement semi-fin, selon vos besoins en termes d'espace.

### Description de la tâche

Réglage du `-space-slo` option à `thick` assure les éléments suivants :

- Le volume entier est préalloué dans l'agrégat. Vous ne pouvez pas utiliser `volume create` ou `volume modify` commande pour configurer les volumes `-space-guarantee` option.
- 100 % de l'espace requis pour les écrasements est réservé. Vous ne pouvez pas utiliser `volume modify` commande pour configurer les volumes `-fractional-reserve` option

Réglage du `-space-slo` option à `semi-thick` assure les éléments suivants :

- Le volume entier est préalloué dans l'agrégat. Vous ne pouvez pas utiliser `volume create` ou `volume modify` commande pour configurer les volumes `-space-guarantee` option.
- Aucun espace n'est réservé aux écrasements. Vous pouvez utiliser le `volume modify` commande pour configurer les volumes `-fractional-reserve` option.
- La suppression automatique des copies Snapshot est activée.

### Étape

1. Configurez les options de provisionnement des volumes :

```
volume create -vserver vs1 -volume vol1 -aggregate
aggregate_name -space-slo none|thick|semi-thick -space-guarantee none|volume
```

Le `-space-guarantee` par défaut, l'option est `none` Pour les systèmes AFF et pour les volumes non-AFF DP. Sinon, elle est définie par défaut sur `volume`. Pour les volumes FlexVol existants, utilisez le `volume modify` commande permettant de configurer les options de provisionnement.

La commande suivante configure vol1 sur SVM vs1 pour le provisionnement fin :

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-guarantee
none
```

La commande suivante configure vol1 sur le SVM vs1 pour le provisionnement Thick :

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo thick
```

La commande suivante configure vol1 sur le SVM vs1 pour le provisionnement semi-lourd :

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-
thick
```



Dans certains cas, l'activation d'une fonctionnalité dans ONTAP peut consommer plus d'espace que prévu. ONTAP vous aide à déterminer la consommation d'espace en fournissant trois perspectives pour afficher l'espace : le volume, l'empreinte du volume au sein de l'agrégat et l'agrégat.

### Afficher l'allocation d'espace

Un volume peut manquer d'espace en raison de sa consommation d'espace ou d'espace insuffisant au sein du volume, de l'agrégat ou d'une combinaison des deux. En voyant une répartition de l'utilisation de l'espace basée sur des fonctionnalités d'un point de vue différent, vous pouvez évaluer les fonctionnalités que vous pourriez vouloir ajuster ou désactiver, ou si vous devez prendre d'autres mesures (telles que l'augmentation de la taille de l'agrégat ou du volume).

Vous pouvez afficher les détails de l'utilisation de l'espace de n'importe lequel de ces points de vue :

- Utilisation de l'espace du volume

Cette perspective fournit des informations détaillées sur l'utilisation de l'espace au sein du volume, notamment sur l'utilisation des copies Snapshot.

Utilisez le `volume show-space` pour voir l'utilisation de l'espace d'un volume.

À partir de ONTAP 9.14.1, sur les volumes avec [Efficacité de stockage sensible à la température \(TSSE\)](#) activé, quantité d'espace utilisée sur le volume indiqué par le `volume show-space -physical used`. La commande inclut les économies d'espace réalisées grâce à TSSE.

- Empreinte du volume au sein de l'agrégat

Cette perspective fournit des informations détaillées sur la quantité d'espace que chaque volume utilise dans l'agrégat contenant, y compris les métadonnées du volume.

Utilisez le `volume show-footprint` pour afficher l'empreinte d'un volume avec l'agrégat.

- Utilisation de l'espace de l'agrégat

Cette perspective inclut les totaux des empreintes de volume de tous les volumes contenus dans l'agrégat, l'espace réservé pour les copies Snapshot agrégées et d'autres métadonnées d'agrégat.

WAFL réserve 10 % de l'espace total sur disque pour les métadonnées et performances au niveau de l'agrégat. L'espace utilisé pour la maintenance des volumes de l'agrégat vient de la réserve WAFL et ne peut pas être modifié.

À partir de ONTAP 9.12.1, la réserve WAFL pour les agrégats de plus de 30 To est passée de 10 à 5 % pour les plateformes AFF et FAS500f. À partir de la version ONTAP 9.14.1, cette réduction s'applique également aux agrégats de toutes les plateformes FAS, ce qui permet d'augmenter de 5 % l'espace utilisable dans les agrégats.

Utilisez le `storage aggregate show-space` pour afficher l'utilisation de l'espace dans l'agrégat.

Certaines fonctionnalités, comme la sauvegarde sur bande et la déduplication, utilisent l'espace pour les métadonnées, aussi bien du volume que de l'agrégat. Ces fonctionnalités affichent une utilisation de l'espace différente entre le point de vue du volume et de l'empreinte des volumes.

## Informations associées

- ["Article de la base de connaissances : utilisation de l'espace"](#)
- ["Libérez jusqu'à 5 % de capacité en passant à ONTAP 9.12.1"](#)

## Métadonnées de volume et rapports sur les mesures des données

À l'origine, plusieurs metrics d'espace de volume ont rapporté la quantité totale de données consommées sous la forme d'une combinaison de deux metrics : les métadonnées et les données utilisateur. À partir de ONTAP 9.15.1, les mesures relatives aux métadonnées et aux données utilisateur sont signalées séparément. Deux nouveaux compteurs de métadonnées ont été introduits pour prendre en charge ce processus :

- total-métadonnées

Ce compteur indique la taille totale des métadonnées à l'intérieur du volume. Elle n'inclut pas les métadonnées du volume résident de l'agrégat. Le reporting séparé permet de déterminer les données logiques allouées par l'utilisateur.

- empreinte-totale-des-métadonnées

Ce compteur correspond à la somme des métadonnées résidentes du volume et des métadonnées du volume résident de l'agrégat. Elle assure l'empreinte totale des métadonnées du volume au sein de l'agrégat. Le reporting séparé permet de déterminer les données physiques allouées par l'utilisateur.

En outre, plusieurs compteurs existants ont été mis à jour pour supprimer le composant de métadonnées et présenter uniquement les données utilisateur :

- Données utilisateur
- Empreinte des données de volume

Ces modifications fournissent une vue plus précise des données consommées par l'utilisateur. Cela présente plusieurs avantages, notamment la possibilité de prendre des décisions de refacturation plus précises.

## Supprimez les copies Snapshot automatiquement

Vous pouvez définir et activer une règle pour la suppression automatique des copies Snapshot et des LUN FlexClone. La suppression automatique des copies Snapshot et des LUN FlexClone vous aide à gérer l'utilisation de l'espace.

### Description de la tâche

Vous pouvez supprimer automatiquement les copies Snapshot des volumes en lecture/écriture et des LUN FlexClone des volumes parents en lecture/écriture. Vous ne pouvez pas configurer la suppression automatique des copies Snapshot de volumes en lecture seule, par exemple des volumes de destination SnapMirror.

### Étape

1. Définissez et activez une règle pour la suppression automatique des copies Snapshot à l'aide du `volume snapshot autodelete modify` commande.

Voir la `volume snapshot autodelete modify` page man pour plus d'informations sur les paramètres que vous pouvez utiliser avec cette commande afin de définir une règle qui répond à vos besoins.

La commande suivante permet la suppression automatique des copies Snapshot et définit le déclencheur sur `snap_reserve`. Pour le volume `vol3`, qui fait partie de la machine virtuelle de stockage

vs0.example.com :

```
cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
-volume vol3 -enabled true -trigger snap_reserve
```

La commande suivante permet la suppression automatique des copies Snapshot et des LUN FlexClone marquées pour la suppression automatique du volume vol3, qui fait partie du SVM vs0.example.com :

```
cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
-volume vol3 -enabled true -trigger volume -commitment try -delete-order
oldest_first -destroy-list lun_clone,file_clone
```



Les copies Snapshot au niveau de l'agrégat fonctionnent différemment des copies Snapshot au niveau des volumes et sont gérées automatiquement par ONTAP. L'option de suppression des copies Snapshot des agrégats est toujours activée et facilite la gestion de l'utilisation de l'espace.

Si le paramètre de déclenchement est défini sur `snap_reserve` Pour un agrégat, les copies Snapshot sont conservées jusqu'à ce que l'espace réservé franchisse le seuil de capacité. Par conséquent, même si le paramètre de déclenchement n'est pas défini sur `snap_reserve`, l'espace utilisé par la copie Snapshot dans la commande sera répertorié comme 0 En effet, ces copies Snapshot sont automatiquement supprimées. De plus, l'espace utilisé par les copies Snapshot d'un agrégat est considéré comme libre et inclus dans le paramètre d'espace disponible de la commande.

### Configurez les volumes de manière à obtenir plus d'espace lorsque ceux-ci sont pleins

Lorsque les volumes FlexVol sont pleins, ONTAP peut utiliser différentes méthodes pour tenter de libérer automatiquement plus d'espace pour le volume. Vous choisissez les méthodes qu'ONTAP peut utiliser et dans quel ordre, en fonction des besoins imposés par votre application et votre architecture de stockage.

#### Description de la tâche

ONTAP offre automatiquement plus d'espace libre à un volume complet, en utilisant l'une des méthodes suivantes ou les deux :

- Augmenter la taille du volume (appelé *Autogrow*).

Cette méthode est utile si l'espace disponible sur l'agrégat du volume est suffisant pour prendre en charge un plus grand volume. Vous pouvez configurer ONTAP de manière à définir une taille maximale pour le volume. L'augmentation est automatiquement déclenchée en fonction de la quantité de données écrites sur le volume par rapport à la quantité d'espace utilisé actuelle, ainsi que des seuils définis.

Le nombre de disques automatique n'est pas déclenché pour prendre en charge la création de copies Snapshot. Si vous tentez de créer une copie Snapshot alors que l'espace est insuffisant, la création de la copie Snapshot échoue, même avec la croissance automatique activée.

- Supprimez les copies Snapshot, les fichiers FlexClone ou les LUN FlexClone.

Par exemple, vous pouvez configurer ONTAP pour supprimer automatiquement les copies Snapshot qui ne sont pas liées aux copies Snapshot dans des volumes ou des LUN clonés. Vous pouvez également définir les copies Snapshot que vous souhaitez ONTAP supprimer en premier lieu, à savoir les copies Snapshot les plus anciennes ou les plus récentes. Vous pouvez également déterminer à quel moment ONTAP doit commencer à supprimer les copies Snapshot, par exemple lorsque le volume est presque plein ou lorsque la réserve Snapshot du volume est presque pleine.

Si vous activez ces deux méthodes, vous pouvez spécifier la méthode ONTAP en premier lorsqu'un volume est presque plein. Si la première méthode ne fournit pas suffisamment d'espace supplémentaire au volume, ONTAP tente l'autre méthode suivante.

Par défaut, ONTAP tente d'augmenter la taille du volume en premier. Dans la plupart des cas, la configuration par défaut est préférable, car lorsqu'une copie Snapshot est supprimée, elle ne peut pas être restaurée. Toutefois, si vous devez éviter d'augmenter la taille d'un volume autant que possible, vous pouvez configurer ONTAP de sorte à supprimer les copies Snapshot avant d'augmenter la taille du volume.

### Étapes

1. Si vous souhaitez qu'un ONTAP tente d'augmenter la taille du volume quand celui-ci est plein, activez la capacité de croissance automatique du volume en utilisant le `volume autosize` commande avec `grow` mode.

N'oubliez pas que, lorsque le volume croît, il consomme plus d'espace libre de son agrégat associé. Si vous êtes en fonction de la capacité du volume à évoluer selon les besoins, vous devez surveiller l'espace libre de l'agrégat associé et en ajouter d'autres, si nécessaire.

2. Si vous souhaitez que ONTAP supprime les copies Snapshot, les fichiers FlexClone ou les LUN FlexClone lorsque le volume est plein, activez la suppression automatique de ces types d'objet.
3. Si vous avez activé à la fois la capacité de croissance automatique du volume et une ou plusieurs fonctionnalités de suppression automatique, sélectionnez la première méthode que ONTAP devrait utiliser pour fournir de l'espace libre à un volume en utilisant le `volume modify` commande avec `-space-mgmt -try-first` option.

Pour spécifier d'abord l'augmentation de la taille du volume (par défaut), utilisez `volume_grow`. Pour spécifier d'abord la suppression des copies Snapshot, utilisez `snap_delete`.

### Configurez les volumes pour qu'ils augmentent ou réduisent automatiquement leur taille

Vous pouvez configurer les volumes FlexVol de façon à les étendre ou les réduire automatiquement en fonction de l'espace dont ils ont besoin actuellement. La croissance automatique contribue à empêcher le manque d'espace d'un volume si l'agrégat peut fournir plus d'espace. La réduction automatique empêche la taille d'un volume que nécessaire, ce qui libère de l'espace dans l'agrégat pour les autres volumes.

### Description de la tâche

Autoshrink ne peut être utilisé qu'en combinaison avec la croissance automatique pour répondre aux demandes d'espace changeantes et n'est pas disponible seul. Lorsque l'option Autoshrink est activée, ONTAP gère automatiquement le comportement de décroissance d'un volume afin d'éviter une boucle infinie d'actions Autoshrink et Autoshrink.

L'augmentation automatique du nombre maximal de fichiers qu'il peut contenir peut s'avérer nécessaire à mesure qu'un volume augmente. Lorsqu'un volume est réduit, le nombre maximal de fichiers qu'il peut contenir reste inchangé et un volume ne peut pas être automatiquement réduit en dessous de la taille qui correspond à

son nombre maximal actuel de fichiers. Par conséquent, il est possible qu'il ne soit pas possible de réduire automatiquement un volume jusqu'à sa taille d'origine.

Par défaut, la taille maximale qu'un volume peut atteindre est de 120 % de la taille à laquelle la croissance automatique est activée. Si vous devez vous assurer que le volume peut augmenter de manière à ce qu'il dépasse, vous devez définir la taille maximale du volume en conséquence.

### Avant de commencer

Le volume FlexVol doit être en ligne.

### Étape

1. Configurez le volume pour qu'il augmente ou diminue automatiquement sa taille :

```
volume autosize -vserver SVM_name -volume volume_name -mode grow_shrink
```

La commande suivante permet de modifier automatiquement la taille d'un volume appelé test2. Le volume est configuré pour commencer à se réduire lorsqu'il est plein à 60 %. Les valeurs par défaut sont utilisées pour le moment où il commence à croître et sa taille maximale.

```
cluster1::> volume autosize -vserver vs2 test2 -shrink-threshold-percent
60
vol autosize: Flexible volume "vs2:test2" autosize settings UPDATED.

Volume modify successful on volume: test2
```

### Conditions requises pour l'activation de la suppression automatique des copies Snapshot et de la suppression automatique des copies

La fonctionnalité de création automatique de rapports peut être utilisée avec la suppression automatique de copies Snapshot, dans la mesure où certaines conditions de configuration sont remplies.

Si vous souhaitez activer à la fois la fonctionnalité d'auto-hrink et la suppression automatique des copies Snapshot, votre configuration doit respecter les exigences suivantes :

- La ONTAP doit être configurée pour tenter d'augmenter la taille du volume avant de tenter de supprimer les copies Snapshot(le) `-space-mgmt-try-first` l'option doit être définie sur `volume_grow`).
- Le déclencheur pour la suppression automatique de copie Snapshot doit être Volume plénitude(le `trigger` le paramètre doit être défini sur `volume`).

### Fonction de suppression automatique et de copie snapshot

La fonctionnalité de copie automatique diminue la taille d'un volume FlexVol ; elle peut donc aussi affecter la suppression automatique des copies Snapshot de volume.

La fonction Autohrink interagit avec la suppression automatique des copies Snapshot de volume de la façon suivante :

- Si les deux `grow_shrink` Le mode de taille automatique et la suppression automatique des copies Snapshot sont activés. Lorsqu'une taille de volume diminue, la suppression d'une copie Snapshot

automatique est possible.

En effet, la réserve Snapshot est basée sur un pourcentage de la taille du volume (5 % par défaut), et ce pourcentage est désormais basé sur une taille de volume inférieure. Cela peut entraîner le déversement de copies Snapshot hors de la réserve et leur suppression automatique.

- Si le `grow_shrink` Le mode taille automatique est activé et vous supprimez manuellement une copie Snapshot, il peut déclencher une réduction automatique du volume.

#### Adressage des alertes de volume FlexVol et sur-allocation

ONTAP publie des messages EMS lorsque les volumes FlexVol sont à court d'espace, ce qui vous permet de mettre en place une action corrective en fournissant davantage d'espace pour le volume complet. Connaître les types d'alertes et les traiter vous aide à assurer la disponibilité de vos données.

Lorsqu'un volume est décrit comme *full*, cela signifie que le pourcentage d'espace du volume disponible pour le système de fichiers actif (données utilisateur) est tombé en dessous d'un seuil (configurable). Lorsqu'un volume devient *suralloué*, l'espace utilisé par ONTAP pour les métadonnées et pour prendre en charge l'accès aux données de base a été épuisé. Parfois, l'espace normalement réservé à d'autres fins peut être utilisé pour maintenir le volume en fonctionnement, mais la réservation d'espace ou la disponibilité des données peuvent être en danger.

La surallocation peut être logique ou physique. *La surallocation logique* signifie que l'espace réservé pour respecter les engagements futurs en matière d'espace, tels que la réservation d'espace, a été utilisé pour un autre but. *La surallocation physique* signifie que le volume n'exécute plus de blocs physiques à utiliser. Les volumes présents dans cet état risquent de refuser les écritures, de se mettre hors ligne ou de provoquer une interruption du contrôleur.

Un volume peut être saturé à plus de 100 % en raison de l'espace utilisé ou réservé par les métadonnées. Cependant, un volume saturé à plus de 100 % peut être saturé, ne pas être surestimé. Si des partages au niveau des qtrees et des volumes sont présents sur le même pool FlexVol ou SCVMM, les qtrees apparaissent comme des répertoires du partage FlexVol. Par conséquent, veillez à ne pas les supprimer accidentellement.

Le tableau ci-dessous décrit les alertes de remplissage et de surallocation du volume, les actions que vous pouvez effectuer pour résoudre le problème et les risques de non-prise d'action :

| Type d'alerte  | Niveau EMS | Configurable ? | Définition                                                                                                                                                                                | Façons de traiter                                                                                                                 | Risque si aucune action n'a été prise                         |
|----------------|------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Presque pleine | Débogage   | Y              | Le système de fichiers a dépassé le seuil défini pour cette alerte (la valeur par défaut est 95 %). Le pourcentage est le <code>Used Total</code> moins la taille de la réserve Snapshot. | <ul style="list-style-type: none"><li>• Augmentation de la taille du volume</li><li>• Réduction des données utilisateur</li></ul> | Écriture de données et disponibilité des données simplifiées. |

| Type d'alerte           | Niveau EMS     | Configurable ? | Définition                                                                                                                                                                   | Façons de traiter                                                                                                                                                                                                                                                | Risque si aucune action n'a été prise                                                                                                                                          |
|-------------------------|----------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pleine                  | Débogage       | Y              | Le système de fichiers a dépassé le seuil défini pour cette alerte (la valeur par défaut est 98 %). Le pourcentage est le Used Total moins la taille de la réserve Snapshot. | <ul style="list-style-type: none"> <li>• Augmentation de la taille du volume</li> <li>• Réduction des données utilisateur</li> </ul>                                                                                                                             | Pas encore de risque pour les opérations d'écriture ou la disponibilité des données, mais le volume est proche du stade où les opérations d'écriture pourraient être menacées. |
| Sur-allocation logique  | Erreur SVC     | N              | En plus de la saturation du système de fichiers, l'espace du volume utilisé pour les métadonnées a été épuisé.                                                               | <ul style="list-style-type: none"> <li>• Augmentation de la taille du volume</li> <li>• Suppression des copies Snapshot</li> <li>• Réduction des données utilisateur</li> <li>• Désactivation de la réservation d'espace pour les fichiers ou les LUN</li> </ul> | Les opérations d'écriture sur les fichiers non réservés peuvent échouer.                                                                                                       |
| Sur-allocation physique | Erreur de nœud | N              | Le volume manque de blocs physiques sur lequel il peut écrire.                                                                                                               | <ul style="list-style-type: none"> <li>• Augmentation de la taille du volume</li> <li>• Suppression des copies Snapshot</li> <li>• Réduction des données utilisateur</li> </ul>                                                                                  | Les opérations d'écriture sont menacées, ainsi que la disponibilité des données ; le volume peut être mis hors ligne.                                                          |

Chaque fois qu'un seuil est franchi pour un volume, que le pourcentage de plénitude augmente ou tombe, un message EMS est généré. Lorsque le niveau de remplissage du volume tombe en dessous d'un seuil, un

volume ok Un message EMS est généré.

#### Adresse des alertes de plénitude et de surallocation des agrégats

ONTAP émet des messages EMS lorsque les agrégats manquent d'espace afin de mettre en place des actions correctives en fournissant davantage d'espace à l'agrégat complet. Connaître les types d'alertes et leur répondre vous aide à assurer la disponibilité de vos données.

Lorsqu'un agrégat est décrit comme *full*, cela signifie que le pourcentage de l'espace de l'agrégat disponible pour une utilisation par volumes est inférieur à un seuil prédéfini. Lorsqu'un agrégat devient *overallocated*, l'espace utilisé par ONTAP pour les métadonnées et pour prendre en charge l'accès aux données de base a été épuisé. Parfois, l'espace réservé normalement à d'autres fins peut être utilisé pour assurer le fonctionnement de l'agrégat, mais il est possible que l'offre de garantie des volumes associés à l'agrégat ou à la disponibilité des données soit menacée.

La surallocation peut être logique ou physique. *La surallocation logique* signifie que l'espace réservé pour respecter les engagements futurs en matière d'espace, tels que les garanties de volume, a été utilisé dans un autre but. *La surallocation physique* signifie que l'agrégat manque de blocs physiques à utiliser. Les agrégats présents dans cet état risquent de refuser les écritures, de se mettre hors ligne ou de provoquer une interruption du contrôleur.

Le tableau suivant décrit les alertes de plénitude et de surallocation d'agrégats, les actions que vous pouvez entreprendre pour résoudre le problème et les risques de non-prise d'action.

| Typ<br>e<br>d'al<br>erte      | Niv<br>eau<br>EM<br>S | Con<br>figu<br>rabil<br>e ? | Définition                                                                                                                                                                                       | Façons de traiter                                                                                                                                                                                                                                                                                                 | Risque si aucune action<br>n'a été prise                      |
|-------------------------------|-----------------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Pre<br>squ<br>e<br>plei<br>ne | Déb<br>oga<br>ge      | N                           | La quantité d'espace alloué aux volumes, y compris leurs garanties, a dépassé le seuil défini pour cette alerte (95 %). Le pourcentage est le Used Total moins la taille de la réserve Snapshot. | <ul style="list-style-type: none"><li>• Ajout de stockage à l'agrégat</li><li>• Réduction ou suppression de volumes</li><li>• Déplacement de volumes vers un autre agrégat disposant de plus d'espace</li><li>• Suppression des garanties de volume (configuration des garanties sur <code>none</code>)</li></ul> | Écriture de données et disponibilité des données simplifiées. |



| Type d'alerte           | Niveau EMS     | Configurable ? | Définition                                                                                                                                                          | Façons de traiter                                                                                                                                                                                                                                                                                                      | Risque si aucune action n'a été prise                                                                                                                                                                          |
|-------------------------|----------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pleine                  | Débo           | N              | Le système de fichiers a dépassé le seuil défini pour cette alerte (98 %).<br>Le pourcentage est le <code>Used Total</code> moins la taille de la réserve Snapshot. | <ul style="list-style-type: none"> <li>• Ajout de stockage à l'agrégat</li> <li>• Réduction ou suppression de volumes</li> <li>• Déplacement de volumes vers un autre agrégat disposant de plus d'espace</li> <li>• Suppression des garanties de volume (configuration des garanties sur <code>none</code>)</li> </ul> | Les garanties de volumes de l'agrégat peuvent être menacées, ainsi que les opérations d'écriture sur ces volumes.                                                                                              |
| Sur-allocation logique  | Erreur SVC     | N              | En plus de l'espace réservé pour les volumes pleins, l'espace de l'agrégat utilisé pour les métadonnées a été épuisé.                                               | <ul style="list-style-type: none"> <li>• Ajout de stockage à l'agrégat</li> <li>• Réduction ou suppression de volumes</li> <li>• Déplacement de volumes vers un autre agrégat disposant de plus d'espace</li> <li>• Suppression des garanties de volume (configuration des garanties sur <code>none</code>)</li> </ul> | Les garanties de volumes de l'agrégat sont menacées, ainsi que les opérations d'écriture de ces volumes.                                                                                                       |
| Sur-allocation physique | Erreur de nœud | N              | L'agrégat manque de blocs physiques sur lequel il peut écrire.                                                                                                      | <ul style="list-style-type: none"> <li>• Ajout de stockage à l'agrégat</li> <li>• Réduction ou suppression de volumes</li> <li>• Déplacement de volumes vers un autre agrégat disposant de plus d'espace</li> </ul>                                                                                                    | Les opérations d'écriture sur les volumes de l'agrégat sont menacées, ainsi que la disponibilité des données ; l'agrégat peut être mis hors ligne. Dans des cas extrêmes, le nœud peut subir une interruption. |

Chaque fois qu'un seuil est franchi pour un agrégat, que le pourcentage de plénitude augmente ou tombe, un message EMS est généré. Lorsque le niveau de remplissage de l'agrégat tombe en dessous d'un seuil, un message `ok` Un message EMS est généré.

La réserve fractionnaire de remplacement, également appelée *LUN Overwrite Reserve*, permet de désactiver la réserve de remplacements pour les LUN et les fichiers réservés à l'espace dans un volume FlexVol. Vous pouvez ainsi optimiser l'utilisation de votre stockage.



Si votre environnement est négativement affecté par l'échec des opérations d'écriture en raison du manque d'espace, vous devez comprendre les exigences que cette configuration peut imposer.

Le paramètre de réserve fractionnaire est exprimé sous forme de pourcentage ; les seules valeurs valides sont 0 et 100 pourcentage. Le paramètre de réserve fractionnaire est un attribut du volume. La définition de la réserve fractionnaire pour 0 augmenter l'utilisation du stockage. Cependant, si l'espace disponible d'une application accédant aux données résidant dans le volume est insuffisant, les données risquent de subir une panne, même si la garantie du volume est définie sur `volume`. Toutefois, grâce à une configuration et à une utilisation appropriées du volume, vous pouvez réduire les risques d'échec des écritures. ONTAP offre une garantie d'écriture « meilleur effort » pour les volumes dont la réserve fractionnaire 0 est définie sur lorsque l'ensemble des exigences suivantes sont satisfaites :

- La déduplication n'est pas utilisée
- La compression n'est pas utilisée
- Les sous-fichiers FlexClone ne sont pas utilisés
- Tous les fichiers FlexClone et les LUN FlexClone sont activés pour la suppression automatique

Ce n'est pas le paramètre par défaut. Vous devez explicitement activer la suppression automatique lors de sa création ou en modifiant le fichier FlexClone ou la LUN après sa création.

- ODX et l'allègement de la charge des copies FlexClone ne sont pas utilisés
- La garantie du volume est définie sur `volume`
- La réservation d'espace fichier ou LUN est `enabled`
- La réserve Snapshot du volume est définie sur 0
- La suppression automatique de la copie Snapshot du volume est `enabled` avec un niveau d'engagement de `destroy`, une liste de destruction de `lun_clone`, `vol_clone`, `cifs_share`, `file_clone`, `sfsr`, et un déclencheur de `volume`

Ce paramètre permet également de s'assurer que les fichiers FlexClone et les LUN FlexClone sont supprimés lorsque nécessaire.



- Si toutes les conditions ci-dessus sont remplies, mais que votre taux de modification est élevé, dans de rares cas, la suppression automatique de la copie Snapshot peut prendre du retard et entraîner un manque d'espace sur le volume.
- Si toutes les conditions ci-dessus sont remplies et que les copies Snapshot ne sont pas utilisées, les écritures de volume ne sont pas à court d'espace.

Vous avez également la possibilité d'utiliser la fonctionnalité de croissance automatique de volumes pour réduire la probabilité de suppression automatique des copies Snapshot de volumes. Si vous activez la capacité de croissance automatique, vous devez surveiller l'espace libre dans l'agrégat associé. Si l'agrégat

devient suffisamment complet que le volume n'a pas pu croître, la quantité de copies Snapshot sera probablement supprimée lorsque l'espace libre dans le volume est épuisé.

Si vous ne pouvez pas remplir l'ensemble des conditions ci-dessus et que vous devez vous assurer que l'espace du volume est insuffisant, vous devez définir le paramètre de réserve fractionnaire du volume sur 100. Cela nécessite davantage d'espace disponible à l'avance, mais garantit que les opérations de modification des données réussiront même si les technologies répertoriées ci-dessus sont en cours d'utilisation.

La valeur par défaut et les valeurs autorisées pour le paramètre de réserve fractionnaire dépendent de la garantie du volume :

| Garantie de volume | Réserve fractionnaire par défaut | Valeurs autorisées |
|--------------------|----------------------------------|--------------------|
| Volumétrie         | 100                              | 0, 100             |
| Aucune             | 0                                | 0, 100             |

### Déterminez l'utilisation des fichiers et des inodes pour un volume

Les volumes FlexVol comportent un nombre maximal de fichiers qu'ils peuvent contenir. Vous pouvez utiliser une commande de l'interface de ligne de commande pour déterminer si vous devez augmenter le nombre d'inodes (publiques) pour vos volumes FlexVol afin d'éviter qu'ils atteignent leur limite de fichiers.

#### Description de la tâche

Les inodes publics peuvent être libres (ils ne sont pas associés à un fichier) ou utilisés (ils pointent vers un fichier). Le nombre d'inodes libres pour un volume correspond au nombre total d'inodes pour le volume moins le nombre d'inodes utilisés (le nombre de fichiers).

Si des partages au niveau des qtrees et des volumes sont présents sur le même pool FlexVol ou SCVMM, les qtrees apparaissent comme des répertoires du partage FlexVol. Par conséquent, veillez à ne pas les supprimer accidentellement.

#### Étapes

1. Pour afficher l'utilisation d'inode pour un volume, entrez la commande suivante :

```
volume show -vserver <SVM_name> -volume <volume_name> -fields files
```

#### Exemple

```
cluster1::*> volume show -vserver vs1 -volume vol1 -fields files
Vserver Name: vs1
Files Used (for user-visible data): 98
```

## Contrôlez et surveillez les performances d'E/S FlexVol volume grâce à la qualité de service de stockage

Vous pouvez contrôler les performances des entrées/sorties (E/S) des volumes FlexVol en affectant des volumes aux groupes de règles de QoS du stockage. Vous pouvez contrôler les performances d'E/S pour permettre aux workloads d'atteindre des objectifs de performance spécifiques ou de limiter les workloads qui ont un impact négatif sur d'autres workloads.

### Description de la tâche

Les groupes de règles appliquent une limite de débit maximal (par exemple, 100 Mo/s). Vous pouvez créer un groupe de règles sans spécifier un débit maximal, ce qui vous permet de contrôler les performances avant de contrôler le workload.

Vous pouvez également attribuer des SVM, des LUN et des fichiers aux groupes de règles.

Prenez en compte les exigences suivantes concernant l'affectation d'un volume à une « policy group » :

- Le volume doit être contenu par le SVM auquel appartient la « policy group ».

Vous spécifiez la SVM lors de la création de la « policy group ».

- Si vous attribuez un volume à une « policy group » alors vous ne pouvez pas attribuer un SVM contenant du volume, ni des LUN ou fichiers enfants à une « policy group ».

Pour plus d'informations sur l'utilisation de la QoS du stockage, consultez le ["Référence de l'administration du système"](#).

### Étapes

1. Utilisez le `qos policy-group create` commande pour créer une « policy group ».
2. Utilisez le `volume create` commande ou le `volume modify` commande avec `-qos-policy-group` paramètre permettant d'affecter un volume à une « policy group ».
3. Utilisez le `qos statistics` commandes pour afficher les données de performances.
4. Si nécessaire, utiliser l' `qos policy-group modify` commande pour ajuster la limite de débit maximale du groupe de règles.

### Supprime un volume FlexVol

Vous pouvez supprimer un volume FlexVol qui n'est plus requis.

#### Ce dont vous avez besoin

Aucune application ne doit accéder aux données du volume que vous souhaitez supprimer.



Si vous supprimez accidentellement un volume, consultez l'article de la base de connaissances ["Comment utiliser la file d'attente de récupération de volume"](#).

### Étapes

1. Si le volume a été monté, démontez-le :

```
volume unmount -vserver vservice_name -volume volume_name
```

2. Si le volume fait partie d'une relation SnapMirror, supprimez la relation en utilisant le `snapmirror delete` commande.
3. Si le volume est en ligne, mettre le volume hors ligne :

```
volume offline -vserver vsilver_name volume_name
```

4. Supprimez le volume :

```
volume delete -vserver vsilver_name volume_name
```

## Résultat

Le volume est supprimé, ainsi que toutes les politiques de quotas et tous les qtrees associés.

## Protection contre les suppressions accidentelles de volume

Le comportement de suppression de volume par défaut facilite la restauration des volumes FlexVol supprimés par erreur.

A `volume delete` requête relative à un volume qui a type RW ou DP (comme illustré dans la `volume show` la sortie de commande) provoque le déplacement du volume vers un état partiellement supprimé. Par défaut, elles sont conservées dans une file d'attente de récupération pendant au moins 12 heures avant leur suppression complète.

Pour plus d'informations, consultez l'article de la base de connaissances ["Comment utiliser la file d'attente de récupération de volume"](#).

## Commandes de gestion des volumes FlexVol

L'interface de ligne de commandes ONTAP fournit des commandes spécifiques pour la gestion des volumes FlexVol. Selon ce que vous devez faire, vous pouvez utiliser les commandes suivantes pour gérer les volumes FlexVol :

| Les fonctions que vous recherchez...                                                         | Utilisez cette commande...                          |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Mettre un volume en ligne                                                                    | <code>volume online</code>                          |
| Modifier la taille d'un volume                                                               | <code>volume size</code>                            |
| Déterminer l'agrégat associé d'un volume                                                     | <code>volume show</code>                            |
| Déterminer l'agrégat associé pour tous les volumes d'une machine virtuelle de stockage (SVM) | <code>volume show -vserver -fields aggregate</code> |
| Détermination du format d'un volume                                                          | <code>volume show -fields block-type</code>         |
| Montez un volume sur un autre volume à l'aide d'une jonction                                 | <code>volume mount</code>                           |

| Les fonctions que vous recherchez... | Utilisez cette commande...   |
|--------------------------------------|------------------------------|
| Placez un volume à l'état restreint  | <code>volume restrict</code> |
| Renommer un volume                   | <code>volume rename</code>   |
| Mettre un volume hors ligne          | <code>volume offline</code>  |

Consultez la page man pour chaque commande pour plus d'informations.

## Commandes permettant d'afficher les informations d'utilisation de l'espace

Vous utilisez le `storage aggregate` et `volume` Commandes pour voir l'espace utilisé dans vos agrégats et volumes et leurs copies Snapshot.

| Pour afficher des informations sur...                                                                                                                                                      | Utilisez cette commande...                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Agrégats, y compris des informations détaillées sur les pourcentages d'espace utilisés et disponibles, la taille de la réserve Snapshot et d'autres informations d'utilisation de l'espace | <code>storage aggregate show storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve</code> |
| Mode d'utilisation des disques et des groupes RAID dans un agrégat et état RAID                                                                                                            | <code>storage aggregate show-status</code>                                                                               |
| Quantité d'espace disque qui serait récupérée si vous avez supprimé une copie Snapshot spécifique                                                                                          | <code>volume snapshot compute-reclaimable</code> (avancé)                                                                |
| Quantité d'espace utilisée par un volume                                                                                                                                                   | <code>volume show -fields size,used,available,percent-used volume show-space</code>                                      |
| Quantité d'espace utilisé par un volume dans l'agrégat contenant                                                                                                                           | <code>volume show-footprint</code>                                                                                       |

## Déplacement et copie de volumes

### Déplacer la présentation d'un volume FlexVol

Vous pouvez déplacer ou copier des volumes pour optimiser l'utilisation de la capacité, améliorer les performances et respecter les contrats de niveau de service. Connaître le fonctionnement du déplacement d'un volume FlexVol vous permet de déterminer si ce déplacement de volume respecte les contrats de niveau de service et de déterminer où il se trouve lors du déplacement d'un volume.

Les volumes FlexVol sont déplacés d'un agrégat ou d'un nœud vers un autre au sein d'un même SVM. Un déplacement de volumes n'interrompt pas l'accès client pendant le déplacement.



Lors de la phase de mise en service d'une opération de déplacement de volumes, vous ne pouvez pas créer de fichiers FlexClone ou de LUN FlexClone d'un volume FlexVol.

Le déplacement d'un volume se produit en plusieurs phases :

- Un nouveau volume est établi sur l'agrégat de destination.
- Les données du volume d'origine sont copiées vers le nouveau volume.

Pendant ce temps, le volume d'origine est intact et accessible pour les clients.

- À la fin du processus de déplacement, l'accès client est temporairement bloqué.

Pendant ce temps, le système exécute une réplication finale du volume source vers le volume de destination, permute les identités des volumes source et de destination, puis change le volume de destination vers le volume source.

- Une fois le déplacement terminé, le système achemine le trafic client vers le nouveau volume source et rétablit l'accès client.

La transition n'engendre pas d'interruption de l'accès aux clients, car l'heure à laquelle l'accès aux clients est bloqué est terminée avant que les clients n'aient constaté une interruption ou une expiration de délai. L'accès client est bloqué pendant 35 secondes par défaut. Si l'opération de déplacement de volume ne peut pas se terminer au moment où l'accès est refusé, le système interrompt cette dernière phase de l'opération de déplacement de volume et autorise l'accès client. Le système tente trois fois la phase finale par défaut. Après la troisième tentative, le système attend une heure avant de tenter à nouveau la séquence de phase finale. Le système exécute la phase finale de l'opération de déplacement de volume jusqu'à ce que le déplacement de volume soit terminé.

## Considérations et recommandations lors du déplacement de volumes

Plusieurs considérations et recommandations sont à prendre en compte lors du déplacement d'un volume. Ils sont basés sur le volume que vous déplacez ainsi que sur la configuration système telle que MetroCluster. Vous devez comprendre tous les problèmes pertinents avant de déplacer un volume.

### Considérations générales et recommandations

- Si vous mettez à niveau la gamme de versions d'un cluster, ne déplacez aucun volume tant que vous n'avez pas mis à niveau tous les nœuds du cluster.

Cette recommandation vous empêche de tenter par inadvertance de déplacer un volume d'une famille de versions plus récente vers une famille de versions plus ancienne.

- Le volume source doit être cohérent.
- Si un ou plusieurs agrégats sont affectés à la machine virtuelle de stockage (SVM) associée, l'agrégat de destination doit être l'un des agrégats affectés.
- Vous ne pouvez pas déplacer un volume vers ou depuis un agrégat CFO de reprise.
- Si un volume contenant des LUN n'est pas activé NVFAIL avant de le déplacer, le volume sera NVFAIL activé après le déplacement.
- Vous pouvez déplacer un volume d'un agrégat Flash Pool vers un autre agrégat Flash Pool.

- Les règles de mise en cache de ce volume sont également déplacées.
- La migration peut affecter les performances des volumes.
- Vous pouvez déplacer des volumes entre un agrégat Flash Pool et un agrégat non-Flash Pool.
  - Si vous déplacez un volume d'un agrégat Flash Pool vers un agrégat non-Flash Pool, ONTAP affiche un message vous informant que le déplacement risque d'affecter les performances du volume et vous demande si vous voulez continuer.
  - Si vous déplacez un volume d'un agrégat non-Flash Pool vers un agrégat Flash Pool, ONTAP attribue la `auto` règle de mise en cache.
- Les volumes bénéficient de la protection des données au repos de l'agrégat sur lequel ils résident. Si vous déplacez un volume d'un agrégat composé de disques NSE vers un volume qui ne le fait pas, celui-ci ne dispose plus de la protection NSE des données au repos.

#### Considérations et recommandations relatives aux volumes FlexClone

- Les volumes FlexClone ne peuvent pas être hors ligne lorsqu'ils sont déplacés.
- Vous pouvez déplacer des volumes FlexClone d'un agrégat vers un autre agrégat du même nœud ou d'un autre nœud du même SVM, sans lancer la `vol clone split start` commande.

En initiant une opération de déplacement de volume sur un volume FlexClone, le volume clone est partagé pendant le processus de déplacement vers un autre agrégat. Une fois la migration de volume effectuée sur le volume clone terminée, le volume déplacé n'apparaît plus comme clone, mais apparaît à la place en tant que volume indépendant sans relation de clonage avec le volume parent précédent.

- Les copies Snapshot de volume FlexClone ne sont pas perdues après le déplacement d'un clone.
- Vous pouvez déplacer les volumes FlexClone parent d'un agrégat à un autre.

Lorsque vous déplacez un volume parent FlexClone, un volume temporaire est placé derrière celui-ci en tant que volume parent pour tous les volumes FlexClone. Aucune opération n'est autorisée sur le volume temporaire, à l'exception de la mettre hors ligne ou de la supprimer. Une fois tous les volumes FlexClone séparés ou détruits, le volume temporaire est nettoyé automatiquement.

- Une fois le volume enfant FlexClone déplacé, il n'est plus un volume FlexClone.
- Les opérations de déplacement FlexClone s'excluent mutuellement entre la copie FlexClone et les opérations de séparation.
- Si une opération de fractionnement du clone est en cours, le déplacement d'un volume peut échouer.

Vous ne devez pas déplacer un volume avant la fin des opérations de fractionnement des clones.

#### Considérations et recommandations de MetroCluster

- Lors d'un déplacement de volume dans une configuration MetroCluster, lorsqu'un volume temporaire est créé sur l'agrégat de destination du cluster source, un enregistrement du volume temporaire correspondant au volume dans le cluster en miroir, mais non intégré, est également créé sur le cluster survivant.
- En cas de basculement MetroCluster avant la mise en service, le volume de destination dispose d'un enregistrement et il s'agit d'un volume temporaire (un volume de type TMP).

Le déplacement du travail redémarre sur le cluster survivant (reprise après sinistre), signale une panne et nettoie tous les éléments liés au déplacement, y compris le volume temporaire. Dans tous les cas où le nettoyage ne peut pas être effectué correctement, un EMS est généré pour avertir l'administrateur système d'effectuer le nettoyage nécessaire.



- En cas de basculement MetroCluster après le démarrage de la mise en service, mais avant la fin du déplacement (c'est-à-dire que le déplacement a atteint une étape où il peut mettre à jour le cluster afin qu'il pointe vers l'agrégat de destination), la tâche de déplacement redémarre sur les autres tâches (reprise sur incident). cluster et s'exécute au bout.

Tous les éléments liés au déplacement sont nettoyés, y compris le volume temporaire (source d'origine). Dans tous les cas où le nettoyage ne peut pas être effectué correctement, un EMS est généré pour avertir l'administrateur système d'effectuer le nettoyage nécessaire.

- Les backs MetroCluster forcés et non forcés ne sont pas autorisés en cas de déplacement de volumes en cours pour les volumes appartenant au site commuté.

Les dispositifs de commutation ne sont pas bloqués lorsque des opérations de déplacement de volume sont en cours pour les volumes locaux vers le site survivant.

- Les mélangeurs MetroCluster non forcés sont bloqués, mais les mélangeurs MetroCluster forcés ne sont pas bloqués si des opérations de déplacement de volume sont en cours.

## Configuration requise pour le déplacement de volumes dans un environnement SAN

Vous devez vous préparer avant de déplacer un volume dans un environnement SAN.

Avant de déplacer un volume contenant des LUN ou des espaces de noms, vous devez respecter les exigences suivantes :

- Pour les volumes contenant une ou plusieurs LUN, vous devez disposer d'au moins deux chemins par LUN (LIF) qui se connectent à chaque nœud du cluster.

Cela élimine les points de défaillance uniques et permet au système de résister aux défaillances des composants.

- Pour les volumes contenant des espaces de noms, le cluster doit exécuter ONTAP 9.6 ou version ultérieure.

Le déplacement de volumes n'est pas pris en charge dans les configurations NVMe qui exécutent ONTAP 9.5.

## Déplacer un volume

Vous pouvez déplacer un volume FlexVol vers un autre agrégat, nœud ou les deux au sein d'un même SVM afin d'équilibrer la capacité de stockage après avoir déterminé qu'il existe un déséquilibre de la capacité de stockage.

### Description de la tâche

Par défaut, si l'opération de mise en service ne s'effectue pas dans les 30 secondes, il est à nouveau possible de procéder à une nouvelle tentative. Vous pouvez régler le comportement par défaut à l'aide du `-cutover-window` et `-cutover-action` paramètres qui nécessitent tous deux un accès au niveau de privilège avancé. Pour plus d'informations, reportez-vous à la `volume move start` page de manuel.

### Étapes

1. Si vous déplacez un miroir de protection des données et que vous n'avez pas initialisé la relation miroir, initialisez la relation miroir à l'aide de `snapmirror initialize` commande.

Les relations de miroir de protection des données doivent être initialisées avant de déplacer l'un des volumes.

2. Déterminer un agrégat dans lequel vous pouvez déplacer le volume à l'aide de `volume move target-aggr show` commande.

L'agrégat que vous sélectionnez doit avoir suffisamment d'espace pour le volume, c'est-à-dire que la taille disponible est supérieure au volume que vous déplacez.

L'exemple suivant montre que le volume `vs2` peut être déplacé vers l'un des agrégats répertoriés :

```
cluster1::> volume move target-aggr show -vserver vs2 -volume user_max
Aggregate Name Available Size Storage Type

aggr2 467.9GB hdd
node12a_aggr3 10.34GB hdd
node12a_aggr2 10.36GB hdd
node12a_aggr1 10.36GB hdd
node12a_aggr4 10.36GB hdd
5 entries were displayed.
```

3. Vérifier que le volume peut être déplacé vers l'agrégat prévu à l'aide de la `volume move start -perform-validation-only` commande permettant d'exécuter une vérification de validation.
4. Déplacez le volume à l'aide de `volume move start` commande.

La commande suivante déplace le volume `user_max` du SVM `vs2` vers l'agrégat `node 12a_aggr3`. Le déplacement s'exécute en arrière-plan.

```
cluster1::> volume move start -vserver vs2 -volume user_max
-destination-aggregate node12a_aggr3
```

5. Déterminez l'état de l'opération de déplacement de volume à l'aide du `volume move show` commande.

L'exemple suivant montre l'état du déplacement d'un volume qui a terminé la phase de réplication et qui est en phase de mise en service :

```
cluster1::> volume move show
Vserver Volume State Move Phase Percent-Complete Time-To-Complete

vs2 user_max healthy cutover - -
```

Le déplacement de volume est terminé lorsqu'il n'apparaît plus dans le `volume move show` sortie de la commande.

## Commandes de déplacement de volumes

L'interface de ligne de commandes ONTAP fournit des commandes spécifiques pour la gestion du déplacement de volumes. En fonction de ce que vous devez faire, utilisez les commandes suivantes pour gérer les règles de quotas et les politiques de quotas :

| Les fonctions que vous recherchez...                                                                                                      | Utilisez cette commande...                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Annuler une opération de déplacement de volume active.                                                                                    | <code>volume move abort</code>                                                                                                                                                                                                                     |
| Montrer l'état d'un volume passant d'un agrégat à un autre.                                                                               | <code>volume move show</code>                                                                                                                                                                                                                      |
| Commencez à déplacer un volume d'un agrégat à un autre.                                                                                   | <code>volume move start</code>                                                                                                                                                                                                                     |
| Gestion des agrégats cibles pour le déplacement de volumes                                                                                | <code>volume move target-aggr</code>                                                                                                                                                                                                               |
| Déclencher la mise en service d'une tâche de déplacement.                                                                                 | <code>volume move trigger-cutover</code>                                                                                                                                                                                                           |
| Modifiez la durée de blocage de l'accès client si la valeur par défaut n'est pas correcte.                                                | <code>volume move start</code> ou <code>volume move modify</code> avec le <code>-cutover-window</code> paramètre. Le <code>volume move modify</code> commande est une commande avancée et le <code>-cutover-window</code> est un paramètre avancé. |
| Déterminez ce que fait le système si l'opération de déplacement de volume ne peut pas être terminée pendant le blocage de l'accès client. | <code>volume move start</code> ou <code>volume move modify</code> avec le <code>-cutover-action</code> paramètre. Le <code>volume move modify</code> commande est une commande avancée et le <code>-cutover-action</code> est un paramètre avancé. |

Consultez la page man pour chaque commande pour plus d'informations.

## Méthodes de copie d'un volume

La méthode de copie d'un volume dépend du fait que vous le copiez dans le même agrégat ou dans un autre agrégat et que vous souhaitiez conserver les copies Snapshot du volume d'origine. La copie d'un volume crée une copie autonome d'un volume que vous pouvez utiliser à des fins de test, entre autres.

Le tableau suivant répertorie les caractéristiques de la copie et les méthodes utilisées pour la créer.

| Pour copier un volume...                                                                                      | Ensuite, la méthode que vous utilisez est...                                                                                                            |
|---------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Au sein du même agrégat et que vous ne souhaitez pas copier les copies Snapshot à partir du volume d'origine. | Création d'un volume FlexClone du volume d'origine                                                                                                      |
| Vers un autre agrégat et vous ne souhaitez pas copier les copies Snapshot à partir du volume d'origine.       | Création d'un volume FlexClone du volume d'origine, puis déplacement du volume vers un autre agrégat en utilisant le <code>volume move</code> commande. |
| Dans un autre agrégat et conservez l'ensemble des copies Snapshot du volume d'origine.                        | Répliquer le volume d'origine à l'aide de SnapMirror, puis casser la relation de SnapMirror pour faire une copie de volume en lecture-écriture.         |

## Utilisez les volumes FlexClone pour créer des copies efficaces de vos volumes FlexVol

### Présentation de l'utilisation des volumes FlexClone

Les volumes FlexClone sont des copies inscriptibles à un point dans le temps d'un volume FlexVol parent. Les volumes FlexClone sont compacts car ils partagent les mêmes blocs de données avec leurs volumes FlexVol parents pour les données communes. La copie Snapshot utilisée pour créer un volume FlexClone est également partagée avec le volume parent.

Vous pouvez cloner un volume FlexClone existant pour créer un autre volume FlexClone. Vous pouvez également créer un clone d'un volume FlexVol contenant des LUN et des clones de LUN.

Vous pouvez également séparer un volume FlexClone de son volume parent. Depuis ONTAP 9.4, pour les volumes non garantis sur les systèmes AFF, l'opération de séparation pour les volumes FlexClone partage les blocs physiques et ne copie pas les données. La division des volumes FlexClone sur les systèmes AFF est donc plus rapide que le fractionnement de FlexClone sur d'autres systèmes FAS dans ONTAP 9.4 et versions ultérieures.

Vous pouvez créer deux types de volumes FlexClone : les volumes FlexClone en lecture/écriture et les volumes FlexClone de protection des données. Vous pouvez créer un volume FlexClone en lecture/écriture d'un volume FlexVol standard, mais vous devez utiliser uniquement un volume secondaire SnapVault pour créer un volume FlexClone de protection des données.

### Créer un volume FlexClone

Vous pouvez créer un volume FlexClone de protection des données à partir d'un volume de destination SnapMirror ou d'un volume FlexVol parent qui est un volume secondaire SnapVault. Depuis ONTAP 9.7, vous pouvez créer un volume FlexClone à partir d'un volume FlexGroup. Une fois le volume FlexClone créé, vous ne pouvez plus supprimer le volume parent tant que le volume FlexClone existe.

### Avant de commencer

- La licence FlexClone doit être installée sur le cluster. Cette licence est incluse avec ["ONTAP One"](#).

- Le volume que vous souhaitez cloner doit être en ligne.



Le clonage d'un volume en tant que volume FlexClone sur un autre SVM n'est pas pris en charge dans les configurations MetroCluster.

## Créez un volume FlexClone d'une FlexVol ou d'une FlexGroup

### Étape

1. Créer un volume FlexClone :

```
volume clone create
```



Lors de la création d'un volume FlexClone en lecture/écriture à partir du volume parent en lecture/écriture, il n'est pas nécessaire de spécifier la copie Snapshot de base. ONTAP crée une copie Snapshot si vous ne nommez aucune copie Snapshot spécifique qui doit être utilisée comme copie Snapshot de base pour le clone. Vous devez spécifier la copie Snapshot de base pour la création d'un volume FlexClone lorsque le volume parent est un volume de protection des données.

### Exemple

- La commande suivante crée un volume FlexClone en lecture-écriture vol1\_clone à partir du volume parent vol1 :

```
volume clone create -vserver vs0 -flexclone vol1_clone -type RW -parent-volume vol1
```

- La commande suivante crée une protection des données FlexClone volume vol\_dp\_clone à partir du volume parent dp\_vol à l'aide de la copie Snapshot de base snap1 :

```
volume clone create -vserver vs1 -flexclone vol_dp_clone -type DP -parent -volume dp_vol -parent-snapshot snap1
```

## Créez un FlexClone de tout type de SnapLock

À partir de ONTAP 9.13.1, vous pouvez spécifier l'un des trois types de SnapLock, `compliance`, `enterprise`, `non-snaplock`. Lors de la création d'un FlexClone d'un volume RW. Par défaut, un volume FlexClone est créé avec le même type de SnapLock que le volume parent. Toutefois, vous pouvez remplacer la valeur par défaut à l'aide du `snaplock-type` Pendant la création du volume FlexClone.

À l'aide du `non-snaplock` paramètre avec le `snaplock-type` Vous pouvez créer un volume FlexClone de type non SnapLock à partir d'un volume parent SnapLock afin de fournir une méthode plus rapide pour remettre les données en ligne si nécessaire.

En savoir plus sur ["SnapLock"](#).

### Avant de commencer

Notez les restrictions de volume FlexClone suivantes lorsqu'elles ont un type SnapLock différent de celui du volume parent.

- Seuls les clones de type RW sont pris en charge. Les clones de type DP avec un type SnapLock différent du volume parent ne sont pas pris en charge.

- Les volumes avec LUN ne peuvent pas être clonés à l'aide de l'option de type snaplock définie sur une valeur autre que « non snaplock », car les volumes SnapLock ne prennent pas en charge les LUN.
- Un volume d'un agrégat en miroir MetroCluster ne peut pas être cloné avec un type SnapLock de conformité, car les volumes SnapLock Compliance ne sont pas pris en charge sur les agrégats en miroir MetroCluster.
- Les volumes de conformité SnapLock avec conservation légale ne peuvent pas être clonés avec un autre type de SnapLock. La conservation légale n'est prise en charge que sur les volumes de conformité SnapLock.
- Le SVM DR ne prend pas en charge les volumes SnapLock. La tentative de création d'un clone SnapLock à partir d'un volume dans un SVM faisant partie d'une relation SVM DR échoue.
- Les bonnes pratiques de FabricPool recommandent que les clones conservent la même règle de hiérarchisation que la règle parente. Cependant, un clone de conformité SnapLock d'un volume activé par FabricPool ne peut pas avoir la même règle de Tiering que le clone parent. La règle de hiérarchisation doit être définie sur `none`. Tentative de création d'un clone de conformité SnapLock à partir d'un parent avec une règle de hiérarchisation autre que `none` échouera.

## Étapes

1. Créer un volume FlexClone de type SnapLock : `volume clone create -vserver svm_name -flexclone flexclone_name -type RW [ -snaplock-type {non-snaplock|compliance|enterprise} ]`

Exemple :

```
> volume clone create -vserver vs0 -flexclone voll_clone -type RW
-snaplock-type enterprise -parent-volume voll
```

## Séparer un volume FlexClone de son volume parent

Vous pouvez séparer un volume FlexClone de son parent pour en faire un volume FlexVol normal.

L'opération de fractionnement de clone a lieu en arrière-plan. Les données sont accessibles sur le clone et sur le parent lors du fractionnement. À partir de la version ONTAP 9.4, l'optimisation de l'espace est préservée. Le processus de fractionnement ne met à jour que les métadonnées et requiert un nombre d'E/S minimal. Aucun bloc de données n'est copié.

### Description de la tâche

- Il est impossible de créer de nouvelles copies Snapshot du volume FlexClone pendant la division.
- Un volume FlexClone ne peut pas être séparé du volume parent s'il appartient à une relation de protection des données ou s'il fait partie d'un miroir de partage de charge.
- Si vous mettez le volume FlexClone hors ligne alors que le fractionnement est en cours, l'opération est suspendue. Lorsque vous remettez le volume FlexClone en ligne, l'opération de fractionnement reprend.
- Après le fractionnement, le volume FlexVol parent et le clone nécessitent l'allocation d'espace complet déterminée par leurs garanties de volume.
- Une fois qu'un volume FlexClone est séparé de son parent, il n'est pas possible de le rejoindre à nouveau.
- Depuis ONTAP 9.4, pour les volumes non garantis sur les systèmes AFF, l'opération de séparation pour les volumes FlexClone partage les blocs physiques et ne copie pas les données. Par conséquent, le

fractionnement des volumes FlexClone sur les systèmes AFF est plus rapide que le fractionnement FlexClone sur d'autres systèmes FAS dans ONTAP 9.4 et versions ultérieures. La division FlexClone optimisée sur les systèmes AFF offre plusieurs avantages :

- L'efficacité du stockage est préservée après le fractionnement du clone du parent.
- Les copies Snapshot existantes ne sont pas supprimées.
- L'opération est plus rapide.
- Le volume FlexClone peut être partagé en tout point de la hiérarchie des clones.

#### Avant de commencer

- Vous devez être un administrateur de cluster.
- Le volume FlexClone doit être en ligne au début de l'opération de fractionnement.
- Le volume parent doit être en ligne pour que le fractionnement réussisse.

#### Étapes

1. Déterminez l'espace libre requis pour terminer l'opération de fractionnement :

```
volume clone show -estimate -vserver vs1 -flexclone clone1 -parent-volume vol1
```

L'exemple suivant fournit des informations sur l'espace libre requis pour séparer le volume FlexClone « clone1 » de son volume parent « vol1 » :

```
cluster1::> volume clone show -estimate -vserver vs1 -flexclone clone1 -parent-volume vol1
```

| Vserver | FlexClone | Split Estimate |
|---------|-----------|----------------|
| vs1     | clone1    | 40.73MB        |

2. Vérifiez que l'agrégat contenant le volume FlexClone et que son parent dispose d'un espace suffisant :

- a. Déterminez la quantité d'espace libre dans l'agrégat contenant le volume FlexClone et son parent :

```
storage aggregate show
```

- b. Si l'agrégat contenant ne dispose pas d'un espace disponible suffisant, ajoutez du stockage à l'agrégat :

```
storage aggregate add-disks
```

3. Démarrer l'opération de fractionnement :

```
volume clone split start -vserver vs1 -flexclone clone1 -parent-volume vol1
```

L'exemple suivant montre comment lancer le processus de séparation du volume FlexClone « clone1 » à partir de son volume parent « vol1 » :

```
cluster1::> volume clone split start -vserver vs1 -flexclone clone1

Warning: Are you sure you want to split clone volume clone1 in Vserver
vs1 ?
{y|n}: y
[Job 1617] Job is queued: Split clone1.
```

#### 4. Surveiller l'état de l'opération de séparation FlexClone :

```
volume clone split show -vserver vs1 -flexclone clone1
```

L'exemple suivant montre l'état de l'opération de séparation FlexClone sur un système AFF :

```
cluster1::> volume clone split show -vserver vs1 -flexclone clone1
```

|          |           | Inodes    |       |         |         |         |
|----------|-----------|-----------|-------|---------|---------|---------|
| Blocks   |           |           |       |         |         |         |
| -----    |           |           |       |         |         |         |
| Vserver  | FlexClone | Processed | Total | Scanned | Updated | % Inode |
| % Block  |           |           |       |         |         |         |
| Complete | Complete  |           |       |         |         |         |
| vs1      | clone1    | 0         | 0     | 411247  | 153600  | 0       |
| 37       |           |           |       |         |         |         |

#### 5. Vérifier que le volume fragmenté n'est plus un volume FlexClone :

```
volume show -volume volume_name -fields clone-volume
```

La valeur du clone-volume L'option est « false » pour un volume qui n'est pas un volume FlexClone.

L'exemple suivant montre comment vérifier si le volume « clone1 » qui est séparé de son parent n'est pas un volume FlexClone.

```
cluster1::> volume show -volume clone1 -fields clone-volume
vserver volume **clone-volume**
----- **-----**
vs1 clone1 **false**
```

### Détermination de l'espace utilisé par un volume FlexClone

Vous pouvez déterminer l'espace utilisé par un volume FlexClone en fonction de sa taille nominale et de la quantité d'espace qu'il partage avec le volume FlexVol parent. Lors de la création d'un volume FlexClone, toutes les données sont partagées avec le volume



parent. Bien que la taille nominale du FlexVol volume soit la même que celle de son parent, il utilise très peu d'espace libre de l'agrégat.

### Description de la tâche

L'espace libre utilisé par un volume FlexClone nouvellement créé est d'environ 0.5 % de sa taille nominale. Cet espace est utilisé pour stocker les métadonnées du volume FlexClone.

Les nouvelles données écrites sur le volume parent ou FlexClone ne sont pas partagées entre les volumes. L'augmentation de la quantité de nouvelles données écrites sur le volume FlexClone entraîne une augmentation de l'espace requis par le volume FlexClone depuis son agrégat contenant.

### Étape

1. Déterminez l'espace physique réel utilisé par le volume FlexClone à l'aide de `volume show` commande.

L'exemple suivant montre l'espace physique total utilisé par le volume FlexClone :

```
cluster1::> volume show -vserver vs01 -volume clone_vol1 -fields
size,used,available,
percent-used,physical-used,physical-used-percent
vserver volume size available used percent-used physical-
used physical-used-percent

vs01 clone_vol1 20MB 18.45MB 564KB 7% 196KB
1%
```

### Considérations relatives à la création d'un volume FlexClone à partir d'une source SnapMirror ou d'un volume de destination

Vous pouvez créer un volume FlexClone depuis le volume source ou de destination dans une relation SnapMirror volume existante. Cela pourrait cependant empêcher les futures opérations de réplication SnapMirror de se terminer correctement.

Il est possible que la réplication ne fonctionne pas, car lorsque vous créez le volume FlexClone, vous pouvez verrouiller une copie Snapshot utilisée par SnapMirror. Dans ce cas, SnapMirror arrête la réplication sur le volume de destination jusqu'à ce que le volume FlexClone soit détruit ou séparé de son volume parent. Vous avez deux options pour résoudre ce problème :

- Si vous avez besoin que le volume FlexClone soit temporaire et que vous pouvez prendre en charge un arrêt temporaire de la réplication SnapMirror, vous pouvez créer le volume FlexClone et le supprimer ou le diviser du volume parent autant que possible.

La réplication SnapMirror se poursuit normalement lorsque le volume FlexClone est supprimé ou est séparé de son parent.

- Si un arrêt temporaire de la réplication SnapMirror n'est pas acceptable, vous pouvez créer une copie Snapshot dans le volume source SnapMirror, puis utiliser cette copie Snapshot pour créer le volume FlexClone. (Si vous créez le volume FlexClone à partir du volume de destination, vous devez attendre que cette copie Snapshot soit répliquée vers le volume de destination SnapMirror.)

Cette méthode de création d'une copie Snapshot dans le volume source SnapMirror vous permet de créer le clone sans verrouiller la copie Snapshot utilisée par SnapMirror.

## Utilisez les fichiers FlexClone et les LUN FlexClone pour créer des copies efficaces de fichiers et de LUN

### Présentation de l'utilisation du fichier FlexClone et du LUN FlexClone

Les fichiers FlexClone et les LUN FlexClone sont des clones inscriptibles et compacts des fichiers parents et des LUN parent, et contribuent à une utilisation efficace de l'espace physique de l'agrégat. Les fichiers FlexClone et les LUN FlexClone sont pris en charge uniquement pour les volumes FlexVol.

Les fichiers FlexClone et les LUN FlexClone utilisent 0.4 % de leur taille pour stocker les métadonnées. Les clones partagent les blocs de données de leurs fichiers parent et de leurs LUN parent, et occupent un espace de stockage négligeable jusqu'à ce que les clients écrivent de nouvelles données soit sur le fichier parent, soit sur la LUN, soit sur le clone.

Les clients peuvent effectuer toutes les opérations liées aux fichiers et aux LUN sur les entités parent et clone.

Vous pouvez utiliser plusieurs méthodes pour supprimer les fichiers FlexClone et les LUN FlexClone.

### Créer un fichier FlexClone ou une LUN FlexClone

Vous pouvez créer des clones rapides et compacts des fichiers et des LUN présents dans les volumes FlexVol ou des volumes FlexClone à l'aide de `volume file clone create` commande.

#### Ce dont vous avez besoin

- La licence FlexClone doit être installée sur le cluster. Cette licence est incluse avec ["ONTAP One"](#).
- Si plusieurs plages de blocs sont utilisées pour le clonage de sous-LUN ou le clonage de sous-fichiers, les numéros de blocs ne doivent pas se chevaucher.
- Si vous créez un sous-LUN ou un sous-fichier sur des volumes dont la compression adaptative est activée, les plages de blocs ne doivent pas être mal alignées.

Cela signifie que le numéro du bloc de début de la source et le numéro du bloc de début de la destination doivent être alignés de manière uniforme ou impaire.

#### Description de la tâche

En fonction des privilèges attribués par l'administrateur du cluster, un administrateur du SVM peut créer des fichiers FlexClone et des LUN FlexClone.

Vous pouvez spécifier le paramètre de suppression automatique des fichiers FlexClone et des LUN FlexClone lors de la création et de la modification de clones. Par défaut, le paramètre de suppression automatique est désactivé.

Lorsque vous créez un clone, vous pouvez le remplacer par une LUN FlexClone ou un fichier FlexClone existant à l'aide du `volume file clone create` commande avec `-overwrite-destination` paramètre.

Lorsque le nœud atteint sa charge maximale de partage, il n'accepte temporairement plus les requêtes de création de fichiers FlexClone et de LUN FlexClone, et émet un `EBUSY` message d'erreur. Lorsque la charge fractionnée du nœud tombe en dessous du maximum, le nœud accepte les demandes de création des fichiers FlexClone et des LUN FlexClone de nouveau. Vous devez patienter jusqu'à ce que le nœud ait la capacité de créer les clones avant de réessayer la requête de création.

### Étapes

1. Créer un fichier FlexClone ou une LUN FlexClone à l'aide du `volume file clone create` commande.

L'exemple suivant montre comment créer un fichier FlexClone `file1_clone` du fichier parent `file1_source` dans le volume `vol1` :

```
cluster1::> volume file clone create -vserver vs0 -volume vol1 -source
-path /file1_source -destination-path /file1_clone
```

Pour plus d'informations sur l'utilisation de cette commande, consultez les pages de manuels.

### Informations associées

["Référence de commande ONTAP"](#)

### Affichez la capacité du nœud avant de créer et de supprimer des fichiers FlexClone et des LUN FlexClone

Vous devez déterminer si un nœud peut recevoir des demandes de création et de suppression de fichiers FlexClone et de LUN FlexClone. Pour ce faire, affichez la charge fractionnée du nœud. Si la charge fractionnée maximale est atteinte, aucune nouvelle demande n'est acceptée jusqu'à ce que la charge fractionnée tombe en dessous du maximum.

### Description de la tâche

Lorsque le nœud atteint sa charge fractionnée maximale, un `EBUSY` un message d'erreur s'affiche en réponse à la création et à la suppression de demandes. Lorsque la charge partagée du nœud tombe en dessous du maximum, le nœud accepte les demandes de création et de suppression des fichiers FlexClone et des LUN FlexClone de nouveau.

Un nœud peut accepter de nouvelles demandes lorsque le `Allowable Split Load` champ affiche la capacité et que la demande de création dépasse la capacité disponible.

### Étapes

1. Afficher la capacité qu'un nœud doit créer et supprimer des fichiers FlexClone et des LUN en utilisant le `volume file clone split load show` commande.

Dans l'exemple suivant, la charge fractionnée est affichée pour tous les nœuds du cluster 1. Tous les nœuds du cluster sont capables de créer et de supprimer des fichiers FlexClone et des LUN FlexClone, comme indiqué dans le champ charge fractionnée autorisée :

```
cluster1::> volume file clone split load show
```

| Node  | Max<br>Split Load | Current<br>Split Load | Token<br>Reserved Load | Allowable<br>Split Load |
|-------|-------------------|-----------------------|------------------------|-------------------------|
| node1 | 15.97TB           | 0B                    | 100MB                  | 15.97TB                 |
| node2 | 15.97TB           | 0B                    | 100MB                  | 15.97TB                 |

2 entries were displayed.

## Afficher les gains d'espace possibles avec FlexClone Files et les LUN FlexClone

Vous pouvez afficher le pourcentage d'espace disque économisé par partage de bloc sur un volume contenant des fichiers FlexClone et des LUN FlexClone. Vous pouvez le faire dans le cadre de la planification de la capacité.

### Étapes

1. Pour afficher les gains d'espace obtenus grâce aux fichiers FlexClone et aux LUN FlexClone, entrez la commande suivante :

```
df -s volname
```

volname Est le nom du volume FlexVol.



Si vous exécutez le `df -s` Sur un volume FlexVol compatible avec la déduplication, vous pouvez afficher l'espace économisé par la déduplication et les fichiers FlexClone et les LUN.

### Exemple

L'exemple suivant montre les économies d'espace réalisées sur un volume FlexClone test1 :

```
systemA> df -s test1
```

| Filesystem  | used | saved | %saved | Vserver |
|-------------|------|-------|--------|---------|
| /vol/test1/ | 4828 | 5744  | 54%    | vs1     |

## Méthodes de suppression des fichiers FlexClone et des LUN FlexClone

Vous pouvez utiliser plusieurs méthodes pour supprimer les fichiers FlexClone et les LUN FlexClone. Pour savoir comment gérer les clones, il est important de connaître les méthodes disponibles.

Vous pouvez utiliser les méthodes suivantes pour supprimer des fichiers FlexClone et des LUN FlexClone :

- Vous pouvez configurer un volume FlexVol afin de supprimer automatiquement des clones lorsque la suppression automatique est activée lorsque l'espace libre d'un volume FlexVol est inférieur à un seuil particulier.
- Vous pouvez configurer des clients afin qu'ils suppriment des clones à l'aide du SDK de gestion NetApp.

- Vous pouvez utiliser des clients pour supprimer des clones à l'aide des protocoles NAS et SAN.

La méthode de suppression la plus lente est activée par défaut, car cette méthode n'utilise pas le SDK de gestion NetApp. Toutefois, vous pouvez configurer le système pour qu'il utilise la méthode de suppression la plus rapide lorsque vous supprimez des fichiers FlexClone à l'aide de `volume file clone deletion` commandes.

## Comment un volume FlexVol peut récupérer de l'espace libre avec le paramètre de suppression automatique

### Les volumes FlexVol et la récupération d'espace libre grâce à la présentation de la suppression automatique

Vous pouvez activer la suppression automatique d'un volume FlexVol pour supprimer automatiquement les fichiers FlexClone et les LUN FlexClone. En activant la suppression automatique, vous pouvez récupérer une quantité cible d'espace libre dans le volume lorsqu'un volume est presque plein.

Vous pouvez configurer un volume pour qu'il commence automatiquement la suppression des fichiers FlexClone et des LUN FlexClone lorsque l'espace libre du volume diminue en dessous d'un seuil particulier, et que l'espace disponible cible est récupéré lorsqu'une quantité d'espace libre dans le volume est arrêté automatiquement. Bien que vous ne puissiez pas spécifier la valeur de seuil au début de la suppression automatique de clones, vous pouvez spécifier si un clone peut être supprimé et vous pouvez spécifier la quantité cible d'espace libre d'un volume.

Un volume supprime automatiquement les fichiers FlexClone et les LUN FlexClone lorsque l'espace libre dans le volume diminue en dessous d'un seuil particulier et lorsque les *deux* des exigences suivantes sont remplies :

- La fonctionnalité de suppression automatique est activée pour le volume qui contient les fichiers FlexClone et les LUN FlexClone.

Vous pouvez activer la fonctionnalité de suppression automatique d'un volume FlexVol à l'aide du `volume snapshot autodelete modify` commande. Vous devez définir le `-trigger` paramètre à `volume` ou `snap_reserve` Pour qu'un volume supprime automatiquement les fichiers FlexClone et les LUN FlexClone.

- La fonctionnalité de suppression automatique est activée pour les fichiers FlexClone et les LUN FlexClone.

Vous pouvez activer la suppression automatique d'un fichier FlexClone ou d'une LUN FlexClone à l'aide du `file clone create` commande avec `-autodelete` paramètre. Par conséquent, vous pouvez préserver certains fichiers FlexClone et certaines LUN FlexClone en désactivant la suppression automatique des clones et en vous assurant que les autres paramètres de volume ne prévalent pas sur le paramètre de clonage.

### Configurer un volume FlexVol pour supprimer automatiquement les fichiers FlexClone et les LUN FlexClone

Vous pouvez activer une FlexVol volume pour supprimer automatiquement des fichiers FlexClone et des LUN FlexClone lorsque l'espace disponible dans le volume diminue en dessous d'un seuil particulier.

#### Ce dont vous avez besoin

- Le volume FlexVol doit contenir des fichiers FlexClone et des LUN FlexClone, et doit être en ligne.

- Le volume FlexVol ne doit pas être un volume en lecture seule.

## Étapes

1. Activez la suppression automatique des fichiers FlexClone et des LUN FlexClone dans le volume FlexVol à l'aide de la `volume snapshot autodelete modify` commande.

- Pour le `-trigger` vous pouvez spécifier un paramètre `volume` ou `snap_reserve`.
- Pour le `-destroy-list` paramètre, vous devez toujours spécifier `lun_clone`, `file_clone` que vous souhaitez supprimer un seul type de clone ou non.

L'exemple suivant montre comment activer la commande `volume vol1` pour déclencher la suppression automatique des fichiers FlexClone et des LUN FlexClone pour la récupération d'espace jusqu'à ce que 25 % du volume se compose d'espace libre :

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume
vol1 -enabled true -commitment disrupt -trigger volume -target-free
-space 25 -destroy-list lun_clone,file_clone
```

```
Volume modify successful on volume:vol1
```



Lors de l'activation des volumes FlexVol pour la suppression automatique, si vous définissez la valeur de `-commitment` paramètre à `destroy`, Tous les fichiers FlexClone et les LUN FlexClone avec `-autodelete` paramètre défini sur `true` il est possible de supprimer l'espace libre dans le volume lorsque la valeur de seuil spécifiée est inférieure à ce seuil. Mais, les fichiers FlexClone et les LUN FlexClone avec `-autodelete` paramètre défini sur `false` ne sera pas supprimé.

2. Vérifier que la suppression automatique des fichiers FlexClone et des LUN FlexClone est activée dans le volume FlexVol à l'aide de la `volume snapshot autodelete show` commande.

L'exemple suivant montre que le volume `vol1` est activé pour la suppression automatique des fichiers FlexClone et des LUN FlexClone :

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1
```

```

Vserver Name: vs1
Volume Name: vol1
Enabled: true
Commitment: disrupt
Defer Delete: user_created
Delete Order: oldest_first
Defer Delete Prefix: (not specified)
Target Free Space: 25%
Trigger: volume
Destroy List: lun_clone,file_clone
Is Constituent Volume: false
```

3. Assurez-vous que la suppression automatique est activée pour les fichiers FlexClone et les LUN FlexClone

dans le volume que vous souhaitez supprimer en effectuant les étapes suivantes :

- a. Activez la suppression automatique d'un fichier FlexClone ou d'une LUN FlexClone spécifique à l'aide de `volume file clone autodelete` commande.

Vous pouvez forcer la suppression automatique d'un fichier FlexClone ou d'une LUN FlexClone spécifique à l'aide du `volume file clone autodelete` commande avec `-force` paramètre.

L'exemple suivant montre que la suppression automatique de la LUN FlexClone LUN1\_clone contenue dans le volume vol1 est activée :

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path
/vol/vol1/lun1_clone -enabled true
```

Vous pouvez activer la suppression automatique lors de la création de fichiers FlexClone et de LUN FlexClone.

- b. Vérifiez que le fichier FlexClone ou la LUN FlexClone est activé pour la suppression automatique à l'aide du `volume file clone show-autodelete` commande.

L'exemple suivant montre que la LUN FlexClone LUN1\_clone est activée pour la suppression automatique :

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone
-path vol/vol1/lun1_clone
Vserver Name: vs1
Clone Path: vol/vol1/lun1_clone
Autodelete Enabled: true
```

Pour plus d'informations sur l'utilisation des commandes, consultez les pages de manuels respectives.

### Empêchez la suppression automatique d'un fichier FlexClone ou d'une LUN FlexClone

Si vous configurez un volume FlexVol pour supprimer automatiquement les fichiers FlexClone et les LUN FlexClone, tout clone répondant aux critères spécifiés risque d'être supprimé. Si vous souhaitez préserver des fichiers FlexClone ou des LUN FlexClone spécifiques, vous pouvez les exclure du processus de suppression automatique de FlexClone.

#### Avant de commencer

Une licence FlexClone doit être installée. Cette licence est incluse avec ["ONTAP One"](#).

#### Description de la tâche

Lorsque vous créez un fichier FlexClone ou une LUN FlexClone, le paramètre de suppression automatique du clone est désactivé par défaut. Les fichiers FlexClone et les LUN FlexClone avec suppression automatique désactivée sont conservés lorsque vous configurez un volume FlexVol afin que vous puissiez supprimer automatiquement des clones pour récupérer de l'espace sur le volume.



Si vous définissez le `commitment` le niveau du volume vers `try` ou `disrupt`, Vous pouvez conserver individuellement des fichiers FlexClone ou des LUN FlexClone en désactivant la suppression automatique de ces clones. Cependant, si vous définissez le `commitment` le niveau du volume vers `destroy` et les listes de destruction incluent `lun_clone`, `file_clone`, Le paramètre de volume remplace le paramètre clone, et tous les fichiers FlexClone et LUN FlexClone peuvent être supprimés indépendamment du paramètre de suppression automatique des clones.

## Étapes

1. Empêcher la suppression automatique d'un fichier FlexClone ou d'une LUN FlexClone spécifique à l'aide du système `volume file clone autodelete` commande.

L'exemple suivant montre comment désactiver la suppression automatique de la LUN FlexClone `LUN1_clone` contenue dans `vol1` :

```
cluster1::> volume file clone autodelete -vserver vs1 -volume vol1
-clone-path lun1_clone -enable false
```

Un fichier FlexClone ou une LUN FlexClone avec la suppression automatique désactivée ne peut pas être supprimé automatiquement pour récupérer de l'espace sur le volume.

2. Vérifiez que la suppression automatique est désactivée pour le fichier FlexClone ou le LUN FlexClone à l'aide du `volume file clone show-autodelete` commande.

L'exemple suivant montre que la suppression automatique est fausse pour la LUN FlexClone `LUN1_clone` :

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path
vol/vol1/lun1_clone
```

|          | Vserver             |
|----------|---------------------|
| Name:    | vs1                 |
|          | Clone Path:         |
|          | vol/vol1/lun1_clone |
|          | Autodelete          |
| Enabled: | false               |

## Commandes permettant de configurer la suppression de fichiers FlexClone

Lorsque les clients suppriment des fichiers FlexClone sans utiliser le SDK de gestion NetApp, vous pouvez utiliser `volume file clone deletion` Commandes permettant de supprimer plus rapidement des fichiers FlexClone d'un volume FlexVol. Les extensions et la taille minimale des fichiers FlexClone sont utilisées pour accélérer la suppression.

Vous pouvez utiliser le `volume file clone deletion` Commandes permettant de spécifier une liste d'extensions prises en charge et une taille minimale pour les fichiers FlexClone dans un volume. La méthode de suppression plus rapide est utilisée uniquement pour les fichiers FlexClone qui répondent aux exigences. Pour les fichiers FlexClone qui ne répondent pas aux exigences, la méthode de suppression plus lente est



utilisée.

Lorsque les clients suppriment les fichiers FlexClone et des LUN FlexClone d'un volume à l'aide du SDK de gestion NetApp, les exigences d'extension et de taille ne s'appliquent pas, car la méthode de suppression plus rapide est toujours utilisée.

| Pour...                                                                                                                                                                                          | Utilisez cette commande...                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Ajoutez une extension à la liste des extensions prises en charge pour le volume                                                                                                                  | <code>volume file clone deletion add-extension</code>    |
| Modifier la taille minimale des fichiers FlexClone pouvant être supprimés du volume à l'aide de la méthode de suppression la plus rapide                                                         | <code>volume file clone deletion modify</code>           |
| Supprimez une extension de la liste des extensions prises en charge pour le volume                                                                                                               | <code>volume file clone deletion remove-extension</code> |
| Afficher la liste des extensions prises en charge et la taille minimale des fichiers FlexClone que les clients peuvent supprimer du volume en utilisant la méthode de suppression la plus rapide | <code>volume file clone deletion show</code>             |

Pour plus d'informations sur ces commandes, consultez la page de manuels appropriée.

## Utilisez des qtrees pour partitionner vos volumes FlexVol

### Qtrees et partitionnement FlexVol volume

Les qtrees vous permettent de partitionner vos volumes FlexVol en segments de plus petite taille, que vous pouvez gérer individuellement. Vous pouvez utiliser des qtrees pour gérer les quotas, le style de sécurité et les oplocks CIFS.

ONTAP crée un qtree par défaut, appelé *qtree0*, pour chaque volume. Si vous ne placez pas les données dans un qtree, elles résident dans *qtree0*.

Les noms des qtree ne doivent pas comporter plus de 64 caractères.

Les répertoires ne peuvent pas être déplacés vers des qtrees. Seuls les fichiers peuvent être déplacés entre les qtrees.

Si vous créez des partages au niveau des qtrees et des partages au niveau des volumes sur le même pool FlexVol ou SCVMM, les qtrees apparaissent comme des répertoires sur le partage FlexVol. Par conséquent, veillez à ne pas les supprimer accidentellement.

### Obtenir un chemin de jonction qtree

Vous pouvez monter un qtree individuellement en obtenant la Junction path ou le namespace du qtree. Le chemin qtree affiché par la commande CLI `qtree show -instance` est du format `/vol/<volume_name>/<qtree_name>`. Toutefois, ce

chemin ne fait pas référence au chemin de jonction ou au chemin d'espace de noms du qtree.

### Description de la tâche

Vous devez connaître la Junction path du volume pour obtenir le Junction path ou le namespace du qtree.

### Étapes

1. Utilisez le `vserver volume junction-path` commande pour obtenir la junction path d'un volume.

L'exemple suivant affiche la Junction path du volume nommé `vol1` situé sur la machine virtuelle de stockage (SVM) nommée `v0` :

```
cluster1::> volume show -volume vol1 -vserver vs0 -fields junction-path

vs0 vol1 /vol1
```

Depuis la sortie ci-dessus, la Junction path du volume est `/vol1`. Étant donné que les qtrees sont toujours enracinés au niveau du volume, la Junction path ou le namespace du qtree sera `/vol1/qtree1`.

### Restrictions relatives aux noms de qtree

Les noms des qtree ne peuvent pas comporter plus de 64 caractères. De plus, l'utilisation de caractères spéciaux dans les noms des qtrees, comme des virgules et des espaces, peut générer des problèmes avec d'autres fonctionnalités et doit être évitée.

["En savoir plus sur le comportement et les contraintes de l'interface de ligne de commande lors de la création de noms de fichiers"](#).

### Les conversions de répertoire en qtree

#### Convertir un répertoire en qtree

Si vous disposez d'un répertoire à la racine d'un FlexVol volume que vous souhaitez convertir en qtree, vous devez migrer les données contenues dans ce répertoire vers un nouveau qtree du même nom, à l'aide de votre application client.

### Description de la tâche

Les étapes que vous effectuez pour convertir un répertoire en qtree dépendent du client que vous utilisez. Le processus suivant décrit les tâches générales à effectuer.

### Avant de commencer

Vous ne pouvez pas supprimer un répertoire s'il est associé à un partage CIFS existant.

### Étapes

1. Renommer le répertoire à créer dans un qtree.
2. Créer un qtree avec le nom du répertoire d'origine.

3. Utiliser l'application client pour déplacer le contenu du répertoire dans le nouveau qtree.
4. Supprimez le répertoire maintenant vide.

#### Convertir un répertoire en qtree à l'aide d'un client Windows

Pour convertir un répertoire en qtree à l'aide d'un client Windows, vous renommez le répertoire, créez un qtree sur le système de stockage et déplacez le contenu du répertoire vers le qtree.

##### Description de la tâche

Vous devez utiliser l'Explorateur Windows pour cette procédure. Vous ne pouvez pas utiliser l'interface de ligne de commande Windows ou l'environnement d'invite DOS.

##### Étapes

1. Ouvrez l'Explorateur Windows.
2. Cliquez sur la représentation du dossier du répertoire à modifier.



Le répertoire doit résider à la racine du volume qui le contient.

3. Dans le menu **fichier**, sélectionnez **Renommer** pour donner un nom différent à ce répertoire.
4. Sur le système de stockage, utilisez le `volume qtree create` commande permettant de créer un qtree avec le nom d'origine du répertoire.
5. Dans l'Explorateur Windows, ouvrez le dossier du répertoire renommé et sélectionnez les fichiers qu'il contient.
6. Faites glisser ces fichiers dans la représentation de dossier du nouveau qtree.



Plus le nombre de sous-dossiers contenus dans le dossier que vous déplacez est important, plus l'opération de déplacement prend de temps.

7. Dans le menu **fichier**, sélectionnez **Supprimer** pour supprimer le dossier de répertoire renommé, maintenant vide.

#### Convertir un répertoire en qtree à l'aide d'un client UNIX

Pour convertir un répertoire en qtree dans UNIX, vous renommez le répertoire, créez un qtree sur le système de stockage et déplacez le contenu du répertoire dans le qtree.

##### Étapes

1. Ouvrez une fenêtre client UNIX.
2. Utilisez le `mv` commande pour renommer le répertoire.

```
client: mv /n/user1/vol1/dir1 /n/user1/vol1/olddir
```

3. Dans le système de stockage, utilisez le `volume qtree create` commande permettant de créer un qtree avec le nom d'origine.

```
system1: volume qtree create /n/user1/vol1/dir1
```

- À partir du client, utilisez le `mv` commande permettant de déplacer le contenu de l'ancien répertoire dans le qtree.



Plus le nombre de sous-répertoires contenus dans un répertoire que vous déplacez est élevé, plus l'opération de déplacement prendra de temps.

```
client: mv /n/user1/vol1/olddir/* /n/user1/vol1/dir1
```

- Utilisez le `rmdir` commande pour supprimer l'ancien répertoire maintenant vide.

```
client: rmdir /n/user1/vol1/olddir
```

### Une fois que vous avez terminé

En fonction de la manière dont votre client UNIX implémente `mv` la commande, la propriété des fichiers et les autorisations peuvent ne pas être préservées. Si cela se produit, mettez à jour les propriétaires de fichiers et les autorisations vers leurs valeurs précédentes.

### Commandes de gestion et de configuration des qtrees

Vous pouvez gérer et configurer des qtrees à l'aide de commandes ONTAP spécifiques. Selon ce que vous devez faire, vous pouvez utiliser les commandes suivantes pour gérer et configurer les qtrees :

| Les fonctions que vous recherchez...              | Utilisez cette commande...                                                                                                                                                                                                                                         |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Créer un qtree                                    | <code>volume qtree create</code>                                                                                                                                                                                                                                   |
| Affiche une liste filtrée des qtrees              | <code>volume qtree show</code>                                                                                                                                                                                                                                     |
| Supprimer un qtree                                | <code>volume qtree delete</code> <div> Commande <code>qtree volume qtree delete</code> échec si le qtree n'est pas vide ou le <code>-force true</code> indicateur ajouté.</div> |
| Modifier les autorisations UNIX d'un qtree        | <code>volume qtree modify -unix-permissions</code>                                                                                                                                                                                                                 |
| Modifier le paramètre des oplocks CIFS d'un qtree | <code>volume qtree oplocks</code>                                                                                                                                                                                                                                  |

|                                              |                                             |
|----------------------------------------------|---------------------------------------------|
| Modifier le paramètre de sécurité d'un qtree | <code>volume qtree security</code>          |
| Renommer un qtree                            | <code>volume qtree rename</code>            |
| Afficher les statistiques d'un qtree         | <code>volume qtree statistics</code>        |
| Réinitialiser les statistiques d'un qtree    | <code>volume qtree statistics -reset</code> |



Le `volume rehost` la commande peut entraîner l'échec d'autres opérations d'administration simultanées ciblées sur ce volume.

## Création de rapports sur l'espace logique et application des volumes

### Présentation des rapports sur l'espace logique et de leur application pour les volumes

Depuis la version ONTAP 9.4, vous pouvez autoriser l'espace logique utilisé dans un volume et l'espace de stockage restant à afficher. Depuis ONTAP 9.5, vous pouvez limiter la quantité d'espace logique consommée par les utilisateurs.

Les fonctions de reporting et d'application de l'espace logique sont désactivées par défaut.

Les types de volumes suivants prennent en charge la création de rapports sur l'espace logique et la mise en œuvre de ces

| Type de volume                    | Les rapports sur l'espace sont-ils pris en charge     | Les applications de l'espace sont-elles prises en charge |
|-----------------------------------|-------------------------------------------------------|----------------------------------------------------------|
| Volumes FlexVol                   | Oui, à partir de ONTAP 9.4                            | Oui, à partir de ONTAP 9.5                               |
| Volumes de destination SnapMirror | Oui, à partir de ONTAP 9.8                            | Oui, à partir de ONTAP 9.13.1                            |
| Volumes FlexGroup                 | Oui, à partir de ONTAP 9.9.1                          | Oui, à partir de ONTAP 9.9.1                             |
| Volumes FlexCache                 | Le paramètre d'origine est utilisé au niveau du cache | Sans objet                                               |

### Application de l'espace logique

L'application de l'espace logique permet d'avertir les utilisateurs lorsqu'un volume est plein ou presque plein. Lorsque vous activez l'application de l'espace logique dans ONTAP 9.5 ou version ultérieure, ONTAP compte les blocs utilisés par logique dans un volume pour déterminer la quantité d'espace disponible pour ce volume. Si aucun espace n'est disponible dans un volume, le système renvoie un message d'erreur ENOSPC (manque d'espace).

L'application de l'espace logique renvoie trois types d'alertes pour vous informer sur l'espace disponible d'un

volume :

- `Monitor.vol.full.inc.sav`: Cette alerte est déclenchée lorsque 98 % de l'espace logique du volume a été utilisé.
- `Monitor.vol.nearFull.inc.sav`: Cette alerte est déclenchée lorsque 95 % de l'espace logique du volume a été utilisé.
- `Vol.log.overalloc.inc.sav`: Cette alerte est déclenchée lorsque l'espace logique utilisé dans le volume est supérieur à la taille totale du volume.

Cette alerte vous indique que l'ajout de la taille du volume risque de ne pas créer d'espace disponible, car cet espace est déjà utilisé par les blocs logiques suralloués.



Total (espace logique) doit être égal à l'espace provisionné, à l'exception de la réserve Snapshot du volume avec application de l'espace logique.

Pour plus d'informations, voir ["Configurez des volumes afin de libérer automatiquement plus d'espace lorsque ceux-ci sont pleins"](#)

## Génération de rapports sur l'espace logique

Lorsque vous activez le reporting sur l'espace logique d'un volume, votre système peut afficher la quantité d'espace logique utilisé et disponible en plus de l'espace total d'un volume. En outre, les utilisateurs des systèmes clients Linux et Windows peuvent voir l'espace utilisé et disponible logique au lieu de l'espace physique utilisé et physique disponible.

Définitions :

- L'espace physique désigne les blocs physiques de stockage disponibles ou utilisés dans le volume.
- L'espace logique désigne l'espace utilisable d'un volume.
- L'espace logique utilisé est l'espace physique utilisé, plus les économies réalisées grâce aux fonctionnalités d'efficacité du stockage (telles que la déduplication et la compression) qui ont été configurées.

Depuis ONTAP 9.5, vous pouvez activer la mise en œuvre de l'espace logique et le reporting sur l'espace.

Lorsque cette option est activée, le rapport d'espace logique affiche les paramètres suivants avec le `volume show` commande :

| Paramètre                  | Signification                                                                                                                                                                                                                                                                                           |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-logical-used</code> | Affiche des informations uniquement sur le ou les volumes dont la taille logique utilisée est spécifiée. Cette valeur inclut l'espace économisé par les fonctionnalités d'efficacité du stockage et l'espace physique utilisé. Cela n'inclut pas la réserve Snapshot, mais le déversement de snapshots. |

| Paramètre                          | Signification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-logical-used-by-afs</code>  | Affiche des informations uniquement sur le ou les volumes dont la taille logique spécifiée est utilisée par le système de fichiers actif. Cette valeur diffère de <code>-logical-used</code> Valeur par la quantité de déversement d'instantanés qui dépasse la réserve d'instantanés.                                                                                                                                                                                                                                       |
| <code>-logical-available</code>    | Lorsque seul le rapport d'espace logique est activé, seul l'espace disponible est affiché. Lorsque le reporting sur l'espace et l'application sont tous deux activés, il affiche la quantité d'espace disponible actuellement en tenant compte de l'espace économisé par les fonctions d'efficacité du stockage comme étant utilisées. Cela n'inclut pas la réserve Snapshot.                                                                                                                                                |
| <code>-logical-used-percent</code> | Affiche le pourcentage du courant <code>-logical-used</code> Valeur avec la taille provisionnée sans la réserve Snapshot du volume.<br><br>Cette valeur peut être supérieure à 100 %, car le <code>-logical-used-by-afs</code> valeur comprenant des économies d'efficacité au niveau du volume. Le <code>-logical-used-by-afs</code> La valeur d'un volume n'inclut pas la fuite de snapshots comme espace utilisé. Le <code>-physical-used</code> La valeur d'un volume inclut la fuite de snapshots comme espace utilisé. |
| <code>-used</code>                 | Affiche la quantité d'espace occupé par les données utilisateur et les métadonnées du système de fichiers. Il diffère de <code>physical-used</code> espace par la somme de l'espace réservé aux écritures futures et de l'espace économisé par l'efficacité du stockage de l'agrégat. Cela inclut la fuite Snapshot (quantité d'espace dont les copies Snapshot dépassent la réserve Snapshot). Elle n'inclut pas la réserve Snapshot.                                                                                       |

L'activation du reporting de l'espace logique dans l'interface de ligne de commandes permet également d'afficher les valeurs de l'espace logique utilisé (%) et de l'espace logique dans System Manager

Les systèmes clients voient l'espace logique affiché comme espace « utilisé » sur les écrans suivants du système :

- Sortie `* df*` sur les systèmes Linux
- Détails de l'espace sous Propriétés utilisation de l'Explorateur Windows sur les systèmes Windows.



Si la génération de rapports sur l'espace logique est activée sans application de l'espace logique, le total affiché sur les systèmes clients peut être supérieur à l'espace provisionné.

## Activez le reporting et l'application des espaces logiques

Depuis ONTAP 9.4, vous pouvez activer la création de rapports sur l'espace logique. À partir de 9.5, vous pouvez activer l'application de l'espace logique, ou à la fois la création de rapports et l'application.

### Description de la tâche

En plus d'activer les fonctions de reporting et d'application de l'espace logique au niveau des volumes individuels, vous pouvez les activer au niveau du SVM pour chaque volume prenant en charge cette

fonctionnalité. Si vous activez les fonctions d'espace logique pour l'ensemble du SVM, vous pouvez également les désactiver pour des volumes individuels.

Depuis ONTAP 9.8, si vous activez la génération de rapports sur l'espace logique sur un volume source SnapMirror, cette fonction est automatiquement activée sur le volume de destination après le transfert.

À partir de ONTAP 9.13.1, si l'option d'application est activée sur un volume source SnapMirror, la destination signale la consommation d'espace logique et honore son application, ce qui permet une meilleure planification de la capacité.



Si vous exécutez une version ONTAP antérieure à ONTAP 9.13.1, vous devez comprendre que bien que le paramètre d'application soit transféré vers le volume de destination SnapMirror, le volume de destination ne prend pas en charge l'application. Par conséquent, la destination signale la consommation d'espace logique mais ne respecte pas son application.

En savoir plus sur ["Prise en charge de ONTAP pour les rapports sur l'espace logique"](#).

## Étapes

Activez une ou plusieurs des options suivantes :

- Activer la génération de rapports sur l'espace logique pour un volume :

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is-space-reporting-logical true
```

- Activer l'application d'espace logique pour un volume :

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is-space-enforcement-logical true
```

- Activez ensemble la création de rapports sur l'espace logique et leur application pour un volume :

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is-space-reporting-logical true -is-space-enforcement-logical true
```

- Activer les fonctions de création de rapports et d'application de l'espace logique pour un nouveau SVM :

```
vserver create -vserver _svm_name_ -rootvolume root-_volume_name_ -rootvolume -security-style unix -data-services {desired-data-services} [-is-space-reporting-logical true] [-is-space-enforcement-logical true]
```

- Activer les fonctions de création de rapports et d'application de l'espace logique pour un SVM existant :

```
vserver modify -vserver _svm_name_ {desired-data-services} [-is-space-reporting-logical true] [-is-space-enforcement-logical true]
```

## Gérez les limites de capacité des SVM

À partir de ONTAP 9.13.1, vous pouvez définir une capacité maximale pour une machine virtuelle de stockage (SVM). Vous pouvez également configurer des alertes lorsque la SVM approche un niveau de capacité seuil.

## Description de la tâche



La capacité d'un SVM est calculée comme la somme des volumes FlexVols, FlexGroup volumes, FlexClones, FlexCache volumes. Les volumes ont un impact sur le calcul de la capacité, même s'ils sont restreints, hors ligne ou dans la file d'attente de restauration après la suppression. Si des volumes sont configurés avec l'extension automatique, la valeur maximale de taille automatique du volume est calculée en fonction de la taille du SVM ; sans l'extension automatique, la taille réelle du volume est calculée.

Le tableau suivant explique comment `autosize-mode` les paramètres ont un impact sur le calcul de la capacité.

|                                        |                                                                       |
|----------------------------------------|-----------------------------------------------------------------------|
| <code>autosize-mode off</code>         | Le paramètre de taille sera utilisé pour le calcul                    |
| <code>autosize-mode grow</code>        | Le <code>max-autosize</code> le paramètre sera utilisé pour le calcul |
| <code>autosize-mode grow-shrink</code> | Le <code>max-autosize</code> le paramètre sera utilisé pour le calcul |

### Avant de commencer

- Vous devez être administrateur du cluster pour définir la limite d'un SVM.
- Les limites de stockage ne peuvent pas être configurées pour des SVM contenant des volumes de protection des données, des volumes dans une relation SnapMirror ou dans une configuration MetroCluster.
- Lorsque vous migrez un SVM, une limite de stockage ne peut pas être activée sur le SVM source. Pour terminer l'opération de migration, désactivez la limite de stockage sur la source, puis terminez la migration.
- La capacité SVM se distingue de [quotas](#). Les quotas ne peuvent pas dépasser la taille maximale.
- Vous ne pouvez pas définir de limite de stockage lorsque d'autres opérations sont en cours sur la SVM. Utilisez le `job show vservser svm_name` pour afficher les travaux existants. Essayez à nouveau d'exécuter la commande une fois les travaux terminés.

### Impact sur la capacité

Lorsque vous atteignez la limite de capacité, les opérations suivantes échouent :

- Création d'une LUN, d'un espace de noms ou d'un volume
- Clonage d'une LUN, d'un espace de noms ou d'un volume
- Modification d'une LUN, d'un espace de noms ou d'un volume
- Augmentation de la taille d'une LUN, d'un espace de noms ou d'un volume
- Extension d'une LUN, d'un espace de noms ou d'un volume
- Réhébergement d'une LUN, d'un espace de noms ou d'un volume

### Définir une limite de capacité sur un nouveau SVM

## System Manager

### Étapes

1. Sélectionnez **stockage > machines virtuelles de stockage**.
2. Faire sélectionner  pour créer le SVM.
3. Nommer le SVM et sélectionner un **protocole d'accès**.
4. Sous **Paramètres de la VM de stockage**, sélectionnez **Activer la limite de capacité maximale**.  
  
Fournir une capacité maximale pour la SVM.
5. Sélectionnez **Enregistrer**.

### CLI

#### Étapes

1. Créer le SVM. Pour définir une limite de stockage, fournissez une `storage-limit` valeur. Pour définir une alerte de seuil pour la limite de stockage, indiquez une valeur de pourcentage pour `-storage-limit-threshold-alert`.

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume root_volume_name -rootvolume-security-style {unix|ntfs|mixed} -storage -limit value [GiB|TiB] -storage-limit-threshold-alert percentage [-ipSPACE IPspace_name] [-language <language>] [-snapshot-policy snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
```

Si vous ne fournissez pas la valeur de seuil, par défaut une alerte sera déclenchée lorsque la SVM est à 90 % de sa capacité. Pour désactiver l'alerte de seuil, indiquez une valeur de zéro.

2. Confirmer la création du SVM réussie :

```
vserver show -vserver vserver_name
```

3. Si vous souhaitez désactiver la limite de stockage, modifier la SVM avec `-storage-limit` paramètre défini sur zéro :

```
vserver modify -vserver vserver_name -storage-limit 0
```


### Définir ou modifier une limite de capacité sur un SVM existant

Vous pouvez définir une alerte de limite de capacité et de seuil sur une SVM existante ou désactiver une limite de capacité.

Une fois que vous avez défini la limite de capacité, vous ne pouvez pas la modifier en une valeur inférieure à la capacité actuellement allouée.

## System Manager

### Étapes

1. Sélectionnez **stockage > machines virtuelles de stockage**.
2. Sélectionner le SVM à modifier. En regard du nom du SVM, sélectionner  puis **Edit**.
3. Pour activer une limite de capacité, cochez la case en regard de **Activer la limite de capacité**. Entrez une valeur pour **capacité maximale** et un pourcentage pour **seuil d'alerte**.

Si vous souhaitez désactiver la limite de capacité, décochez la case en regard de **Activer la limite de capacité**.

4. Sélectionnez **Enregistrer**.

### CLI

### Étapes

1. Sur le cluster hébergeant le SVM, lancer `vserver modify` commande. Indiquez une valeur numérique pour `-storage-limit` et un pourcentage pour `-storage-limit-threshold-alert`.

```
vserver modify -vserver vserver_name -storage-limit value [GiB|TiB]
-storage-limit-threshold-alert percentage
```

Si vous ne fournissez pas de valeur de seuil, vous obtenez une alerte par défaut à 90 % de la capacité. Pour désactiver l'alerte de seuil, indiquez une valeur de zéro.

2. Si vous souhaitez désactiver la limite de stockage, modifier la SVM avec `-storage-limit` défini sur zéro :

```
vserver modify -vserver vserver_name -storage-limit 0
```

## Atteindre les limites de capacité

Lorsque vous atteignez la capacité maximale ou le seuil d'alerte, vous pouvez consulter le `vserver.storage.threshold` Messages EMS ou utilisez la page **Insights** de System Manager pour en savoir plus sur les actions possibles. Les résolutions possibles sont :

- Modification des limites de capacité maximale des SVM
- Purge de la file d'attente de restauration des volumes pour libérer de l'espace
- Supprimez le snapshot pour libérer de l'espace pour le volume

## Informations supplémentaires

- [Mesures de la capacité dans System Manager](#)
- [Contrôle de la capacité dans System Manager](#)

## Utilisez des quotas pour limiter ou suivre l'utilisation des ressources

### Présentation du processus de quotas

## Compréhension des quotas, des règles de quotas et des politiques de quotas

Les quotas sont définis dans des règles de quotas spécifiques aux volumes FlexVol. Ces règles de quotas sont collectées ensemble dans une politique de quotas pour une machine virtuelle de stockage (SVM) et activées sur chaque volume de la SVM.

Une règle de quotas est toujours spécifique à un volume. Les règles de quota n'ont aucun effet tant que des quotas ne sont pas activés sur le volume défini dans la règle de quotas.

Une politique de quotas est un ensemble de règles de quotas pour tous les volumes d'une SVM. Les règles de quotas ne sont pas partagées entre les SVM. Un SVM peut disposer jusqu'à cinq politiques de quotas, ce qui vous permet d'avoir des copies de sauvegarde de politiques de quotas. Une politique de quotas est attribuée à un SVM à tout moment donné. Lorsque vous initialisez ou redimensionnez les quotas sur un volume, vous activez les règles des quotas dans la politique de quotas qui est actuellement attribuée à la SVM.

Un quota correspond à la restriction réelle que ONTAP applique ou au suivi réel effectué par ONTAP. Une règle de quotas entraîne toujours au moins un quota et peut entraîner de nombreux quotas dérivés supplémentaires. La liste complète des quotas appliqués n'est visible que dans les rapports de quotas.

L'activation consiste à déclencher une ONTAP afin de créer des quotas appliqués à partir de l'ensemble actuel de règles de quotas dans la politique de quotas attribuée. L'activation s'effectue volume par volume. La première activation des quotas sur un volume est appelée initialisation. Les activations suivantes sont appelées soit réinitialisation, soit redimensionnement, en fonction de la portée des modifications.

### Avantages de l'utilisation des quotas

Vous pouvez utiliser des quotas pour gérer et surveiller l'utilisation des ressources avec les volumes FlexVol.

La définition des quotas présente plusieurs avantages. Vous pouvez utiliser les quotas par défaut, explicites, dérivés et de suivi pour gérer l'utilisation des disques de la manière la plus efficace possible.

### Limitez la consommation des ressources

Vous pouvez limiter la quantité d'espace disque ou le nombre de fichiers utilisés par un utilisateur ou un groupe ou contenus dans un qtree.

### Suivre l'utilisation des ressources

La quantité d'espace disque ou le nombre de fichiers utilisés par un utilisateur, un groupe ou qtree peut être suivie sans imposer de limite.

### Avertir les utilisateurs

Des notifications peuvent être générées lorsque l'utilisation des ressources atteint des niveaux spécifiques. Ceci avertit les utilisateurs lorsque leur utilisation de disque ou de fichier est trop élevée.

### Processus de quotas

Les quotas permettent de limiter ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree. Les quotas group sont appliqués à un volume FlexVol ou à un qtree spécifique.

Les quotas peuvent être conditionnels ou inconditionnels. Lors du dépassement de limites définies, les quotas conditionnels entraînent l'envoi d'une notification par ONTAP, tandis que les quotas inconditionnels empêcheront toute opération d'écriture.

Lorsqu'ONTAP reçoit une demande d'un utilisateur ou d'un groupe d'utilisateurs d'écrire sur un volume FlexVol, il vérifie si les quotas sont activés sur ce volume pour l'utilisateur ou le groupe d'utilisateurs et détermine les éléments suivants :

- Indique si la limite stricte sera atteinte

Si oui, l'opération d'écriture échoue lorsque la limite stricte est atteinte et que la notification de quota stricte est envoyée.

- Indique si la limite soft sera enfreinte

Si oui, l'opération d'écriture réussit lorsque la limite soft est dépassée et que la notification soft quota est envoyée.

- Indique si une opération d'écriture ne dépassera pas la limite soft

Si oui, l'opération d'écriture réussit et aucune notification n'est envoyée.

#### **Différences entre les quotas conditionnels, inconditionnels et inconditionnels**

Les quotas matériels empêchent les opérations tandis que les quotas conditionnels déclenchent des notifications.

Les quotas matériels imposent une limite stricte aux ressources système, toute opération qui entraînerait un dépassement de la limite. Les paramètres suivants créent des quotas matériels :

- Paramètre de limite de disque
- Paramètre de limite de fichiers

Les quotas conditionnels envoient un message d'avertissement lorsque l'utilisation des ressources atteint un certain niveau, mais n'affectent pas les opérations d'accès aux données. Vous pouvez ainsi prendre les mesures appropriées avant le dépassement du quota. Les paramètres suivants créent des quotas conditionnels :

- Seuil du paramètre limite de disque
- Paramètre limite de disque logiciel
- Paramètre de limite des fichiers logiciels

Les quotas Threshold et Soft Disk permettent aux administrateurs de recevoir plus d'une notification concernant un quota. En général, les administrateurs définissent le seuil de limite de disque sur une valeur légèrement inférieure à la limite de disque, de sorte que le seuil fournit un « avertissement final » avant que les écritures ne commencent à échouer.

#### **À propos des notifications de quotas**

Les notifications de quota sont des messages envoyés vers le système de gestion des événements (EMS) et configurés également en tant que traps SNMP.

Les notifications sont envoyées en réponse aux événements suivants :

- Un quota difficile est atteint ; en d'autres termes, on tente de le dépasser
- Un quota logiciel est dépassé

- Un quota soft n'est plus dépassé

Les seuils sont légèrement différents des autres quotas conditionnels. Les seuils déclenchent des notifications uniquement lorsqu'ils sont dépassés, pas lorsqu'ils ne sont plus dépassés.

Les notifications Hard-quota sont configurables via la commande `volume quota modify`. Vous pouvez les désactiver complètement et modifier leur fréquence, par exemple pour éviter l'envoi de messages redondants.

Les notifications de soft quota ne sont pas configurables car il est peu probable qu'elles génèrent des messages redondants et leur seul objectif est la notification.

Le tableau suivant répertorie les événements que les quotas envoient au système EMS :

| Lorsque cela se produit...                                              | Cet événement est envoyé à l'EMS...                                                                                                                   |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Une limite stricte est atteinte dans un quota d'arborescence            | <code>wافل.quota.qtree.exceeded</code>                                                                                                                |
| Une limite stricte est atteinte dans un quota utilisateur sur le volume | <code>wافل.quota.user.exceeded</code> (Pour un utilisateur UNIX)<br><code>wافل.quota.user.exceeded.win</code> (Pour un utilisateur Windows)           |
| Une limite stricte est atteinte dans un quota utilisateur sur un qtree  | <code>wافل.quota.userQtree.exceeded</code> (Pour un utilisateur UNIX)<br><code>wافل.quota.userQtree.exceeded.win</code> (Pour un utilisateur Windows) |
| Une limite stricte est atteinte dans un quota de groupe sur le volume   | <code>wافل.quota.group.exceeded</code>                                                                                                                |
| Une limite stricte est atteinte dans un quota de groupe sur un qtree    | <code>wافل.quota.groupQtree.exceeded</code>                                                                                                           |
| Une limite soft, y compris un seuil, est dépassée                       | <code>quota.softlimit.exceeded</code>                                                                                                                 |
| Une limite souple n'est plus dépassée                                   | <code>quota.softlimit.normal</code>                                                                                                                   |

Le tableau suivant répertorie les traps SNMP générés par les quotas :

| Lorsque cela se produit...                        | Cette interruption SNMP est envoyée...  |
|---------------------------------------------------|-----------------------------------------|
| Une limite stricte est atteinte                   | Cédée                                   |
| Une limite soft, y compris un seuil, est dépassée | QuotaExceeemia et softQuotaExceeecediét |
| Une limite souple n'est plus dépassée             | QuotaNormal et SoftQuotaNormal          |




Les notifications contiennent des numéros d’ID de qtree plutôt que des noms de qtree. Vous pouvez mettre en corrélation les noms de qtree avec des numéros d’ID en utilisant le `volume qtree show -id` commande.

## Types et cibles de quotas

Chaque quota a un type spécifique. La cible du quota est dérivée du type et spécifie l’utilisateur, le groupe ou qtree auquel les limites du quota sont appliquées.

Le tableau suivant répertorie les cibles de quota, les types de quotas auxquels chaque cible de quota est associée et la manière dont chaque cible de quota est représentée.

| Cible de quota | Type de quota                                | Mode de représentation de la cible                                                                                                                                                                                                                               | Remarques                                                                                                                                                                                                                                          |
|----------------|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| utilisateur    | quota utilisateur                            | Nom d'utilisateur UNIX<br>UID UNIX<br><br>Fichier ou répertoire dont l'UID correspond à l'utilisateur<br><br>Nom d'utilisateur Windows au format pré-Windows 2000<br><br>SID Windows<br><br>Fichier ou répertoire avec un ACL détenu par le SID de l'utilisateur | Les quotas utilisateur peuvent être appliqués pour un volume ou qtree spécifique.                                                                                                                                                                  |
| groupe         | quota de groupe                              | Nom du groupe UNIX<br>GID UNIX<br><br>Fichier ou répertoire dont le GID correspond au groupe                                                                                                                                                                     | Les quotas group peuvent être appliqués pour un volume ou qtree spécifique.<br><br> La ONTAP ne s'applique pas aux quotas de groupe basés sur les ID Windows. |
| qtree          | quota d'arbre                                | nom du qtree                                                                                                                                                                                                                                                     | Les quotas d'arborescence sont appliqués à un volume en particulier et n'affectent pas les qtrees des autres volumes.                                                                                                                              |
| ""             | quota rroup utilisateur<br><br>quota d'arbre | Guillemets doubles ("" )                                                                                                                                                                                                                                         | Une cible de quota de "" désigne un quota <i>default</i> . Pour les quotas par défaut, le type de quota est déterminé par la valeur du champ type.                                                                                                 |

## Types spéciaux de quotas

## Fonctionnement des quotas par défaut

Vous pouvez utiliser des quotas par défaut pour appliquer un quota à toutes les instances d'un type de quota donné. Par exemple, un quota utilisateur par défaut affecte tous les utilisateurs du système pour le volume FlexVol ou qtree spécifié. Par ailleurs, les quotas par défaut vous permettent de modifier facilement vos quotas.

Vous pouvez utiliser des quotas par défaut pour appliquer automatiquement une limite à un grand ensemble de cibles de quotas sans avoir à créer de quotas distincts pour chaque cible. Par exemple, si vous souhaitez limiter la plupart des utilisateurs à 10 Go d'espace disque, vous pouvez spécifier un quota utilisateur par défaut de 10 Go d'espace disque au lieu de créer un quota pour chaque utilisateur. Si vous avez des utilisateurs spécifiques pour lesquels vous souhaitez appliquer une limite différente, vous pouvez créer des quotas explicites pour ces utilisateurs. (Quotas explicites—quotas avec une cible ou une liste spécifique de cibles—outrepasser les quotas par défaut.)

En outre, les quotas par défaut vous permettent d'utiliser le redimensionnement plutôt que la réinitialisation lorsque vous souhaitez que les modifications de quotas prennent effet. Par exemple, si vous ajoutez un quota utilisateur explicite à un volume qui dispose déjà d'un quota utilisateur par défaut, vous pouvez activer le nouveau quota en le redimensionnant.

Les quotas par défaut peuvent être appliqués aux trois types de cibles de quota (utilisateurs, groupes et qtrees).

Les quotas par défaut n'ont pas nécessairement des limites spécifiées ; un quota par défaut peut être un quota de suivi.

Un quota est indiqué par une cible qui est soit une chaîne vide ("" ) soit un astérisque (\*), selon le contexte :

- Lorsque vous créez un quota à l'aide de `volume quota policy rule create` commande, paramétrage du `-target` le paramètre d'une chaîne vide ("" ) crée un quota par défaut.
- Dans le `volume quota policy rule create` commande, le `-qtree` paramètre spécifie le nom du qtree vers lequel la règle de quotas s'applique. Ce paramètre n'est pas applicable aux règles de type d'arborescence. Pour les règles de type utilisateur ou groupe au niveau du volume, ce paramètre doit contenir « ».
- Dans la sortie du `volume quota policy rule show` commande, un quota par défaut apparaît avec une chaîne vide ("" ) comme cible.
- Dans la sortie du `volume quota report` Commande, un quota par défaut apparaît avec un astérisque (\*) comme identifiant et indicateur de quota.

## Exemple de quota utilisateur par défaut

La règle de quota suivante utilise un quota utilisateur par défaut pour appliquer une limite de 50 Mo à chaque utilisateur pour vol1 :



```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

|              |        |       |                 |       |       |              |       |
|--------------|--------|-------|-----------------|-------|-------|--------------|-------|
| Vserver: vs0 |        |       | Policy: default |       |       | Volume: vol1 |       |
|              |        |       |                 |       | Soft  |              | Soft  |
|              |        |       | User            | Disk  | Disk  | Files        | Files |
| Type         | Target | Qtree | Mapping         | Limit | Limit | Limit        | Limit |
| Threshold    |        |       |                 |       |       |              |       |
| -----        | -----  | ----- | -----           | ----- | ----- | -----        | ----- |
| -----        | -----  |       |                 |       |       |              |       |
| user         | ""     | ""    | off             | 50MB  | -     | -            | -     |
| -            |        |       |                 |       |       |              |       |

Si un utilisateur du système entre une commande qui ferait que les données de l'utilisateur prennent plus de 50 Mo dans vol1 (par exemple, l'écriture dans un fichier à partir d'un éditeur), la commande échoue.

### Comment utiliser des quotas explicites

Vous pouvez utiliser des quotas explicites pour spécifier un quota pour une cible de quota spécifique ou pour remplacer un quota par défaut pour une cible spécifique.

Un quota explicite spécifie une limite pour un utilisateur, un groupe ou un qtree spécifique. Un quota explicite remplace tout quota par défaut en place pour la même cible.

Lorsque vous ajoutez un quota utilisateur explicite pour un utilisateur possédant un quota utilisateur dérivé, vous devez utiliser le même paramètre de mappage utilisateur que le quota utilisateur par défaut. Sinon, lorsque vous redimensionnez des quotas, le quota utilisateur explicite est rejeté car il est considéré comme un nouveau quota.

Les quotas explicites n'affectent que les quotas par défaut au même niveau (volume ou qtree). Par exemple, un quota utilisateur explicite pour un qtree n'affecte pas le quota utilisateur par défaut pour le volume qui contient ce qtree. Cependant, le quota utilisateur explicite pour les remplacements de qtree (remplace les limites définies par) le quota utilisateur par défaut pour ce qtree.

### Exemples de quotas explicites

Les règles de quota suivantes définissent un quota utilisateur par défaut qui limite tous les utilisateurs de vol1 à 50 Mo d'espace. Cependant, un utilisateur, jsmith, est autorisé à 80 Mo d'espace, en raison du quota explicite (indiqué en gras) :

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m
```

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith" -qtree "" -disk-limit 80m
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

| Vserver: vs0 |        |       | Policy: default |            |                 | Volume: vol1 |                  |
|--------------|--------|-------|-----------------|------------|-----------------|--------------|------------------|
| Type         | Target | Qtree | User Mapping    | Disk Limit | Soft Disk Limit | Files Limit  | Soft Files Limit |
| user         | ""     | ""    | off             | 50MB       | -               | -            | -                |
| user         | jsmith | ""    | off             | 80MB       | -               | -            | -                |

La règle de quota suivante limite l'utilisateur spécifié, représenté par quatre ID, à 550 Mo d'espace disque et 10,000 fichiers dans le volume vol1 :

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544" -qtree "" -disk
-limit 550m -file-limit 10000
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

| Vserver: vs0 |                                                          |       | Policy: default |            |                 | Volume: vol1 |                  |
|--------------|----------------------------------------------------------|-------|-----------------|------------|-----------------|--------------|------------------|
| Type         | Target                                                   | Qtree | User Mapping    | Disk Limit | Soft Disk Limit | Files Limit  | Soft Files Limit |
| user         | "jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544" | ""    | off             | 550MB      | -               | 10000        | -                |

La règle de quota suivante limite le groupe eng1 à 150 Mo d'espace disque et un nombre illimité de fichiers dans le qtree proj1 :

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type group -target "eng1" -qtree "proj1" -disk-limit
150m
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol2
```

|              |        |       |                 |       |       |              |       |
|--------------|--------|-------|-----------------|-------|-------|--------------|-------|
| Vserver: vs0 |        |       | Policy: default |       |       | Volume: vol2 |       |
|              |        |       |                 |       | Soft  |              | Soft  |
|              |        |       | User            | Disk  | Disk  | Files        | Files |
| Type         | Target | Qtree | Mapping         | Limit | Limit | Limit        | Limit |
| Threshold    |        |       |                 |       |       |              |       |
| -----        | -----  | ----- | -----           | ----- | ----- | -----        | ----- |
| -----        |        |       |                 |       |       |              |       |
| group        | eng1   | proj1 | off             | 150MB | -     | -            | -     |
| -            |        |       |                 |       |       |              |       |

La règle de quota suivante limite le qtree proj1 du volume vol2 à 750 Mo d'espace disque et 75,000 fichiers :

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type tree -target "proj1" -disk-limit 750m -file
-limit 75000
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol2
```

|              |        |       |                 |       |       |              |       |
|--------------|--------|-------|-----------------|-------|-------|--------------|-------|
| Vserver: vs0 |        |       | Policy: default |       |       | Volume: vol2 |       |
|              |        |       |                 |       | Soft  |              | Soft  |
|              |        |       | User            | Disk  | Disk  | Files        | Files |
| Type         | Target | Qtree | Mapping         | Limit | Limit | Limit        | Limit |
| Threshold    |        |       |                 |       |       |              |       |
| -----        | -----  | ----- | -----           | ----- | ----- | -----        | ----- |
| -----        |        |       |                 |       |       |              |       |
| tree         | proj1  | ""    | -               | 750MB | -     | 75000        | -     |
| -            |        |       |                 |       |       |              |       |

## Fonctionnement des quotas dérivés

Un quota appliqué à la suite d'un quota par défaut, plutôt qu'un quota explicite (un quota avec une cible spécifique), est appelé quota *dérivé*.

Le nombre et l'emplacement des quotas dérivés dépendent du type de quota :

- Un quota Tree par défaut sur un volume crée des quotas Tree par défaut pour chaque qtree du volume.
- Un quota d'utilisateur ou de groupe par défaut crée un quota d'utilisateur ou de groupe dérivé pour chaque utilisateur ou groupe qui possède un fichier au même niveau (volume ou qtree).

- Un quota d'utilisateur ou de groupe par défaut sur un volume crée un quota d'utilisateur ou de groupe par défaut sur chaque qtree qui possède également un quota Tree.

Les paramètres, y compris les limites et le mappage des utilisateurs, des quotas dérivés sont les mêmes que ceux des quotas par défaut correspondants. Par exemple, un quota Tree par défaut avec une limite de disque de 20 Go sur un volume crée des quotas d'arborescence dérivés avec des limites de disque de 20 Go sur les qtrees du volume. Si un quota par défaut est un quota de suivi (sans limites), les quotas dérivés sont également le suivi des quotas.

Pour voir les quotas dérivés, vous pouvez générer un rapport de quota. Dans le rapport, un quota d'utilisateur ou de groupe dérivé est indiqué par un indicateur de quota vierge ou astérisque (\*). Un quota d'arborescence dérivé, cependant, a un Spécifier de quota ; pour identifier un quota d'arborescence dérivé, vous devez rechercher un quota d'arborescence par défaut sur le volume avec les mêmes limites.

Les quotas explicites interagissent avec les quotas dérivés de la manière suivante :

- Les quotas dérivés ne sont pas créés si un quota explicite existe déjà pour la même cible.
- Si un quota dérivé existe lorsque vous créez un quota explicite pour une cible, vous pouvez activer le quota explicite en le redimensionnant au lieu d'avoir à effectuer une initialisation complète du quota.

### Utiliser des quotas de suivi

Un quota de suivi génère un rapport sur l'utilisation des disques et des fichiers et ne limite pas l'utilisation des ressources. Lorsque des quotas de suivi sont utilisés, la modification des valeurs de quota est moins perturbatrice car vous pouvez redimensionner les quotas plutôt que de les désactiver puis de les activer à nouveau.

Pour créer un quota de suivi, vous omettez les paramètres limite de disque et limite de fichiers. Cela permet à ONTAP de surveiller l'utilisation des disques et des fichiers pour cette cible à ce niveau (volume ou qtree), sans imposer de limites. Les quotas de suivi sont indiqués dans la sortie de `show` commandes et le rapport de quota avec un tiret ("-") pour toutes les limites. ONTAP crée automatiquement des quotas de suivi lorsque vous utilisez l'interface utilisateur de System Manager pour créer des quotas explicites (quotas avec des cibles spécifiques). Lors de l'utilisation de l'interface de ligne de commandes, l'administrateur du stockage crée des quotas de suivi en plus des quotas explicites.

Vous pouvez également spécifier un quota de suivi par défaut\_, qui s'applique à toutes les instances de la cible. Les quotas par défaut de suivi vous permettent de suivre l'utilisation de toutes les instances d'un type de quota (par exemple, tous les qtrees ou tous les utilisateurs). De plus, elles vous permettent d'utiliser le redimensionnement plutôt que la réinitialisation lorsque vous voulez que les modifications de quotas soient appliquées.

### Exemples

Le résultat d'une règle de suivi affiche les quotas de suivi en place pour un qtree, un utilisateur et un groupe, comme illustré dans l'exemple suivant pour une règle de suivi au niveau des volumes :

| Vserver: vs0 |        |       | Policy: default |       |            | Volume: fv1 |             |           |
|--------------|--------|-------|-----------------|-------|------------|-------------|-------------|-----------|
|              |        |       | User            | Disk  | Soft       | Files       | Soft        |           |
| Type         | Target | Qtree | Mapping         | Limit | Disk Limit | Files Limit | Files Limit | Threshold |
| -----        | -----  | ----- | -----           | ----- | -----      | -----       | -----       | -----     |
| tree         | ""     | ""    | -               | -     | -          | -           | -           | -         |
| user         | ""     | ""    | off             | -     | -          | -           | -           | -         |
| group        | ""     | ""    | -               | -     | -          | -           | -           | -         |

### Mode d'application des quotas

La compréhension de l'application des quotas vous permet de configurer correctement les quotas et de définir les limites attendues.

Chaque fois qu'une tentative de création d'un fichier ou d'écriture des données dans un fichier d'un volume FlexVol sur lequel des quotas sont activés, les limites des quotas sont vérifiées avant la fin de l'opération. Si l'opération dépasse la limite du disque ou la limite des fichiers, l'opération est empêchée.

Les limites de quota sont vérifiées dans l'ordre suivant :

1. Le quota Tree pour ce qtree (cette vérification n'est pas pertinente si le fichier est en cours de création ou d'écriture sur qtree0.)
2. Quota utilisateur pour l'utilisateur propriétaire du fichier sur le volume
3. Quota de groupe pour le groupe propriétaire du fichier sur le volume
4. Le quota utilisateur pour l'utilisateur propriétaire du fichier sur le qtree (cette vérification n'est pas pertinente si le fichier est créé ou écrit sur qtree0.)
5. Le quota de groupe pour le groupe qui détient le fichier sur le qtree (cette vérification n'est pas pertinente si le fichier est créé ou écrit sur qtree0.)

Le quota avec la limite la plus petite peut ne pas être celui qui est dépassé en premier. Par exemple, si un quota utilisateur pour le volume vol1 est de 100 Go, Et le quota utilisateur pour le qtree q2 contenu dans le volume vol1 est de 20 Go, la limite du volume peut être atteinte en premier si l'utilisateur a déjà écrit plus de 80 Go de données dans le volume vol1 (mais en dehors du qtree q2).

### Informations associées

- ["Mode d'application des quotas à l'utilisateur racine"](#)
- ["Mode d'application des quotas aux utilisateurs avec plusieurs ID"](#)

### Considérations relatives à l'attribution de politiques de quotas

Une politique de quotas est un regroupement des règles de quotas pour l'ensemble des volumes FlexVol d'un SVM. Vous devez tenir compte de certaines considérations lors de l'attribution des politiques de quotas.

- Un SVM dispose d'une politique de quotas attribuée à tout moment. Lorsqu'un SVM est créé, une politique de quotas vierge est créée et attribuée à la SVM. Cette politique de quotas par défaut porte le nom « default », sauf si un autre nom est spécifié lors de la création de la SVM.

- Un SVM peut disposer jusqu'à cinq politiques de quotas. Si un SVM possède cinq politiques de quotas, vous ne pouvez pas créer une nouvelle politique de quotas pour la SVM jusqu'à ce que vous ayez supprimé une politique de quotas existante.
- Lorsque vous devez créer une règle de quotas ou modifier les règles de quotas pour une politique de quotas, vous pouvez choisir l'une des approches suivantes :
  - Si vous travaillez dans une politique de quotas qui est attribuée à un SVM, vous n'avez pas besoin d'affecter la politique de quotas à la SVM.
  - Si vous travaillez dans une politique de quotas non attribuée, puis affectez-lui la politique de quotas, vous devez sauvegarder la politique de quotas auxquels vous pourrez revenir si nécessaire.

Par exemple, vous pouvez faire une copie de la politique de quotas attribuée, modifier la copie, affecter la copie à la SVM et renommer la politique de quotas d'origine.

- Vous pouvez renommer une politique de quotas même lorsqu'elle est attribuée à la SVM.

## Fonctionnement des quotas avec les utilisateurs et les groupes

### Présentation du fonctionnement des quotas avec les utilisateurs et les groupes

Vous pouvez spécifier un utilisateur ou un groupe comme cible d'un quota. Il y a plusieurs différences de mise en œuvre à prendre en compte lors de la définition d'un quota.

Voici quelques-unes des différences dont vous devez tenir compte :

- Utilisateur ou groupe
- UNIX ou Windows
- Utilisateurs et groupes spéciaux
- Plusieurs ID sont-ils inclus

Il existe également différentes façons de spécifier les ID des utilisateurs en fonction de votre environnement.

### Spécifiez les utilisateurs UNIX pour les quotas

Vous pouvez spécifier un utilisateur UNIX pour un quota dans l'un des différents formats.

Les trois formats disponibles lors de la spécification d'un utilisateur UNIX pour un quota sont les suivants :

- Le nom d'utilisateur (par exemple jsmith).



Vous ne pouvez pas utiliser un nom d'utilisateur UNIX pour spécifier un quota si ce nom comprend une barre oblique inverse (\) ou un signe @. Ceci est dû au fait que ONTAP traite les noms contenant ces caractères comme des noms Windows.

- ID utilisateur ou UID (par exemple, 20).
- Le chemin d'accès d'un fichier ou d'un répertoire appartenant à cet utilisateur, de sorte que l'UID du fichier corresponde à celui de l'utilisateur.



Si vous spécifiez un nom de fichier ou de répertoire, vous devez sélectionner un fichier ou un répertoire qui durera tant que le compte utilisateur reste sur le système.

La spécification d'un nom de fichier ou de répertoire pour l'UID n'entraîne pas ONTAP l'application d'un quota à ce fichier ou répertoire.

## Spécifiez les utilisateurs Windows pour les quotas

Vous pouvez spécifier un utilisateur Windows pour un quota dans l'un des différents formats.

Les trois formats disponibles lors de la spécification d'un utilisateur Windows pour un quota sont les suivants :

- Le nom Windows au format pré-Windows 2000.
- L'ID de sécurité (SID) tel qu'affiché par Windows sous forme de texte, tel que S-1-5-32-544.
- Nom d'un fichier ou d'un répertoire qui possède un ACL appartenant au SID de cet utilisateur.



Si vous spécifiez un nom de fichier ou de répertoire, vous devez sélectionner un fichier ou un répertoire qui durera tant que le compte utilisateur reste sur le système.

Pour que ONTAP puisse obtenir le SID à partir de la liste de contrôle d'accès, la liste de contrôle d'accès doit être valide.

Si le fichier ou le répertoire existe dans un qtree de style UNIX, ou si le système de stockage utilise le mode UNIX pour l'authentification utilisateur, ONTAP applique le quota utilisateur à l'utilisateur dont **UID**, et non SID, correspond à celui du fichier ou du répertoire.

La spécification d'un nom de fichier ou de répertoire pour identifier un utilisateur pour un quota n'entraîne pas l'application par ONTAP d'un quota à ce fichier ou ce répertoire.

## Comment les quotas d'utilisateur et de groupe par défaut créent des quotas dérivés

Lorsque vous créez des quotas d'utilisateur ou de groupe par défaut, les quotas d'utilisateur ou de groupe dérivés correspondants sont automatiquement créés pour chaque utilisateur ou groupe qui possède des fichiers au même niveau.

Les quotas d'utilisateur et de groupe dérivés sont créés de l'une des manières suivantes :

- Un quota utilisateur par défaut sur un volume FlexVol crée des quotas utilisateur dérivés pour chaque utilisateur propriétaire d'un fichier n'importe où sur le volume.
- Un quota utilisateur par défaut sur un qtree crée des quotas d'utilisateur dérivés pour chaque utilisateur qui possède un fichier dans le qtree.
- Un quota de groupe par défaut sur un volume FlexVol crée des quotas de groupe dérivés pour chaque groupe qui possède un fichier n'importe où sur le volume.
- Un quota de groupe par défaut sur un qtree crée des quotas de groupe dérivés pour chaque groupe qui possède un fichier dans le qtree.

Si un utilisateur ou un groupe ne possède pas de fichiers au niveau d'un quota utilisateur ou groupe par défaut, les quotas dérivés ne sont pas créés pour l'utilisateur ou le groupe. Par exemple, si un quota utilisateur

par défaut est créé pour qtree proj1 et que l'utilisateur jsmith possède des fichiers sur un qtree différent, aucun quota utilisateur dérivé n'est créé pour jsmith.

Les quotas dérivés ont les mêmes paramètres que les quotas par défaut, y compris les limites et le mappage des utilisateurs. Par exemple, si un quota utilisateur par défaut a une limite de disque de 50 Mo et que le mappage des utilisateurs est activé, tous les quotas dérivés résultant ont également une limite de disque de 50 Mo et un mappage des utilisateurs activés.

Cependant, il n'existe aucune limite dans les quotas dérivés pour trois utilisateurs et groupes spéciaux. Si les utilisateurs et groupes suivants possèdent des fichiers au niveau d'un quota utilisateur ou groupe par défaut, un quota dérivé est créé avec le même paramètre de mappage utilisateur que le quota utilisateur ou groupe par défaut, mais il ne s'agit que d'un quota de suivi (sans limites) :

- Utilisateur root UNIX (UID 0)
- Groupe racine UNIX (GID 0)
- Groupe Windows BUILTIN\Administrators

Comme les quotas pour les groupes Windows sont suivis comme des quotas d'utilisateur, un quota dérivé pour ce groupe est un quota d'utilisateur dérivé d'un quota d'utilisateur par défaut, et non d'un quota de groupe par défaut.

**Exemple de quotas d'utilisateur dérivés**

Si vous avez un volume où trois utilisateurs (fichiers root, jsmith et bob) sont propriétaires, et que vous créez un quota d'utilisateur par défaut sur le volume, ONTAP crée automatiquement trois quotas d'utilisateurs dérivés. Ainsi, une fois de nouveau initialisez les quotas sur le volume, quatre nouveaux quotas apparaissent dans le rapport quota :

```
cluster1::> volume quota report
Vserver: vs1

Volume Tree Type ID ----Disk---- ----Files----- Quota
Specifier Used Limit Used Limit
----- -
vol1 user * 0B 50MB 0 - *
vol1 user root 5B - 1 -
vol1 user jsmith 30B 50MB 10 - *
vol1 user bob 40B 50MB 15 - *
4 entries were displayed.
```

La première nouvelle ligne est le quota utilisateur par défaut que vous avez créé, qui est identifiable par l'astérisque (\*) comme ID. Les autres nouvelles lignes sont les quotas d'utilisateur dérivés. Les quotas dérivés pour jsmith et bob ont la même limite de disque de 50 Mo que le quota par défaut. Le quota dérivé pour l'utilisateur root est un quota de suivi sans limites.

**Mode d'application des quotas à l'utilisateur racine**

L'utilisateur root (UID=0) sur les clients UNIX est soumis à des quotas d'arborescence, mais pas à des quotas d'utilisateur ou de groupe. Cela permet à l'utilisateur root de



prendre des actions pour le compte d'autres utilisateurs qui seraient autrement empêchés par un quota.

Lorsque l'utilisateur root effectue une modification de propriété de fichier ou de répertoire ou une autre opération (telle que la `chown` commande UNIX) pour le compte d'un utilisateur avec moins de Privileges, ONTAP vérifie les quotas en fonction du nouveau propriétaire mais ne signale pas d'erreurs ou n'arrête pas l'opération, même si les restrictions de quota matériel du nouveau propriétaire sont dépassées. Cela peut être utile lorsqu'une action administrative, telle que la récupération de données perdues, entraîne un dépassement temporaire des quotas.



Une fois le transfert de propriété effectué, un système client signale une erreur d'espace disque si l'utilisateur tente d'allouer plus d'espace disque alors que le quota est encore dépassé.

#### Informations associées

- ["Mode d'application des quotas"](#)
- ["Mode d'application des quotas aux utilisateurs avec plusieurs ID"](#)

#### Fonctionnement des quotas avec des groupes Windows spéciaux

Il existe plusieurs groupes Windows spéciaux qui traitent les quotas différemment des autres groupes Windows. Vous devez comprendre comment les quotas sont appliqués à ces groupes spéciaux.



ONTAP ne prend pas en charge les quotas de groupe basés sur les ID de groupe Windows. Si vous spécifiez un ID de groupe Windows comme cible de quota, le quota est considéré comme un quota utilisateur.

#### Tout le monde

Lorsque la cible de quota est le groupe Everyone, un fichier avec une ACL indiquant le propriétaire est Everyone est compté sous le SID pour tout le monde.

#### INTÉGRÉ\administrateurs

Lorsque la cible de quota est le groupe BUILTIN\Administrators, l'entrée est considérée comme un quota utilisateur et est utilisée uniquement pour le suivi. Vous ne pouvez pas imposer de restrictions à BUILTIN\Administrators. Si un membre de BUILTIN\Administrators crée un fichier, ce dernier appartient à BUILTIN\Administrators et est compté sous le SID pour BUILTIN\Administrators (pas le SID personnel de l'utilisateur).

#### Mode d'application des quotas aux utilisateurs avec plusieurs ID

Un utilisateur peut être représenté par plusieurs ID. Vous pouvez définir un quota utilisateur unique pour un tel utilisateur en spécifiant une liste d'ID comme cible de quota. Un fichier appartenant à l'un de ces ID est soumis à la restriction du quota d'utilisateur.

Supposons qu'un utilisateur possède l'UID UNIX 20 et les ID Windows `corp\john_smith` et `engineering\jsmith`. Pour cet utilisateur, vous pouvez spécifier un quota où la cible de quota est une liste des ID UID et Windows. Lorsque cet utilisateur écrit sur le système de stockage, le quota spécifié s'applique, que l'écriture provient de 20 l'UID, `corp\john_smith`, ou `engineering\jsmith`.

Notez que des règles de quota distinctes sont considérées comme des cibles séparées, même si les ID

appartiennent au même utilisateur. Par exemple, pour le même utilisateur, vous pouvez spécifier un quota qui limite l'UID 20 à 1 Go d'espace disque et un autre quota qui limite corp\john\_smith à 2 Go d'espace disque, même si les deux ID représentent le même utilisateur. ONTAP applique des quotas à l'UID 20 et corp\john\_smith séparément. Dans ce cas, aucune limite n'est appliquée à engineering\jsmith, même si des limites sont appliquées aux autres ID utilisés par le même utilisateur.

**Informations associées**

- ["Mode d'application des quotas"](#)
- ["Mode d'application des quotas à l'utilisateur racine"](#)

**La manière dont ONTAP détermine les ID d'utilisateur dans un environnement mixte**

Si des utilisateurs accèdent à votre stockage ONTAP à partir de clients Windows et UNIX, la sécurité Windows et UNIX sert à déterminer la propriété des fichiers. Plusieurs facteurs déterminent si ONTAP utilise un ID UNIX ou Windows lors de l'application de quotas d'utilisateur.

Si le style de sécurité du volume qtree ou FlexVol qui contient le fichier est uniquement NTFS ou UNIX, le style de sécurité détermine le type d'ID utilisé lors de l'application de quotas d'utilisateur. Pour les qtrees avec le style de sécurité mixte, le type d'ID utilisé est déterminé par le type d'ACL du fichier.

Le tableau suivant récapitule le type d'ID utilisé.

| Style de sécurité | ACL        | Aucune ACL |
|-------------------|------------|------------|
| UNIX              | ID UNIX    | ID UNIX    |
| Mixte             | ID Windows | ID UNIX    |
| NTFS              | ID Windows | ID Windows |

**Fonctionnement des quotas avec plusieurs utilisateurs**

Lorsque vous placez plusieurs utilisateurs dans la même cible de quota, les limites définies par le quota ne sont pas appliquées à chaque utilisateur individuel. Au contraire, les limites de quota sont partagées entre tous les utilisateurs de la cible de quota.

Contrairement aux commandes permettant de gérer des objets, telles que les volumes et les qtrees, vous ne pouvez pas renommer une cible de quota, y compris un quota multi-utilisateurs. Cela signifie qu'après la définition d'un quota multi-utilisateurs, vous ne pouvez pas modifier les utilisateurs dans la cible du quota et vous ne pouvez pas ajouter d'utilisateurs à une cible ou supprimer des utilisateurs d'une cible. Si vous souhaitez ajouter ou supprimer un utilisateur d'un quota multi-utilisateurs, le quota contenant cet utilisateur doit être supprimé et une nouvelle règle de quota avec l'ensemble des utilisateurs dans la cible définie.



Si vous combinez des quotas d'utilisateur distincts en un quota multi-utilisateurs, vous pouvez activer la modification en redimensionnant les quotas. Cependant, si vous souhaitez supprimer des utilisateurs d'une cible de quota avec plusieurs utilisateurs ou ajouter des utilisateurs à une cible qui a déjà plusieurs utilisateurs, vous devez réinitialiser les quotas avant que la modification ne prenne effet.

## Exemple de plusieurs utilisateurs dans une règle de quotas

Dans l'exemple suivant, deux utilisateurs sont répertoriés dans l'entrée quota. Les deux utilisateurs peuvent utiliser jusqu'à 80 Mo d'espace combiné. Si l'un utilise 75 Mo, l'autre ne peut utiliser que 5 Mo.

```
cluster1::> volume quota policy rule create -vserver vs0 -volume voll
-policy-name default -type user -target "jsmith,chen" -qtree "" -disk
-limit 80m
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume voll
```

| Vserver: vs0 |               |       | Policy: default |       | Volume: voll |       |       |
|--------------|---------------|-------|-----------------|-------|--------------|-------|-------|
|              |               |       | User            | Disk  | Soft         | Soft  |       |
| Type         | Target        | Qtree | Mapping         | Limit | Disk         | Files | Files |
| Threshold    |               |       |                 |       | Limit        | Limit | Limit |
| -----        | -----         | ----- | -----           | ----- | -----        | ----- | ----- |
| -----        |               |       |                 |       |              |       |       |
| user         | "jsmith,chen" | ""    | off             | 80MB  | -            | -     | -     |
| -            |               |       |                 |       |              |       |       |

## Liaison de noms UNIX et Windows pour les quotas

Dans un environnement mixte, les utilisateurs peuvent se connecter en tant qu'utilisateurs Windows ou UNIX. Vous pouvez configurer des quotas pour reconnaître que l'ID UNIX et l'ID Windows d'un utilisateur représentent le même utilisateur.

Les quotas pour le nom d'utilisateur Windows sont mappés vers un nom d'utilisateur UNIX, ou vice versa, lorsque les deux conditions suivantes sont remplies :

- Le `user-mapping` le paramètre est défini sur « on » dans la règle de quotas pour l'utilisateur.
- Les noms d'utilisateur ont été mappés avec le `vserver name-mapping` commandes.

Lorsqu'un nom UNIX et Windows sont mappés ensemble, ils sont traités comme la même personne pour déterminer l'utilisation d'un quota.

## Fonctionnement des quotas d'arbres

### Présentation du fonctionnement des quotas d'arborescence

Vous pouvez créer un quota avec un `qtree` en tant que cible pour limiter la taille du `qtree` cible. Ces quotas sont également appelés *Tree quotas*.



Vous pouvez également créer des quotas d'utilisateur et de groupe pour un `qtree` spécifique. De plus, les quotas d'un volume FlexVol sont parfois hérités des `qtrees` contenu par ce volume.

Lorsque vous appliquez un quota à un `qtree`, le résultat est similaire à une partition de disque, sauf que vous pouvez modifier la taille maximale du `qtree` à tout moment en modifiant le quota. Lors de l'application d'un quota Tree, ONTAP limite l'espace disque et le nombre de fichiers dans le `qtree`, indépendamment de leurs

propriétaires. Aucun utilisateur, y compris la racine et les membres du groupe BUILTIN\Administrators, ne peut écrire dans le qtree si l'opération d'écriture entraîne le dépassement du quota Tree.

La taille du quota ne garantit aucune quantité spécifique d'espace disponible. La taille du quota peut être supérieure à la quantité d'espace libre disponible pour le qtree. Vous pouvez utiliser le `volume quota report` commande permettant de déterminer la quantité réelle d'espace disponible dans le qtree.

### Fonctionnement des quotas d'utilisateurs et de groupes avec les qtrees

Les quotas d'arborescence limitent la taille globale du qtree. Pour éviter que des utilisateurs ou groupes individuels ne consomment l'intégralité du qtree, vous spécifiez un quota d'utilisateur ou de groupe pour ce qtree.

#### Exemple de quota d'utilisateur dans un qtree

Supposons que vous ayez les règles de quota suivantes :

```
cluster1::> volume quota policy rule show -vserver vs0 -volume voll
```

| Vserver: vs0 |        |       | Policy: default |            | Volume: voll    |             |                  |
|--------------|--------|-------|-----------------|------------|-----------------|-------------|------------------|
| Type         | Target | Qtree | User Mapping    | Disk Limit | Soft Disk Limit | Files Limit | Soft Files Limit |
| Threshold    |        |       |                 |            |                 |             |                  |
| -----        | -----  | ----- | -----           | -----      | -----           | -----       | -----            |
| -----        |        |       |                 |            |                 |             |                  |
| user         | ""     | ""    | off             | 50MB       | -               | -           | -                |
| 45MB         |        |       |                 |            |                 |             |                  |
| user         | jsmith | ""    | off             | 80MB       | -               | -           | -                |
| 75MB         |        |       |                 |            |                 |             |                  |

Vous remarquez qu'un certain utilisateur, kjones, occupe trop d'espace dans un qtree critique, proj1, qui réside dans vol1. Vous pouvez restreindre l'espace de cet utilisateur en ajoutant la règle de quota suivante :

```
cluster1::> volume quota policy rule create -vserver vs0 -volume voll
-policy-name default -type user -target "kjones" -qtree "proj1" -disk
-limit 20m -threshold 15m
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume voll
```

| Vserver: vs0 |        |       | Policy: default |            | Volume: voll    |             |                  |
|--------------|--------|-------|-----------------|------------|-----------------|-------------|------------------|
| Type         | Target | Qtree | User Mapping    | Disk Limit | Soft Disk Limit | Files Limit | Soft Files Limit |
| user         | ""     | ""    | off             | 50MB       | -               | -           | -                |
| 45MB         |        |       |                 |            |                 |             |                  |
| user         | jsmith | ""    | off             | 80MB       | -               | -           | -                |
| 75MB         |        |       |                 |            |                 |             |                  |
| user         | kjones | proj1 | off             | 20MB       | -               | -           | -                |
| 15MB         |        |       |                 |            |                 |             |                  |

### Comment les quotas par défaut des arborescences d'un volume FlexVol créent des quotas d'arborescence dérivés

Lorsque vous créez un quota Tree par défaut sur un volume FlexVol, les quotas d'arborescence dérivés correspondants sont automatiquement créés pour chaque qtree de ce volume.

Ces quotas d'arborescence dérivés ont les mêmes limites que le quota d'arborescence par défaut. S'il n'existe pas de quotas supplémentaires, les limites ont les effets suivants :

- Les utilisateurs peuvent utiliser autant d'espace dans un qtree qu'ils sont alloués à l'intégralité du volume (à condition qu'ils n'aient pas dépassé la limite du volume en utilisant l'espace à la racine ou à un autre qtree).
- Chaque qtree peut être davantage de capacité à consommer la totalité du volume.

L'existence d'un quota Tree par défaut sur un volume continue d'affecter tous les nouveaux qtrees qui sont ajoutés au volume. Chaque fois qu'un qtree est créé, un quota Tree dérivé est également créé.

Comme tous les quotas dérivés, les quotas d'arborescence dérivés affichent les comportements suivants :

- Sont créés uniquement si la cible ne dispose pas déjà d'un quota explicite.
- S'affiche dans les rapports de quotas, mais n'apparaît pas lorsque vous affichez les règles de quota avec le `volume quota policy rule show` commande.

### Exemple de quotas d'arborescence dérivés

Vous disposez d'un volume avec trois qtrees (proj1, proj2 et proj3), et le seul quota Tree est un quota explicite sur le qtree proj1 qui limite sa taille de disque à 10 Go. Si vous créez un quota d'arborescence par défaut sur le volume et que vous réinitialisez les quotas sur le volume, le rapport quota contient maintenant quatre quotas

d'arborescence :

| Volume<br>Specifier | Tree  | Type  | ID    | ----Disk---- |       | ----Files----- |       | Quota |
|---------------------|-------|-------|-------|--------------|-------|----------------|-------|-------|
|                     |       |       |       | Used         | Limit | Used           | Limit |       |
| -----               | ----- | ----- | ----- | -----        | ----- | -----          | ----- |       |
| -----               |       |       |       |              |       |                |       |       |
| vol1                | proj1 | tree  | 1     | 0B           | 10GB  | 1              | -     | proj1 |
| vol1                |       | tree  | *     | 0B           | 20GB  | 0              | -     | *     |
| vol1                | proj2 | tree  | 2     | 0B           | 20GB  | 1              | -     | proj2 |
| vol1                | proj3 | tree  | 3     | 0B           | 20GB  | 1              | -     | proj3 |
| ...                 |       |       |       |              |       |                |       |       |

La première ligne montre le quota explicite d'origine sur le qtree proj1. Ce quota reste inchangé.

La seconde ligne affiche le nouveau quota Tree par défaut sur le volume. L'astérisque (\*) quota Specyfier indique qu'il s'agit d'un quota par défaut. Ce quota est le résultat de la règle de quotas que vous avez créée.

Les deux dernières lignes montrent de nouveaux quotas d'arborescence dérivés pour les qtrees proj2 et proj3. ONTAP a automatiquement créé ces quotas en raison du quota Tree par défaut sur le volume. Ces quotas d'arborescence dérivés ont la même limite de disque de 20 Go que le quota d'arborescence par défaut sur le volume. ONTAP n'a pas créé de quota Tree dérivé pour le qtree proj1 car le qtree proj1 disposait déjà d'un quota explicite.

### La manière dont les quotas d'utilisateur par défaut d'un volume FlexVol affectent les quotas des qtrees de ce volume

Lorsqu'un quota utilisateur par défaut est défini pour un volume FlexVol, un quota utilisateur par défaut est automatiquement créé pour chaque qtree contenu par ce volume pour lequel un quota Tree explicite ou dérivé existe.

Si un quota utilisateur par défaut sur le qtree existe déjà, il reste inchangé lorsque le quota utilisateur par défaut sur le volume est créé.

Les quotas d'utilisateur par défaut créés automatiquement sur les qtrees ont les mêmes limites que le quota d'utilisateur par défaut que vous créez pour le volume.

Un quota utilisateur explicite pour des remplacements de qtree (remplace les limites appliquées par) le quota utilisateur par défaut créé automatiquement, de la même manière qu'il remplace un quota utilisateur par défaut sur ce qtree créé par un administrateur.

### Comment les modifications des qtrees affectent les quotas

Lorsque vous supprimez, renommez ou modifiez le style de sécurité d'un qtree, les quotas appliqués par ONTAP peuvent changer en fonction des quotas actuels.

### Suppressions de qtree et quotas d'arborescence

Lorsque vous supprimez un qtree, tous les quotas applicables à ce qtree, qu'ils soient explicites ou dérivées, ne sont plus appliqués par ONTAP.

La persistance ou non des règles de quota dépend de l'endroit où vous supprimez le qtree :

- Si vous supprimez un qtree via ONTAP, les règles de quotas de ce qtree sont automatiquement supprimées, y compris les règles de quotas d'arborescence, ainsi que toutes les règles de quotas d'utilisateurs et de groupes configurées pour ce qtree.
- Si vous supprimez un qtree à l'aide de votre client CIFS ou NFS, vous devez supprimer toute règle de quotas applicable à ce qtree pour éviter d'obtenir des erreurs lors de la réinitialisation des quotas. Si vous créez un qtree avec le même nom que celui que vous avez supprimé, les règles de quota existantes ne s'appliquent pas au nouveau qtree tant que vous n'avez pas réinitialisé des quotas.

### La manière dont la modification du nom d'un qtree affecte les quotas

Lorsque vous renommez un qtree en utilisant ONTAP, les règles de quotas correspondant à ce qtree sont automatiquement mises à jour. Si vous renommez un qtree en utilisant vos clients CIFS ou NFS, vous devez mettre à jour les règles de quotas de ce qtree.



Si vous renommez un qtree en utilisant votre client CIFS ou NFS et que vous ne mettez pas à jour les règles de quota pour ce qtree avec le nouveau nom avant de réinitialiser les quotas, les quotas ne seront pas appliqués au qtree. Les quotas explicites pour le qtree, y compris les quotas d'arborescence et les quotas d'utilisateurs ou de groupes pour le qtree, peuvent être convertis en quotas dérivés

### Styles de sécurité qtree et quotas d'utilisateurs

Vous pouvez appliquer des listes de contrôle d'accès (ACL) sur les qtrees en utilisant des styles de sécurité NTFS ou mixte, mais pas en utilisant le style de sécurité UNIX. La modification du style de sécurité d'un qtree peut affecter le calcul des quotas. Vous devez toujours réinitialiser les quotas après avoir modifié le style de sécurité d'un qtree.

Si vous modifiez le style de sécurité d'un qtree de NTFS ou Mixed à UNIX, toutes les ACL des fichiers de ce qtree sont ignorées et l'utilisation du fichier est comptabilisée par rapport aux ID d'utilisateurs UNIX.

Si vous modifiez le style de sécurité d'un qtree d'UNIX vers un qtree NTFS ou mixte, les ACL précédemment masquées sont visibles. De plus, les ACL ignorés sont de nouveau effectives et les informations utilisateur NFS sont ignorées. Si aucune ACL n'existait auparavant, les informations NFS continuent à être utilisées dans le calcul du quota.



Pour s'assurer que les utilisations des quotas d'utilisateurs UNIX et Windows sont correctement calculées après la modification du style de sécurité d'un qtree, vous devez réinitialiser les quotas du volume contenant ce qtree.

### Exemple

L'exemple suivant montre comment une modification du style de sécurité d'un qtree entraîne l'utilisation d'un utilisateur différent pour l'utilisation d'un fichier dans ce qtree.

Supposons que la sécurité NTFS soit en vigueur sur le qtree A et qu'une liste de contrôle d'accès confère à `corp\joe` l'utilisateur Windows la propriété d'un fichier de 5 Mo. L'utilisateur `corp\joe` est facturé avec 5 Mo d'espace disque utilisé pour le qtree A.

Vous modifiez maintenant le style de sécurité du qtree A de NTFS à UNIX. Une fois les quotas réinitialisés, l'utilisateur Windows `corp\joe` n'est plus facturé pour ce fichier ; à la place, l'utilisateur UNIX correspondant à l'UID du fichier est facturé pour le fichier. L'UID peut être un utilisateur UNIX mappé à `corp\joe` ou à l'utilisateur root.

### Présentation de l'activation des quotas

Les nouveaux quotas et les modifications des quotas existants doivent être activés pour prendre effet. L'activation est effectuée au niveau du volume. Connaître le fonctionnement de l'activation des quotas peut vous aider à gérer vos quotas avec moins d'interruptions.

Les quotas sont activés soit par *initializing* (les activer) soit par *resizing*. Désactiver les quotas et les rallumer est appelé réinitialisation.

La durée du processus d'activation et son impact sur l'application des quotas dépendent du type d'activation :

- Le processus d'initialisation comprend deux parties : un `quota on` et une analyse de quota de l'intégralité du système de fichiers du volume. L'acquisition commence après le `quota on` le travail s'est terminé avec succès. L'analyse de quota peut prendre un certain temps ; plus il y a de fichiers, plus il prend de temps. Tant que l'analyse n'est pas terminée, l'activation du quota n'est pas terminée et les quotas ne sont pas appliqués.
- Le processus de redimensionnement n'implique qu'un `quota resize` travail. Le redimensionnement prend moins de temps qu'une initialisation des quotas, car il n'implique pas d'analyse des quotas. Lors d'un processus de redimensionnement, les quotas continuent d'être appliqués.

Par défaut, le `quota on` et `quota resize` les travaux s'exécutent en arrière-plan, ce qui vous permet d'utiliser d'autres commandes en même temps.

Les erreurs et avertissements du processus d'activation sont envoyés au système de gestion des événements. Si vous utilisez le `-foreground` paramètre avec le `volume quota on` ou `volume quota resize` commandes, la commande ne retourne pas tant que le travail n'est pas terminé ; ceci est utile si vous êtes en cours de réinitialisation à partir d'un script. Pour afficher les erreurs et les avertissements ultérieurement, vous pouvez utiliser le `volume quota show` commande avec `-instance` paramètre.

L'activation du quota persiste entre les halts et les redémarrages. Le processus d'activation des quotas n'affecte pas la disponibilité des données du système de stockage.

### Comprendre quand utiliser le redimensionnement

Le redimensionnement de quota est une fonctionnalité ONTAP utile. Et comme le redimensionnement est plus rapide que l'initialisation des quotas, vous devez utiliser le redimensionnement autant que possible. Cependant, il y a quelques restrictions que vous devez connaître.

Le redimensionnement ne fonctionne que pour certains types de modifications de quota. Vous pouvez redimensionner les quotas en apportez les types de modifications suivants aux règles de quotas :

- Modifier un quota existant.

Par exemple, la modification des limites d'un quota existant.

- Ajout d'un quota pour une cible de quota pour laquelle il existe un quota par défaut ou un quota de suivi par défaut.
- Suppression d'un quota pour lequel une entrée de quota par défaut ou de quota de suivi par défaut est



spécifiée.

- Combinaison de quotas d'utilisateurs distincts dans un quota multi-utilisateurs.



Après avoir apporté de nombreuses modifications de quotas, vous devez procéder à une réinitialisation complète pour vous assurer que toutes les modifications prennent effet.



Si vous tentez de redimensionner ou non la totalité de vos modifications des quotas peut être incorporée à l'aide d'une opération de redimensionnement, ONTAP émet un avertissement. Vous pouvez déterminer dans le rapport de quotas si votre système de stockage effectue le suivi de l'utilisation de disques pour un utilisateur, un groupe ou un qtree spécifique. Si vous voyez un quota dans le rapport sur les quotas, cela signifie que le système de stockage suit l'espace disque et le nombre de fichiers appartenant à la cible de quota.

### Exemple de modifications de quotas qui peuvent être effectuées efficacement par le redimensionnement

Certaines modifications de la règle de quotas peuvent être effectuées efficacement par le redimensionnement. Prenez en compte les quotas suivants :

```
#Quota Target type disk files thold sdisk sfile
#-----
* user@/vol/vol2 50M 15K
* group@/vol/vol2 750M 85K
* tree@/vol/vol2 - -
jdoe user@/vol/vol2/ 100M 75K
kbuck user@/vol/vol2/ 100M 75K
```

Supposons que vous apportez les modifications suivantes :

- Augmentez le nombre de fichiers pour la cible utilisateur par défaut.
- Ajoutez un nouveau quota d'utilisateur pour un nouvel utilisateur, boris, qui a besoin de plus de limite de disque que le quota d'utilisateur par défaut.
- Supprimez l'entrée de quota explicite de l'utilisateur kbuck ; le nouvel utilisateur n'a désormais besoin que des limites de quota par défaut.

Ces modifications entraînent les quotas suivants :

```
#Quota Target type disk files thold sdisk sfile
#-----
* user@/vol/vol2 50M 25K
* group@/vol/vol2 750M 85K
* tree@/vol/vol2 - -
jdoe user@/vol/vol2/ 100M 75K
boris user@/vol/vol2/ 100M 75K
```

Le redimensionnement active toutes ces modifications ; une réinitialisation complète du quota n'est pas nécessaire.

## **Lorsqu'une réinitialisation complète du quota est requise**

Bien que le redimensionnement des quotas soit plus rapide, vous devez procéder à une réinitialisation complète des quotas si vous apportez certaines modifications de petite ou de grande taille à vos quotas.

Une réinitialisation complète du quota est nécessaire dans les cas suivants :

- Vous créez un quota pour une cible qui n'avait pas auparavant de quota (ni un quota explicite, ni un quota dérivé d'un quota par défaut).
- Vous modifiez le style de sécurité d'un qtree d'UNIX vers ou de NTFS.
- Vous modifiez le style de sécurité d'un qtree : mélange ou NTFS à UNIX.
- Vous supprimez des utilisateurs d'une cible de quota avec plusieurs utilisateurs ou ajoutez des utilisateurs à une cible qui possède déjà plusieurs utilisateurs.
- Vous apportez d'importantes modifications à vos quotas.

### **Exemple de modifications de quotas qui nécessitent l'initialisation**

Supposons que vous disposez d'un volume qui contient trois qtrees et que les seuls quotas du volume sont trois quotas hiérarchiques explicites. Vous décidez d'effectuer les modifications suivantes :

- Ajouter un nouveau qtree et créer un nouveau quota Tree pour celui-ci.
- Ajoutez un quota utilisateur par défaut pour le volume.

Ces deux modifications nécessitent une initialisation complète du quota. Le redimensionnement ne rend pas efficaces les quotas.

## **Comment pouvez-vous afficher les informations sur les quotas**

### **Présentation de l'affichage des informations de quota**

Vous pouvez utiliser les rapports de quota pour afficher des détails tels que la configuration des règles et des règles de quota, les quotas appliqués et configurés et les erreurs qui se sont produites lors du redimensionnement et de la réinitialisation des quotas.

L'affichage des informations sur les quotas est utile dans les situations suivantes :

- Configuration des quotas, par exemple pour configurer des quotas et vérifier les configurations
- Répondre aux notifications pour vous indiquer que les limites d'espace disque ou de fichiers seront bientôt atteintes ou que ces limites ont été atteintes
- Réponse aux demandes d'espace plus important

### **Voir quels quotas sont en vigueur à l'aide du rapport des quotas**

En raison des différentes façons dont les quotas interagissent, plus de quotas sont en vigueur que seulement ceux que vous avez explicitement créés. Pour connaître les quotas en vigueur, vous pouvez afficher le rapport sur les quotas.

Les exemples suivants présentent les rapports de quotas pour différents types de quotas appliqués sur un

volume FlexVol vol1, et un qtree q1 contenu dans ce volume :

### Exemple avec aucun quota d'utilisateur spécifié pour le qtree

Dans cet exemple, il existe un qtree, q1, qui est contenue par le volume vol1. L'administrateur a créé trois quotas :

- Limite de quota d'arborescence par défaut sur vol1 de 400 Mo
- Limite de quota utilisateur par défaut sur vol1 de 100 Mo
- Limite explicite de quota utilisateur sur vol1 de 200 Mo pour l'utilisateur jsmith

Les règles de quota pour ces quotas sont similaires à l'exemple suivant :

```
cluster1::*> volume quota policy rule show -vserver vs1 -volume vol1
```

| Vserver: vs1 |        |       | Policy: default |       |       | Volume: vol1 |       |
|--------------|--------|-------|-----------------|-------|-------|--------------|-------|
|              |        |       | User            | Disk  | Soft  | Files        | Soft  |
| Type         | Target | Qtree | Mapping         | Limit | Disk  | Limit        | Files |
| Threshold    |        |       |                 |       | Limit | Limit        | Limit |
| tree         | ""     | ""    | -               | 400MB | -     | -            | -     |
| -            |        |       |                 |       |       |              |       |
| user         | ""     | ""    | off             | 100MB | -     | -            | -     |
| -            |        |       |                 |       |       |              |       |
| user         | jsmith | ""    | off             | 200MB | -     | -            | -     |
| -            |        |       |                 |       |       |              |       |

Le rapport des quotas pour ces quotas ressemble à l'exemple suivant :

```
cluster1::> volume quota report
```

| Vserver: vs1 |      |      |        | ----Disk---- |       | ----Files---- |       | Quota  |
|--------------|------|------|--------|--------------|-------|---------------|-------|--------|
| Volume       | Tree | Type | ID     | Used         | Limit | Used          | Limit |        |
| Specifier    |      |      |        |              |       |               |       |        |
| vol1         | -    | tree | *      | 0B           | 400MB | 0             | -     | *      |
| vol1         | -    | user | *      | 0B           | 100MB | 0             | -     | *      |
| vol1         | -    | user | jsmith | 150B         | 200MB | 7             | -     | jsmith |
| vol1         | q1   | tree | 1      | 0B           | 400MB | 6             | -     | q1     |
| vol1         | q1   | user | *      | 0B           | 100MB | 0             | -     |        |
| vol1         | q1   | user | jsmith | 0B           | 100MB | 5             | -     |        |
| vol1         | -    | user | root   | 0B           | 0MB   | 1             | -     |        |
| vol1         | q1   | user | root   | 0B           | 0MB   | 8             | -     |        |

Les trois premières lignes du rapport des quotas affichent les trois quotas spécifiés par l'administrateur. Comme deux de ces quotas sont des quotas par défaut, ONTAP crée automatiquement des quotas dérivés.

La quatrième ligne affiche le quota Tree qui est dérivé du quota Tree par défaut pour chaque qtree en vol1 (dans cet exemple, uniquement q1).

La cinquième ligne affiche le quota utilisateur par défaut créé pour le qtree en raison de l'existence du quota utilisateur par défaut sur le volume et le quota qtree.

La sixième ligne affiche le quota utilisateur dérivé créé pour jsmith sur le qtree car il existe un quota utilisateur par défaut pour le qtree (ligne 5) et l'utilisateur jsmith possède des fichiers sur ce qtree. Notez que la limite appliquée à l'utilisateur jsmith dans le qtree q1 n'est pas déterminée par la limite du quota utilisateur explicite (200 Mo). En effet, la limite explicite de quota utilisateur est sur le volume, ce qui n'affecte donc pas de limites pour le qtree. Au lieu de cela, le quota utilisateur maximal pour le qtree est déterminé par le quota utilisateur par défaut pour le qtree (100 Mo).

Les deux dernières lignes affichent plus de quotas d'utilisateur dérivés des quotas d'utilisateur par défaut sur le volume et sur le qtree. Un quota utilisateur dérivé a été créé pour l'utilisateur root sur le volume et le qtree, car l'utilisateur root possédait des fichiers sur le volume et le qtree. Comme l'utilisateur root bénéficie d'un traitement spécial en termes de quotas, ses quotas dérivés sont uniquement le suivi des quotas.

### **Exemple avec les quotas d'utilisateur spécifiés pour le qtree**

Cet exemple est similaire à la précédente, sauf que l'administrateur a ajouté deux quotas sur le qtree.

Il y a toujours un volume, vol1, et un qtree, q1. L'administrateur a créé les quotas suivants :

- Limite de quota d'arborescence par défaut sur vol1 de 400 Mo
- Limite de quota utilisateur par défaut sur vol1 de 100 Mo
- Limite explicite de quota utilisateur sur vol1 pour l'utilisateur jsmith de 200 Mo
- Quota utilisateur par défaut sur le qtree q1 de 50 Mo
- Limite de quota utilisateur explicite sur qtree q1 pour l'utilisateur jsmith de 75 Mo

Les règles de quota pour ces quotas se ressemblent à celles-ci :

```
cluster1::> volume quota policy rule show -vserver vs1 -volume vol1
```

```
Vserver: vs1 Policy: default Volume: vol1
 Soft
 Disk
 Files
 Soft
Type Target Qtree User Disk Disk Files Files
Threshold Limit Limit Limit Limit

tree "" "" - 400MB - - -
-
user "" "" off 100MB - - -
-
user "" q1 off 50MB - - -
-
user jsmith "" off 200MB - - -
-
user jsmith q1 off 75MB - - -
-
```

Le rapport sur les quotas de ces quotas se présente comme suit :

```
cluster1::> volume quota report
```

```
Vserver: vs1
 ----Disk---- ----Files----- Quota
Volume Tree Type ID Used Limit Used Limit
Specifier

vol1 - tree * 0B 400MB 0 - *
vol1 - user * 0B 100MB 0 - *
vol1 - user jsmith 2000B 200MB 7 - jsmith
vol1 q1 user * 0B 50MB 0 - *
vol1 q1 user jsmith 0B 75MB 5 - jsmith
vol1 q1 tree 1 0B 400MB 6 - q1
vol1 - user root 0B 0MB 2 - -
vol1 q1 user root 0B 0MB 1 - -
```

Les cinq premières lignes du rapport de quota affichent les cinq quotas créés par l'administrateur. Comme certains de ces quotas sont des quotas par défaut, ONTAP crée automatiquement des quotas dérivés.

La sixième ligne affiche le quota Tree qui est dérivé du quota Tree par défaut pour chaque qtree en vol1 (dans cet exemple, uniquement q1).

Les deux dernières lignes affichent les quotas d'utilisateur dérivés des quotas d'utilisateur par défaut sur le

volume et sur le qtree. Un quota utilisateur dérivé a été créé pour l'utilisateur root sur le volume et le qtree, car l'utilisateur root possédait des fichiers sur le volume et le qtree. Comme l'utilisateur root bénéficie d'un traitement spécial en termes de quotas, ses quotas dérivés sont uniquement le suivi des quotas.

Aucun autre quota par défaut ou quota dérivé n'a été créé pour les raisons suivantes :

- Un quota utilisateur dérivé n'a pas été créé pour l'utilisateur jsmith, même si l'utilisateur possède des fichiers à la fois sur le volume et sur le qtree, car l'utilisateur dispose déjà de quotas explicites aux deux niveaux.
- Aucun quota utilisateur dérivé n'a été créé pour d'autres utilisateurs, car aucun autre utilisateur ne possède de fichiers sur le volume ou le qtree.
- Le quota utilisateur par défaut sur le volume n'a pas créé de quota utilisateur par défaut sur le qtree, car le qtree disposait déjà d'un quota utilisateur par défaut.

### **Pourquoi les quotas appliqués diffèrent des quotas configurés**

Les quotas appliqués diffèrent des quotas configurés car les quotas dérivés sont appliqués sans être configurés mais les quotas configurés ne sont appliqués qu'une fois qu'ils ont été initialisés. Comprendre ces différences peut vous aider à comparer les quotas appliqués qui sont affichés dans les rapports de quotas aux quotas que vous avez configurés.

Les quotas appliqués, qui apparaissent dans les rapports de quotas, peuvent différer des règles de quotas configurées pour les raisons suivantes :

- Les quotas dérivés sont appliqués sans être configurés en tant que règles de quotas. ONTAP crée automatiquement des quotas dérivés en réponse aux quotas par défaut.
- Il se peut que les quotas n'aient pas été réinitialisés sur un volume après la configuration des règles de quotas.
- Des erreurs peuvent se produire lors de l'initialisation de quotas sur un volume.

### **Utilisez le rapport quota pour déterminer les quotas limitant les écritures dans un fichier spécifique**

Vous pouvez utiliser la commande `volume quota report` avec un chemin de fichier spécifique pour déterminer quelles limites de quota affectent les opérations d'écriture dans un fichier. Cela peut vous aider à comprendre quel quota empêche une opération d'écriture.

#### **Étapes**

1. Utiliser la commande `volume quota report` avec le paramètre `-path`

#### **Exemple d'affichage des quotas affectant un fichier spécifique**

L'exemple suivant montre la commande et la sortie pour déterminer les quotas en vigueur pour les écritures dans le fichier `file1`, qui réside dans le qtree `q1` dans le volume `FlexVol vol2` :

```
cluster1:> volume quota report -vserver vs0 -volume vol2 -path
/vol/vol2/q1/file1
Virtual Server: vs0
```

| Volume           | Tree | Type  | ID          | ----Disk---- |       | ----Files----- |       | Quota |
|------------------|------|-------|-------------|--------------|-------|----------------|-------|-------|
|                  |      |       |             | Used         | Limit | Used           | Limit |       |
| Volume Specifier |      |       |             |              |       |                |       |       |
| vol2             | q1   | tree  | jsmith      | 1MB          | 100MB | 2              | 10000 | q1    |
| vol2             | q1   | group | eng         | 1MB          | 700MB | 2              | 70000 |       |
| vol2             |      | group | eng         | 1MB          | 700MB | 6              | 70000 | *     |
| vol2             |      | user  | corp\jsmith | 1MB          | 50MB  | 1              | -     | *     |
| vol2             | q1   | user  | corp\jsmith | 1MB          | 50MB  | 1              | -     |       |

5 entries were displayed.

## Commandes permettant d'afficher des informations relatives aux quotas

Vous pouvez utiliser les commandes pour afficher un rapport de quota contenant les quotas appliqués et l'utilisation des ressources, afficher des informations sur l'état des quotas et les erreurs, ou sur les stratégies de quotas et les règles de quotas.



Vous ne pouvez exécuter les commandes suivantes que sur les volumes FlexVol.

| Les fonctions que vous recherchez...                                                               | Utilisez cette commande...                                              |
|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Afficher des informations sur les quotas appliqués                                                 | <code>volume quota report</code>                                        |
| Afficher l'utilisation des ressources (espace disque et nombre de fichiers) des cibles de quota    | <code>volume quota report</code>                                        |
| Déterminez les limites de quota affectées lorsqu'une écriture dans un fichier est autorisée        | <code>volume quota report</code> avec le <code>-path</code> paramètre   |
| Affiche l'état du quota, par exemple on, off, et initializing                                      | <code>volume quota show</code>                                          |
| Afficher les informations relatives à la journalisation des messages de quota                      | <code>volume quota show</code> avec le <code>-logmsg</code> paramètre   |
| Afficher les erreurs qui se produisent lors de l'initialisation et du redimensionnement des quotas | <code>volume quota show</code> avec le <code>-instance</code> paramètre |
| Afficher des informations sur les politiques de quotas                                             | <code>volume quota policy show</code>                                   |

| Les fonctions que vous recherchez...                                                                                       | Utilisez cette commande...                                         |
|----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Afficher des informations sur les règles de quotas                                                                         | <code>volume quota policy rule show</code>                         |
| Afficher le nom de la politique de quotas attribué à une machine virtuelle de stockage (SVM, anciennement appelée Vserver) | <code>vserver show</code> avec le <code>-instance</code> paramètre |

Consultez la page man pour chaque commande pour plus d'informations.

### Quand utiliser les commandes de la règle de quota de volume `show` et de rapport de quota de volume

Les deux commandes affichent des informations sur les quotas, mais la `volume quota policy rule show` affiche rapidement les règles de quota configurées pendant que l' `volume quota report` commande, qui consomme plus de temps et de ressources, affiche les quotas appliqués et l'utilisation des ressources.

Le `volume quota policy rule show` la commande est utile aux fins suivantes :

- Vérifier la configuration des règles de quota avant de les activer

Cette commande affiche toutes les règles de quotas configurées si les quotas ont été initialisés ou redimensionnés.

- Affichez rapidement les règles de quotas sans affecter les ressources système

Comme elle n'affiche pas l'utilisation des disques et des fichiers, cette commande n'est pas aussi gourmande en ressources qu'un rapport de quota.

- Afficher les règles de quota dans une politique de quota qui n'est pas assignée à la SVM.

Le `volume quota report` la commande est utile aux fins suivantes :

- Afficher les quotas appliqués, y compris les quotas dérivés
- Affichez l'espace disque et le nombre de fichiers utilisés par chaque quota en vigueur, y compris les cibles affectées par les quotas dérivés

(Pour les quotas par défaut, l'utilisation apparaît comme « 0 » car l'utilisation est suivie par rapport au quota dérivé résultant.)

- Déterminez les limites de quota affectent lorsqu'une écriture dans un fichier est autorisée

Ajoutez le `-path` paramètre au `volume quota report` commande.



Le rapport sur les quotas est une opération à forte intensité de ressources. Si vous l'exécutez sur plusieurs volumes FlexVol du cluster, ce délai peut être long. Une manière plus efficace serait d'afficher le rapport de quotas pour un volume particulier dans un SVM.



### Présentation de la différence d'utilisation de l'espace affichée par un rapport de quota et un client UNIX

La valeur de l'espace disque utilisé affichée dans un rapport de quota pour un FlexVol volume ou qtrees peut être différente de la valeur affichée par un client UNIX pour le même volume ou qtrees. La différence dans ces valeurs est due aux différentes méthodes suivies par le rapport de quota et les commandes UNIX pour le calcul des blocs de données dans le volume ou qtrees.

Par exemple, si un volume contient un fichier présentant des blocs de données vides (vers lesquels les données ne sont pas écrites), le rapport quota du volume ne compte pas les blocs de données vides lors de l'utilisation de l'espace. Cependant, lorsque le volume est monté sur un client UNIX et que le fichier est affiché comme sortie du `ls` commande, les blocs de données vides sont également inclus dans l'utilisation d'espace. Par conséquent, le `ls` la commande affiche une taille de fichier supérieure par rapport à l'utilisation de l'espace affichée par le rapport aux quotas.

De même, les valeurs d'utilisation de l'espace affichées dans un rapport de quota peuvent également différer des valeurs indiquées à la suite de commandes UNIX telles que `df` et `du`.

### Comment un rapport de quota tient compte de l'espace disque et de l'utilisation des fichiers

Le nombre de fichiers utilisés et la quantité d'espace disque spécifié dans un rapport de quotas pour un volume FlexVol ou un qtrees dépendent du nombre de blocs de données utilisés correspondant à chaque inode du volume ou du qtrees.

Le nombre de blocs inclut à la fois les blocs directs et indirects utilisés pour les fichiers normaux et les fichiers de flux. Les blocs utilisés pour les répertoires, les listes de contrôle d'accès (ACL), les répertoires de flux et les métafichiers ne sont pas pris en compte dans le rapport sur les quotas. Dans le cas de fichiers parse UNIX, des blocs de données vides ne sont pas inclus dans le rapport des quotas.

Le sous-système de quotas est conçu pour prendre en compte et inclure uniquement les aspects contrôlables par l'utilisateur du système de fichiers. Les répertoires, les listes de contrôle d'accès et l'espace des snapshots sont autant d'exemples d'espace exclu des calculs de quotas. Les quotas sont utilisés pour appliquer des limites et non des garanties, et ils fonctionnent uniquement sur le système de fichiers actif. La comptabilité des quotas ne compte pas certaines constructions du système de fichiers ni seulement pour l'efficacité du stockage (comme la compression et la déduplication).

### Disparité entre la commande `ls` et le rapport de quota pour l'utilisation de l'espace

Lorsque vous utilisez `ls` la commande pour afficher le contenu d'un FlexVol volume monté sur un client UNIX, les tailles de fichier affichées dans le résultat peuvent différer de l'utilisation de l'espace affichée dans le rapport de quota pour le volume en fonction du type de blocs de données pour le fichier.

La sortie du `ls` commande affiche uniquement la taille d'un fichier et n'inclut pas les blocs indirects utilisés par le fichier. Tous les blocs vides du fichier sont également inclus dans la sortie de la commande.

Par conséquent, si un fichier ne contient pas de blocs vides, la taille affichée par le `ls` la commande peut être inférieure à l'utilisation du disque spécifiée par un rapport de quota en raison de l'inclusion de blocs indirects dans le rapport de quota. Inversement, si le fichier contient des blocs vides, alors la taille affichée par le `ls` la commande peut être supérieure à l'utilisation du disque spécifiée par le rapport de quota.

La sortie du `ls` commande affiche uniquement la taille d'un fichier et n'inclut pas les blocs indirects utilisés par le fichier. Tous les blocs vides du fichier sont également inclus dans la sortie de la commande.

### Exemple de différence entre l'utilisation de l'espace comptabilisée par la commande `ls` et un rapport de quota

Le rapport de quotas suivant montre la limite de 10 Mo pour un q1 qtree :

| Volume     | Tree  | Type  | ID    | ----Disk---- |       | ----Files----- |       | Quota |
|------------|-------|-------|-------|--------------|-------|----------------|-------|-------|
|            |       |       |       | Used         | Limit | Used           | Limit |       |
| Specifieur |       |       |       |              |       |                |       |       |
| -----      | ----- | ----- | ----- | -----        | ----- | -----          | ----- |       |
| -----      |       |       |       |              |       |                |       |       |
| voll       | q1    | tree  | user1 | 10MB         | 10MB  | 1              | -     | q1    |
| ...        |       |       |       |              |       |                |       |       |

Un fichier présent dans le même qtree peut avoir une taille supérieure à la limite de quota lorsqu'il est visualisé à partir d'un client UNIX en utilisant le `ls` comme indiqué dans l'exemple suivant :

```
[user1@lin-sys1 q1]$ ls -lh
-rwxr-xr-x 1 user1 nfsuser **27M** Apr 09 2013 file1
```

### Comment la commande `df` tient compte de la taille des fichiers

La manière dont dans le `df` la commande signale l'utilisation de l'espace dépend de deux conditions : que les quotas soient activés ou désactivés pour le volume qui contient le qtree, et que l'utilisation des quotas au sein du qtree est suivie.

Lorsque les quotas sont activés pour le volume contenant l'utilisation du qtree et du quota au sein du qtree est suivie, l'utilisation de l'espace est signalée par le `df` commande égale la valeur spécifiée par le rapport de quota. Dans ce cas, l'utilisation des quotas exclut les blocs utilisés par les répertoires, les ACL, les répertoires de flux et les métafichiers.

Lorsque les quotas ne sont pas activés sur le volume, ou si le qtree n'a pas configuré de règle de quotas, l'utilisation de l'espace signalé inclut les blocs utilisés par les répertoires, les listes de contrôle d'accès, les répertoires de flux et les métafichiers pour tout le volume, y compris les autres qtrees du volume. Dans ce cas, l'utilisation de l'espace signalée par le `df` la commande est supérieure à la valeur attendue signalée lors du suivi des quotas.

Lorsque vous exécutez le `df` commande provenant du point de montage d'un qtree pour lequel l'utilisation du quota est suivie, la sortie de la commande affiche la même utilisation de l'espace que la valeur spécifiée par le rapport quota. Dans la plupart des cas, lorsque la règle de quota d'arborescence a une limite de disque dur, la taille totale signalée par le `df` commande égale la limite du disque et l'espace disponible équivaut à la différence entre la limite du disque de quota et l'utilisation des quotas.

Toutefois, dans certains cas, l'espace disponible indiqué par le `df` la commande peut correspondre à l'espace disponible dans le volume dans son ensemble. Cela peut se produire lorsqu'aucune limite de disque dur n'est configurée pour le qtree. Depuis la version ONTAP 9.9.1, il peut également se produire lorsque l'espace

disponible dans le volume dans son ensemble est inférieur à l'espace de quota Tree restant. Lorsque l'une ou l'autre de ces conditions se produit, la taille totale signalée par le `df` Commande est un nombre synthétisé égal au quota utilisé dans le qtree plus l'espace disponible dans le volume FlexVol.



Cette taille totale n'est ni la limite des disques qtree, ni la taille du volume configurée. Ils peuvent également varier en fonction de l'activité d'écriture dans d'autres qtrees ou de l'activité d'efficacité du stockage en arrière-plan.

**Exemple d'utilisation de l'espace représenté par le `df` commande et rapport de quota**

Le rapport de quota suivant indique une limite de disque de 1 Go pour qtree alice, 2 Go pour qtree bob, et aucune limite pour le projet qtree project1 :

```
C1_vsim1::> quota report -vserver vs0
Vserver: vs0
```

| Volume    | Tree     | Type  | ID    | ----Disk---- |       | ----Files---- |       | Quota |
|-----------|----------|-------|-------|--------------|-------|---------------|-------|-------|
|           |          |       |       | Used         | Limit | Used          | Limit |       |
| Specifier |          |       |       |              |       |               |       |       |
| -----     | -----    | ----- | ----- | -----        | ----- | -----         | ----- |       |
| vol2      | alice    | tree  | 1     | 502.0MB      | 1GB   | 2             | -     | alice |
| vol2      | bob      | tree  | 2     | 1003MB       | 2GB   | 2             | -     | bob   |
| vol2      | project1 | tree  | 3     | 200.8MB      | -     | 2             | -     |       |
| project1  |          |       |       |              |       |               |       |       |
| vol2      |          | tree  | *     | 0B           | -     | 0             | -     | *     |

4 entries were displayed.

Dans l'exemple suivant, la sortie du `df` Commande sur les qtrees alice et bob indiquent le même espace utilisé que le rapport de quota, et la même taille totale (en termes de blocs de 1 million) que la limite du disque. En effet, les règles de quota pour les qtrees alice et bob ont une limite de disque définie et l'espace disponible du volume (1211 Mo) est supérieur à l'espace de quota Tree restant pour qtree alice (523 Mo) et qtree bob (1045 Mo).

```
linux-client1 [~]$ df -m /mnt/vol2/alice
Filesystem 1M-blocks Used Available Use% Mounted on
172.21.76.153:/vol2 1024 502 523 50% /mnt/vol2

linux-client1 [~]$ df -m /mnt/vol2/bob
Filesystem 1M-blocks Used Available Use% Mounted on
172.21.76.153:/vol2 2048 1004 1045 50% /mnt/vol2
```

Dans l'exemple suivant, la sortie du `df` La commande sur qtree project1 indique le même espace utilisé que le rapport de quota, mais la taille totale est synthétisée en ajoutant l'espace disponible dans le volume dans son ensemble (1211 Mo) à l'utilisation du quota de qtree project1 (201 Mo) pour donner un total de 1412 Mo. En

effet, la règle de quota pour qtree project1 n'a aucune limite de disque.

```
linux-client1 [~]$ df -m /mnt/vol2/project1
Filesystem 1M-blocks Used Available Use% Mounted on
172.21.76.153:/vol2 1412 201 1211 15% /mnt/vol2
```

L'exemple suivant montre comment la sortie de l' df la commande sur le volume dans son ensemble indique le même espace disponible que le project1.



```
linux-client1 [~]$ df -m /mnt/vol2
Filesystem 1M-blocks Used Available Use% Mounted on
172.21.76.153:/vol2 2919 1709 1211 59% /mnt/vol2
```

**Disparité entre la commande du et le rapport de quota pour l'utilisation de l'espace**

Lorsque vous exécutez le du Commande pour vérifier l'utilisation de l'espace disque pour un volume qtree ou FlexVol monté sur un client UNIX, la valeur d'utilisation peut être supérieure à la valeur affichée par un rapport de quotas pour le qtree ou le volume.

La sortie du du la commande contient l'utilisation combinée de l'espace de tous les fichiers par l'intermédiaire de l'arborescence de répertoires commençant au niveau du répertoire où la commande est émise. Car la valeur d'utilisation affichée par le du la commande inclut également les blocs de données pour les répertoires, elle est supérieure à la valeur affichée par un rapport de quota.

**Exemple de la différence entre l'utilisation de l'espace comptabilisée par la commande du et un rapport de quota**

Le rapport de quotas suivant montre la limite de 10 Mo pour un q1 qtree :

| Volume<br>Specifieur | Tree  | Type  | ID    | ----Disk---- |       | ----Files----- |       | Quota |
|----------------------|-------|-------|-------|--------------|-------|----------------|-------|-------|
|                      |       |       |       | Used         | Limit | Used           | Limit |       |
| -----                | ----- | ----- | ----- | -----        | ----- | -----          | ----- |       |
| -----                |       |       |       |              |       |                |       |       |
| vol1                 | q1    | tree  | user1 | 10MB         | 10MB  | 1              | -     | q1    |
| ...                  |       |       |       |              |       |                |       |       |

Dans l'exemple suivant, l'espace disque utilisé comme sortie du du la commande affiche une valeur plus élevée qui dépasse la limite du quota :

```
[user1@lin-sys1 q1]$ du -sh
11M q1
```

## Exemples de configuration de quota

Ces exemples vous aident à comprendre comment configurer les quotas et lire les rapports de quotas.

### À propos de ces exemples

Pour les exemples suivants, supposons que vous disposez d'un système de stockage qui inclut un SVM, `vs1`, avec un volume, `vol1`.

1. Pour commencer à définir des quotas, on crée une nouvelle politique de quotas pour la SVM :

```
cluster1::>volume quota policy create -vserver vs1 -policy-name
quota_policy_vs1_1
```

2. Étant donné que la politique de quotas est nouvelle, on l'affecte au SVM :

```
cluster1::>vserver modify -vserver vs1 -quota-policy quota_policy_vs1_1
```

### Exemple 1 : quota utilisateur par défaut

1. Vous décidez d'imposer une limite stricte de 50 Mo pour chaque utilisateur dans `vol1`:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 50MB
-qtree ""
```

2. Pour activer la nouvelle règle, vous initialisez les quotas sur le volume :

```
cluster1::>volume quota on -vserver vs1 -volume vol1 -foreground
```

3. Le rapport sur les quotas s'affiche :

```
cluster1::>volume quota report
```

Le rapport sur les quotas ainsi obtenu est similaire au rapport suivant :

Vserver: vs1

| Volume<br>Specifier | Tree | Type | ID     | ----Disk---- |       | ----Files----- |       | Quota |
|---------------------|------|------|--------|--------------|-------|----------------|-------|-------|
|                     |      |      |        | Used         | Limit | Used           | Limit |       |
|                     |      |      |        | -----        |       |                |       |       |
|                     |      |      |        | -----        |       |                |       |       |
| vol1                |      | user | *      | 0B           | 50MB  | 0              | -     | *     |
| vol1                |      | user | jsmith | 49MB         | 50MB  | 37             | -     | *     |
| vol1                |      | user | root   | 0B           | -     | 1              | -     |       |

La première ligne affiche le quota utilisateur par défaut que vous avez créé, y compris la limite du disque. Comme tous les quotas par défaut, ce quota utilisateur par défaut n'affiche pas d'informations sur l'utilisation du disque ou du fichier. Outre le quota qui a été créé, deux autres quotas apparaissent. Il existe un quota pour chaque utilisateur qui possède actuellement des fichiers sur vol1. Ces quotas supplémentaires sont des quotas d'utilisateur qui ont été dérivés automatiquement du quota d'utilisateur par défaut. Le quota utilisateur dérivé pour l'utilisateur jsmith a la même limite de disque de 50 Mo que le quota utilisateur par défaut. Le quota d'utilisateur dérivé pour l'utilisateur root est un quota de suivi (sans limites).

Si un utilisateur du système (autre que l'utilisateur root) tente d'exécuter une action qui utiliserait plus de 50 Mo dans vol1 (par exemple, l'écriture dans un fichier à partir d'un éditeur), l'action échoue.

### Exemple 2 : quota utilisateur explicite remplaçant un quota utilisateur par défaut

1. Si vous devez fournir davantage d'espace dans le volume vol1 à l'utilisateur jsmith, entrez la commande suivante :

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit
80MB -qtree ""
```

Il s'agit d'un quota utilisateur explicite, car l'utilisateur est explicitement répertorié comme cible de la règle de quotas.

Il s'agit d'une modification d'une limite de quota existante, car elle modifie la limite de disque du quota utilisateur dérivé pour l'utilisateur jsmith sur le volume. Par conséquent, il n'est pas nécessaire de réinitialiser les quotas sur le volume pour activer la modification.

2. Pour redimensionner les quotas :

```
cluster1::>volume quota resize -vserver vs1 -volume vol1 -foreground
```

Les quotas restent en vigueur pendant le redimensionnement, et le processus de redimensionnement est court.

Le rapport sur les quotas ainsi obtenu est similaire au rapport suivant :

```
cluster1::> volume quota report
Vserver: vs1
```

| Volume    | Tree | Type | ID     | ----Disk---- |       | ----Files----- |       | Quota  |
|-----------|------|------|--------|--------------|-------|----------------|-------|--------|
|           |      |      |        | Used         | Limit | Used           | Limit |        |
| Specifier |      |      |        |              |       |                |       |        |
| vol1      |      | user | *      | 0B           | 50MB  | 0              | -     | *      |
| vol1      |      | user | jsmith | 50MB         | 80MB  | 37             | -     | jsmith |
| vol1      |      | user | root   | 0B           | -     | 1              | -     |        |

3 entries were displayed.

La deuxième ligne affiche maintenant une limite de disque de 80MB et un spécificateur de quota de jsmith.

Par conséquent jsmith, peut utiliser jusqu'à 80 Mo d'espace sur vol1 même si tous les autres utilisateurs sont toujours limités à 50 Mo.

### Exemple 3 : seuils

Supposons que vous souhaitiez recevoir une notification lorsque les utilisateurs atteignent 5 Mo de leurs limites de disque.

1. Pour créer un seuil de 45 Mo pour tous les utilisateurs et un seuil de 75 Mo pour jsmith, vous modifiez les règles de quota existantes :

```
cluster1::>volume quota policy rule modify -vserver vs1 -policy
quota_policy_vs1_1 -volume vol1 -type user -target "" -qtree ""
-threshold 45MB
cluster1::>volume quota policy rule modify -vserver vs1 -policy
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -qtree ""
-threshold 75MB
```

Comme la taille des règles existantes est modifiée, vous redimensionnez les quotas sur le volume afin d'activer les modifications. Vous attendez que le processus de redimensionnement soit terminé.

2. Pour afficher le rapport de quota avec des seuils, vous ajoutez le `-thresholds` paramètre au `volume quota report` commande :

```
cluster1::>volume quota report -thresholds
Vserver: vs1
```

| Volume    | Tree  | Type  | ID     | ----Disk---- |                  | ----Files----- |       | Quota  |
|-----------|-------|-------|--------|--------------|------------------|----------------|-------|--------|
|           |       |       |        | Used         | Limit<br>(Thold) | Used           | Limit |        |
| Specifier |       |       |        |              |                  |                |       |        |
| -----     | ----- | ----- | -----  | -----        | -----            | -----          | ----- |        |
| -----     |       |       |        |              |                  |                |       |        |
| vol1      |       | user  | *      | 0B           | 50MB<br>(45MB)   | 0              | -     | *      |
| vol1      |       | user  | jsmith | 59MB         | 80MB<br>(75MB)   | 55             | -     | jsmith |
| vol1      |       | user  | root   | 0B           | -<br>( -)        | 1              | -     |        |

3 entries were displayed.

Les seuils apparaissent entre parenthèses dans la colonne limite de disque.

#### Exemple 4 : quotas sur les qtrees

Supposons que vous ayez besoin de partitionner de l'espace pour deux projets. Vous pouvez créer deux qtrees, nommés `proj1` et `proj2`, pour prendre en charge ces projets dans `vol1`.

Actuellement, les utilisateurs peuvent utiliser autant d'espace dans un qtree qu'ils sont alloués à l'intégralité du volume (à condition qu'ils n'aient pas dépassé la limite du volume en utilisant l'espace à la racine ou à un autre qtree). De plus, chaque qtree peut être outre mesure d'augmenter la capacité de consommer la totalité du volume.

1. Si vous souhaitez vous assurer que aucun qtree ne dépasse 20 Go, vous pouvez créer un quota Tree par défaut sur le volume :

```
cluster1:>>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type tree -target "" -disk-limit 20GB
```



Le type correct est *Tree*, pas *qtree*.

2. Étant donné qu'il s'agit d'un nouveau quota, vous ne pouvez pas l'activer en le redimensionnant. Vous réinitialisez les quotas sur le volume :

```
cluster1:>>volume quota off -vserver vs1 -volume vol1
cluster1:>>volume quota on -vserver vs1 -volume vol1 -foreground
```





Vous devez vous assurer que vous attendez environ cinq minutes avant de réactiver les quotas sur chaque volume affecté, car vous tentez de les activer presque immédiatement après l'exécution du `volume quota off` la commande peut entraîner des erreurs. Vous pouvez également exécuter les commandes pour réinitialiser les quotas d'un volume à partir du nœud qui contient ce volume.

Les quotas ne sont pas appliqués lors du processus de réinitialisation, ce qui prend plus de temps que le processus de redimensionnement.

Lorsque vous affichez un rapport de quota, il comporte plusieurs nouvelles lignes. Certaines lignes correspondent à des quotas d'arborescence et certaines correspondent à des quotas d'utilisateur dérivés.

Les nouvelles lignes suivantes concernent les quotas d'arborescence :

| Volume     | Tree  | Type  | ID    | ----Disk---- |       | ----Files----- |       | Quota |
|------------|-------|-------|-------|--------------|-------|----------------|-------|-------|
| Specifieur |       |       |       | Used         | Limit | Used           | Limit |       |
| -----      | ----- | ----- | ----- | -----        | ----- | -----          | ----- |       |
| ...        |       |       |       |              |       |                |       |       |
| vol1       |       | tree  | *     | 0B           | 20GB  | 0              | -     | *     |
| vol1       | proj1 | tree  | 1     | 0B           | 20GB  | 1              | -     | proj1 |
| vol1       | proj2 | tree  | 2     | 0B           | 20GB  | 1              | -     | proj2 |
| ...        |       |       |       |              |       |                |       |       |

Le quota d'arborescence par défaut que vous avez créé apparaît dans la première nouvelle ligne, qui comporte un astérisque (\*) dans la colonne ID. En réponse au quota Tree par défaut sur un volume, ONTAP crée automatiquement des quotas Tree dérivés pour chaque qtree du volume. Elles sont indiquées dans les lignes où `proj1` et `proj2` apparaissent dans la Tree colonne.

Les nouvelles lignes suivantes concernent les quotas d'utilisateurs dérivés :

| Volume     | Tree  | Type  | ID    | ----Disk---- |       | ----Files----- |       | Quota |
|------------|-------|-------|-------|--------------|-------|----------------|-------|-------|
| Specifieur |       |       |       | Used         | Limit | Used           | Limit |       |
| -----      | ----- | ----- | ----- | -----        | ----- | -----          | ----- |       |
| ...        |       |       |       |              |       |                |       |       |
| vol1       | proj1 | user  | *     | 0B           | 50MB  | 0              | -     |       |
| vol1       | proj1 | user  | root  | 0B           | -     | 1              | -     |       |
| vol1       | proj2 | user  | *     | 0B           | 50MB  | 0              | -     |       |
| vol1       | proj2 | user  | root  | 0B           | -     | 1              | -     |       |
| ...        |       |       |       |              |       |                |       |       |

Les quotas d'utilisateur par défaut d'un volume sont automatiquement hérités de tous les qtrees contenus par ce volume si les quotas sont activés pour les qtrees. Lorsque vous avez ajouté le premier quota qtree, vous avez activé les quotas sur les qtrees. Par conséquent, des quotas d'utilisateur par défaut dérivés ont été créés

pour chaque qtree. Elles sont affichées dans les lignes où l'ID est un astérisque (\*).

Étant donné que l'utilisateur root est le propriétaire d'un fichier, lorsque des quotas d'utilisateur par défaut ont été créés pour chacun des qtrees, des quotas de suivi spéciaux ont également été créés pour l'utilisateur root sur chacun des qtrees. Elles sont affichées dans les lignes où l'ID est racine.

**Exemple 5 : quota utilisateur sur un qtree**

- 1. Vous décidez de limiter l'espace dans le proj1 qtree au-delà de ce qu'ils obtiennent dans le volume dans son ensemble. Vous souhaitez les empêcher d'utiliser plus de 10 Mo dans le proj1 qtree. Par conséquent, vous créez un quota utilisateur par défaut pour le qtree :

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume voll1 -type user -target "" -disk-limit 10MB
-qtrees proj1
```

Il s'agit d'un changement de quota existant car il modifie le quota utilisateur par défaut pour le qtree proj1 qui a été dérivé du quota utilisateur par défaut sur le volume. Par conséquent, vous activez la modification en redimensionnant les quotas. Lorsque le processus de redimensionnement est terminé, vous pouvez afficher le rapport de quota.

La nouvelle ligne suivante apparaît dans le rapport de quota montrant le nouveau quota utilisateur explicite pour le qtree :

|           |       |       |       | ----Disk---- |       | ----Files----- |       | Quota |
|-----------|-------|-------|-------|--------------|-------|----------------|-------|-------|
| Volume    | Tree  | Type  | ID    | Used         | Limit | Used           | Limit |       |
| Specifier |       |       |       |              |       |                |       |       |
| -----     | ----- | ----- | ----- | -----        | ----- | -----          | ----- |       |
| -----     |       |       |       |              |       |                |       |       |
| voll      | proj1 | user  | *     | 0B           | 10MB  | 0              | -     | *     |

Cependant, il jsmith est impossible à l'utilisateur d'écrire plus de données sur le qtree proj1, car le quota que vous avez créé pour remplacer le quota utilisateur par défaut (pour fournir plus d'espace) se trouvait sur le volume. Comme vous avez ajouté un quota utilisateur par défaut sur le proj1 qtree, ce quota est appliqué et limite l'espace de tous les utilisateurs dans ce qtree, y compris jsmith.

- 2. Pour fournir plus d'espace jsmith à l'utilisateur, vous ajoutez une règle de quota utilisateur explicite pour le qtree avec une limite de disque de 80 Mo afin de remplacer la règle de quota utilisateur par défaut pour le qtree :

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume voll1 -type user -target jsmith -disk-limit
80MB -qtrees proj1
```

Comme il s'agit d'un quota explicite pour lequel un quota par défaut existe déjà, vous activez la modification en redimensionnant les quotas. Lorsque le processus de redimensionnement est terminé, un rapport de quota s'affiche.

La nouvelle ligne suivante apparaît dans le rapport de quota :

| Volume     | Tree  | Type  | ID     | ----Disk---- |       | ----Files----- |       | Quota  |
|------------|-------|-------|--------|--------------|-------|----------------|-------|--------|
|            |       |       |        | Used         | Limit | Used           | Limit |        |
| Specifieur |       |       |        |              |       |                |       |        |
| -----      | ----- | ----- | -----  | -----        | ----- | -----          | ----- |        |
| -----      |       |       |        |              |       |                |       |        |
| vol1       | proj1 | user  | jsmith | 61MB         | 80MB  | 57             | -     | jsmith |

Le rapport final sur les quotas est similaire au rapport suivant :

```
cluster1::>volume quota report
Vserver: vs1
```

| Volume     | Tree  | Type  | ID     | ----Disk---- |       | ----Files----- |       | Quota  |
|------------|-------|-------|--------|--------------|-------|----------------|-------|--------|
|            |       |       |        | Used         | Limit | Used           | Limit |        |
| Specifieur |       |       |        |              |       |                |       |        |
| -----      | ----- | ----- | -----  | -----        | ----- | -----          | ----- |        |
| -----      |       |       |        |              |       |                |       |        |
| vol1       |       | tree  | *      | 0B           | 20GB  | 0              | -     | *      |
| vol1       |       | user  | *      | 0B           | 50MB  | 0              | -     | *      |
| vol1       |       | user  | jsmith | 70MB         | 80MB  | 65             | -     | jsmith |
| vol1       | proj1 | tree  | 1      | 0B           | 20GB  | 1              | -     | proj1  |
| vol1       | proj1 | user  | *      | 0B           | 10MB  | 0              | -     | *      |
| vol1       | proj1 | user  | root   | 0B           | -     | 1              | -     |        |
| vol1       | proj2 | tree  | 2      | 0B           | 20GB  | 1              | -     | proj2  |
| vol1       | proj2 | user  | *      | 0B           | 50MB  | 0              | -     |        |
| vol1       | proj2 | user  | root   | 0B           | -     | 1              | -     |        |
| vol1       |       | user  | root   | 0B           | -     | 3              | -     |        |
| vol1       | proj1 | user  | jsmith | 61MB         | 80MB  | 57             | -     | jsmith |

11 entries were displayed.

L'utilisateur `jsmith` doit respecter les limites de quota suivantes pour écrire dans un fichier dans `proj1`:

1. Quota Tree pour le `proj1` qtree.
2. Quota utilisateur sur le `proj1` qtree.
3. Quota utilisateur sur le volume.

## Configurez des quotas sur un SVM

Vous pouvez définir des quotas sur un nouveau SVM afin de gérer et de surveiller l'utilisation des ressources.

### Description de la tâche

À un niveau élevé, plusieurs étapes sont impliquées lors de la configuration des quotas, notamment :

1. Créer une politique de quotas
2. Ajouter les règles de quota à la politique
3. Assigner la politique au SVM
4. Initialiser les quotas sur chaque FlexVol volume du SVM

## Étapes

1. Saisissez la commande `vserver show -instance` Pour afficher le nom de la politique de quotas par défaut qui a été automatiquement créée lors de la création de la SVM.

Si un nom n'a pas été spécifié lors de la création du SVM, le nom est « default ». Vous pouvez utiliser le `vserver quota policy rename` commande permettant de donner un nom à la règle par défaut.



Vous pouvez également créer une nouvelle stratégie à l'aide de `volume quota policy create` commande.

2. Utilisez le `volume quota policy rule create` Commande pour créer *any* des règles de quotas suivantes pour chaque volume de la SVM :
  - Règles de quotas par défaut pour tous les utilisateurs
  - Règles de quotas explicites pour des utilisateurs spécifiques
  - Règles de quotas par défaut pour tous les groupes
  - Règles de quotas explicites pour des groupes spécifiques
  - Règles de quotas par défaut pour tous les qtrees
  - Règles de quotas explicites pour les qtrees spécifiques
3. Utilisez le `volume quota policy rule show` commande pour vérifier que les règles de quota sont correctement configurées.
4. Si vous travaillez sur une nouvelle politique, utilisez le `vserver modify` Commande pour assigner la nouvelle politique à la SVM.
5. Utilisez le `volume quota on` Commande permettant d'initialiser les quotas sur chaque volume du SVM.

Vous pouvez surveiller le processus d'initialisation de l'une des manières suivantes :

- Lorsque vous utilisez le `volume quota on` vous pouvez ajouter la commande `-foreground` paramètre pour exécuter le quota sur le travail au premier plan. (Par défaut, le travail s'exécute en arrière-plan.)

Lorsque le travail s'exécute en arrière-plan, vous pouvez surveiller sa progression à l'aide du `job show` commande.

- Vous pouvez utiliser le `volume quota show` commande permettant de surveiller le statut de l'initialisation du quota.
6. Utilisez le `volume quota show -instance` commande pour vérifier les erreurs d'initialisation, telles que les règles de quota qui n'ont pas pu être initialisés.
  7. Utilisez le `volume quota report` commande permettant d'afficher un rapport de quota afin de vous assurer que les quotas appliqués correspondent à vos attentes.

## Modifier ou redimensionner les limites de quota

Vous pouvez modifier ou redimensionner les quotas sur tous les volumes affectés, ce qui est plus rapide que de réinitialiser les quotas sur ces volumes.

### Description de la tâche

Il s'agit d'un serveur virtuel de stockage (SVM, précédemment appelé vServer) avec des quotas appliqués. Vous souhaitez modifier les limites de taille des quotas existants ou ajouter ou supprimer des quotas pour les cibles qui possèdent déjà des quotas dérivés.

### Étapes

1. Utilisez le `vserver show` commande avec `-instance` Paramètre permettant de déterminer le nom de la politique actuellement assignée à la SVM.
2. Modifiez les règles de quota en effectuant l'une des actions suivantes :
  - Utilisez le `volume quota policy rule modify` commande permettant de modifier les limites de disque ou de fichier des règles de quotas existantes.
  - Utilisez le `volume quota policy rule create` commande permettant de créer des règles de quota explicites pour les cibles (utilisateurs, groupes ou qtrees) qui possèdent actuellement des quotas dérivés.
  - Utilisez le `volume quota policy rule delete` commande permettant de supprimer des règles de quota explicites pour les cibles (utilisateurs, groupes ou qtrees) qui possèdent également des quotas par défaut.
3. Utilisez le `volume quota policy rule show` commande pour vérifier que les règles de quota sont correctement configurées.
4. Utilisez le `volume quota resize` commande sur chaque volume où vous avez modifié des quotas, pour activer les modifications apportées à chaque volume.

Vous pouvez surveiller le processus de redimensionnement de l'une des manières suivantes :

- Lorsque vous utilisez le `volume quota resize` vous pouvez ajouter la commande `-foreground` paramètre pour exécuter le travail de redimensionnement au premier plan. (Par défaut, le travail s'exécute en arrière-plan.)

Lorsque le travail s'exécute en arrière-plan, vous pouvez surveiller sa progression à l'aide du `job show` commande.

- Vous pouvez utiliser le `volume quota show` commande permettant de surveiller l'état de redimensionnement.

5. Utilisez le `volume quota show -instance` commande pour vérifier si les erreurs de redimensionnement telles que les règles de quota qui n'ont pas pu être redimensionnées.

En particulier, vérifiez les erreurs de « nouvelle définition » qui se produisent lorsque vous redimensionnez les quotas après avoir ajouté un quota explicite pour une cible qui n'a pas encore de quota dérivé.

6. Utilisez le `volume quota report` commande permettant d'afficher un rapport de quota afin de vous assurer que les quotas appliqués correspondent à vos besoins.

## Réinitialisez les quotas après avoir effectué des modifications importantes

Après avoir apporté des modifications importantes aux définitions de quota existantes, vous devez réinitialiser les quotas sur tous les volumes affectés. Un exemple de ce type de modification est l'ajout ou la suppression de quotas pour les cibles qui n'ont pas de quotas appliqués.

### Description de la tâche

Vous disposez d'une machine virtuelle de stockage (SVM) avec des quotas appliqués et vous souhaitez apporter des modifications nécessitant une réinitialisation complète des quotas.

### Étapes

1. Utilisez le `vserver show` commande avec `-instance` Paramètre permettant de déterminer le nom de la politique actuellement assignée à la SVM.
2. Modifiez les règles de quota en effectuant l'une des actions suivantes :

| Les fonctions que vous recherchez...                    | Alors...                                                          |
|---------------------------------------------------------|-------------------------------------------------------------------|
| Créer de nouvelles règles de quotas                     | Utilisez le <code>volume quota policy rule create</code> commande |
| Modifiez les paramètres des règles de quotas existantes | Utilisez le <code>volume quota policy rule modify</code> commande |
| Supprimez les règles de quotas existantes               | Utilisez le <code>volume quota policy rule delete</code> commande |

3. Utilisez le `volume quota policy rule show` commande pour vérifier que les règles de quota sont correctement configurées.
4. Réinitialisez les quotas sur chaque volume où vous avez modifié les quotas en désactivant les quotas, puis en activant les quotas pour ces volumes.
  - a. Utilisez le `volume quota off` commande sur chaque volume affecté pour désactiver les quotas sur ce volume.
  - b. Utilisez le `volume quota on` sur chaque volume affecté, commande permettant d'activer les quotas sur ce volume.



Vous devez vous assurer que vous attendez environ cinq minutes avant de réactiver les quotas sur chaque volume affecté, car vous tentez de les activer presque immédiatement après l'exécution du `volume quota off` la commande peut entraîner des erreurs.

Vous pouvez également exécuter les commandes pour réinitialiser les quotas d'un volume à partir du nœud qui contient ce volume.

Vous pouvez surveiller le processus d'initialisation de l'une des manières suivantes :

- Lorsque vous utilisez le `volume quota on` vous pouvez ajouter la commande `-foreground` paramètre pour exécuter le quota sur le travail au premier plan. (Par défaut, le travail s'exécute en

arrière-plan.)

Lorsque le travail s'exécute en arrière-plan, vous pouvez surveiller sa progression à l'aide du `job show` commande.

- Vous pouvez utiliser le `volume quota show` commande permettant de surveiller le statut de l'initialisation du quota.

5. Utilisez le `volume quota show -instance` commande pour vérifier les erreurs d'initialisation, telles que les règles de quota qui n'ont pas pu être initialisés.
6. Utilisez le `volume quota report` commande permettant d'afficher un rapport de quota afin de vous assurer que les quotas appliqués correspondent à vos attentes.

## Commandes permettant de gérer les règles de quotas et les politiques de quotas

Les `volume quota policy rule` commandes vous permettent de configurer des règles de quota, et les `volume quota policy` commandes et certaines commandes `vserver` vous permettent de configurer des politiques de quota. En fonction de ce que vous devez faire, utilisez les commandes suivantes pour gérer les règles de quotas et les politiques de quotas :



Vous ne pouvez exécuter les commandes suivantes que sur les volumes FlexVol.

### Commandes pour la gestion des règles de quotas

| Les fonctions que vous recherchez...                          | Utilisez cette commande...                   |
|---------------------------------------------------------------|----------------------------------------------|
| Créer une nouvelle règle de quotas                            | <code>volume quota policy rule create</code> |
| Supprimez une règle de quotas existante                       | <code>volume quota policy rule delete</code> |
| Modifiez une règle de quotas existante                        | <code>volume quota policy rule modify</code> |
| Affiche des informations sur les règles de quotas configurées | <code>volume quota policy rule show</code>   |

### Commandes pour la gestion des politiques de quotas

| Les fonctions que vous recherchez...                                                         | Utilisez cette commande...              |
|----------------------------------------------------------------------------------------------|-----------------------------------------|
| Dupliquer une politique de quotas et les règles de quotas qu'elle contient                   | <code>volume quota policy copy</code>   |
| Créer une nouvelle politique de quotas vierge                                                | <code>volume quota policy create</code> |
| Supprimer une politique de quotas existante non attribuée à un SVM (Storage Virtual machine) | <code>volume quota policy delete</code> |

| Les fonctions que vous recherchez...                        | Utilisez cette commande...                                |
|-------------------------------------------------------------|-----------------------------------------------------------|
| Renommer une politique de quotas                            | <code>volume quota policy rename</code>                   |
| Affiche des informations sur les politiques de quotas       | <code>volume quota policy show</code>                     |
| Assigner une politique de quotas à une SVM                  | <code>vserver modify -quota-policy<br/>policy_name</code> |
| Afficher le nom de la politique de quotas assignée à un SVM | <code>vserver show</code>                                 |

Voir la ["Référence de commande ONTAP"](#) pour chaque commande pour plus d'informations.

### Commandes pour activer et modifier les quotas

`volume quota` les commandes vous permettent de modifier l'état des quotas et de configurer la journalisation des messages des quotas. Selon ce que vous devez faire, vous pouvez utiliser les commandes suivantes pour activer et modifier les quotas :

| Les fonctions que vous recherchez...                                                                                                 | Utilisez cette commande...       |
|--------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| Activer les quotas (également appelés <i>initializing</i> eux)                                                                       | <code>volume quota on</code>     |
| Redimensionner les quotas existants                                                                                                  | <code>volume quota resize</code> |
| Désactivez les quotas                                                                                                                | <code>volume quota off</code>    |
| Modifiez la journalisation des messages des quotas, activez les quotas, désactivez les quotas ou redimensionnez les quotas existants | <code>volume quota modify</code> |

Consultez la page man pour chaque commande pour plus d'informations.

## Utilisez la déduplication, la compression et la compaction des données pour améliorer l'efficacité du stockage

### Déduplication, compression, compaction et efficacité du stockage

Vous pouvez exécuter la déduplication, la compression et la compaction des données de manière indépendante ou simultanément pour réaliser des économies d'espace optimales sur un volume FlexVol. La déduplication permet d'éliminer les blocs de données dupliqués. La compression des données compresse les blocs de données afin de réduire la quantité d'espace de stockage physique nécessaire. Efficacité du stockage accrue grâce à la compaction des données qui stocke plus de données dans moins d'espace.





Depuis ONTAP 9.2, toutes les fonctionnalités d'efficacité du stockage à la volée, telles que la déduplication et la compression à la volée, sont activées par défaut sur les volumes AFF.

## Activer la déduplication sur un volume

Vous pouvez activer la déduplication sur un volume FlexVol afin d'optimiser l'efficacité du stockage. Vous pouvez activer la déduplication post-traitement sur tous les volumes et la déduplication à la volée sur les volumes résidant dans des agrégats AFF ou Flash Pool.

Si vous souhaitez activer la déduplication à la volée sur d'autres types de volumes, consultez l'article de la base de connaissances ["Comment activer la déduplication à la volée des volumes sur des agrégats non AFF \(100 % Flash FAS\)"](#).

### Avant de commencer

Pour un volume FlexVol, il faut avoir vérifié qu'il existe un espace libre suffisant pour les métadonnées de la déduplication dans les volumes et les agrégats. Les métadonnées de la déduplication requièrent un espace disponible minimal dans l'agrégat. Cette quantité correspond à 3 % de la quantité totale de données physiques pour l'ensemble des volumes FlexVol dédupliqués ou des composants de données au sein de l'agrégat. Chaque volume FlexVol ou composant de données doit présenter 4 % de l'espace libre total des données physiques, pour un total de 7 %.



Depuis ONTAP 9.2, la déduplication à la volée est activée par défaut sur les systèmes AFF.

### Choix

- Utilisez le `volume efficiency on` pour activer la déduplication post-traitement.

La commande suivante active la déduplication post-traitement sur volume Vola :

```
volume efficiency on -vserver vs1 -volume VolA
```

- Utilisez le `volume efficiency on` suivi de la commande `volume efficiency modify` avec `-inline-deduplication` option définie sur `true` pour activer à la fois la déduplication post-traitement et la déduplication à la volée.

Les commandes suivantes permettent la déduplication post-traitement et la déduplication à la volée sur le volume Vola :

```
volume efficiency on -vserver vs1 -volume VolA
```

```
volume efficiency modify -vserver vs1 -volume VolA -inline-dedupe true
```

- Utilisez le `volume efficiency on` suivi de la commande `volume efficiency modify` avec `-inline-deduplication` option définie sur `true` et le `-policy` option définie sur `inline-only` pour activer uniquement la déduplication à la volée.

Les commandes suivantes permettent uniquement la déduplication à la volée sur le volume Vola :

```
volume efficiency on -vserver vs1 -volume VolA
```

```
volume efficiency modify -vserver vs1 -volume VolA -policy inline-only -inline-dedupe true
```

## Une fois que vous avez terminé

Vérifiez que le paramètre a été modifié en consultant les paramètres d'efficacité du volume :

```
volume efficiency show -instance
```

## Désactiver la déduplication sur un volume

Vous pouvez désactiver la déduplication post-traitement et la déduplication en ligne indépendamment sur un volume.

### Ce dont vous avez besoin

Arrêtez toutes les opérations d'efficacité du volume actuellement actives sur le volume : `volume efficiency stop`

### Description de la tâche

Si vous avez activé la compression des données sur le volume, exécutez le `volume efficiency off` commande désactive la compression des données.

### Choix

- Utilisez le `volume efficiency off` commande pour désactiver à la fois la déduplication post-traitement et la déduplication à la volée.

La commande suivante désactive la déduplication post-traitement et la déduplication à la volée sur volume Vola :

```
volume efficiency off -vserver vs1 -volume VolA
```

- Utilisez le `volume efficiency modify` commande avec `-policy inline only` pour désactiver la déduplication post-traitement, mais la déduplication à la volée reste activée.

La commande suivante désactive la déduplication post-traitement, mais la déduplication à la volée reste activée sur le volume Vola :

```
volume efficiency modify -vserver vs1 -volume VolA -policy inline-only
```

- Utilisez le `volume efficiency modify` commande avec `-inline-deduplication` option définie sur `false` pour désactiver uniquement la déduplication à la volée.

La commande suivante désactive uniquement la déduplication à la volée sur volume Vola :

```
volume efficiency modify -vserver vs1 -volume VolA -inline-deduplication false
```

## Déduplication en arrière-plan automatique au niveau des volumes sur les systèmes AFF

À partir de ONTAP 9.3, vous pouvez configurer la déduplication en arrière-plan au niveau des volumes pour qu'elle s'exécute automatiquement à l'aide d'un outil prédéfini `auto` Politique de AFF. Aucune configuration manuelle des planifications n'est requise. Le `auto` cette règle exécute la déduplication continue en arrière-plan.

Le `auto` il est défini sur la règle pour tous les volumes nouvellement créés et pour tous les volumes mis à niveau qui n'ont pas été configurés manuellement pour la déduplication en arrière-plan. C'est possible "[modifier la règle](#)" à `default` ou toute autre stratégie de désactivation de la fonction.

Si un volume est déplacé d'un système non AFF vers un système AFF, la `auto` règle est activée par défaut sur le nœud de destination. Si un volume est déplacé d'un nœud AFF vers un nœud non AFF, la `auto` règle sur le nœud de destination est remplacée par le `inline-only` règle par défaut.

Sous AFF, le système contrôle tous les volumes qui ont le `auto` les règles et dépriorise le volume qui a moins d'économies ou a fréquemment remplacé. Les volumes dépriorisés ne participent plus à la déduplication automatique en arrière-plan. La journalisation des modifications sur les volumes non prioritaires est désactivée et les métadonnées sur le volume sont tronquées.

Les utilisateurs peuvent promouvoir le volume dépriorisé pour participer de nouveau à la déduplication automatique en arrière-plan à l'aide de la `volume efficiency promote` commande disponible au niveau de privilège avancé.

**Gérez la déduplication à la volée au niveau de l'agrégat sur les systèmes AFF**

La déduplication au niveau de l'agrégat élimine les blocs dupliqués sur les volumes appartenant au même agrégat. Depuis ONTAP 9.2, il est possible d'effectuer une déduplication à la volée au niveau de l'agrégat sur les systèmes AFF. La fonctionnalité est activée par défaut sur tous les volumes nouvellement créés et sur tous les volumes mis à niveau alors que la déduplication à la volée des volumes est activée.

**Description de la tâche**

Le processus de déduplication élimine les blocs dupliqués avant que les données ne soient écrites sur le disque. Uniquement les volumes avec le `space guarantee` réglé sur `none` peut participer à la déduplication à la volée au niveau des agrégats. Il s'agit du paramètre par défaut sur les systèmes AFF.



La déduplication à la volée au niveau des agrégats est parfois appelée déduplication à la volée entre les volumes.

**Étape**

- 1. Gérez la déduplication à la volée au niveau de l'agrégat sur les systèmes AFF :

| Les fonctions que vous recherchez...                                  | Utilisez cette commande                                                                                         |
|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Activez la déduplication à la volée au niveau des agrégats            | <code>volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe true</code>  |
| Désactiver la déduplication à la volée au niveau des agrégats         | <code>volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe false</code> |
| Afficher l'état de la déduplication à la volée au niveau de l'agrégat | <code>volume efficiency config -volume vol_name</code>                                                          |

**Exemples**

La commande suivante affiche l'état de la déduplication à la volée au niveau de l'agrégat :

```
wfit-8020-03-04::> volume efficiency config -volume choke0_wfit_8020_03_0
Vserver: vs0
Volume: choke0_wfit_8020_03_0
Schedule: -
Policy: choke_VE_policy
Compression: true
Inline Compression: true
Inline Dedupe: true
Data Compaction: true
Cross Volume Inline Deduplication: false
```

## Gérez la déduplication en arrière-plan au niveau de l'agrégat sur des systèmes AFF

La déduplication au niveau de l'agrégat élimine les blocs dupliqués sur les volumes appartenant au même agrégat. Depuis ONTAP 9.3, il est possible d'effectuer la déduplication au niveau de l'agrégat en arrière-plan sur les systèmes AFF. La fonctionnalité est activée par défaut sur tous les volumes nouvellement créés et sur tous les volumes mis à niveau lorsque la déduplication en arrière-plan des volumes est activée.

### Description de la tâche

L'opération est déclenchée automatiquement lorsqu'un pourcentage suffisamment important du journal des modifications a été rempli. Aucun programme ou règle n'est associé à l'opération.

Depuis ONTAP 9.4, les utilisateurs AFF peuvent également exécuter le processus de déduplication au niveau de l'agrégat pour éliminer les doublons des données existantes sur les volumes de l'agrégat. Vous pouvez utiliser le `storage aggregate efficiency cross-volume-dedupe start` commande avec `-scan -old-data=true` option de démarrage du scanner :

```
cluster-1::> storage aggregate efficiency cross-volume-dedupe start
-aggregate aggr1 -scan-old-data true
```

L'analyse de la déduplication peut prendre du temps. Vous pouvez exécuter l'opération en dehors des heures de pointe.



La déduplication en arrière-plan au niveau de l'agrégat est parfois appelée déduplication en arrière-plan inter-volumes.

### Étapes

1. Gérez la déduplication en arrière-plan au niveau de l'agrégat sur les systèmes AFF :

| Les fonctions que vous recherchez...                                       | Utilisez cette commande                                                                                                              |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Activer la déduplication en arrière-plan au niveau de l'agrégat            | <code>volume efficiency modify -vserver &lt;vserver_name\&gt; -volume &lt;vol_name\&gt; -cross-volume-background-dedupe true</code>  |
| Désactiver la déduplication en arrière-plan au niveau de l'agrégat         | <code>volume efficiency modify -vserver &lt;vserver_name\&gt; -volume &lt;vol_name\&gt; -cross-volume-background-dedupe false</code> |
| Afficher l'état de la déduplication en arrière-plan au niveau de l'agrégat | <code>aggregate efficiency cross-volume-dedupe show</code>                                                                           |

## Présentation de l'efficacité du stockage sensible à la température

ONTAP offre des avantages en termes d'efficacité du stockage sensibles à la température en évaluant la fréquence d'accès aux données de votre volume et en mappant cette fréquence au niveau de compression appliqué à ces données. Pour les données inactives peu utilisées, les blocs de données plus volumineux sont compressés et pour les données actives, qui sont fréquemment utilisées et remplacées plus souvent, les blocs de données plus petits sont compressés, ce qui améliore l'efficacité du processus.

L'efficacité du stockage sensible à la température, introduite dans ONTAP 9.8, est automatiquement activée sur les volumes AFF nouvellement créés à provisionnement fin. Vous pouvez activer l'efficacité du stockage sensible à la température sur les volumes AFF existants et sur les volumes non-AFF DP à provisionnement fin.

### Introduction des modes « par défaut » et « efficace »

À partir de ONTAP 9.10.1, les modes d'efficacité du stockage *default* et *Efficient* au niveau du volume sont introduits uniquement pour les systèmes AFF. Les deux modes permettent de choisir entre la compression de fichiers (par défaut), qui est le mode par défaut lors de la création de nouveaux volumes AFF, ou l'efficacité du stockage sensible à la température (efficace), ce qui permet d'obtenir une efficacité du stockage sensible à la température. Avec ONTAP 9.10.1, "[l'efficacité du stockage sensible à la température doit être définie de manière explicite](#)" pour activer la compression auto-adaptative. Cependant, d'autres fonctionnalités d'efficacité du stockage telles que la compaction des données, la déduplication automatique, la déduplication à la volée, la déduplication à la volée entre volumes et la déduplication en arrière-plan entre volumes sont activées par défaut sur les plateformes AFF pour les modes par défaut et efficaces.

Les deux modes d'efficacité du stockage (par défaut et efficace) sont pris en charge sur les agrégats compatibles avec FabricPool et avec tous les types de règles de Tiering.

### Efficacité du stockage sensible à la température activée sur les plateformes C-Series

L'efficacité du stockage sensible à la température est activée par défaut sur les plates-formes AFF série C et lors de la migration de volumes d'une plate-forme non TSSE vers une plate-forme C-Series compatible TSSE à l'aide de Volume Move ou de SnapMirror avec les versions suivantes installées sur la destination :

- ONTAP 9.12.1P4 et versions ultérieures
- ONTAP 9.13.1 et versions ultérieures

Pour plus d'informations, voir ["Efficacité du stockage avec déplacement de volumes et opérations SnapMirror"](#).

Pour les volumes existants, l'efficacité du stockage sensible à la température n'est pas activée automatiquement, mais elle le peut ["modifier le mode d'efficacité du stockage"](#) manuellement pour passer en mode efficace.



Une fois que vous avez défini le mode d'efficacité du stockage sur efficace, vous ne pouvez plus le redéfinir.

**Amélioration de l'efficacité du stockage grâce à la compression séquentielle des blocs physiques contigus**

Depuis la version ONTAP 9.13.1, l'efficacité du stockage sensible à la température ajoute la compaction séquentielle des blocs physiques contigus afin d'améliorer encore l'efficacité du stockage. Sur les volumes dont l'efficacité du stockage sensible à la température est activée automatiquement, la compression séquentielle est activée lorsque vous mettez à niveau des systèmes vers ONTAP 9.13.1. Une fois l'emballage séquentiel activé, vous devez le faire ["reconditionnement manuel des données existantes"](#).

**Mise à niveau**

Lors de la mise à niveau vers ONTAP 9.10.1 et versions ultérieures, un mode d'efficacité du stockage est attribué aux volumes existants, basé sur le type de compression actuellement activé sur les volumes. Au cours d'une mise à niveau, le mode par défaut est attribué aux volumes dont la compression est activée et le mode efficace est activé pour les volumes dont l'efficacité de stockage est sensible à la température. Si la compression n'est pas activée, le mode d'efficacité du stockage reste vide.

**Efficacité du stockage avec déplacement de volumes et opérations SnapMirror**

Le comportement de l'efficacité du stockage peut être affecté par d'autres opérations de stockage actives ou lancées en même temps. Vous devez être conscient de l'impact de ces opérations sur l'efficacité du stockage.

Dans plusieurs cas, d'autres opérations peuvent affecter l'efficacité du stockage d'un volume. Cela inclut lorsque vous effectuez un déplacement de volume ou une opération SnapMirror et ce qui se passe lorsque vous effectuez une interruption SnapMirror et activez manuellement l'efficacité du stockage sensible à la température (TSSE) dépend du type d'efficacité du volume source.

Le tableau suivant décrit le comportement d'un volume source et d'un volume de destination lorsque vous effectuez l'une de ces opérations.

| Efficacité du volume source | Comportement par défaut du volume de destination |                     |                                | Comportement par défaut après activation manuelle de TSSE (après coupure SnapMirror) |                     |                                |
|-----------------------------|--------------------------------------------------|---------------------|--------------------------------|--------------------------------------------------------------------------------------|---------------------|--------------------------------|
|                             | Type d'efficacité du stockage                    | Nouvelles écritures | Compression de données à froid | Type d'efficacité du stockage                                                        | Nouvelles écritures | Compression de données à froid |
|                             |                                                  |                     |                                |                                                                                      |                     |                                |

|                                                  |                                                                                                                                 |                                                                                                       |                                                                                                                                                                                                                                                                          |                                                                    |                                                     |                                                                                                                                                                                                                                                                          |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aucune efficacité du stockage (probablement FAS) | Compression de fichiers                                                                                                         | Une tentative de compression de fichier est effectuée à la volée sur les données nouvellement écrites | Pas de compression des données inactives. Les données restent telles qu'elles sont                                                                                                                                                                                       | TSSE avec algorithme d'acquisition de données inactives comme ZSTD | Tentative de compression en ligne 8k au format TSSE | <p><b>Fichier données compressées:</b> N/A</p> <p><b>Données non compressées :</b> tentative de compression de 32 K après la période de jours seuil atteinte</p> <p><b>Données nouvellement écrites :</b> tentative de compression de 32 K après la période de seuil</p> |
| Aucune efficacité du stockage (probablement FAS) | Compression de fichiers sur les plateformes C-Series utilisant ONTAP 9.11.1P10 ou ONTAP 9.12.1P3                                | Pas de compression de données inactives compatible TSSE                                               | <b>Fichier données compressées:</b> N/A                                                                                                                                                                                                                                  | TSSE avec algorithme d'acquisition de données inactives comme ZSTD | Compression à la volée de 8 Ko                      | <p><b>Fichier données compressées:</b> N/A</p> <p><b>Données non compressées :</b> tentative de compression de 32 K après la période de jours seuil atteinte</p> <p><b>Données nouvellement écrites :</b> tentative de compression de 32 K après la période de seuil</p> |
| Aucune efficacité du stockage (probablement FAS) | TSSE sur les plateformes de la série C utilisant ONTAP 9.12.1P4 et versions ultérieures ou ONTAP 9.13.1 et versions ultérieures | Tentative de compression en ligne 8K au format TSSE                                                   | <p><b>Fichier données compressées:</b> N/A</p> <p><b>Données non compressées :</b> tentative de compression de 32 K après la période de jours seuil atteinte</p> <p><b>Données nouvellement écrites :</b> tentative de compression de 32 K après la période de seuil</p> | TSSE avec algorithme d'acquisition de données inactives comme ZSTD | Tentative de compression en ligne 8K au format TSSE | <p><b>Fichier données compressées:</b> N/A</p> <p><b>Données non compressées :</b> tentative de compression de 32 K après la période de jours seuil atteinte</p> <p><b>Données nouvellement écrites :</b> tentative de compression de 32 K après la période de seuil</p> |

|                                    |                                                                                                    |                                                                                                       |                                                                                                                                                                        |                                                                                                                 |                                                     |                                                                                                                                                                                                                                                                                                     |
|------------------------------------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Groupe de compression de fichiers  | Identique à la source                                                                              | Une tentative de compression de fichier est effectuée à la volée sur les données nouvellement écrites | Pas de compression des données inactives. Les données restent telles qu'elles sont                                                                                     | TSSE avec algorithme d'acquisition de données inactives comme ZSTD                                              | Tentative de compression en ligne 8k au format TSSE | <b>Fichier données compressées</b> : non compressées<br><br><b>Données non compressées</b> : la compression de 32 K est tentée après la période de jours de seuil atteinte<br><br><b>Données nouvellement écrites</b> : la compression de 32 K est tentée après le nombre de jours de seuil atteint |
| Analyse des données inactives TSSE | TSSE utilisant le même algorithme de compression que le volume source (LZOPro→LZOPro et ZSTD→ZSTD) | Tentative de compression en ligne de 8 Ko au format TSSE                                              | Tentative de compression de 32 K avec LzoPro après la période de froid basée sur le seuil est atteinte sur les données existantes et les données nouvellement écrites. | TSSE est activé. REMARQUE : l'algorithme d'acquisition de données inactives LZOPro peut être remplacé par ZSTD. | Tentative de compression en ligne 8K au format TSSE | Une tentative de compression de 32 K est effectuée après la période de froid des jours de seuil atteinte pour les données existantes et les données nouvellement écrites.                                                                                                                           |

## Définissez le mode d'efficacité du stockage lors de la création du volume

Depuis ONTAP 9.10.1, vous pouvez définir le mode d'efficacité du stockage lors de la création d'un nouveau volume AFF.

### Description de la tâche

Vous pouvez contrôler le mode d'efficacité du stockage sur un nouveau volume AFF à l'aide du paramètre `-storage-efficiency-mode`. Le volume peut être configuré pour utiliser le mode d'efficacité ou le mode de performances par défaut. Les deux modes permettent de choisir entre la compression de fichiers ou l'efficacité du stockage sensible à la température. La compression de fichier est le mode par défaut lors de la création de nouveaux volumes AFF. L'efficacité du stockage sensible à la température assure une efficacité du stockage sensible à la température. Notez que le paramètre `-storage-efficiency-mode` n'est pas pris en charge sur les volumes non AFF ou sur les volumes de protection des données.


### Étapes

Vous pouvez effectuer cette tâche à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes de ONTAP.



## System Manager

À partir de ONTAP 9.10.1, System Manager vous permet d'accroître l'efficacité du stockage en utilisant la fonctionnalité d'efficacité du stockage sensible à la température. L'efficacité du stockage basée sur les performances est activée par défaut.

1. Cliquez sur **Storage > volumes**.
2. Recherchez le volume sur lequel vous souhaitez activer ou désactiver l'efficacité du stockage, puis cliquez sur .
3. Cliquez sur **Modifier > volumes** et faites défiler jusqu'à **efficacité du stockage**.
4. Sélectionnez **Activer une efficacité de stockage supérieure**.

## CLI

### Créez un nouveau volume en utilisant le mode efficace

Pour définir le mode d'efficacité du stockage sensible à la température lors de la création d'un volume, vous pouvez utiliser le `-storage-efficiency-mode` paramètre avec la valeur `efficient`.

1. Créez un nouveau volume avec le mode d'efficacité activé :

```
volume create -vserver <vserver name> -volume <volume name> -aggregate
<aggregate name> -size <volume size> -storage-efficiency-mode efficient
```

```
volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1
-storage-efficiency-mode efficient -size 10g
```

### Créer un volume à l'aide du mode performances

Le mode performances est défini par défaut lorsque vous créez de nouveaux volumes AFF avec efficacité du stockage. Bien que cela ne soit pas nécessaire, vous pouvez éventuellement utiliser le `default` valeur avec le `-storage-efficiency-mode` Paramètre lors de la création d'un volume AFF.

1. Créer un volume à l'aide du mode d'efficacité du stockage des performances « par défaut » :

```
volume create -vserver <vserver name> -volume <volume name> -aggregate
<aggregate name> -size <volume size> -storage-efficiency-mode default
```

```
volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1 -storage
-efficiency-mode default -size 10g
```

## Modifiez le seuil de compression des données inactives du volume

Vous pouvez modifier la fréquence d'analyse des données inactives d'ONTAP en modifiant le seuil de froid sur les volumes grâce à l'efficacité du stockage sensible à la température.

### Avant de commencer

Vous devez être administrateur du cluster ou du SVM et utiliser le niveau de privilège avancé de l'interface de ligne de commandes ONTAP.

## Description de la tâche

Le seuil de froid peut être de 1 à 60 jours. Le seuil par défaut est de 14 jours.

### Étapes

1. Définissez le niveau de privilège :

```
set -privilege advanced
```

2. Modifier la compression des données inactives sur un volume :

```
volume efficiency inactive-data-compression modify -vserver <vserver_name>
-volume <volume_name> -threshold-days <integer>
```

Pour plus d'informations sur, reportez-vous à la page man "[modification de la compression des données inactives](#)".

### Vérifiez le mode d'efficacité du volume

Vous pouvez utiliser le `volume-efficiency-show` Commande sur un volume AFF pour vérifier si l'efficacité est définie et pour afficher le mode d'efficacité actuel.

#### Étape

1. Vérifier le mode d'efficacité sur un volume :

```
volume efficiency show -vserver <vserver name> -volume <volume name> -fields
storage-efficiency-mode
```

### Changer le mode d'efficacité du volume

À partir de ONTAP 9.10.1, les modes d'efficacité du stockage au niveau des volumes *default* et *Efficient* sont pris en charge uniquement pour les systèmes AFF. Ces modes permettent de choisir entre la compression de fichier (par défaut), qui est le mode par défaut lors de la création de nouveaux volumes AFF, ou l'efficacité du stockage sensible à la température (efficace), ce qui permet d'optimiser l'efficacité du stockage en fonction de la température. Vous pouvez utiliser `volume efficiency modify` la commande pour faire passer le mode d'efficacité du stockage d'un volume AFF de `default` à `efficient` ou vous pouvez définir un mode d'efficacité lorsque l'efficacité des volumes n'est pas déjà définie.

### Étapes

1. Modifiez le mode d'efficacité du volume :

```
volume efficiency modify -vserver <vserver name> -volume <volume name>
-storage-efficiency-mode <default|efficient>
```

**Affichez les économies d'empreinte des volumes avec ou sans efficacité du stockage sensible à la température**

En fonction de la version de ONTAP utilisée, vous pouvez afficher les économies d'encombrement physique de chaque volume. Vous pouvez le faire pour évaluer l'efficacité de vos processus administratifs ou dans le cadre de la planification des capacités.

**Description de la tâche**

Depuis la version ONTAP 9.11.1, vous pouvez utiliser la commande `volume show-footprint` pour afficher les économies d'encombrement physique sur les volumes pour lesquels l'efficacité de stockage sensible à la température (TSSE) est activée. À partir de ONTAP 9.13.1, vous pouvez utiliser la même commande pour afficher les économies d'encombrement physique sur les volumes non activés avec TSSE.

**Étapes**

- 1. Afficher les économies d'empreinte du volume :

```
volume show-footprint
```

**Exemple de sortie avec TSSE activé**

|                           |                            |       |  |
|---------------------------|----------------------------|-------|--|
| Vserver                   | : vs0                      |       |  |
| Volume                    | : vol_tsse_75_per_compress |       |  |
| Feature                   | Used                       | Used% |  |
| -----                     | -----                      | ----- |  |
| Volume Data Footprint     | 10.15GB                    | 13%   |  |
| Volume Guarantee          | 0B                         | 0%    |  |
| Flexible Volume Metadata  | 64.25MB                    | 0%    |  |
| Delayed Frees             | 235.0MB                    | 0%    |  |
| File Operation Metadata   | 4KB                        | 0%    |  |
| Total Footprint           | 10.45GB                    | 13%   |  |
| Footprint Data Reduction  | 6.85GB                     | 9%    |  |
| Auto Adaptive Compression | 6.85GB                     | 9%    |  |
| Effective Total Footprint | 3.59GB                     | 5%    |  |

## Exemple de sortie sans TSSE activé

```
Vserver : vs0
Volume : vol_file_cg_75_per_compress

Feature Used Used%
----- -
Volume Data Footprint 5.19GB 7%
Volume Guarantee 0B 0%
Flexible Volume Metadata 32.12MB 0%
Delayed Frees 90.17MB 0%
File Operation Metadata 4KB 0%

Total Footprint 5.31GB 7%

Footprint Data Reduction 1.05GB 1%
 Data Compaction 1.05GB 1%
Effective Total Footprint 4.26GB 5%
```

### Informations associées

- ["Définissez le mode d'efficacité du stockage lors de la création du volume"](#)

### Activer la compression des données sur un volume

Vous pouvez activer la compression des données sur un volume FlexVol afin de réaliser des économies d'espace en utilisant le `volume efficiency modify` commande. Vous pouvez également attribuer un type de compression à votre volume si vous ne souhaitez pas que le type de compression par défaut soit défini.

### Avant de commencer

Vous devez avoir activé la déduplication sur le volume.



- La déduplication doit uniquement être activée et elle n'a pas besoin d'être exécutée sur le volume.
- Le scanner de compression doit être utilisé pour compresser les données existantes sur les volumes présents dans les plateformes AFF.

### ["Activation de la déduplication sur un volume"](#)

### Description de la tâche

- Dans les agrégats de disques durs et les agrégats Flash Pool, vous pouvez activer la compression à la volée et post-traitement ou uniquement la compression post-traitement sur un volume.

Si vous activez les deux, vous devez activer la compression post-traitement sur le volume avant d'activer la compression à la volée.

- Sur les plateformes AFF, seule la compression à la volée est prise en charge.

Avant d'activer la compression à la volée, vous devez activer la compression post-traitement sur le volume. Cependant, comme la compression post-traitement n'est pas prise en charge sur les plateformes AFF, aucune compression post-traitement n'a lieu sur ces volumes et un message EMS est généré vous informant que la compression post-traitement a été ignorée.

- L'efficacité du stockage sensible aux températures est introduite dans ONTAP 9.8. Grâce à cette fonctionnalité, l'efficacité du stockage est appliquée même si les données sont actives ou inactives. Pour les données inactives, les blocs de données de taille supérieure sont compressés et pour les données fortement sollicitées, qui sont écrasées plus souvent, les blocs de données plus petits sont compressés, ce qui optimise l'efficacité du processus. L'efficacité du stockage sensible à la température est activée automatiquement sur les nouveaux volumes AFF à provisionnement fin.
- Le type de compression est automatiquement attribué en fonction de la plateforme de l'agrégat :

| Plateforme/agrégats      | Type de compression    |
|--------------------------|------------------------|
| AFF                      | Compression adaptative |
| Les agrégats Flash Pool  | Compression adaptative |
| Agrégats de disques durs | Compression secondaire |

## Choix

- Utilisez le `volume efficiency modify` commande pour activer la compression des données avec le type de compression par défaut.

La commande suivante active la compression post-traitement sur le volume Vola du SVM vs1 :

```
volume efficiency modify -vserver vs1 -volume VolA -compression true
```

La commande suivante active à la fois la compression post-traitement et la compression en ligne sur le volume Vola du SVM vs1 :

```
volume efficiency modify -vserver vs1 -volume VolA -compression true -inline
-compression true
```

- Utilisez le `volume efficiency modify` commande au niveau de privilège avancé pour activer la compression des données avec un type de compression spécifique.
  - a. Utilisez le `set -privilege advanced` commande permettant de changer le niveau de privilège en avancé.
  - b. Utilisez le `volume efficiency modify` commande permettant d'affecter un type de compression à un volume.

La commande suivante active la compression post-traitement et attribue le type de compression adaptative au volume Vola du SVM vs1 :

```
volume efficiency modify -vserver vs1 -volume VolA -compression true
-compression-type adaptive
```

La commande suivante active la compression post-traitement et la compression en ligne et attribue le type de compression adaptative au volume Vola du SVM vs1 :

```
volume efficiency modify -vserver vs1 -volume VolA -compression true
-compression-type adaptive -inline-compression true
```

- a. Utilisez le set `-privilege admin` commande permettant de changer le niveau de privilège en admin.

### Passez de la compression secondaire à la compression adaptative

Vous pouvez basculer entre la compression secondaire et la compression adaptative en fonction du volume de données lu. La compression adaptative est recommandée lorsqu'un grand volume de lectures aléatoires est important sur le système et que des performances plus élevées sont requises. Cette méthode est privilégiée lorsque les données sont écrites de manière séquentielle et que des économies de compression élevées sont requises.

#### Description de la tâche

Le type de compression par défaut est sélectionné en fonction de vos agrégats et de vos plateformes.

#### Étapes

1. Désactiver l'efficacité sur le volume :

```
volume efficiency off
```

Par exemple, la commande suivante désactive l'efficacité sur le volume vol1 :

```
volume efficiency off -vserver vs1 -volume vol1
```

2. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

3. Décompresser les données compressées :

```
volume efficiency undo
```

Par exemple, la commande suivante décompresse les données compressées sur le volume vol1 :

```
volume efficiency undo -vserver vs1 -volume vol1 -compression true
```



Vous devez vérifier que l'espace disponible sur le volume est suffisant pour prendre en charge les données décompressées.

4. Changement au niveau de privilège admin :

```
set -privilege admin
```

5. Vérifier que l'état de l'opération est inactif :

```
volume efficiency show
```

Par exemple, la commande suivante affiche le statut d'une opération d'efficacité sur le volume vol1 :

```
volume efficiency show -vserver vs1 -volume vol1
```

6. Activer l'efficacité pour le volume :

volume efficiency on Par exemple, la commande suivante active l'efficacité sur le volume vol1 :

```
volume efficiency on -vserver vs1 -volume vol1
```

7. Activer la compression des données, puis définir le type de compression :

```
volume efficiency modify
```

Par exemple, la commande suivante active la compression des données et définit le type de compression comme compression secondaire sur le volume vol1 :

```
volume efficiency modify -vserver vs1 -volume vol1 -compression true
-compression-type secondary
```



Cette étape active uniquement la compression secondaire sur le volume. Les données du volume n'ont pas été compressées.

- Pour compresser les données existantes sur les systèmes AFF, il faut lancer le scanner de compression en arrière-plan.
- Pour compresser les données existantes dans des agrégats Flash Pool ou des agrégats HDD, vous devez exécuter la compression en arrière-plan.

8. Facultatif : activer la compression à la volée :

```
volume efficiency modify
```

Par exemple, la commande suivante active la compression en ligne sur le volume vol1 :

```
volume efficiency modify -vserver vs1 -volume vol1 -inline-compression true
```

## Désactiver la compression des données sur un volume

Vous pouvez désactiver la compression des données sur un volume en utilisant le `volume efficiency modify` commande.

### Description de la tâche

Pour désactiver la compression post-traitement, vous devez d'abord désactiver la compression inline sur le volume.

### Étapes

1. Arrêtez toutes les opérations d'efficacité du volume actuellement actives sur le volume :

```
volume efficiency stop
```

2. Désactiver la compression des données :

```
volume efficiency modify
```

Les données compressées existantes resteront compressées sur le volume. Seules les nouvelles écritures entrant dans le volume ne sont pas compressées.

## Exemples

La commande suivante désactive la compression à la volée sur le volume Vola :

```
volume efficiency modify -vserver vs1 -volume VolA -inline-compression false
```

La commande suivante désactive la compression post-traitement et la compression à la volée sur volume Vola :

```
volume efficiency modify -vserver vs1 -volume VolA -compression false -inline
-compression false
```

## Gérez la compaction des données à la volée des systèmes AFF

Vous pouvez contrôler la compaction des données à la volée sur les systèmes AFF au niveau des volumes à l'aide de la `volume efficiency modify` commande. Elle est activée par défaut sur tous les volumes des systèmes AFF.

### Avant de commencer

La compaction des données requiert que la garantie d'espace du volume soit définie sur `none`. Il s'agit de l'option par défaut pour les systèmes AFF.



La garantie d'espace par défaut sur les volumes de protection des données non AFF est définie sur aucune.

### Étapes

1. Pour vérifier le paramètre de garantie d'espace pour le volume :

```
volume show -vserver vserver_name -volume volume_name -fields space-guarantee
```

2. Pour activer la compaction des données :

```
volume efficiency modify -vserver vserver_name -volume volume_name -data
-compaction true
```

3. Pour désactiver la compaction des données :

```
volume efficiency modify -vserver vserver_name -volume volume_name -data
-compaction false
```

4. Pour afficher l'état de compactage des données :

```
volume efficiency show -instance
```

## Exemples

```
cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data-compaction
true cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data
-compaction false
```



## Utilisez la compaction des données à la volée pour les systèmes FAS

Vous pouvez activer la compaction des données à la volée sur les systèmes FAS dotés d'agrégats Flash Pool (hybrides) ou de disques durs au niveau du volume ou de l'agrégat à l'aide de `volume efficiency` la commande `cluster shell`. Par défaut, la compaction est désactivée sur les systèmes FAS.

### Description de la tâche

Si vous activez la compaction des données au niveau des agrégats, celle-ci est activée sur tout nouveau volume créé avec la garantie d'espace du volume de `none` dans l'agrégat. L'activation de la compaction des données sur un volume dans un agrégat HDD utilise des ressources CPU supplémentaires.

### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Vérifier l'état de compaction des volumes et des agrégats du nœud souhaité :

```
volume efficiency show -volume <volume_name>
```

3. Activer la compaction des données sur un volume :

```
volume efficiency modify -volume <volume_name> -data-compaction true
```



Si la compaction est définie sur `false` pour un agrégat ou un volume, celle-ci échoue. L'activation de la compaction ne compacte pas les données existantes ; seules les nouvelles écritures dans le système sont compactées. La `volume efficiency start` commande contient plus d'informations sur la façon de compacter des données existantes (dans ONTAP 9.1 et versions ultérieures). Pour plus d'informations, voir "[Référence de commande ONTAP](#)".

4. Afficher les statistiques de compactage :

```
volume efficiency show -volume <volume_name>
```

## Efficacité du stockage à la volée activée par défaut sur les systèmes AFF

Les fonctionnalités d'efficacité du stockage sont activées par défaut sur tous les volumes nouvellement créés sur les systèmes AFF. À partir de ONTAP 9.2, toutes les fonctionnalités d'efficacité du stockage à la volée sont activées par défaut sur tous les volumes existants et nouvellement créés sur tous les systèmes AFF.

Les fonctionnalités d'efficacité du stockage incluent la déduplication et la déduplication à la volée, ainsi que la

compression en ligne entre plusieurs volumes. Elles sont activées par défaut sur les systèmes AFF, comme illustré dans le tableau.



Le comportement de compaction des données sur les volumes AFF est inchangé dans la ONTAP 9.2, car il est déjà activé par défaut.

| Conditions de volume                            | Fonctionnalités d'efficacité du stockage activées par défaut dans ONTAP 9.2 |                                            |                        |
|-------------------------------------------------|-----------------------------------------------------------------------------|--------------------------------------------|------------------------|
|                                                 | Déduplication à la volée                                                    | Déduplication entre les volumes à la volée | Compression à la volée |
| Mise à niveau du cluster vers la version 9.2    | Oui.                                                                        | Oui.                                       | Oui.                   |
| Transition de ONTAP 7-mode vers clustered ONTAP | Oui.                                                                        | Oui.                                       | Oui.                   |
| Déplacement de volumes                          | Oui.                                                                        | Oui.                                       | Oui.                   |
| Volumes à provisionnement lourd                 | Oui.                                                                        | Non                                        | Oui.                   |
| Volumes chiffrés                                | Oui.                                                                        | Non                                        | Oui.                   |

Les exceptions suivantes s'appliquent à une ou plusieurs fonctionnalités d'efficacité du stockage à la volée :

- Seuls les volumes en lecture/écriture peuvent prendre en charge l'efficacité du stockage à la volée par défaut.
- Les volumes dont les économies en termes de compression sont omis de l'activation de la compression à la volée.
- Les volumes sur lesquels la déduplication post-traitement est activée ne sont pas inclus dans l'activation de la compression à la volée.
- Pour les volumes sur lesquels l'efficacité des volumes est désactivée, le système remplace les paramètres de règles d'efficacité des volumes existants et le définit pour activer la règle à la volée uniquement.

## Visualisation de l'efficacité du stockage

Utilisez le `storage aggregate show-efficiency` commande pour afficher des informations sur l'efficacité du stockage de tous les agrégats du système.

Le `storage aggregate show-efficiency` la commande comporte trois vues différentes qui peuvent être invoquées en passant des options de commande.

### Vue par défaut

La vue par défaut affiche le ratio global pour chaque agrégat.

```
cluster1::> storage aggregate show-efficiency
```

## Vue détaillée

Appelez la vue détaillée avec le `-details` option de commande. Cette vue affiche les éléments suivants :

- Ratio d'efficacité global pour chaque agrégat.
- Ratio global sans copies Snapshot.
- Répartition du rapport pour les technologies d'efficacité suivantes : déduplication de volume, compression de volume, copies Snapshot, clones, compaction des données, et déduplication à la volée dans l'agrégat.

```
cluster1::> storage aggregate show-efficiency -details
```

## Vue avancée

La vue avancée est similaire à la vue détaillée et affiche les détails logiques et physiques utilisés.

Vous devez exécuter cette commande au niveau de privilège avancé. Passez au privilège avancé à l'aide du `set -privilege advanced` commande.

L'invite de commande devient `cluster::*>`.

```
cluster1::> set -privilege advanced
```

Appelez la vue avancée avec le `-advanced` option de commande.

```
cluster1::*> storage aggregate show-efficiency -advanced
```

Pour afficher les ratios d'un seul agrégat, appelez le `-aggregate aggregate_name` commande. Cette commande peut être exécutée au niveau admin, ainsi qu'au niveau de privilège avancé.

```
cluster1::> storage aggregate show-efficiency -aggregate aggr1
```

## Création d'une règle d'efficacité des volumes pour exécuter les opérations d'efficacité

### Créez une règle d'efficacité des volumes

Vous pouvez créer une stratégie d'efficacité des volumes pour exécuter la déduplication ou la compression des données, suivie de la déduplication sur un volume pendant une durée spécifique, puis spécifier la planification des tâches à l'aide du `volume efficiency policy create` commande.

### Avant de commencer

Vous devez avoir créé une planification cron à l'aide de `job schedule cron create` commande. Pour plus d'informations sur la gestion des planifications cron, reportez-vous à la ["Référence d'administration du système"](#).

### Description de la tâche

Un administrateur SVM avec des rôles prédéfinis par défaut ne peut pas gérer les règles de déduplication. Toutefois, l'administrateur du cluster peut modifier les privilèges affectés à un administrateur SVM en utilisant les rôles personnalisés. Pour plus d'informations sur les fonctionnalités de l'administrateur du SVM, consultez ["Authentification de l'administrateur et RBAC"](#).



Vous pouvez exécuter des opérations de déduplication ou de compression des données à une heure programmée, ou en créant une planification avec une durée spécifique, ou en spécifiant un pourcentage seuil, qui attend que les nouvelles données dépassent ce seuil et déclenche l'opération de déduplication ou de compression des données. Cette valeur de seuil correspond au pourcentage du nombre total de blocs utilisés dans le volume. Par exemple, si vous définissez la valeur de seuil sur un volume à 20 % lorsque le nombre total de blocs utilisés sur le volume est de 50 %, la déduplication ou la compression des données déclenche automatiquement lorsque les nouvelles données écrites sur le volume atteignent 10 % (20 % des 50 % de blocs utilisés). Si nécessaire, vous pouvez obtenir le nombre total de blocs utilisés à partir du `df` sortie de la commande.

## Étapes

1. Utilisez le `volume efficiency policy create` commande pour créer une règle d'efficacité du volume.

## Exemples

La commande suivante crée une politique d'efficacité du volume nommée `pol1` qui déclenche une opération d'efficacité quotidienne :

```
volume efficiency policy create -vserver vs1 -policy pol1 -schedule daily
```

La commande suivante crée une règle d'efficacité du volume nommée `pol2` qui déclenche une opération d'efficacité lorsque le pourcentage de seuil atteint 20 % :

```
volume efficiency policy create -vserver vs1 -policy pol2 -type threshold -start
-threshold-percent 20%
```

## Affecter une stratégie d'efficacité du volume à un volume

Vous pouvez attribuer une règle d'efficacité à un volume pour exécuter les opérations de déduplication ou de compression des données à l'aide de la `volume efficiency modify` commande.

## Avant de commencer

Assurez-vous que vous ["créez la règle d'efficacité des volumes"](#) avant de l'affecter à un volume.

## Description de la tâche

Lorsqu'une stratégie d'efficacité est attribuée à un volume secondaire SnapVault, seul l'attribut de priorité d'efficacité du volume est pris en compte lors de l'exécution des opérations d'efficacité du volume. Les planifications de tâches sont ignorées et le processus de déduplication est exécuté lorsque des mises à jour incrémentielles sont effectuées sur le volume secondaire SnapVault.

## Étape

1. Utilisez le `volume efficiency modify` commande permettant d'affecter une policy à un volume.

## Exemple

La commande suivante attribue la règle d'efficacité du volume nommée `new_policy` au volume `VolA`:

```
volume efficiency modify -vserver vs1 -volume VolA -policy new_policy
```

## Modifier une règle d'efficacité du volume

Vous pouvez modifier une stratégie d'efficacité des volumes pour exécuter la déduplication et la compression des données pendant une durée différente ou modifier la planification des tâches à l'aide de `volume efficiency policy modify` commande.

### Étapes

1. Utilisez le `volume efficiency policy modify` commande permettant de modifier une règle d'efficacité du volume.

### Exemples

La commande suivante modifie la politique d'efficacité du volume politique1 afin qu'elle s'exécute toutes les heures :

```
volume efficiency policy modify -vserver vs1 -policy policy1 -schedule hourly
```

La commande suivante modifie une politique d'efficacité du volume nommée pol2 pour atteindre un seuil de 30 % :

```
volume efficiency policy modify -vserver vs1 -policy pol1 -type threshold -start -threshold-percent 30%
```

## Afficher une règle d'efficacité des volumes

Vous pouvez afficher la règle d'efficacité des volumes, y compris le nom, la planification, la durée et la description.

### Description de la tâche

La commande `volume efficiency policy show` permet d'afficher une règle d'efficacité des volumes. Lorsque vous exécutez la commande dans l'étendue du cluster, les politiques cluster-scoped ne sont pas affichées. Toutefois, vous pouvez afficher les politiques de cluster-scoped dans le contexte du SVM.

### Étapes

1. Utilisez le `volume efficiency policy show` commande pour afficher les informations relatives à une règle d'efficacité du volume.

La sortie dépend des paramètres que vous spécifiez. Pour plus d'informations sur l'affichage d'une vue détaillée et d'autres paramètres, reportez-vous à la page man de cette commande.

### Exemples

La commande suivante affiche des informations sur les politiques créées pour le SVM vs1 :

```
volume efficiency policy show -vserver vs1
```

La commande suivante affiche les politiques pour lesquelles la durée est définie sur 10 heures :

```
volume efficiency policy show -duration 10
```

## Dissociation d'une règle d'efficacité du volume à partir d'un volume

Vous pouvez déassocier une règle d'efficacité des volumes d'un volume pour arrêter l'exécution des autres opérations de déduplication et de compression des données planifiées sur le volume. Une fois que vous avez dissocié une règle d'efficacité du

volume, vous devez la déclencher manuellement.

### Étape

1. Utilisez le `volume efficiency modify` commande pour dissocier une règle d'efficacité du volume d'un volume.

### Exemple

La commande suivante dissocie la règle d'efficacité du volume de Volume Vola : `volume efficiency modify -vserver vs1 -volume VolA -policy -`

### Supprimez une règle d'efficacité du volume

Vous pouvez supprimer une règle d'efficacité du volume à l'aide de `volume efficiency policy delete` commande.

### Ce dont vous avez besoin

Vous devez vous assurer que la règle à supprimer n'est associée à aucun volume.



Vous ne pouvez pas supprimer la stratégie d'efficacité *inline-only* et la stratégie d'efficacité prédéfinie *default*.

### Étape

1. Utilisez le `volume efficiency policy delete` commande de suppression d'une règle d'efficacité du volume.

### Exemple

La commande suivante supprime une politique d'efficacité du volume nommée politique1 : `volume efficiency policy delete -vserver vs1 -policy policy1`

## Gérez manuellement les opérations d'efficacité des volumes

### Gérer les opérations d'efficacité des volumes manuellement

Vous pouvez gérer la façon dont les opérations d'efficacité s'exécutent sur un volume en exécutant manuellement les opérations d'efficacité.

Vous pouvez également contrôler la manière dont les opérations d'efficacité s'exécutent dans les conditions suivantes :

- Utilisez des points de contrôle ou non
- Exécutez les opérations d'efficacité sur des données existantes ou uniquement sur de nouvelles données
- Arrêtez les opérations d'efficacité si nécessaire

Vous pouvez utiliser le `volume efficiency show` commande avec `schedule` comme valeur pour le `-fields` pour afficher la planification attribuée aux volumes.

### Exécuter une opération d'efficacité manuellement

Vous pouvez exécuter manuellement des opérations d'efficacité sur un volume. Vous pouvez le faire lorsque la planification des opérations d'efficacité n'est pas appropriée.

## Avant de commencer

Selon l'opération d'efficacité que vous souhaitez exécuter manuellement, vous devez avoir activé la déduplication ou la compression des données et la déduplication sur un volume.

## Description de la tâche

Cette opération s'effectue à l'aide de la `volume efficiency start` commande. Lorsque l'efficacité du stockage sensible à la température est activée sur un volume, la déduplication est exécutée initialement, suivie de la compression des données.

La déduplication est un processus d'arrière-plan qui consomme des ressources système pendant son exécution. Si les données ne sont pas modifiées fréquemment dans un volume, il est préférable d'exécuter la déduplication moins souvent. Plusieurs opérations de déduplication simultanées exécutées sur un système de stockage entraînent une consommation supérieure des ressources système.

Vous pouvez exécuter jusqu'à huit opérations de déduplication ou de compression des données simultanées par nœud. Si des opérations d'efficacité supplémentaires sont planifiées, les opérations sont mises en attente.

À partir de ONTAP 9.13.1, si l'efficacité du stockage sensible à la température est activée sur un volume, vous pouvez exécuter l'efficacité du volume sur les données existantes pour tirer parti de la compression séquentielle afin d'améliorer encore l'efficacité du stockage.

## Exécuter l'efficacité manuellement

### Étapes

1. Démarrer l'opération d'efficacité sur un volume : `volume efficiency start`

### Exemple

+ la commande suivante vous permet de lancer manuellement uniquement la déduplication ou la déduplication, suivie de la compression logique et de la compression des conteneurs sur le volume Vola

+

```
volume efficiency start -vserver vs1 -volume Vola
```

## Remballer les données existantes

Pour tirer parti de la compression séquentielle des données introduite dans ONTAP 9.13.1 sur les volumes sur lesquels l'efficacité du stockage sensible à la température est activée, vous pouvez reballer les données existantes. Vous devez être en mode privilège avancé pour utiliser cette commande.

### Étapes

1. Définissez le niveau de privilège : `set -privilege advanced`
2. Remballer les données existantes : `volume efficiency inactive-data-compression start -vserver vserver_name -volume volume_name -scan-mode extended_recompression`

### Exemple

```
volume efficiency inactive-data-compression start -vserver vs1 -volume
vol1 -scan-mode extended_recompression
```

## Informations associées

- ["Exécutez manuellement les opérations d'efficacité sur les données existantes"](#)

## Points de contrôle et opérations d'efficacité

Les points de contrôle sont utilisés en interne pour consigner le processus d'exécution d'une opération d'efficacité. Lorsqu'une opération d'efficacité est arrêtée pour quelque raison que ce soit (arrêt du système, interruption du système, redémarrage, ou parce que la dernière opération d'efficacité a échoué ou a été arrêtée) et qu'il existe des données de point de contrôle, l'opération d'efficacité peut reprendre à partir du dernier fichier de point de contrôle.

Un point de contrôle est créé :

- à chaque étape ou sous-stations de l'opération
- lorsque vous exécutez le `sis stop` commande
- à l'expiration de la durée

## Reprendre une opération d'efficacité interrompue

Si une opération d'efficacité est interrompue en raison d'un arrêt du système, d'une interruption du système ou d'un redémarrage, vous pouvez reprendre l'opération d'efficacité à partir du point où elle a été interrompue. Cela permet d'économiser du temps et des ressources en n'ayant pas besoin de redémarrer l'opération depuis le début.

## Description de la tâche

Si vous avez activé uniquement la déduplication sur le volume, la déduplication s'exécute sur les données. Si vous avez activé la déduplication et la compression des données sur un volume, la compression des données s'exécute en premier, suivie de la déduplication.

Vous pouvez afficher les détails du point de contrôle d'un volume en utilisant le `volume efficiency show` commande.

Par défaut, les opérations d'efficacité reprennent à partir des points de contrôle. Cependant, si un point de contrôle correspondant à une opération d'efficacité précédente (la phase lorsque le `volume efficiency start` la commande `-scan-old-data` est exécutée) est antérieure à 24 heures, alors l'opération d'efficacité ne reprend pas automatiquement à partir du point de contrôle précédent. Dans ce cas, l'opération d'efficacité commence dès le début. Toutefois, si vous savez que des changements significatifs n'ont pas eu lieu dans le volume depuis la dernière acquisition, vous pouvez forcer la poursuite à partir du point de contrôle précédent en utilisant le `-use-checkpoint` option.

## Étapes

1. Utilisez le `volume efficiency start` commande avec `-use-checkpoint` option pour reprendre une opération d'efficacité.

La commande suivante vous permet de reprendre une opération d'efficacité sur les nouvelles données du volume `VolA` :

```
volume efficiency start -vserver vs1 -volume VolA -use-checkpoint true
```



La commande suivante vous permet de reprendre une opération d'efficacité sur les données existantes sur le volume Vola :

```
volume efficiency start -vserver vs1 -volume VolA -scan-old-data true -use
-checkpoint true
```

#### Exécutez manuellement une opération d'efficacité sur les données existantes

Vous pouvez exécuter manuellement les opérations d'efficacité sur les données se trouvant dans des volumes qui ne sont pas sensibles à la température avant d'activer la déduplication, la compression ou la compaction des données. Vous pouvez exécuter ces opérations avec des versions ONTAP antérieures à ONTAP 9.8.

#### Description de la tâche

Cette opération s'effectue à l'aide de la `volume efficiency start` commande avec le `-scan-old-data` paramètre. L' `-compression` option ne fonctionne pas avec `-scan-old-data` sur les volumes d'efficacité du stockage sensibles à la température. La compression des données inactives s'exécute automatiquement sur les données préexistantes pour les volumes sensibles à la température d'efficacité du stockage dans ONTAP 9.8 et versions ultérieures.

Si vous activez uniquement la déduplication sur un volume, la déduplication s'exécute sur les données. Si vous activez la déduplication, la compression et la compaction des données sur un volume, la compression des données s'exécute en premier, suivie de la déduplication et de la compaction.

Lorsque vous exécutez la compression des données sur des données existantes, l'opération de compression ignore par défaut les blocs de données partagés par la déduplication et les blocs de données verrouillés par les copies Snapshot. Si vous choisissez d'exécuter la compression des données sur des blocs partagés, l'optimisation est désactivée, puis les informations relatives aux empreintes sont collectées et utilisées à nouveau pour le partage. Vous pouvez modifier le comportement par défaut de la compression des données lors de la compression des données existantes.

Vous pouvez exécuter jusqu'à huit opérations de déduplication, de compression des données ou de compaction des données simultanément par nœud. Les opérations restantes sont mises en file d'attente.



La compression post-traitement ne s'exécute pas sur les plateformes AFF. Un message EMS est généré pour vous informer que cette opération a été ignorée.

#### Étapes

1. Utilisez le `volume efficiency start -scan-old-data` commande permettant d'exécuter manuellement la déduplication, la compression ou la compaction des données sur les données existantes.

La commande suivante vous permet d'exécuter ces opérations manuellement sur les données existantes du volume Vola :

```
volume efficiency start -vserver vs1 -volume VolA -scan-old-data true [-
compression | -dedupe | -compaction] true
```

#### Informations associées

- ["Exécutez les opérations d'efficacité manuellement"](#)

## Gérez l'efficacité des volumes à l'aide des plannings

Exécutez une opération d'efficacité basée sur la quantité de nouvelles données écrites

Vous pouvez modifier la planification des opérations d'efficacité pour exécuter la déduplication ou la compression des données lorsque le nombre de nouveaux blocs écrits sur le volume après la précédente opération d'efficacité dépasse un pourcentage de seuil spécifié. Cela s'applique que l'opération d'efficacité précédente ait été effectuée manuellement ou planifiée.

### Description de la tâche

Si le `schedule` l'option est définie sur `auto`, l'opération d'efficacité planifiée s'exécute lorsque la quantité de nouvelles données dépasse le pourcentage spécifié. La valeur de seuil par défaut est de 20 %. Cette valeur de seuil correspond au pourcentage du nombre total de blocs déjà traités par l'opération d'efficacité.

### Étapes

1. Utilisez le `volume efficiency modify` commande avec `auto@num` option permettant de modifier la valeur du pourcentage de seuil.

`num` est un nombre à deux chiffres pour spécifier le pourcentage.

### Exemple

La commande suivante modifie la valeur seuil en pourcentage à 30 pour cent pour le volume Vola :

```
volume efficiency modify -vserver vs1 -volume -VolA -schedule auto@30
```

### Informations associées

- ["Exécutez les opérations d'efficacité via la planification"](#)

### Exécuter une opération d'efficacité à l'aide de la planification

Vous pouvez modifier la planification des opérations de déduplication ou de compression des données sur un volume. Les options de configuration d'une planification et de la règle d'efficacité des volumes s'excluent mutuellement.

### Description de la tâche

Cette opération s'effectue à l'aide de la `volume efficiency modify` commande.

### Étapes

1. Utilisez le `volume efficiency modify` commande permettant de modifier la planification des opérations de déduplication ou de compression des données sur un volume.

### Exemples

La commande suivante modifie la planification des opérations d'efficacité pour Vola à 11 h, du lundi au vendredi :

```
volume efficiency modify -vserver vs1 -volume VolA -schedule mon-fri@23
```

### Informations associées

- ["Exécutez les opérations d'efficacité en fonction du volume de nouvelles données écrites"](#)

## Surveiller les opérations d'efficacité du volume

### Afficher l'état et les opérations d'efficacité

Vous pouvez voir si la déduplication ou la compression des données est activée sur un volume. Vous pouvez également afficher l'état, l'état, le type de compression et la progression des opérations d'efficacité sur un volume.

Deux tâches sont disponibles. Les deux utilisent la commande `volume efficiency show`.

### Afficher l'état de l'efficacité

#### Étapes

1. Afficher l'état d'une opération d'efficacité sur un volume : `volume efficiency show`

La commande suivante affiche le statut d'une opération d'efficacité sur volume Vola qui se voit attribuer le type de compression adaptative :

```
volume efficiency show -instance -vserver vs1 -volume VolA
```

Si l'opération d'efficacité est activée sur volume Vola et que l'opération est inactive, vous pouvez voir les éléments suivants dans la sortie système :

```
cluster1::> volume efficiency show -vserver vs1 -volume VolA

Vserver Name: vs1
Volume Name: VolA
Volume Path: /vol/VolA
 State: Enabled
 Status: Idle
Progress: Idle for 00:03:20
```

## Déterminez si les volumes contiennent des données compressées de manière séquentielle

Vous pouvez afficher la liste des volumes pour lesquels la compression séquentielle est activée, par exemple, lorsque vous devez revenir à une version ONTAP antérieure à la version 9.13.1. Vous devez être en mode privilège avancé pour utiliser cette commande.

#### Étapes

1. Définissez le niveau de privilège : `set -privilege advanced`
2. Répertorier les volumes pour lesquels la compression séquentielle est activée :

```
volume efficiency show -extended-auto-adaptive-compression true
```

### Afficher les gains d'espace pour l'efficacité

Vous pouvez afficher le gain d'espace obtenu grâce à la déduplication et à la compression des données sur un volume. Vous pouvez le faire pour évaluer l'efficacité de

vos processus administratifs ou dans le cadre de la planification des capacités.

### Description de la tâche

Vous devez utiliser la commande `volume show` pour afficher les économies d'espace sur un volume. Notez que le gain d'espace obtenu par les copies Snapshot n'est pas inclus dans le calcul du gain d'espace réalisé sur un volume. L'utilisation de la déduplication n'affecte pas les quotas de volume. Les quotas sont signalés au niveau logique et restent inchangés.

### Étapes

1. Utilisez le `volume show` commande pour afficher les gains d'espace réalisés sur un volume grâce à la déduplication et à la compression des données.

### Exemple

La commande suivante permet d'afficher les économies d'espace réalisées grâce à la déduplication et à la compression des données sur le volume Vola : `volume show -vserver vs1 -volume Vola`

```
cluster1::> volume show -vserver vs1 -volume Vola

Vserver Name: vs1
Volume Name: Vola

...
 Space Saved by Storage Efficiency: 115812B
Percentage Saved by Storage Efficiency: 97%
 Space Saved by Deduplication: 13728B
Percentage Saved by Deduplication: 81%
 Space Shared by Deduplication: 1028B
 Space Saved by Compression: 102084B
Percentage Space Saved by Compression: 97%

...
```

### Afficher les statistiques d'efficacité d'un volume FlexVol

Vous pouvez afficher les détails des opérations d'efficacité exécutées sur un FlexVol volume. Vous pouvez le faire pour évaluer l'efficacité de vos processus administratifs ou dans le cadre de la planification des capacités.

### Étapes

1. Utilisez le `volume efficiency stat` Commande pour afficher les statistiques des opérations d'efficacité sur un volume FlexVol.

### Exemple

La commande suivante vous permet d'afficher les statistiques des opérations d'efficacité sur le volume Vola : `volume efficiency stat -vserver vs1 -volume Vola`

```
cluster1::> volume efficiency stat -vserver vs1 -volume VolA
```

```
Vserver Name: vs1
```

```
Volume Name: VolA
```

```
Volume Path: /vol/VolA
```

```
Inline Compression Attempts: 0
```

## Arrêt des opérations d'efficacité du volume

Vous pouvez arrêter une opération de déduplication ou de compression post-traitement.

### Description de la tâche

Cette opération utilise la commande `volume efficiency stop`. Cette commande génère automatiquement un point de contrôle.

### Étapes

1. Utilisez le `volume efficiency stop` commande pour arrêter une opération de déduplication ou de compression post-traitement active.

Si vous spécifiez le `-all` les opérations d'efficacité actives et mises en file d'attente sont abandonnées.

### Exemples

La commande suivante arrête le processus de déduplication ou de compression post-traitement actuellement actif sur le volume VolA :

```
volume efficiency stop -vserver vs1 -volume VolA
```

La commande suivante interrompt à la fois les opérations de déduplication ou de compression post-traitement actives et mises en attente sur le volume VolA :

```
volume efficiency stop -vserver vs1 -volume VolA -all true
```

## Informations supplémentaires sur la suppression des économies d'espace d'un volume

Vous pouvez choisir de supprimer les économies d'espace obtenues en exécutant des opérations d'efficacité sur un volume. Toutefois, vous devez disposer d'un espace suffisant pour permettre une inversion.

Plusieurs ressources connexes sont disponibles pour vous aider à planifier et à mettre en œuvre la suppression des économies d'espace.

### Informations associées

- ["Découvrez les économies d'espace obtenues grâce à la déduplication, à la compression et à la compaction dans ONTAP 9"](#)
- ["Découvrez comment annuler les économies réalisées grâce à l'efficacité du stockage dans ONTAP"](#)

## Réhébergement d'un volume aussi bien issus d'un SVM que d'un autre

### Préparer le réhébergement d'un volume d'un SVM à un autre SVM

Une opération de réhébergement de volume vous permet de réaffecter un volume NAS ou SAN d'un SVM à un autre sans avoir besoin d'une copie SnapMirror. La procédure de réhébergement exacte dépend du protocole d'accès client utilisé et du type de volume. Le réhébergement de volumes sont aussi une opération disruptive pour l'accès aux données et la gestion des volumes.

Avant de pouvoir réhéberger un volume d'un SVM vers un autre, les conditions suivantes doivent être remplies :

- Le volume doit être en ligne.
- San ou NAS multiprotocole

Pour le protocole NAS, le volume doit être démonté.

- Si le volume réside dans une relation SnapMirror, la relation doit être supprimée ou rompue avant le réhébergement du volume.

Vous pouvez resynchroniser la relation SnapMirror après une opération de réhébergement de volume.

### Réhébergez un volume SMB

Vous pouvez réhéberger un volume qui diffuse des données à l'aide du protocole SMB. Pour permettre aux clients de continuer à accéder aux données après l'opération de réhébergement, vous devez configurer manuellement les stratégies et les règles associées.

#### Description de la tâche

- Le réhébergement représente aussi une opération disruptive.
- En cas d'échec de l'opération de réhébergement, vous devrez peut-être reconfigurer les stratégies de volume et les règles associées sur le volume source.
- Si les domaines Active Directory du SVM source et du SVM cible sont différents, il est possible que l'accès aux objets du volume soit perdu.
- À partir de ONTAP 9.8, le réhébergement d'un volume avec NetApp Volume Encryption (NVE) est pris en charge. Si vous utilisez un gestionnaire de clés intégré, les métadonnées chiffrées seront modifiées lors de l'opération de réhébergement. Les données utilisateur ne sont pas modifiées.

Si vous utilisez ONTAP 9.8 ou une version antérieure, vous devez annuler le chiffrement du volume avant d'effectuer l'opération de réhébergement.

- Lorsque le SVM source possède des utilisateurs et des groupes locaux, les autorisations pour les fichiers et répertoires (ACL) définis ne sont plus effectives après l'opération de réhébergement de volume.

Il en va de même pour les listes de contrôle d'accès d'audit (CLS)

- Une fois le réhébergement, les règles, règles et configurations de volume suivantes perdues du volume source et doivent être reconfigurées manuellement sur le volume réhébergé :

- Règles d'exportation de volumes et de qtrees
- Politiques antivirus
- Règle d'efficacité du volume
- Règles de qualité de services
- Règles relatives aux snapshots
- Règles de quotas
- règle et règles d'exportation de la configuration des services de noms et de commutateur ns
- ID d'utilisateur et de groupe

### Avant de commencer

- Le volume doit être en ligne.
- Les opérations de gestion de volumes, telles que le déplacement de volumes ou de LUN, ne doivent pas être en cours d'exécution.
- L'accès aux données au volume qui est réhébergé doit être arrêté.
- La configuration des services de nom et de commutateur ns-switch du SVM cible doit être configurée pour prendre en charge l'accès aux données du volume de réhébergement.
- Le SVM source et le SVM de destination doivent avoir le même domaine Active Directory et realmDNS.
- L'ID utilisateur et l'ID groupe du volume doivent être disponibles dans le SVM cible ou modifiés sur le volume d'hébergement.



Si des utilisateurs et des groupes locaux sont configurés et si des fichiers et des répertoires sont présents sur ce volume avec des autorisations définies pour ces utilisateurs ou groupes, ces autorisations ne sont plus effectives.

### Étapes

1. Enregistrez des informations sur les partages CIFS pour éviter de perdre des informations sur les partages CIFS en cas d'échec de l'opération de réhébergement de volume.

2. Démontez le volume du volume parent :

```
volume unmount
```

3. Basculer vers le niveau de privilège avancé :

```
set -privilege advanced
```

4. Réhébergement « volume » sur le SVM de destination :

```
volume rehost -vserver source_svm -volume vol_name -destination-vserver
destination_svm
```

5. Monter le volume sous la Junction path appropriée dans le SVM de destination :

```
volume mount
```

6. Créer des partages CIFS pour le volume réhébergé :

```
vserver cifs share create
```

7. Si les domaines DNS diffèrent entre le SVM source et le SVM de destination, créer de nouveaux utilisateurs et groupes.
8. Mettre à jour le client CIFS avec les nouvelles LIFs du SVM de destination et Junction path vers le volume réhébergé.

### **Une fois que vous avez terminé**

Vous devez reconfigurer manuellement les stratégies et les règles associées sur le volume réhébergé.

["Configuration SMB"](#)

["Configuration multiprotocole SMB et NFS"](#)

### **Réhébergement d'un volume NFS**

Vous pouvez réhéberger un volume qui diffuse des données à l'aide du protocole NFS. Pour permettre aux clients d'accéder aux données après l'opération de réhébergement, vous devez associer le volume à la export policy du SVM et configurer manuellement les politiques et les règles associées.

#### **Description de la tâche**

- Le réhébergement représente aussi une opération disruptive.
- En cas d'échec de l'opération de réhébergement, vous devrez peut-être reconfigurer les stratégies de volume et les règles associées sur le volume source.
- À partir de ONTAP 9.8, le réhébergement d'un volume avec NetApp Volume Encryption (NVE) est pris en charge. Si vous utilisez un gestionnaire de clés intégré, les métadonnées chiffrées seront modifiées lors de l'opération de réhébergement. Les données utilisateur ne sont pas modifiées.

Si vous utilisez ONTAP 9.8 ou une version antérieure, vous devez annuler le chiffrement du volume avant d'effectuer l'opération de réhébergement.

- Une fois le réhébergement, les règles, règles et configurations de volume suivantes perdues du volume source et doivent être reconfigurées manuellement sur le volume réhébergé :
  - Règles d'exportation de volumes et de qtrees
  - Politiques antivirus
  - Règle d'efficacité du volume
  - Règles de qualité de services
  - Règles relatives aux snapshots
  - Règles de quotas
  - règle et règles d'exportation de la configuration des services de noms et de commutateur ns
  - ID d'utilisateur et de groupe

#### **Avant de commencer**

- Le volume doit être en ligne.
- Les opérations de gestion de volumes, telles que les déplacements de volumes ou de LUN, ne doivent pas être en cours d'exécution.
- L'accès aux données au volume qui est réhébergé doit être arrêté.



- La configuration des services de nom et de commutateur ns-switch du SVM cible doit être configurée pour prendre en charge l'accès aux données du volume de réhébergement.
- L'ID utilisateur et l'ID groupe du volume doivent être disponibles dans le SVM cible ou modifiés sur le volume d'hébergement.

## Étapes

1. Enregistrez des informations sur les règles d'exportation NFS pour éviter de perdre des informations sur les règles NFS en cas d'échec de l'opération de réhébergement de volume.

2. Démontez le volume du volume parent :

```
volume unmount
```

3. Basculer vers le niveau de privilège avancé :

```
set -privilege advanced
```

4. Réhébergement « volume » sur le SVM de destination :

```
volume rehost -vserver source_svm -volume volume_name -destination-vserver
destination_svm
```

La export policy par défaut du SVM de destination est appliquée au volume réhébergé.

5. Création de la export policy :

```
vserver export-policy create
```

6. Mettre à jour les export policy du volume réhébergé vers une export policy définie par l'utilisateur :

```
volume modify
```

7. Monter le volume sous la Junction path appropriée dans le SVM de destination :

```
volume mount
```

8. Vérifier que le service NFS s'exécute sur le SVM de destination.

9. Reprenez l'accès NFS au volume hébergé.

10. Mettre à jour les identifiants du client NFS et les configurations LIF pour refléter les LIFs du SVM de destination.

En effet, les chemins d'accès aux volumes (LIF et Junction path) ont subi des changements.

## Une fois que vous avez terminé

Vous devez reconfigurer manuellement les stratégies et les règles associées sur le volume réhébergé. Voir ["Configuration NFS"](#) pour plus d'informations.

## Réhébergez un volume SAN

Vous pouvez réhéberger un volume SAN qui transmet des données via des LUN mappées. Après avoir recréé le groupe initiateur (igroup) sur le SVM de destination, l'opération de réhébergement de volume peut automatiquement mapper le volume sur le

même SVM.

### Description de la tâche

- Le réhébergement représente aussi une opération disruptive.
- En cas d'échec de l'opération de réhébergement, vous devrez peut-être reconfigurer les stratégies de volume et les règles associées sur le volume source.
- À partir de ONTAP 9.8, le réhébergement d'un volume avec NetApp Volume Encryption (NVE) est pris en charge. Si vous utilisez un gestionnaire de clés intégré, les métadonnées chiffrées seront modifiées lors de l'opération de réhébergement. Les données utilisateur ne sont pas modifiées.

Si vous utilisez ONTAP 9.8 ou une version antérieure, vous devez annuler le chiffrement du volume avant d'effectuer l'opération de réhébergement.

- Une fois le réhébergement, les règles, règles et configurations de volume suivantes perdues du volume source et doivent être reconfigurées manuellement sur le volume hébergé :
  - Politiques antivirus
  - Règle d'efficacité du volume
  - Règles de qualité de services
  - Règles relatives aux snapshots
  - règle et règles d'exportation de la configuration des services de noms et de commutateur ns
  - ID d'utilisateur et de groupe

### Avant de commencer

- Le volume doit être en ligne.
- Les opérations de gestion de volumes, telles que les déplacements de volumes ou de LUN, ne doivent pas être en cours d'exécution.
- Aucune E/S active ne doit être constatée sur les volumes ou les LUN.
- Vous devez avoir vérifié que le SVM de destination ne dispose pas d'un groupe initiateur du même nom, mais que des initiateurs différents.

Si le groupe initiateur porte le même nom, vous devez l'avoir renommé dans l'un des SVM (source ou destination).

- Vous devez avoir activé `force-unmap-luns` option.
  - La valeur par défaut du `force-unmap-luns` l'option est `false`.
  - Aucun message d'avertissement ou de confirmation ne s'affiche lorsque vous avez défini le `force-unmap-luns` option à `true`.

### Étapes

1. Enregistrer les informations de mappage de LUN sur le volume cible :

```
lun mapping show volume volume vserver source_svm
```

Cette étape de précaution permet d'éviter de perdre des informations sur le mappage de LUN en cas de défaillance du réhébergement de volume.

2. Supprimez les igroups associés avec le volume cible.

### 3. Réhébergement le volume cible auprès du SVM de destination :

```
volume rehost -vserver source_svm -volume volume_name -destination-vserver
destination_svm
```

### 4. Mapper les LUN sur le volume cible sur les igroups appropriés :

- Le réhébergement de volume conserve les LUN sur le volume cible, mais les LUN ne sont pas mappées.
- Utiliser l'ensemble du port SVM de destination lors du mappage des LUN.
- Si le `auto-remap-luns` l'option est définie sur `true`, Les LUN sont mappées automatiquement après le réhébergement.

## Réhébergez un volume dans une relation SnapMirror

Vous pouvez réhéberger un volume défini dans le cadre d'une relation SnapMirror. Il y a plusieurs problèmes que vous devez prendre en compte avant de réhéberger la relation.

### Description de la tâche

- Le réhébergement représente aussi une opération disruptive.
- En cas d'échec de l'opération de réhébergement, vous devrez peut-être reconfigurer les stratégies de volume et les règles associées sur le volume source.
- Une fois le réhébergement, les règles, règles et configurations de volume suivantes perdues du volume source et doivent être reconfigurées manuellement sur le volume hébergé :
  - Règles d'exportation de volumes et de qtrees
  - Politiques antivirus
  - Règle d'efficacité du volume
  - Règles de qualité de services
  - Règles relatives aux snapshots
  - Règles de quotas
  - règle et règles d'exportation de la configuration des services de noms et de commutateur ns
  - ID d'utilisateur et de groupe

### Avant de commencer

- Le volume doit être en ligne.
- Les opérations de gestion de volumes, telles que les déplacements de volumes ou de LUN, ne doivent pas être en cours d'exécution.
- L'accès aux données au volume qui est réhébergé doit être arrêté.
- La configuration des services de nom et de commutateur ns-switch du SVM cible doit être configurée pour prendre en charge l'accès aux données du volume de réhébergement.
- L'ID utilisateur et l'ID groupe du volume doivent être disponibles dans le SVM cible ou modifiés sur le volume d'hébergement.

### Étapes

#### 1. Enregistrez le type de relation SnapMirror :

```
snapmirror show
```

Ceci est une étape de précaution qui permet d'éviter de perdre des informations sur le type de relation SnapMirror en cas de défaillance du nouvel hôte du volume.

2. Depuis le cluster destination, supprimer la relation SnapMirror :

```
snapmirror delete
```

Vous ne devez pas interrompre la relation SnapMirror ; sinon, la capacité de protection des données du volume de destination est perdue et la relation ne peut pas être rétablie après l'opération de réhébergement.

3. Depuis le cluster source, supprimer les informations relatives à la relation SnapMirror :

```
snapmirror release relationship-info-only true
```

Réglage du `relationship-info-only` paramètre à `true` Supprime les informations relatives à la relation source sans supprimer les copies Snapshot.

4. Basculer vers le niveau de privilège avancé :

```
set -privilege advanced
```

5. Réhébergement « volume » sur le SVM de destination :

```
volume rehost -vserver source_svm -volume vol_name -destination-vserver
destination_svm
```

6. Si la relation de SVM peering n'est pas présente, créer la relation de pairs SVM entre la SVM source et la SVM destination :

```
vserver peer create
```

7. Créer la relation SnapMirror entre le volume source et le volume de destination :

```
snapmirror create
```

Vous devez exécuter le `snapmirror create` Commande du SVM qui héberge le volume DP Le volume réhébergé peut être la source ou la destination de la relation SnapMirror.

8. Resynchroniser la relation SnapMirror.

### Fonctionnalités non prises en charge avec un réhébergement de volume

Plusieurs fonctionnalités ONTAP ne prennent pas en charge le réhébergement de volumes. Vous devez connaître ces fonctions avant de tenter une opération de réhébergement.

Les fonctionnalités suivantes ne sont pas prises en charge avec un réhébergement de volume :

- REPRISE APRÈS INCIDENT DES SVM
- Configurations MetroCluster



Le clonage d'un volume en tant que volume FlexClone sur un autre SVM n'est pas non plus pris en charge dans les configurations MetroCluster.

- Volumes SnapLock
- Volumes NetApp Volume Encryption (NVE) (dans les versions d'ONTAP antérieures à 9.8)

Dans les versions ONTAP antérieures à la version 9.8, vous devez annuler le chiffrement du volume avant de le réhéberger. Les clés de chiffrement de volume dépendent de clés SVM. Lorsqu'un volume est déplacé vers un autre SVM et que la configuration d'une clé mutualisée est activée sur le SVM source ou de destination, le volume et les clés SVM ne correspondent pas.

À partir de ONTAP 9.8, vous pouvez réhéberger un volume avec NVE.

- Volumes FlexGroup
- Clones de volumes

## **Combinaisons de configuration de volumes et de fichiers ou de LUN recommandées**

### **Présentation des combinaisons de configurations de volume et de fichier ou LUN recommandées**

Il existe des combinaisons spécifiques de configurations de volumes et fichiers FlexVol ou LUN qui peuvent être utilisées, en fonction des exigences de l'application et de l'administration. En comprenant les avantages et les coûts de ces combinaisons, vous pourrez déterminer la configuration la plus adaptée à votre environnement.

Les combinaisons de configuration de volume et de LUN suivantes sont recommandées :

- Fichiers ou LUN réservés en espace avec provisionnement d'un volume lourd
- Fichiers ou LUN non réservés en espace avec le provisionnement fin du volume
- Fichiers ou LUN réservés en espace avec provisionnement de volumes semi-lourds

Vous pouvez utiliser le provisionnement fin SCSI sur vos LUN en association avec l'une de ces combinaisons de configuration.

#### **Fichiers ou LUN réservés en espace avec provisionnement d'un volume lourd**

##### **Avantages :**

- Toutes les opérations d'écriture dans les fichiers réservés à l'espace sont garanties ; elles ne échoueront pas en raison de l'espace insuffisant.
- Les technologies d'efficacité du stockage et de protection des données présentes sur le volume ne sont pas soumises à restrictions.

##### **Coûts et limitations:**

- L'espace doit être suffisant en dehors de l'agrégat pour prendre en charge le volume bénéficiant du provisionnement.
- Un espace égal à deux fois la taille de la LUN est alloué au volume au moment de sa création.

## Fichiers ou LUN non réservés en espace avec le provisionnement fin du volume

### Avantages :

- Les technologies d'efficacité du stockage et de protection des données présentes sur le volume ne sont pas soumises à restrictions.
- L'espace est alloué uniquement lorsqu'il est utilisé.

### Coûts et restrictions:

- Les opérations d'écriture ne sont pas garanties ; elles peuvent échouer si le volume vient à manquer d'espace.
- Vous devez gérer efficacement l'espace libre dans l'agrégat pour empêcher ce dernier de manquer d'espace.

## Fichiers ou LUN réservés en espace avec provisionnement de volumes semi-lourds

### Avantages :

L'espace réservé est inférieur à celui du provisionnement d'un volume non lourd et la garantie d'écriture optimale est toujours fournie.

### Coûts et restrictions:

- Cette option permet d'échouer les opérations d'écriture.

Vous pouvez réduire ce risque en équilibrant correctement l'espace libre du volume par rapport à la volatilité des données.

- Vous ne pouvez pas compter sur la conservation des objets de protection des données tels que les copies Snapshot, les fichiers FlexClone et les LUN.
- Vous ne pouvez pas utiliser les fonctionnalités ONTAP d'efficacité du stockage de partage de blocs qui ne peuvent pas être supprimées automatiquement, notamment la déduplication, la compression et ODX/déchargement des copies.

## Déterminez la configuration de volume et de LUN adaptée à vos besoins

En répondant à quelques questions de base sur votre environnement, vous pourrez déterminer la meilleure configuration de volumes FlexVol et de LUN pour votre environnement.

### Description de la tâche

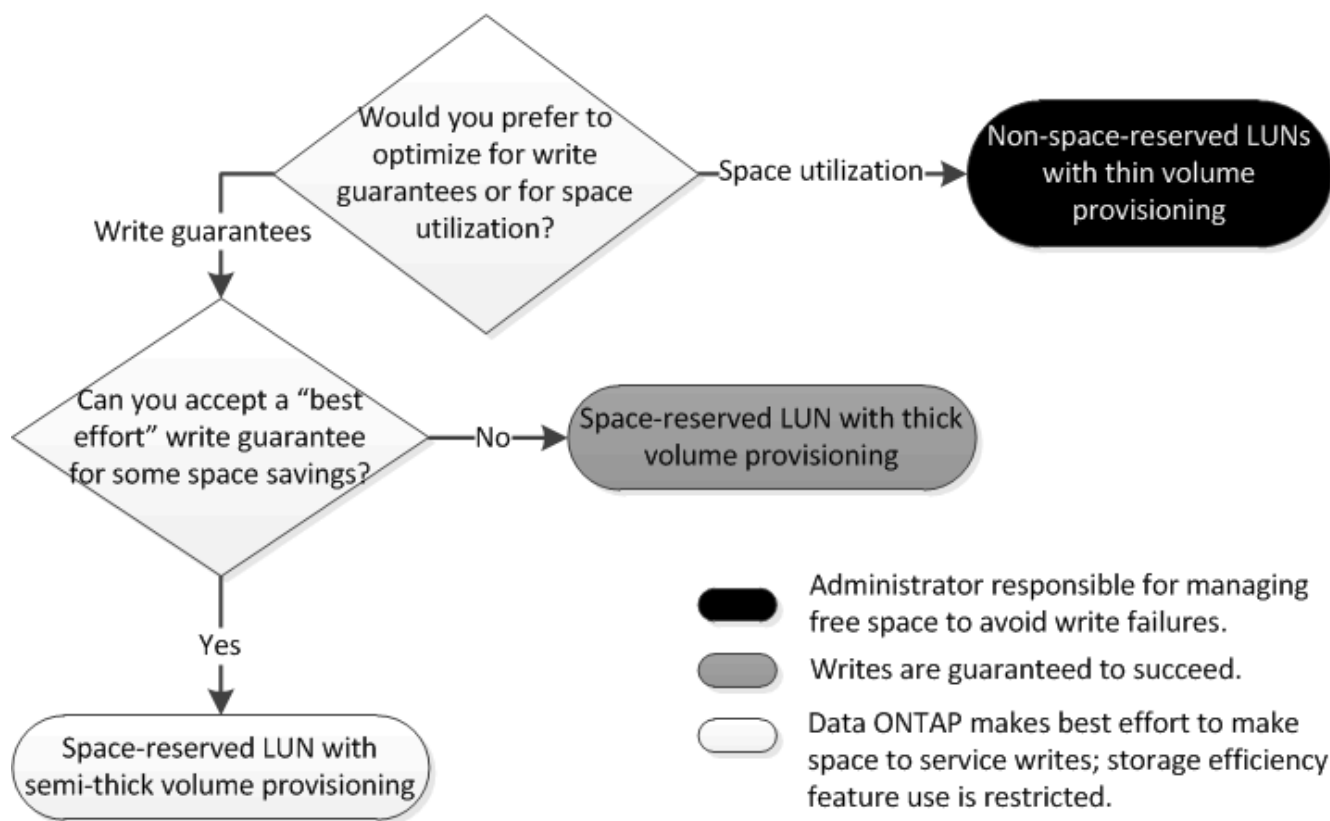
Vous pouvez optimiser les configurations des LUN et des volumes pour optimiser l'utilisation du stockage ou pour garantir la sécurité de l'écriture. En fonction de vos besoins en matière d'utilisation du stockage et de votre capacité à surveiller et à assurer la capacité des stocks disponibles rapidement, vous devez déterminer le volume FlexVol et les volumes LUN appropriés à votre installation.



Aucun volume n'est nécessaire pour chaque LUN.

### Étape

1. Utilisez l'arbre de décision suivant pour déterminer la meilleure combinaison de configuration de volumes et de LUN pour votre environnement :



### Paramètres de configuration pour les fichiers réservés en espace ou les LUN avec des volumes à provisionnement lourd

Vous pouvez utiliser plusieurs combinaisons de configuration de FlexVol volume et de configurations de fichiers ou de LUN. Cette combinaison basée sur des volumes à provisionnement lourd permet d'utiliser des technologies d'efficacité du stockage et ne nécessite pas de surveiller activement l'espace disponible car un espace suffisant est alloué au préalable.

Les paramètres suivants sont nécessaires pour configurer un fichier ou une LUN réservé à l'espace dans un volume à l'aide du provisionnement Thick :

| Réglage du volume                       | Valeur                                                                                               |
|-----------------------------------------|------------------------------------------------------------------------------------------------------|
| Résultats garantis                      | Volumétrie                                                                                           |
| Réserve fractionnaire                   | 100                                                                                                  |
| Réserve Snapshot                        | Toutes                                                                                               |
| Suppression automatique de l'instantané | Facultatif                                                                                           |
| Croissance automatique                  | Facultatif. Si cette option est activée, l'espace libre de l'agrégat doit être activement surveillé. |

| Paramètre fichier ou LUN | Valeur |
|--------------------------|--------|
| Réservation d'espace     | Activé |

#### Informations associées

- ["Présentation des combinaisons de configuration de volumes et fichiers ou LUN recommandées"](#)

#### Paramètres pour les fichiers non réservés à espace ou les LUN avec des volumes à provisionnement fin

Cette combinaison de configuration de volumes et de fichiers FlexVol ou de LUN requiert la réduction de la quantité de stockage allouée à l'avance, mais elle exige une gestion de l'espace libre actif pour éviter les erreurs liées au manque d'espace.

Les paramètres suivants sont requis pour configurer un LUN ou des fichiers non réservés en espace dans un volume à provisionnement fin :

| Réglage du volume                       | Valeur     |
|-----------------------------------------|------------|
| Résultats garantis                      | Aucune     |
| Réserve fractionnaire                   | 0          |
| Réserve Snapshot                        | Toutes     |
| Suppression automatique de l'instantané | Facultatif |
| Croissance automatique                  | Facultatif |

| Paramètre fichier ou LUN | Valeur    |
|--------------------------|-----------|
| Réservation d'espace     | Désactivé |

#### Autres considérations

Lorsque l'espace est insuffisant pour le volume ou l'agrégat, les opérations d'écriture sur le fichier ou la LUN peuvent échouer.

Pour ne pas contrôler activement l'espace disponible pour le volume et l'agrégat, vous devez activer la croissance automatique du volume et définir la taille maximale du volume sur la taille de l'agrégat. Dans cette configuration, vous devez surveiller activement l'espace libre des agrégats, mais il n'est pas nécessaire de surveiller l'espace libre dans le volume.

#### Paramètres de configuration pour les fichiers réservés en espace ou les LUN avec provisionnement de volumes semi-lourds

Vous pouvez utiliser plusieurs combinaisons de configuration de FlexVol volume et de configurations de fichiers ou de LUN. Cette combinaison basée sur un provisionnement de volumes semi-épais requiert moins de stockage à allouer en amont que la



combinaison entièrement provisionnée. Mais cela impose des restrictions sur les technologies d'efficacité que vous pouvez utiliser pour le volume. Les écrasements sont effectués par le meilleur effort pour cette combinaison de configuration.

Les paramètres suivants sont nécessaires pour configurer une LUN Space-Reserved dans un volume à l'aide du provisionnement semi-thick :

| Réglage du volume                       | Valeur                                                                                                                                                                                                                                            |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Résultats garantis                      | Volumétrie                                                                                                                                                                                                                                        |
| Réserve fractionnaire                   | 0                                                                                                                                                                                                                                                 |
| Réserve Snapshot                        | 0                                                                                                                                                                                                                                                 |
| Suppression automatique de l'instantané | On, avec un niveau d'engagement de destruction, une liste de destruction qui inclut tous les objets, le déclencheur défini sur volume, ainsi que toutes les LUN FlexClone et tous les fichiers FlexClone activés pour la suppression automatique. |
| Croissance automatique                  | Facultatif. Si cette option est activée, l'espace libre de l'agrégat doit être activement surveillé.                                                                                                                                              |

| Paramètre fichier ou LUN | Valeur |
|--------------------------|--------|
| Réservation d'espace     | Activé |

### Restrictions technologiques

Pour cette combinaison de configuration, vous ne pouvez pas utiliser les technologies suivantes d'efficacité du stockage de volumes :

- Compression
- Déduplication
- ODX et allègement de la charge des copies FlexClone
- LUN FlexClone et fichiers FlexClone non marqués pour la suppression automatique (clones actifs)
- Sous-fichiers FlexClone
- ODX/allègement de la charge des copies

### Autres considérations

Lors de l'utilisation de cette combinaison de configuration, vous devez tenir compte des éléments suivants :

- Lorsque le volume prenant en charge cette LUN fonctionne peu d'espace, les données de protection (LUN et fichiers FlexClone, copies Snapshot) sont détruites.
- Les opérations d'écriture peuvent entraîner un temps d'attente et l'échec lorsque l'espace disponible est insuffisant.

Par défaut, la compression est activée pour les plateformes AFF. Vous devez désactiver explicitement la compression pour tout volume pour lequel vous souhaitez utiliser un provisionnement semi-lourd sur une plateforme AFF.

#### Informations associées

- ["Présentation des combinaisons de configuration de volumes et fichiers ou LUN recommandées"](#)

## Précautions et considérations relatives à la modification de la capacité des fichiers et des répertoires

### Nombre maximal de fichiers autorisé pour les volumes FlexVol

Les volumes FlexVol comportent un nombre maximal de fichiers qu'ils peuvent contenir. Vous pouvez modifier ce maximum, mais avant de le faire, vous devez comprendre comment ce changement affecte le volume.

Si vos données requièrent un grand nombre de fichiers ou de répertoires très volumineux, vous pouvez étendre la capacité des fichiers ou des répertoires ONTAP. Cependant, vous devez connaître les limites et les restrictions qui s'appliquent avant de continuer.

Le nombre de fichiers qu'un volume peut contenir est déterminé par le nombre d'inodes qu'il possède. Un *inode* est une structure de données qui contient des informations sur les fichiers. Les volumes ont des inodes privés et publics. Les inodes publics sont utilisés pour les fichiers visibles par l'utilisateur ; les inodes privés sont utilisés pour les fichiers utilisés en interne par ONTAP. Vous pouvez modifier uniquement le nombre maximal d'inodes publics pour un volume. Vous ne pouvez pas affecter le nombre d'inodes privés.

ONTAP définit automatiquement le nombre maximal d'inodes publics pour un volume récemment créé, d'après la taille du volume : 1 inode pour 1 32 Ko de taille de volume. Lorsque la taille d'un volume augmente, soit directement par un administrateur, soit automatiquement par ONTAP via la fonctionnalité de taille automatique, ONTAP augmente également (si nécessaire) le nombre maximal d'inodes publics de façon à ce qu'il y ait au moins 1 inode par taille de volume de 32 Ko, Jusqu'à ce que le volume atteigne environ 680 Go.

Dans les versions de ONTAP antérieures à 9.13.1, l'augmentation de la taille du volume supérieure à 680 Go n'entraîne pas automatiquement plus d'inodes, car ONTAP ne crée pas automatiquement plus de 22,369,621 inodes. Si vous avez besoin de plus de fichiers que le nombre par défaut pour un volume de taille quelconque, vous pouvez utiliser la commande `volume modify` pour augmenter le nombre maximal d'inodes pour le volume.

À partir de ONTAP 9.13.1, le nombre maximal d'inodes continue d'augmenter, il y a donc une inode par 32 Ko d'espace de volume, même si le volume est supérieur à 680 Go. Cette croissance se poursuit jusqu'à ce que le volume atteigne le maximum de l'inode de 2,147,483,632.

Vous pouvez également réduire le nombre maximal d'inodes publics. La diminution du nombre d'inodes publiques modifie *non* la quantité d'espace allouée aux inodes, mais réduit la quantité maximale d'espace que le fichier d'inodes public peut consommer. Une fois l'espace alloué aux inodes, il n'est jamais restitué au volume. Par conséquent, la diminution du nombre maximal d'inodes en dessous du nombre d'inodes actuellement alloués ne renvoie pas l'espace utilisé par les inodes alloués.

#### Plus d'informations

- [Déterminez l'utilisation des fichiers et des inodes pour un volume](#)

### Taille maximale du répertoire pour les volumes FlexVol

Pour augmenter la taille maximale par défaut d'un volume FlexVol spécifique, utilisez le

-maxdir-size de la volume modify la commande, mais cela pourrait avoir un impact sur les performances du système. Consultez l'article de la base de connaissances ["Qu'est-ce que maxdirsize ?"](#).

Pour en savoir plus sur les tailles de répertoire maximales dépendantes du modèle des volumes FlexVol, rendez-vous sur le ["NetApp Hardware Universe"](#).

### Restrictions applicables aux volumes root et aux agrégats root

Vous devez connaître les restrictions qui régissent le volume racine et l'agrégat racine d'un nœud.



Le volume racine d'un nœud contient des répertoires et des fichiers spéciaux pour le nœud. Le volume root est contenu dans l'agrégat root.

Le volume racine d'un nœud est un volume FlexVol installé en usine ou par le logiciel d'installation. Il est réservé aux fichiers système, aux fichiers journaux et aux fichiers core. Le nom du répertoire est `/mroot`, qui n'est accessible que via le systemshell par le support technique. La taille minimale du volume racine d'un nœud dépend du modèle de plateforme.

- Les règles suivantes régissent le volume racine du nœud :
  - À moins d'en recevoir l'instruction du support technique, ne modifiez pas la configuration ou le contenu du volume racine.
  - Ne stockez pas les données utilisateur sur le volume racine.

Le stockage des données utilisateur dans le volume racine augmente le temps de rétablissement du stockage entre les nœuds d'une paire haute disponibilité.

- Vous pouvez déplacer le volume root vers un autre agrégat.

#### ["Transfert des volumes racines vers de nouveaux agrégats"](#)

- L'agrégat root est dédié uniquement au volume root du nœud.

ONTAP vous empêche de créer d'autres volumes dans l'agrégat racine.

["NetApp Hardware Universe"](#)

### Transfert d'un volume racine vers de nouveaux agrégats

La procédure de remplacement racine migre l'agrégat racine actuel vers un autre jeu de disques sans interruption. Vous devrez peut-être effectuer cette opération dans le cadre d'un processus de remplacement de disque ou de maintenance préventive.

#### Description de la tâche

Vous pouvez modifier l'emplacement du volume root vers un nouvel agrégat dans les scénarios suivants :

- Lorsque les agrégats racines ne sont pas sur le disque de votre choix
- Lorsque vous souhaitez réorganiser les disques connectés au nœud
- Lorsque vous effectuez un remplacement des tiroirs disques EOS

## Étapes

### 1. Transférer l'agrégat racine :

```
system node migrate-root -node node_name -disklist disk_list -raid-type
raid_type
```

- **-noeud**

Spécifie le nœud qui possède l'agrégat racine que vous souhaitez migrer.

- **-disklist**

Spécifie la liste des disques sur lesquels le nouvel agrégat racine sera créé. Tous les disques doivent être des disques de secours et appartenir au même nœud. Le nombre minimum de disques requis dépend du type RAID.

- **-raid-type**

Spécifie le type RAID de l'agrégat racine. La valeur par défaut est `raid-dp`. Il s'agit du seul type pris en charge en mode avancé.

### 2. Surveiller la progression de la tâche :

```
job show -id jobid -instance
```

## Résultats

Si toutes les vérifications préalables ont réussi, la commande démarre un travail de remplacement de volume racine et se ferme.

## Fonctionnalités prises en charge par FlexClone Files et les LUN FlexClone

### Fonctionnalités prises en charge par FlexClone Files et les LUN FlexClone

Les fichiers FlexClone et les LUN FlexClone fonctionnent avec différentes fonctionnalités ONTAP, telles que la déduplication, les copies Snapshot, les quotas et SnapMirror volume.

Les fonctionnalités suivantes sont prises en charge par FlexClone Files et les LUN FlexClone :

- Déduplication
- Copies Snapshot
- Listes de contrôle d'accès
- Quotas
- Volumes FlexClone
- NDMP
- SnapMirror volume
- Le `volume move` commande
- Réservation d'espace

- Configuration DE L'INFRASTRUCTURE HA

## Déduplication avec FlexClone Files et les LUN FlexClone

Vous pouvez efficacement utiliser l'espace de stockage physique des blocs de données en créant un fichier FlexClone ou une LUN FlexClone du fichier parent et de la LUN parent dans un volume activé pour la déduplication.

Le mécanisme de partage des blocs utilisé par les fichiers et les LUN FlexClone est également utilisé par la déduplication. Vous pouvez optimiser les économies d'espace réalisées sur un volume FlexVol en activant la déduplication sur le volume, puis en clonant le volume pour lequel la déduplication a été activée.



Lors de l'exécution du `sis undo` Sur un volume activé pour la déduplication, vous ne pouvez pas créer les fichiers FlexClone et les LUN FlexClone des fichiers parent et des LUN parent qui résident sur ce volume.

## Fonctionnement des copies Snapshot avec les fichiers FlexClone et les LUN FlexClone

Il existe une synergie entre les copies Snapshot et les fichiers FlexClone et les LUN FlexClone. Si vous travaillez avec ces technologies, vous devez être conscient de ce qui est possible ainsi que des restrictions pertinentes.

### Création de fichiers FlexClone et de LUN

Vous pouvez créer un fichier FlexClone ou une LUN FlexClone à partir d'une copie Snapshot existante. La copie repose sur les fichiers parents et les LUN parents contenus dans une FlexVol volume.

### Supprimer une copie Snapshot

Vous ne pouvez pas supprimer manuellement une copie Snapshot à partir de laquelle des fichiers FlexClone ou des LUN FlexClone sont en cours de création. La copie Snapshot reste verrouillée jusqu'à la fin du processus de partage des blocs en arrière-plan. Si vous essayez de supprimer une copie Snapshot verrouillée, le système affiche un message vous demandant de réessayer l'opération après un certain temps. Dans ce cas, vous devez continuer à essayer de nouveau l'opération de suppression. Vous pourrez supprimer la copie Snapshot une fois le partage de blocs terminé.

## Héritage des listes de contrôle d'accès par fichiers FlexClone et LUN FlexClone

Les fichiers FlexClone et les LUN FlexClone héritent des listes de contrôle d'accès de leurs fichiers et LUN parents.

Si les fichiers parents contiennent des flux Windows NT, les fichiers FlexClone héritent également des informations du flux. Cependant, les fichiers parents contenant plus de six flux ne peuvent pas être clonés.

## Fonctionnement des quotas avec les fichiers FlexClone et les LUN FlexClone

Vous devez connaître le fonctionnement des quotas avec les fichiers FlexClone et les LUN FlexClone avant de les utiliser.

Des limites de quota sont appliquées à la taille logique totale des fichiers FlexClone ou des LUN FlexClone. Les opérations de clonage n'échouent pas, même si le partage de blocs est dépassé.

Lorsque vous créez un fichier FlexClone ou une LUN FlexClone, les quotas ne reconnaissent pas les

économies d'espace. Par exemple, si vous créez un fichier FlexClone d'un fichier parent de 10 Go, vous n'utilisez que 10 Go d'espace physique, mais l'utilisation du quota est enregistrée à 20 Go (10 Go pour le fichier parent et 10 Go pour le fichier FlexClone).

Si la création d'un fichier FlexClone ou d'une LUN entraîne le dépassement du quota de groupe ou d'utilisateur, l'opération de clonage réussit à condition que le volume FlexVol dispose de suffisamment d'espace pour contenir les métadonnées du clone. Cependant, le quota pour cet utilisateur ou ce groupe est sursouscrit.

### **Volumes FlexClone, fichiers FlexClone et LUN FlexClone associés**

Vous pouvez créer un volume FlexClone d'un volume FlexVol doté d'un fichier FlexClone et d'un LUN FlexClone et de son fichier parent ou d'une LUN.

Les fichiers FlexClone ou les LUN FlexClone ainsi que les fichiers ou LUN parents présents dans le volume FlexClone continuent de partager les blocs de la même manière que dans le volume FlexVol parent. En fait, les entités FlexClone et leurs parents partagent les mêmes blocs de données physiques sous-jacents, ce qui minimise l'utilisation de l'espace disque physique.

Si le volume FlexClone est séparé de son volume parent, les fichiers FlexClone ou les LUN FlexClone et leurs fichiers parent ou LUN cessent de partager les blocs dans le clone du volume FlexClone. Elles existent ensuite en tant que fichiers ou LUN indépendants. Le clone du volume utilise donc plus d'espace qu'avant l'opération de fractionnement.

### **Fonctionnement de NDMP avec les fichiers FlexClone et les LUN FlexClone**

NDMP fonctionne au niveau logique avec des fichiers FlexClone et des LUN FlexClone. Tous les fichiers ou LUN FlexClone sont sauvegardés en tant que fichiers ou LUN distincts.

Lorsque vous utilisez les services NDMP pour sauvegarder un qtree ou un volume FlexVol contenant des fichiers FlexClone ou des LUN FlexClone, le partage de blocs entre les entités parent et clone n'est pas préservé, et les entités clonées sont sauvegardées sur bande en tant que fichiers ou LUN distincts. Le gain de place est perdu. Par conséquent, la bande sur laquelle vous effectuez la sauvegarde doit disposer d'un espace suffisant pour stocker la quantité de données étendue. Lors de la restauration, tous les fichiers FlexClone et les LUN FlexClone sont restaurés en tant que fichiers physiques et LUN distincts. Vous pouvez activer la déduplication sur le volume pour restaurer les avantages du partage de blocs.



Lorsque des fichiers FlexClone et des LUN FlexClone sont créés à partir d'une copie Snapshot existante d'un volume FlexVol, il est impossible de sauvegarder le volume sur bande jusqu'à ce que le processus de partage des blocs, qui se déroule en arrière-plan, soit terminé. Si vous utilisez NDMP sur le volume lorsque le processus de partage de blocs est en cours, le système affiche un message vous invitant à réessayer l'opération après un certain temps. Dans ce cas, vous devez continuer à essayer de nouveau l'opération de sauvegarde sur bande pour qu'elle réussisse une fois le partage de bloc terminé.

### **Fonctionnement de SnapMirror volume avec les fichiers FlexClone et les LUN FlexClone**

L'utilisation de SnapMirror de volume avec des fichiers FlexClone et des LUN FlexClone contribue à conserver les économies d'espace, car les entités clonées sont répliquées une seule fois.

Si un volume FlexVol est une source SnapMirror volume et contient des fichiers FlexClone ou des LUN FlexClone, SnapMirror volume transfère uniquement le bloc physique partagé et une petite quantité de métadonnées vers le système de destination SnapMirror volume. La destination ne stocke qu'une seule copie du bloc physique, et ce bloc est partagé entre les entités parent et clonée. Par conséquent, le volume de destination est une copie exacte du volume source et tous les fichiers ou LUN clones du volume de destination partagent le même bloc physique.

### **Fonctionnement de la réservation d'espace avec les fichiers FlexClone et les LUN FlexClone**

Lorsque vous utilisez des fichiers FlexClone et des LUN FlexClone, vous devez comprendre le fonctionnement de l'attribut de réservation d'espace.

Par défaut, les fichiers FlexClone et les LUN héritent respectivement de l'attribut de réservation d'espace du fichier parent et de la LUN parent. Toutefois, vous pouvez créer des fichiers FlexClone et des LUN FlexClone avec la réservation d'espace désactivée si la FlexVol volume manque d'espace. Ceci est possible même si l'attribut dans le parent respectif est activé.

Notez que si la FlexVol volume ne contient pas assez d'espace pour créer un fichier FlexClone ou une LUN FlexClone avec la même réservation d'espace que celle du parent, l'opération de clonage échoue.

### **Fonctionnement d'une configuration haute disponibilité avec les fichiers FlexClone et les LUN FlexClone**

Les opérations liées aux fichiers FlexClone et aux LUN FlexClone sont prises en charge dans une configuration haute disponibilité.

Dans une paire haute disponibilité, vous ne pouvez pas créer de fichiers FlexClone ou de LUN FlexClone sur le partenaire pendant l'opération de basculement ou de rétablissement. Toutes les opérations de partage de blocs en attente du partenaire sont reprises après la fin de l'opération de basculement ou de rétablissement.

## **Provisionnez le stockage NAS pour les systèmes de fichiers volumineux à l'aide de FlexGroup volumes**

Un volume FlexGroup est un conteneur NAS évolutif qui fournit des performances élevées et une distribution automatique de la charge. Les volumes FlexGroup offrent une capacité massive (en pétaoctets) qui dépasse considérablement les limites du volume FlexVol, sans surcharge administrative.

Les rubriques de cette section expliquent comment gérer les volumes FlexGroup avec System Manager dans ONTAP 9.7 et les versions ultérieures. Si vous utilisez System Manager classique (disponible uniquement dans ONTAP 9.7 et versions antérieures), reportez-vous à la rubrique suivante :

- ["Créer des volumes FlexGroup"](#)

Depuis la version ONTAP 9.9.1, les relations « fan out » de SnapMirror de deux volumes FlexGroup ou plus sont prises en charge avec un maximum de huit pieds en mode « fan out ». System Manager ne prend pas en charge les relations de volume FlexGroup en cascade SnapMirror.

ONTAP sélectionne automatiquement les niveaux locaux nécessaires à la création du volume FlexGroup.

Depuis ONTAP 9.8, lorsque vous provisionnez le stockage, la QoS est activée par défaut. Vous pouvez désactiver QoS ou choisir une règle de QoS personnalisée lors du processus de provisionnement ou

ultérieurement.

### Étapes

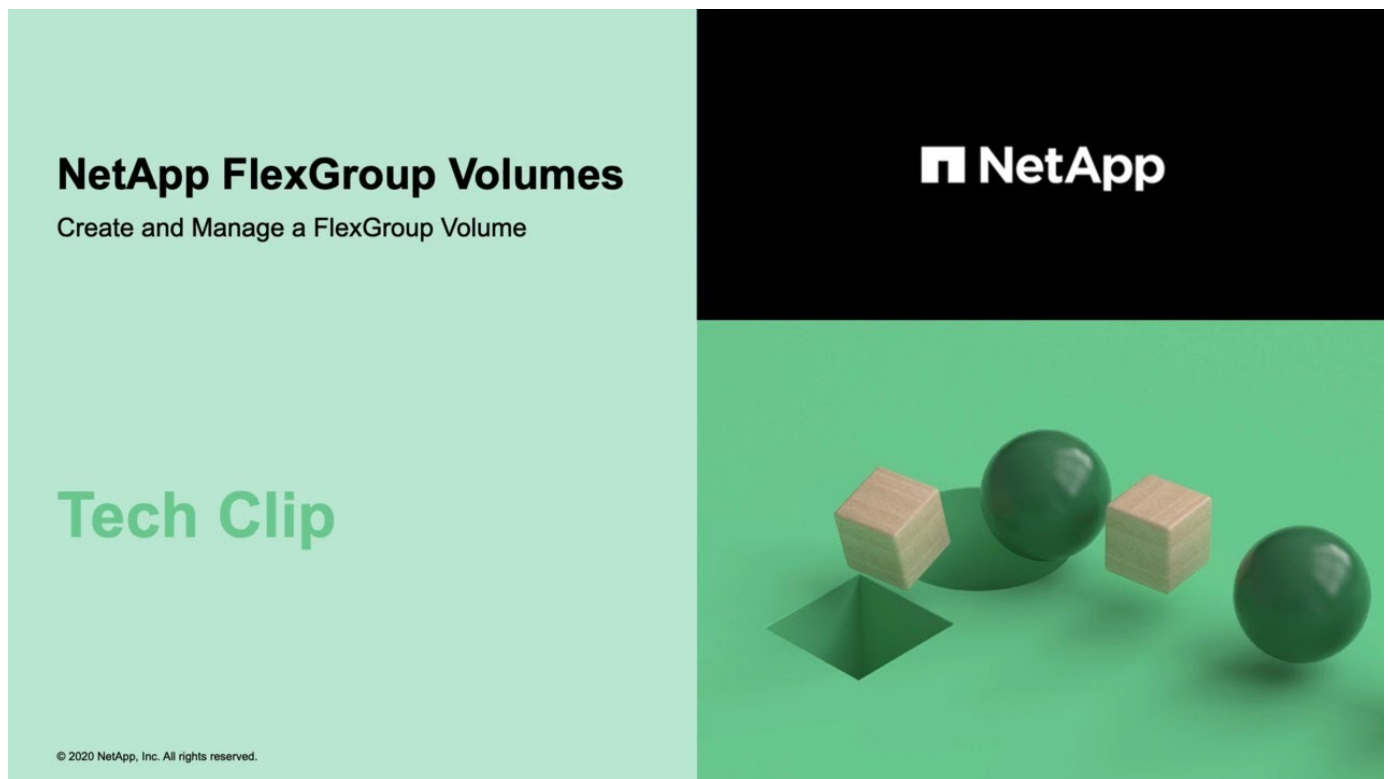
1. Cliquez sur **Storage > volumes**.
2. Cliquez sur **Ajouter**.
3. Cliquez sur **plus d'options**, puis sélectionnez **distribuer les données de volume à travers le cluster**.



Si vous exécutez ONTAP 9.8 ou une version ultérieure et que vous souhaitez désactiver QoS ou choisir une stratégie QoS personnalisée, cliquez sur **plus d'options**, puis sous **stockage et optimisation**, sélectionnez **niveau de service de performances**.

### Vidéos

Créez et gérez un volume FlexGroup



Volumes FlexGroup : faire plus avec moins

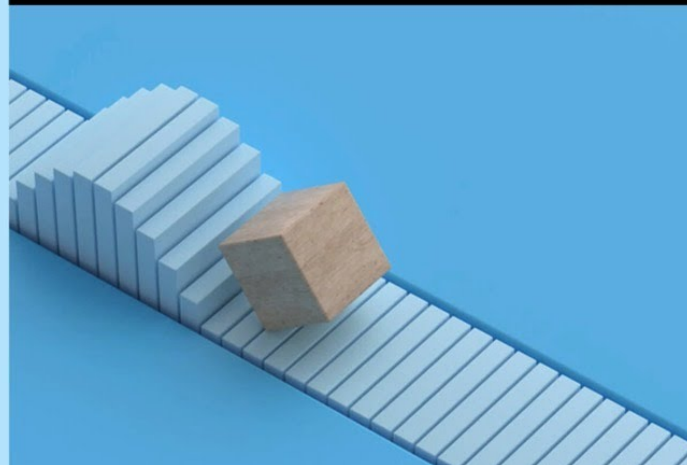


# NetApp FlexGroup Volumes

Do More with Less

## Use Case

© 2020 NetApp, Inc. All rights reserved.



## Gestion des volumes FlexGroup via l'interface de ligne de commandes

### Présentation de la gestion des volumes FlexGroup avec l'interface de ligne de commandes

Vous pouvez configurer, gérer et protéger les volumes FlexGroup pour garantir l'évolutivité et les performances. Les volumes FlexGroup sont des volumes scale-out qui fournissent des performances élevées et une répartition automatique de la charge.

Vous pouvez configurer des volumes FlexGroup si les conditions suivantes sont vraies :

- Vous exécutez ONTAP 9.1 ou une version ultérieure.
- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.
- Vous disposez des privilèges d'administrateur de cluster et non des privilèges d'administrateur de SVM.



Depuis ONTAP 9.5, FlexGroups remplace Infinite volumes, qui ne sont pas pris en charge dans ONTAP 9.5 ou versions ultérieures.

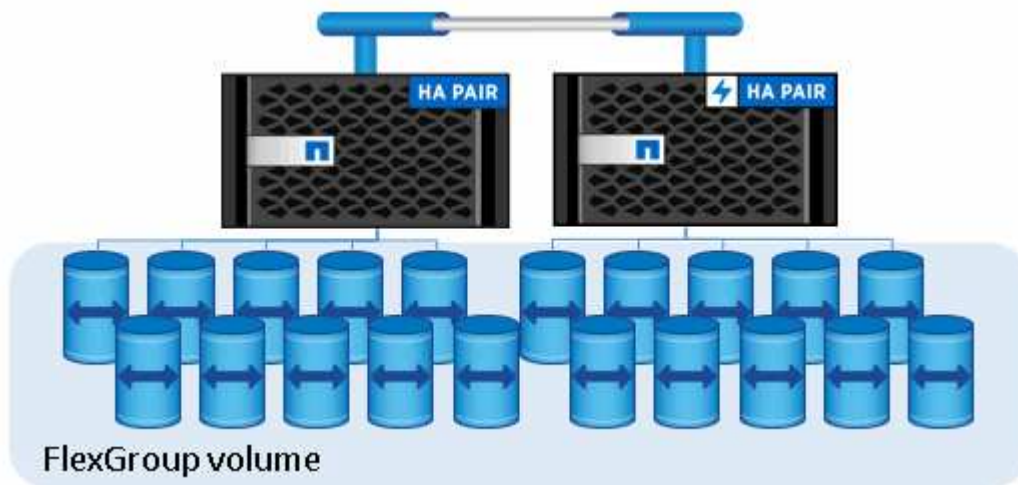
Voir la ["Configurations prises en charge et non prises en charge pour les volumes FlexGroup"](#) pour en savoir plus.

### Informations associées

Les informations conceptuelles sur les volumes FlexVol sont applicables aux volumes FlexGroup. Pour plus d'informations sur les volumes FlexVol et la technologie ONTAP, consultez la bibliothèque de référence ONTAP et les rapports techniques (TR).

## Qu'est-ce qu'un volume FlexGroup

Un volume FlexGroup est un conteneur NAS scale-out qui offre de hautes performances, une évolutivité et une distribution automatique de la charge. Un volume FlexGroup contient plusieurs composants qui partagent le trafic de manière automatique et transparente. *Comments* sont les volumes FlexVol sous-jacents qui composent un volume FlexGroup.



Les volumes FlexGroup offrent les avantages suivants :

- Haute évolutivité

La taille maximale d'un volume FlexGroup dans ONTAP 9.1 et les versions ultérieures est de 20 po, avec 400 milliards de fichiers sur un cluster à 10 nœuds.

- Hautes performances

Les volumes FlexGroup peuvent utiliser les ressources du cluster pour gérer les charges de travail qui bénéficient d'un débit élevé et d'une faible latence.

- Une gestion simplifiée

Un volume FlexGroup est un conteneur d'espace de noms unique qui peut être géré de la même manière que les volumes FlexVol.

## Configurations prises en charge et non prises en charge pour les volumes FlexGroup

Notez les fonctionnalités de ONTAP prises en charge par les volumes FlexGroup dans ONTAP 9.

### Fonctions prises en charge à partir de ONTAP 9.14.1

- Balisage des copies Snapshot : prise en charge de la création, de la modification et de la suppression de balises de copie Snapshot (libellés et commentaires SnapMirror) pour les copies Snapshot sur des volumes FlexGroup à l'aide du `volume snapshot` commande.

## Fonctions prises en charge à partir de ONTAP 9.13.1

- Protection anti-ransomware autonome (ARP) pour les volumes FlexGroup, incluant les fonctionnalités prises en charge suivantes :
  - FlexGroup étend les opérations : un nouveau composant hérite des attributs de protection anti-ransomware autonome.
  - Conversions FlexVol en FlexGroup : les conversions de FlexVols avec la protection anti-ransomware autonome active sont possibles.
  - Rééquilibrage de FlexGroup : la protection anti-ransomware autonome est prise en charge lors des opérations de rééquilibrage fluide et sans interruption.
- Planifiez une seule opération de rééquilibrage des FlexGroup.
- SnapMirror fanout relations avec SVM DR sur volumes FlexGroup. Prend en charge la ventilation jusqu'à huit sites.

## Fonctionnalités prises en charge à partir d'ONTAP 9.12.1

- Rééquilibrage FlexGroup
- SnapLock pour SnapVault
- FabricPool, FlexGroup et SVM DR fonctionnent ensemble. (Dans les versions antérieures à ONTAP 9.12.1, deux de ces fonctionnalités fonctionnaient ensemble, mais pas les trois en même temps.)
- Taille du composant de volume FlexGroup jusqu'à 300 To maximum sur les plateformes AFF et FAS avec ONTAP 9.12.1 P2 et versions ultérieures.

## Fonctionnalités prises en charge à partir d'ONTAP 9.11.1

- Volumes SnapLock

SnapLock ne prend pas en charge les fonctionnalités suivantes avec les volumes FlexGroup :

- Obligation légale
- Conservation basée sur les événements
- SnapLock pour SnapVault

Vous configurez SnapLock au niveau de FlexGroup. Vous ne pouvez pas configurer SnapLock au niveau du composant.

### [Qu'est-ce que SnapLock](#)

- Suppression du répertoire asynchrone du client

[Gérer les droits des clients pour supprimer rapidement des répertoires](#)

## Fonctionnalités prises en charge à partir d'ONTAP 9.10.1

- Conversion de volumes FlexVol en volumes FlexGroup au sein d'une source SVM-DR

[Conversion d'un volume FlexVol en volume FlexGroup au sein d'une relation SVM-DR](#)

- Prise en charge de FlexClone pour la reprise après incident des SVM pour les volumes FlexGroup

[En savoir plus sur la création de volumes FlexClone.](#)

### Fonctionnalités prises en charge à partir d'ONTAP 9.9.1

- Reprise d'activité de SVM

Le clonage d'un volume FlexGroup faisant partie d'une relation SVM-DR n'est pas pris en charge.

- SnapMirror gère 2 relations ou plus (A à B, A à C), avec un maximum de 8 pieds en éventail.

[Considérations relatives à la création de relations SnapMirror en cascade et avec fanout pour FlexGroups](#)

- Relations SnapMirror en cascade (de A à B à C) jusqu'à deux niveaux

[Considérations relatives à la création de relations SnapMirror en cascade et avec fanout pour FlexGroups](#)

### Fonctionnalités prises en charge à partir d'ONTAP 9.8

- Restauration d'un seul fichier à partir d'un coffre-fort FlexGroup SnapMirror ou d'une destination UDP
  - La restauration peut être d'un volume FlexGroup de n'importe quelle géométrie vers un volume FlexGroup de n'importe quelle géométrie
  - Un seul fichier par opération de restauration est pris en charge

- La conversion des volumes a été effectuée à partir de systèmes 7-mode vers des volumes FlexGroup

Pour plus d'informations, consultez l'article de la base de connaissances ["Comment convertir un FlexVol converti en FlexGroup"](#).

- NFSv4.2
- Suppression asynchrone de fichiers et de répertoires
- Analyse du système de fichiers (FSA)
- FlexGroup en tant que datastore VMware vSphere
- Prise en charge supplémentaire de la sauvegarde sur bande et de la restauration via NDMP, notamment :
  - Extension de sauvegarde redémarrable NDMP (RBE) et extension de gestion Snapshot (SSME)
  - Les variables d'environnement EXCLUDE et MULTI\_SUBTREE\_NAMES prennent en charge les sauvegardes FlexGroup
  - Introduction de la variable d'environnement IGNORE\_CTIME\_MTIME pour les sauvegardes FlexGroup
  - Restauration de fichiers individuels dans un FlexGroup à l'aide du message NDMP\_SNAP\_RECOVER, qui fait partie de l'extension 0x2050  
Les sessions de vidage et de restauration sont abandonnées au cours d'une mise à niveau ou d'une restauration.

### Fonctions prises en charge à partir de ONTAP 9.7

- Volume FlexClone
- NFSv4 et NFSv4.1
- PNFS
- Sauvegarde sur bande et restauration à l'aide de NDMP

Pour la prise en charge de NDMP sur les volumes FlexGroup, vous devez connaître les points suivants :

- Le message NDMP\_SNAP\_RECOVER de la classe d'extension 0x2050 ne peut être utilisé que pour restaurer un volume FlexGroup entier.

Les fichiers individuels d'un volume FlexGroup ne peuvent pas être restaurés.

- L'extension de sauvegarde NDMP redémarrable (RBE) n'est pas prise en charge pour les volumes FlexGroup.
- Les variables d'environnement EXCLUDE et MULTI\_SUBTREE\_NAMES ne sont pas prises en charge pour les volumes FlexGroup.
- Le `ndmpcopy` La commande est prise en charge pour le transfert de données entre les volumes FlexVol et FlexGroup.

Si vous restaurez Data ONTAP 9.7 vers une version antérieure, les informations de transfert incrémentiel des transferts précédents ne sont pas conservées. Par conséquent, vous devez effectuer une copie de base après le rétablissement.

- VMware vStorage APIs for Array Integration (VAAI)
- Conversion d'un volume FlexVol en volume FlexGroup
- Volumes FlexGroup en tant que volumes d'origine FlexCache

### Fonctions prises en charge à partir de ONTAP 9.6

- Partages SMB disponibles en permanence
- Configurations MetroCluster
- Modification du nom d'un volume FlexGroup (`volume rename` commande)
- Réduction ou réduction de la taille d'un volume FlexGroup (`volume size` commande)
- Dimensionnement élastique
- Chiffrement d'agrégat NetApp (NAE)
- Cloud Volumes ONTAP

### Fonctions prises en charge à partir de ONTAP 9.5

- Allègement de la charge des copies (ODX)
- Protection d'accès au niveau du stockage
- Améliorations apportées aux notifications de modification pour les partages SMB

Des notifications de modification sont envoyées pour les modifications apportées au répertoire parent sur lequel l'`changenotify` la propriété est définie et pour les modifications apportées à tous les sous-répertoires de ce répertoire parent.

- FabricPool
- Application des quotas
- Statistiques `qtree`
- QoS adaptative pour les fichiers dans les volumes FlexGroup
- FlexCache (cache uniquement ; FlexGroup en tant qu'origine pris en charge dans ONTAP 9.7)

## Fonctions prises en charge à partir de ONTAP 9.4

- FPolicy
- Audit de fichiers
- Débit au sol (QoS min) et QoS adaptative pour les volumes FlexGroup
- Débit maximal (QoS Max) et débit au sol (QoS min) pour les fichiers dans les volumes FlexGroup

Vous utilisez le `volume file modify` Commande pour gérer la « QoS policy group » associée à un fichier.

- Limites SnapMirror détendues
- Multicanal SMB 3.x

## Fonctions prises en charge à partir de ONTAP 9.3

- Configuration antivirus
- Notifications de modification pour les partages SMB

Les notifications sont envoyées uniquement pour les modifications apportées au répertoire parent sur lequel l' `changenotify` la propriété est définie. Les notifications de modification ne sont pas envoyées pour les modifications apportées aux sous-répertoires du répertoire parent.

- Qtrees
- Plafond de débit (QoS max)
- Étendre le volume FlexGroup source et le volume FlexGroup de destination dans une relation SnapMirror
- La sauvegarde et la restauration de SnapVault
- Relations unifiées de protection des données
- Option croissance automatique et option Autohrink
- Le nombre d'inodes a été prévu pour l'ingestion

## Fonctionnalité prise en charge depuis ONTAP 9.2

- Chiffrement de volume
- Déduplication à la volée dans l'agrégat (déduplication entre plusieurs volumes)
- Chiffrement de volume NetApp (NVE)

## Fonctions prises en charge à partir de ONTAP 9.1

Les volumes FlexGroup ont été introduits avec la prise en charge de plusieurs fonctionnalités d'ONTAP dans ONTAP 9.1.

- Technologie SnapMirror
- Copies Snapshot
- Active IQ
- Compression adaptative à la volée
- Déduplication à la volée

- Compaction des données à la volée
- AFF
- Création de rapports sur les quotas
- Technologie Snapshot de NetApp
- Logiciel SnapRestore (niveau FlexGroup)
- Agrégats hybrides
- Déplacement du volume du composant ou du membre
- Déduplication post-traitement
- Technologie NetApp RAID-TEC
- Point de cohérence par agrégat
- Partage d'FlexGroup avec un volume FlexVol sur le même SVM

### Configurations non prises en charge dans ONTAP 9

| Protocoles non pris en charge                                                                                                                                         | Fonctionnalités de protection des données non prises en charge                                                                                                                                                                                                                         | Autres fonctionnalités ONTAP non prises en charge                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• PNFS (ONTAP 9.0 à 9.6)</li> <li>• SMB 1.0</li> <li>• Basculement transparent SMB (ONTAP 9.0 à 9.5)</li> <li>• SAN</li> </ul> | <ul style="list-style-type: none"> <li>• Volumes SnapLock (ONTAP 9.10.1 et versions antérieures)</li> <li>• SMTape</li> <li>• SnapMirror synchrone</li> <li>• Reprise après incident SVM avec volumes FlexGroup contenant FabricPool (ONTAP 9.11.1 et versions antérieures)</li> </ul> | <ul style="list-style-type: none"> <li>• Service VSS (Remote Volume Shadow Copy Service)</li> <li>• Mobilité des données des SVM</li> </ul> |

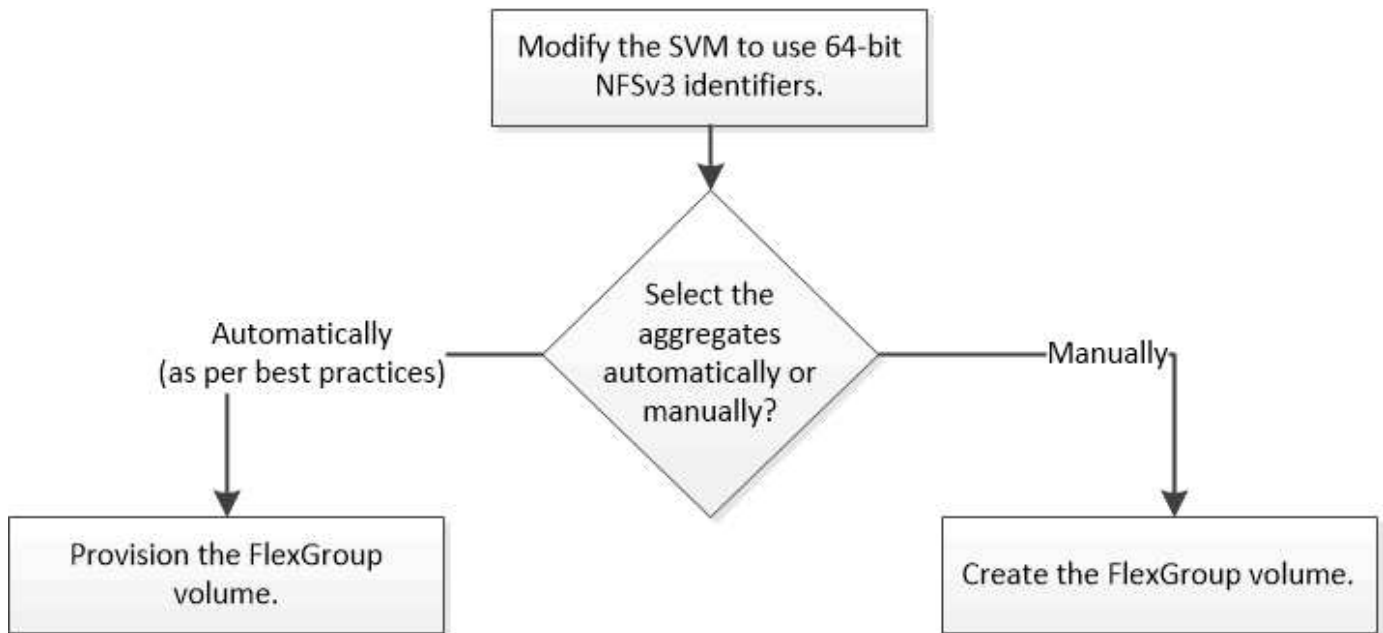
### Informations associées

["Centre de documentation ONTAP 9"](#)

## Configuration de volumes FlexGroup

### Workflow de configuration de volumes FlexGroup

Vous pouvez provisionner un volume FlexGroup où ONTAP sélectionne automatiquement les agrégats selon les meilleures pratiques pour des performances optimales, ou créer un volume FlexGroup en sélectionnant manuellement les agrégats et en le configurant pour un accès aux données.



### Ce dont vous avez besoin

On doit avoir créé le SVM avec NFS et SMB ajouté à la liste des protocoles autorisés pour la SVM.

### Description de la tâche

Le provisionnement automatique d'un volume FlexGroup n'est possible que sur les clusters dont quatre nœuds ou moins. Dans les clusters de plus de quatre nœuds, vous devez créer un volume FlexGroup manuellement.

### Activer les identifiants NFSv3 64 bits sur un SVM

Pour prendre en charge le nombre élevé de fichiers de volumes FlexGroup et éviter les collisions avec des ID de fichiers, il est recommandé d'activer des identifiants de fichiers 64 bits sur la SVM sur laquelle le volume FlexGroup doit être créé.

### Étapes

1. Connectez-vous au niveau de privilège avancé : `set -privilege advanced`
2. Modifier le SVM pour utiliser les FSID NFSv3 64 bits et les ID de fichiers : `vserver nfs modify -vserver svm_name -v3-64bit-identifiers enabled`



```
cluster1::*> vserver nfs modify -vserver vs0 -v3-64bit-identifiers
enabled

Warning: You are attempting to increase the number of bits used for
NFSv3
 FSIDs and File IDs from 32 to 64 on Vserver "vs0". This could
 result in older client software no longer working with the
volumes
 owned by Vserver "vs0".
Do you want to continue? {y|n}: y

Warning: Based on the changes you are making to the NFS server on
Vserver
 "vs0", it is highly recommended that you remount all NFSv3
clients
 connected to it after the command completes.
Do you want to continue? {y|n}: y
```

### Une fois que vous avez terminé

Tous les clients doivent être remontés. Cette opération est requise car les ID du système de fichiers changent, et les clients peuvent recevoir des messages de traitement des fichiers obsolètes lors d'une tentative d'exécution des opérations NFS.

### Provisionner automatiquement un volume FlexGroup

Lorsque vous créez un volume FlexGroup, vous pouvez choisir que ONTAP provisionne automatiquement le volume FlexGroup en sélectionnant les agrégats. Les agrégats sont sélectionnés en fonction des meilleures pratiques pour des performances et une capacité optimales.

#### Avant de commencer

Chaque nœud du cluster doit disposer d'au moins un agrégat.



Pour créer un volume FlexGroup pour FabricPool dans ONTAP 9.5, chaque nœud doit disposer d'au moins un agrégat FabricPool.

#### Description de la tâche


ONTAP sélectionne deux agrégats disposant de la plus grande quantité d'espace utilisable sur chaque nœud pour créer le volume FlexGroup. Si deux agrégats ne sont pas disponibles, ONTAP sélectionne un agrégat par nœud pour créer le volume FlexGroup.

À partir de ONTAP 9.15.1, lorsque vous provisionnez automatiquement un volume FlexGroup, ONTAP utilise le placement équilibré (BP) pour choisir la disposition des agrégats et des composants FlexGroup. L'un des aspects de BP est la façon dont elle limite le sur-provisionnement des agrégats lors de la création de volumes FlexGroup non garantis. La taille du volume FlexGroup global est limitée par la quantité d'espace libre sur les agrégats, bien que la limite soit supérieure à celle des volumes FlexGroup garantis par « volume ». La création d'un volume FlexGroup à l'aide d'API REST ou `auto-provision-as` de l'interface de ligne de commandes

ONTAP peut entraîner l'échec du provisionnement en raison d'un espace insuffisant pour cause de cette limite. Vous pouvez éviter cela en créant des volumes FlexGroup plus petits ou en ["Création d'un volume FlexGroup et sélection manuelle des agrégats"](#) utilisant le `aggr-list` paramètre.

Étapes

- 1. Provisionnez le volume FlexGroup :

| Si vous utilisez...             | Utilisez cette commande...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ONTAP 9.2 ou version ultérieure | <div><pre>volume create -vserver svm_name -volume fg_vol_name -auto-provision-as flexgroup -size fg_size [-encrypt true] [-qos-policy-group qos_policy_group_name] [-support- tiering true]</pre></div> <p>Depuis ONTAP 9.5, vous pouvez créer des volumes FlexGroup pour FabricPool. Pour provisionner automatiquement un volume FlexGroup sur FabricPool, vous devez définir la <code>-support-tiering</code> paramètre à <code>true</code>. La garantie de volume doit toujours être définie sur <code>none</code> Pour FabricPool. Vous pouvez également spécifier la règle de Tiering ainsi que la période de refroidissement minimale de Tiering du volume FlexGroup.</p> <p><a href="#">"Gestion des disques et des agrégats"</a></p> <p>Depuis la version ONTAP 9.3, vous pouvez spécifier une limite de débit (QoS max) pour les volumes FlexGroup, ce qui limite les ressources de performance pouvant être utilisées par le volume FlexGroup. À partir de la version ONTAP 9.4, vous pouvez spécifier les niveaux de débit (QoS min) et la QoS adaptative pour les volumes FlexGroup.</p> <p><a href="#">"Gestion des performances"</a></p> <p>Vous pouvez définir les paramètres à partir de ONTAP 9.2 <code>-encrypt</code> paramètre à <code>true</code> Si vous souhaitez activer le chiffrement sur le volume FlexGroup. Pour créer un volume chiffré, vous devez avoir installé la licence de chiffrement de volume et le gestionnaire de clés.</p> <div><div></div><div><p>Vous devez activer le chiffrement sur les volumes FlexGroup au moment de la création. Vous ne pouvez pas activer le chiffrement sur les volumes FlexGroup existants.</p></div></div> <p><a href="#">"Cryptage des données au repos"</a></p> |

```
volume flexgroup deploy -vserver
svm_name -size fg_size
```

Le `size` Paramètre spécifie la taille du volume FlexGroup en Ko, Mo, Go, To ou po.

L'exemple suivant montre comment provisionner un volume FlexGroup de 400 To dans ONTAP 9.2 :

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

L'exemple suivant montre comment créer une « policy group » QoS pour le plafond de débit et comment l'appliquer à un volume FlexGroup :

```
cluster1::> qos policy-group create -policy group pg-vs1 -vserver vs1
-max-throughput 5000iops
```

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB -qos-policy-group pg-vs1
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

L'exemple suivant montre comment provisionner un volume FlexGroup de 400 To sur des agrégats de FabricPool dans ONTAP 9.5 :

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB -support-tiering true -tiering-policy auto
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

Le volume FlexGroup est créé avec huit composants sur chaque nœud du cluster. Les composants sont répartis de manière égale entre les deux agrégats les plus importants de chaque nœud.

Par défaut, le volume FlexGroup est créé avec le volume Paramètre de garantie d'espace disponible sauf sur les systèmes AFF. Pour les systèmes AFF, le volume FlexGroup est créé par défaut avec le `none` garantie d'espace.

2. Montez le volume FlexGroup avec une Junction path : `volume mount -vserver vs0 -volume fg2 -junction-path /fg2`

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg2
```

### Une fois que vous avez terminé

Vous devez monter le volume FlexGroup à partir du client.

Si vous exécutez ONTAP 9.6 ou version antérieure et si la machine virtuelle de stockage (SVM) a configuré NFSv3 et NFSv4, le montage du volume FlexGroup du client peut échouer. Dans ce cas, vous devez spécifier de manière explicite la version NFS lors du montage du volume FlexGroup à partir du client.

```
mount -t nfs -o vers=3 192.53.19.64:/fg2 /mnt/fg2
ls /mnt/fg2
file1 file2
```

### Créer un volume FlexGroup

Vous pouvez créer un volume FlexGroup en sélectionnant manuellement les agrégats sur lesquels le volume FlexGroup doit être créé, puis en précisant le nombre de composants sur chaque agrégat.

#### Description de la tâche

Vous devez connaître l'espace requis par les agrégats pour la création d'un volume FlexGroup.

Lors de la création d'un volume FlexGroup, vous devez prendre en compte les directives suivantes pour obtenir les meilleures performances avec un volume FlexGroup :

- Un volume FlexGroup ne doit couvrir que les agrégats situés sur des systèmes matériels identiques.

L'utilisation de systèmes matériels identiques permet d'offrir des performances prévisibles sur l'ensemble du volume FlexGroup.

- Un volume FlexGroup doit couvrir plusieurs agrégats avec les mêmes configurations de type de disque et de groupe RAID.

Pour assurer des performances prévisibles, vous devez vous assurer que tous les agrégats se trouvent sur tous les SSD, tous les disques durs ou tous les agrégats hybrides. En outre, les agrégats doivent avoir le même nombre de disques et de groupes RAID sur le volume FlexGroup.

- Un volume FlexGroup peut couvrir plusieurs parties d'un cluster.

Un volume FlexGroup n'a pas besoin d'être configuré pour couvrir l'ensemble du cluster, mais il peut donc tirer parti des ressources matérielles disponibles.

- Lors de la création d'un volume FlexGroup, il est préférable que les agrégats sur lesquels le volume FlexGroup est déployé présentent les caractéristiques suivantes :
  - Une quantité approximative d'espace libre doit être disponible sur plusieurs agrégats, notamment en cas de provisionnement fin.
  - Environ 3 % de l'espace libre doit être réservé aux métadonnées de l'agrégat après la création du volume FlexGroup.
- Pour les systèmes FAS, il est recommandé d'avoir deux agrégats par nœud et pour les systèmes AFF, vous devez disposer d'un agrégat par nœud pour le volume FlexGroup.
- Pour chaque volume FlexGroup, vous devez créer au moins huit composants répartis sur deux agrégats ou plus sur les systèmes FAS et sur un ou plusieurs agrégats sur les systèmes AFF.

### Avant de commencer

- À partir de ONTAP 9.13.1, vous pouvez créer des volumes dont l'analyse de la capacité et le suivi des activités sont activés. Pour activer le suivi de la capacité ou des activités, exécutez le volume `create` commande avec `-analytics-state` ou `-activity-tracking-state` réglés sur `on`.

Pour en savoir plus sur l'analyse de la capacité et le suivi des activités, reportez-vous à la section ["Activez l'analyse du système de fichiers"](#).

### Étapes

1. Créer le volume FlexGroup : `volume create -vserver svm_name -volume flexgroup_name -aggr-list aggr1,aggr2,... -aggr-list-multiplier constituents_per_aggr -size fg_size [-encrypt true] [-qos-policy-group qos_policy_group_name]`

- Le `-aggr-list` Le paramètre spécifie la liste des agrégats à utiliser pour les composants de volume FlexGroup.

Chaque entrée de la liste crée un composant sur l'agrégat spécifié. Vous pouvez spécifier un agrégat plusieurs fois afin d'avoir plusieurs composants créés sur l'agrégat.

Pour assurer des performances prévisibles sur l'ensemble du volume FlexGroup, tous les agrégats doivent utiliser les mêmes configurations de type de disque et de groupe RAID.

- Le `-aggr-list-multiplier` le paramètre spécifie le nombre de fois pour effectuer l'itération sur les agrégats répertoriés avec le `-aggr-list` Paramètre lors de la création d'un volume FlexGroup.

La valeur par défaut du `-aggr-list-multiplier` le paramètre est 4.

- Le `size` Paramètre spécifie la taille du volume FlexGroup en Ko, Mo, Go, To ou po.
- Depuis ONTAP 9.5, vous pouvez créer des volumes FlexGroup pour FabricPool, qui n'utilisent que tous les agrégats SSD.

Pour créer un volume FlexGroup pour FabricPool, tous les agrégats spécifiés avec le `-aggr-list` Le paramètre doit être FabricPool. La garantie de volume doit toujours être définie sur `none` Pour FabricPool. Vous pouvez également spécifier la règle de Tiering ainsi que la période de refroidissement minimale de Tiering du volume FlexGroup.

### [Gestion des disques et des agrégats](#)

- À partir de la version ONTAP 9.4, vous pouvez spécifier les niveaux de débit (QoS min) et la QoS adaptative pour les volumes FlexGroup.

### "Gestion des performances"

- Depuis la version ONTAP 9.3, vous pouvez spécifier une limite de débit (QoS max) pour les volumes FlexGroup, ce qui limite les ressources de performance pouvant être utilisées par le volume FlexGroup.
- Vous pouvez définir les paramètres à partir de ONTAP 9.2 `-encrypt` paramètre à `true` Si vous souhaitez activer le chiffrement sur le volume FlexGroup.

Pour créer un volume chiffré, vous devez avoir installé la licence de chiffrement de volume et le gestionnaire de clés.



Vous devez activer le chiffrement sur les volumes FlexGroup au moment de la création. Vous ne pouvez pas activer le chiffrement sur les volumes FlexGroup existants.

### "Cryptage des données au repos"

```
cluster-1::> volume create -vserver vs0 -volume fg2 -aggr-list
aggr1,aggr2,aggr3,aggr1 -aggr-list-multiplier 2 -size 500TB
```

```
Warning: A FlexGroup "fg2" will be created with the following number of
constituents of size 62.50TB: 8.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 43] Job succeeded: Successful
```

Dans l'exemple précédent, si vous souhaitez créer le volume FlexGroup pour FabricPool, tous les agrégats (aggr1, aggr2 et aggr3) doivent être des agrégats dans FabricPool. Montez le volume FlexGroup avec une `Junction path` :

```
volume mount -vserver vserver_name -volume vol_name -junction-path
junction_path
```

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg
```

### Une fois que vous avez terminé

Vous devez monter le volume FlexGroup à partir du client.

Si vous exécutez ONTAP 9.6 ou version antérieure et si la machine virtuelle de stockage (SVM) a configuré NFSv3 et NFSv4, le montage du volume FlexGroup du client peut échouer. Dans ce cas, vous devez spécifier explicitement la version NFS lorsque vous montez le volume FlexGroup depuis le client.

```
mount -t nfs -o vers=3 192.53.19.64:/fg /mnt/fg2
ls /mnt/fg2
file1 file2
```

## Informations associées

"Rapport technique de NetApp 4571 : Guide des meilleures pratiques et d'implémentation de NetApp FlexGroup"

## Gérer des volumes FlexGroup

### Surveiller l'utilisation de l'espace d'un volume FlexGroup

Vous pouvez afficher un volume FlexGroup et ses composants, et surveiller l'espace utilisé par le volume FlexGroup.

#### Description de la tâche

Depuis la version ONTAP 9.6, le dimensionnement flexible est pris en charge. ONTAP développe automatiquement un composant d'un volume FlexGroup s'il n'occupe pas d'espace en rétrécit tout autre composant du volume FlexGroup dont l'espace libre est disponible d'une quantité équivalente. Le dimensionnement flexible évite toute erreur de manque d'espace générée en raison d'un ou plusieurs volumes composant FlexGroup manquer d'espace.



Depuis ONTAP 9.9.1, les fonctions de reporting et d'application des espaces logiques sont également disponibles pour les volumes FlexGroup. Pour plus d'informations, voir "[Création de rapports sur l'espace logique et application des volumes](#)".

#### Étape

1. Afficher l'espace utilisé par le volume FlexGroup et ses composants : `volume show -vserver vs1 -volume-style-extended flexgroup vs1 -volume-style-extended [flexgroup | flexgroup-constituent]`

```
cluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup
Vserver Volume Aggregate State Type Size
Available Used%

vs1 fg1 - online RW 500GB
207.5GB 56%
```

```
ccluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup-
constituent
```

| Vserver   | Volume    | Aggregate | State  | Type  | Size    |
|-----------|-----------|-----------|--------|-------|---------|
| Available | Used%     |           |        |       |         |
| -----     | -----     | -----     | -----  | ----- | -----   |
| -----     | -----     |           |        |       |         |
| vs1       | fg1__0001 | aggr3     | online | RW    | 31.25GB |
| 12.97GB   | 56%       |           |        |       |         |
| vs1       | fg1__0002 | aggr1     | online | RW    | 31.25GB |
| 12.98GB   | 56%       |           |        |       |         |
| vs1       | fg1__0003 | aggr1     | online | RW    | 31.25GB |
| 13.00GB   | 56%       |           |        |       |         |
| vs1       | fg1__0004 | aggr3     | online | RW    | 31.25GB |
| 12.88GB   | 56%       |           |        |       |         |
| vs1       | fg1__0005 | aggr1     | online | RW    | 31.25GB |
| 13.00GB   | 56%       |           |        |       |         |
| vs1       | fg1__0006 | aggr3     | online | RW    | 31.25GB |
| 12.97GB   | 56%       |           |        |       |         |
| vs1       | fg1__0007 | aggr1     | online | RW    | 31.25GB |
| 13.01GB   | 56%       |           |        |       |         |
| vs1       | fg1__0008 | aggr1     | online | RW    | 31.25GB |
| 13.01GB   | 56%       |           |        |       |         |
| vs1       | fg1__0009 | aggr3     | online | RW    | 31.25GB |
| 12.88GB   | 56%       |           |        |       |         |
| vs1       | fg1__0010 | aggr1     | online | RW    | 31.25GB |
| 13.01GB   | 56%       |           |        |       |         |
| vs1       | fg1__0011 | aggr3     | online | RW    | 31.25GB |
| 12.97GB   | 56%       |           |        |       |         |
| vs1       | fg1__0012 | aggr1     | online | RW    | 31.25GB |
| 13.01GB   | 56%       |           |        |       |         |
| vs1       | fg1__0013 | aggr3     | online | RW    | 31.25GB |
| 12.95GB   | 56%       |           |        |       |         |
| vs1       | fg1__0014 | aggr3     | online | RW    | 31.25GB |
| 12.97GB   | 56%       |           |        |       |         |
| vs1       | fg1__0015 | aggr3     | online | RW    | 31.25GB |
| 12.88GB   | 56%       |           |        |       |         |
| vs1       | fg1__0016 | aggr1     | online | RW    | 31.25GB |
| 13.01GB   | 56%       |           |        |       |         |

16 entries were displayed.

Vous pouvez utiliser l'espace disponible et le pourcentage d'espace utilisés pour surveiller l'utilisation de l'espace du volume FlexGroup.



### Augmenter la taille d'un volume FlexGroup

Pour augmenter la taille d'un volume FlexGroup, vous pouvez soit ajouter de la capacité aux composants existants du volume FlexGroup, soit étendre le volume FlexGroup avec de nouveaux composants.

#### Ce dont vous avez besoin

Un espace suffisant doit être disponible dans les agrégats.

#### Description de la tâche

Si vous souhaitez ajouter de l'espace, vous pouvez augmenter la taille collective du volume FlexGroup. L'augmentation de la taille d'un volume FlexGroup permet de dimensionner les composants existants du volume FlexGroup.

Pour améliorer les performances, vous pouvez étendre le volume FlexGroup. Il peut être utile de développer un volume FlexGroup et d'ajouter de nouveaux composants dans les situations suivantes :

- De nouveaux nœuds ont été ajoutés au cluster.
- Les nouveaux agrégats ont été créés sur les nœuds existants.
- Les composants existants du volume FlexGroup ont atteint la taille de FlexVol maximale du matériel, ce qui ne permet pas de redimensionner le volume FlexGroup.

Dans les versions antérieures à ONTAP 9.3, vous ne devez pas étendre les volumes FlexGroup après l'établissement d'une relation SnapMirror. Si vous développez le volume FlexGroup source après avoir rompu la relation SnapMirror dans des versions antérieures à ONTAP 9.3, vous devez à nouveau effectuer un transfert de base vers le volume FlexGroup de destination. Depuis ONTAP 9.3, vous pouvez étendre les volumes FlexGroup faisant partie d'une relation SnapMirror.

#### Étape

1. Augmentez la taille du volume FlexGroup en augmentant la capacité ou les performances du volume FlexGroup, selon les besoins :

| Si vous voulez augmenter le... | Alors, procédez comme ça...                                                                                                                    |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Capacité du volume FlexGroup   | Redimensionner les composants du volume FlexGroup :<br><br><pre>volume modify -vserver vs_server_name<br/>-volume fg_name -size new_size</pre> |

## Les performances au volume FlexGroup

Développez le volume FlexGroup en ajoutant de nouveaux composants :

```
volume expand -vserver vs_server_name
-volume fg_name -aggr-list aggregate
name,... [-aggr-list-multiplier
constituents_per_aggr]
```

La valeur par défaut du `-aggr-list`  
`-multiplier` paramètre 1.

Pour développer un volume FlexGroup pour  
FabricPool dans ONTAP 9.5, tout nouvel agrégat  
doit être FabricPool.

Dans la mesure du possible, vous devez augmenter la capacité d'un volume FlexGroup. Si vous devez développer un volume FlexGroup, vous devez ajouter des composants aux mêmes multiples que les composants du volume FlexGroup existant pour garantir la cohérence des performances. Par exemple, si le volume FlexGroup existant dispose de 16 composants avec huit composants par nœud, vous pouvez étendre le volume FlexGroup existant d'un volume de 8 ou 16 composants.

### Exemples

#### Exemple d'augmentation de la capacité des constituants existants

L'exemple suivant montre comment ajouter 20 To d'espace à un volume FlexGroup Volx :

```
cluster1::> volume modify -vserver svm1 -volume volX -size +20TB
```

Si le volume FlexGroup dispose de 16 composants, l'espace de chaque composant est augmenté de 1.25 To.

#### Exemple d'amélioration de la performance par l'ajout de nouveaux composants

L'exemple suivant montre comment ajouter deux composants supplémentaires au volume FlexGroup Volx :

```
cluster1::> volume expand -vserver vs1 -volume volX -aggr-list aggr1,aggr2
```

La taille des nouveaux constituants est la même que celle des constituants existants.

### Réduire la taille d'un volume FlexGroup

Depuis ONTAP 9.6, vous pouvez redimensionner un volume FlexGroup à une valeur inférieure à sa taille actuelle afin de libérer l'espace inutilisé du volume. Si vous réduisez la taille d'un volume FlexGroup, ONTAP redimensionne automatiquement tous les composants FlexGroup.

#### Étape

1. Vérifiez la taille actuelle du volume FlexGroup : `'taille du volume -vserver vs_server_name -volume fg_name'`

2. Réduire la taille du volume FlexGroup : `volume size -vserver vsrv_name -volume fg_name new_size`

Lorsque vous spécifiez la nouvelle taille, vous pouvez spécifier une valeur inférieure à la taille actuelle ou une valeur négative à l'aide du signe moins (-) par lequel la taille actuelle du volume FlexGroup est réduite.



Si la réduction automatique est activée pour le volume (`volume autosize` commande), la taille automatique minimale est définie sur la nouvelle taille du volume.

L'exemple suivant affiche la taille actuelle du volume FlexGroup nommé Volx et redimensionne le volume à 10 To :

```
cluster1::> volume size -vserver svm1 -volume volX
(volume size)
vol size: FlexGroup volume 'svm1:volX' has size 15TB.

cluster1::> volume size -vserver svm1 -volume volX 10TB
(volume size)
vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
```

L'exemple suivant affiche la taille actuelle du volume FlexGroup nommé Volx et réduit la taille du volume de 5 To :

```
cluster1::> volume size -vserver svm1 -volume volX
(volume size)
vol size: FlexGroup volume 'svm1:volX' has size 15TB.

cluster1::> volume size -vserver svm1 -volume volX -5TB
(volume size)
vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
```

## Configurez les volumes FlexGroup pour qu'ils augmentent ou réduisent automatiquement leur taille

Depuis ONTAP 9.3, vous pouvez configurer des volumes FlexGroup pour qu'ils puissent croître ou diminuer automatiquement en fonction de l'espace dont ils ont besoin actuellement.

### Ce dont vous avez besoin

Le volume FlexGroup doit être en ligne.

### Description de la tâche

Deux modes sont disponibles pour la dimensionnement automatique des volumes FlexGroup :

- Augmentez automatiquement la taille du volume (`grow mode`)

La croissance automatique permet d'éviter que le volume FlexGroup manque d'espace si l'agrégat peut

fournir plus d'espace. Vous pouvez configurer la taille maximale du volume. L'augmentation est automatiquement déclenchée en fonction de la quantité de données écrites sur le volume par rapport à la quantité d'espace utilisé actuelle, ainsi que des seuils définis.

Par défaut, la taille maximale qu'un volume peut atteindre est de 120 % de la taille à laquelle la croissance automatique est activée. Si vous devez vous assurer que le volume peut augmenter de manière à ce qu'il dépasse, vous devez définir la taille maximale du volume en conséquence.

- Réduisez la taille du volume automatiquement (`grow_shrink` mode)

La réduction automatique empêche la taille d'un volume que nécessaire, ce qui libère de l'espace dans l'agrégat pour les autres volumes.

Autoshrink ne peut être utilisé qu'en combinaison avec la croissance automatique pour répondre aux demandes d'espace changeantes et n'est pas disponible seul. Lorsque l'option Autoshrink est activée, ONTAP gère automatiquement le comportement de décroissance d'un volume afin d'éviter une boucle infinie d'actions Autoshrink et Autoshrink.

L'augmentation automatique du nombre maximal de fichiers qu'il peut contenir peut s'avérer nécessaire à mesure qu'un volume augmente. Lorsqu'un volume est réduit, le nombre maximal de fichiers qu'il peut contenir reste inchangé et un volume ne peut pas être automatiquement réduit en dessous de la taille qui correspond à son nombre maximal actuel de fichiers. Par conséquent, il est possible qu'il ne soit pas possible de réduire automatiquement un volume jusqu'à sa taille d'origine.

## Étape

1. Configurez le volume pour qu'il augmente ou diminue automatiquement sa taille : `volume autosize -vserver vs_server_name -volume vol_name -mode [grow | grow_shrink]`

Vous pouvez également spécifier la taille maximale, la taille minimale et les seuils pour agrandir ou réduire le volume.

La commande suivante active les changements de taille automatiques pour un volume appelé `fg1`. Le volume est configuré pour atteindre une taille maximale de 5 To lorsqu'il est plein à 70 %.

```
cluster1::> volume autosize -volume fg1 -mode grow -maximum-size 5TB
-grow-threshold-percent 70
vol autosize: volume "vs_src:fg1" autosize settings UPDATED.
```

## Supprimez rapidement les répertoires du cluster

Depuis ONTAP 9.8, vous pouvez utiliser la fonctionnalité *FAST-Directory delete* à faible latence pour supprimer les répertoires des partages clients Linux et Windows de manière asynchrone (c'est-à-dire en arrière-plan). Les administrateurs du cluster et des SVM peuvent effectuer des suppressions asynchrones sur les volumes FlexVol et FlexGroup.

Si vous utilisez une version de ONTAP antérieure à ONTAP 9.11.1, vous devez être un administrateur de cluster ou un administrateur de SVM en utilisant le mode de privilège avancé.

Depuis ONTAP 9.11.1, un administrateur de stockage peut accorder des droits sur un volume pour permettre aux clients NFS et SMB d'effectuer des opérations de suppression asynchrone. Pour plus d'informations, voir ["Gérer les droits des clients pour supprimer rapidement des répertoires"](#).

Depuis ONTAP 9.8, vous pouvez utiliser la fonctionnalité de suppression rapide des répertoires à l'aide de l'interface de ligne de commande ONTAP. Depuis la version ONTAP 9.9.1, vous pouvez utiliser cette fonctionnalité avec System Manager. Pour plus d'informations sur ce processus, reportez-vous à ["Prendre les mesures correctives basées sur l'analytique"](#) la section .

## System Manager

1. Cliquez sur **Storage > volumes**, puis sur **Explorer**.

Lorsque vous placez le pointeur de la souris sur un fichier ou un dossier, l'option de suppression apparaît. Vous ne pouvez supprimer qu'un seul objet à la fois.



Lorsque des répertoires et des fichiers sont supprimés, les nouvelles valeurs de capacité de stockage ne sont pas affichées immédiatement.

## CLI

### Utilisez l'interface de ligne de commande pour effectuer une suppression rapide du répertoire

1. Entrer en mode de privilège avancé :

```
-privilege advance
```

2. Supprimez des répertoires sur un volume FlexVol ou FlexGroup :

```
volume file async-delete start -vserver vs1 -volume vol1
-path file_path -throttle throttle
```

La valeur minimale de l'accélérateur est 10, la valeur maximale est 100,000 et la valeur par défaut est 5000.

L'exemple suivant supprime le répertoire nommé d2, qui se trouve dans le répertoire nommé d1.

```
cluster::*>volume file async-delete start -vserver vs1 -volume vol1
-path d1/d2
```

3. Vérifiez que le répertoire a été supprimé :

```
event log show
```

L'exemple suivant montre les valeurs de sortie du journal des événements lorsque le répertoire a été supprimé avec succès.

```
cluster-cli::*> event log show
Time Node Severity Event

MM/DD/YYYY 00:11:11 cluster-vsim INFORMATIONAL
asyncDelete.message.success: Async delete job on path d1/d2 of
volume (MSID: 2162149232) was completed.
```

### Annuler un travail de suppression de répertoire

1. Entrer en mode de privilège avancé :

```
set -privilege advanced
```

2. Vérifiez que la suppression du répertoire est en cours :

```
volume file async-delete show
```

Si le SVM, le volume, l'ID de travail et le chemin d'accès de votre répertoire sont affichés, vous pouvez annuler le travail.

3. Annuler la suppression du répertoire :

```
volume file async-delete cancel -vserver SVM_name -volume volume_name
-jobid job_id
```

## Gérer les droits des clients pour supprimer rapidement des répertoires

Depuis ONTAP 9.11.1, les administrateurs de stockage peuvent accorder des droits sur un volume pour permettre aux clients NFS et SMB d'effectuer eux-mêmes des opérations de suppression\_ rapides dans le répertoire à faible latence. Lorsque la suppression asynchrone est activée sur le cluster, les utilisateurs clients Linux peuvent utiliser le `mv` Les utilisateurs de client Windows et de commande peuvent utiliser le `rename` commande pour supprimer rapidement un répertoire sur le volume spécifié en le déplaçant vers un répertoire caché nommé par défaut `.ontapashbin`.

### Activer la suppression asynchrone du répertoire du client

#### Étapes

1. Depuis l'interface de ligne de commandes du cluster, entrez le mode de privilège avancé : `-privilege advance`
2. Activez la suppression asynchrone du client et, si vous le souhaitez, indiquez un autre nom pour le répertoire trashbin :

```
volume file async-delete client enable volume volname vserver vserverName
trashbinname name
```

Exemple utilisant le nom de corbeille par défaut :

```
cluster1::*> volume file async-delete client enable -volume v1 -vserver
vs0
```

```
Info: Async directory delete from the client has been enabled on volume
"v1" in
Vserver "vs0".
```

Exemple de spécification d'un autre nom de corbeille :

```
cluster1::*> volume file async-delete client enable -volume test
-trashbin .ntaptrash -vserver vs1

Success: Async directory delete from the client is enabled on volume
"v1" in
 Vserver "vs0".
```

### 3. Vérifiez que la suppression asynchrone du client est activée :

```
volume file async-delete client show
```

Exemple :

```
cluster1::*> volume file async-delete client show

Vserver Volume async-delete client TrashBinName

vs1 vol1 Enabled .ntaptrash
vs2 vol2 Disabled -

2 entries were displayed.
```

## Désactiver la suppression asynchrone du répertoire du client

### Étapes

1. Depuis l'interface de ligne de commande du cluster, désactiver le répertoire asynchrone du client delete :

```
volume file async-delete client disable volume volname vserver vserverName
```

Exemple :

```
cluster1::*> volume file async-delete client disable -volume vol1
-vserver vs1

 Success: Asynchronous directory delete client disabled
successfully on volume.
```

2. Vérifiez que la suppression asynchrone du client est désactivée :

```
volume file async-delete client show
```

Exemple :



```
cluster1::*> volume file async-delete client show
```

| Vserver | Volume | async-delete client | TrashBinName |
|---------|--------|---------------------|--------------|
| vs1     | vol1   | Disabled            | -            |
| vs2     | vol2   | Disabled            | -            |

```
2 entries were displayed.
```

## Créez des qtrees avec les volumes FlexGroup

Depuis ONTAP 9.3, vous pouvez créer des qtrees avec les volumes FlexGroup. Les qtrees vous permettent de partitionner vos volumes FlexGroup en segments de plus petite taille, que vous pouvez gérer individuellement.

### Description de la tâche

- Si vous souhaitez revenir à ONTAP 9.2 ou une version antérieure et si vous avez créé un ou plusieurs qtrees dans le volume FlexGroup ou modifié les attributs (style de sécurité et oplocks SMB) du qtree par défaut, Vous devez supprimer tous les qtrees non par défaut, puis désactiver la fonctionnalité qtree sur chaque volume FlexGroup avant de revenir à ONTAP 9.2 ou version antérieure.

["Désactivez la fonctionnalité qtree dans les volumes FlexGroup avant de procéder au rétablissement"](#).

- Si le volume FlexGroup source contient des qtrees dans une relation SnapMirror, le cluster de destination doit exécuter ONTAP 9.3 ou version ultérieure (une version du logiciel ONTAP qui prend en charge les qtrees).
- Depuis ONTAP 9.5, les statistiques qtree sont prises en charge pour les volumes FlexGroup.

### Étapes

1. Créer un qtree dans le volume FlexGroup :

```
volume qtree create -vserver vs1 -volume fgl -qtree qtree1
```

Vous pouvez éventuellement spécifier le style de sécurité, les oplocks SMB, les autorisations UNIX et la règle d'exportation pour le qtree.

```
cluster1::> volume qtree create -vserver vs0 -volume fgl -qtree qtree1
-security-style mixed
```

### Informations associées

["Gestion du stockage logique"](#)

## Utilisez des quotas pour les volumes FlexGroup

Avec ONTAP 9.4 et les versions antérieures, vous pouvez appliquer des règles de quotas aux volumes FlexGroup uniquement à des fins de reporting, mais pas pour appliquer des limites de quotas. À partir de ONTAP 9.5, vous pouvez appliquer des limites aux règles

de quotas appliquées aux volumes FlexGroup.

### Description de la tâche

- Depuis ONTAP 9.5, vous pouvez spécifier des quotas matériels, logiciels et seuils limites pour les volumes FlexGroup.

Vous pouvez spécifier ces limites pour limiter la quantité d'espace, le nombre de fichiers qu'un utilisateur, un groupe ou un qtree peut créer, ou les deux. Les limites de quota génèrent des messages d'avertissement dans les scénarios suivants :

- Lorsque l'utilisation dépasse une limite logicielle configurée, ONTAP émet un message d'avertissement, mais le trafic supplémentaire est toujours autorisé.

Si l'utilisation se reproduit plus tard en dessous de la limite logicielle configurée, un message « tout effacer » s'affiche.

- Lorsque l'utilisation dépasse une limite de seuil configurée, ONTAP émet un second message d'avertissement.

Aucun message administratif « tout-clair » n'est émis lorsque l'utilisation ultérieure descend en dessous d'une limite de seuil configurée.

- Si l'utilisation atteint une limite matérielle configurée, ONTAP empêche une consommation de ressources supplémentaire en rejetant le trafic.
- Dans ONTAP 9.5, aucune règle de quotas ne peut être créée ou activée sur le volume FlexGroup de destination d'une relation SnapMirror.
- Lors de l'initialisation des quotas, les quotas ne sont pas appliqués et aucune notification de quotas non respectés suite à l'initialisation des quotas.


Pour vérifier si les quotas ont été enfreintes lors de l'initialisation du quota, vous pouvez utiliser le `volume quota report` commande.

### Types et cibles de quotas

Les quotas ont un type : ils peuvent être soit utilisateur, groupe, soit arborescence. Les cibles de quota spécifient l'utilisateur, le groupe ou le qtree pour lequel les limites du quota sont appliquées.

Le tableau suivant répertorie les types de cibles de quota, les types de quotas associés à chaque cible de quota et la façon dont chaque cible de quota est représentée :

| Cible de quota | Type de quota     | Mode de représentation de la cible                                                                                | Remarques                                                                         |
|----------------|-------------------|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| utilisateur    | quota utilisateur | Nom d'utilisateur UNIX<br>UID UNIX<br><br>Nom d'utilisateur Windows au format pré-Windows 2000<br><br>SID Windows | Les quotas utilisateur peuvent être appliqués pour un volume ou qtree spécifique. |

|        |                                         |                                   |                                                                                                                                                                                                                                                             |
|--------|-----------------------------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| groupe | quota de groupe                         | Nom du groupe UNIX<br>GID<br>UNIX | Les quotas group peuvent être appliqués pour un volume ou qtree spécifique.<br><br><div> La ONTAP ne s'applique pas aux quotas de groupe basés sur les ID Windows.</div> |
| qtree  | quota d'arbre                           | nom du qtree                      | Les quotas d'arborescence sont appliqués à un volume en particulier et n'affectent pas les qtrees des autres volumes.                                                                                                                                       |
| ""     | quota roup utilisateur<br>quota d'arbre | Guillemets doubles ("" )          | Une cible de quota de "" désigne un quota <i>default</i> . Pour les quotas par défaut, le type de quota est déterminé par la valeur du champ type.                                                                                                          |

### Comportement des volumes FlexGroup lorsque les limites de quota sont dépassées

Depuis ONTAP 9.5, les limites de quota sont prises en charge sur les volumes FlexGroup. La façon dont les limites de quotas sont appliquées sur un volume FlexGroup par rapport à un volume FlexVol est différentes.

Lorsque les volumes FlexGroup peuvent afficher les comportements suivants, lorsque les limites des quotas sont dépassées :

- L'utilisation d'espace et de fichiers dans un volume FlexGroup peut atteindre jusqu'à 5 % de plus que la limite matérielle configurée avant de limiter le quota en rejetant le trafic supplémentaire.

Pour optimiser les performances, ONTAP peut permettre à la consommation d'espace de dépasser la limite matérielle configurée de manière minime avant le début de l'application des quotas. Cette consommation d'espace supplémentaire ne dépasse pas 5 % des limites matérielles configurées, 1 Go ou 65536 fichiers, selon la valeur la plus faible.

- Une fois la limite du quota atteinte, si un utilisateur ou un administrateur supprime certains fichiers ou répertoires de telle sorte que l'utilisation du quota soit désormais inférieure à la limite, l'opération suivante de fichiers consommant beaucoup de quota peut reprendre avec un délai (peut prendre jusqu'à 5 secondes pour reprendre).
- Lorsque l'espace total et l'utilisation des fichiers d'un volume FlexGroup dépassent les limites de quotas configurés, la journalisation d'un message journal d'événements peut légèrement différer.

- Vous risquez d'obtenir des erreurs « pas d'espace » si certains composants du volume FlexGroup sont pleins, mais que les limites des quotas ne sont pas atteintes.
- Les opérations telles que le renommage d'un fichier ou d'un répertoire, ou le déplacement de fichiers entre des qtrees, sur des cibles de quota, pour lesquelles des limites strictes de quota sont configurées, peuvent prendre plus de temps que d'autres opérations similaires sur des volumes FlexVol.

### Exemples d'application de quotas pour les volumes FlexGroup

Vous pouvez utiliser ces exemples pour comprendre comment configurer des quotas avec des limites dans ONTAP 9.5 et versions ultérieures.

#### Exemple 1 : application d'une règle de quotas avec des limites de disques

1. Vous devez créer une règle de quotas de type `user` avec une limite de disque dur et une limite de disque dur réalisable.

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
default -volume FG -type user -target "" -qtree "" -disk-limit 1T -soft
-disk-limit 800G
```

2. Vous pouvez afficher la règle de quotas :

```
cluster1::> volume quota policy rule show -vserver vs0 -policy-name
default -volume FG
```

| Vserver: vs0 |        |       | Policy: default |            | Volume: FG      |             |                  |
|--------------|--------|-------|-----------------|------------|-----------------|-------------|------------------|
| Type         | Target | Qtree | User Mapping    | Disk Limit | Soft Disk Limit | Files Limit | Soft Files Limit |
| user         | ""     | ""    | off             | 1TB        | 800GB           | -           | -                |

3. Pour activer la nouvelle règle de quota, vous initialisez les quotas sur le volume :

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. Vous pouvez afficher les informations relatives à l'utilisation des disques et des fichiers du volume FlexGroup à l'aide du rapport de quota.

```
cluster1::> volume quota report -vserver vs0 -volume FG
Vserver: vs0
```

| Volume<br>Specifier | Tree | Type | ID   | ----Disk---- |       | ----Files----- |       | Quota |
|---------------------|------|------|------|--------------|-------|----------------|-------|-------|
|                     |      |      |      | Used         | Limit | Used           | Limit |       |
| FG                  |      | user | root | 50GB         | -     | 1              | -     |       |
| FG                  |      | user | *    | 800GB        | 1TB   | 0              | -     | *     |

2 entries were displayed.

Une fois la limite du disque dur atteinte, la cible de la règle de politique de quota (utilisateur, dans ce cas) est bloquée pour écrire plus de données dans les fichiers.

## Exemple 2 : application d'une règle de quotas pour plusieurs utilisateurs

1. Vous devez créer une règle de quotas de type `user`, Où plusieurs utilisateurs sont spécifiés dans la cible de quota (utilisateurs UNIX, utilisateurs SMB ou une combinaison des deux) et où la règle a à la fois une limite de disque logiciel réalisable et une limite de disque dur.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target "rdavis,ABCCORP\RobertDavis" -qtree ""
-disk-limit 1TB -soft-disk-limit 800GB
```

2. Vous pouvez afficher la règle de quotas :

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG
```

| Vserver: vs0 |                              |       | Policy: default |               |                       | Volume: FG     |                        |
|--------------|------------------------------|-------|-----------------|---------------|-----------------------|----------------|------------------------|
| Type         | Target                       | Qtree | User<br>Mapping | Disk<br>Limit | Soft<br>Disk<br>Limit | Files<br>Limit | Soft<br>Files<br>Limit |
| user         | "rdavis,ABCCORP\RobertDavis" | ""    | off             | 1TB           | 800GB                 | -              | -                      |

3. Pour activer la nouvelle règle de quota, vous initialisez les quotas sur le volume :

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. Vous pouvez vérifier que l'état du quota est actif :

```
cluster1::> volume quota show -vserver vs0 -volume FG
Vserver Name: vs0
Volume Name: FG
Quota State: on
Scan Status: -
Logging Messages: on
Logging Interval: 1h
Sub Quota Status: none
Last Quota Error Message: -
Collection of Quota Errors: -
```

5. Vous pouvez afficher les informations relatives à l'utilisation des disques et des fichiers du volume FlexGroup à l'aide du rapport de quota.

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0
```

| Volume                     | Tree  | Type  | ID                         | -----Disk----- | -----Files----- | Quota |       |
|----------------------------|-------|-------|----------------------------|----------------|-----------------|-------|-------|
| Specifier                  |       |       |                            | Used           | Limit           | Used  | Limit |
| -----                      | ----- | ----- | -----                      | -----          | -----           | ----- | ----- |
| FG                         |       | user  | rdavis,ABCCORP\RobertDavis | 0B             | 1TB             | 0     | -     |
| rdavis,ABCCORP\RobertDavis |       |       |                            |                |                 |       |       |

La limite du quota est partagée entre tous les utilisateurs répertoriés dans la cible du quota.

Une fois la limite du disque dur atteinte, les utilisateurs répertoriés dans la cible du quota sont bloqués afin d'écrire plus de données sur les fichiers.

### Exemple 3 : application de quotas avec mappage utilisateur activé

1. Vous devez créer une règle de quotas de type `user`, Spécifiez un utilisateur UNIX ou Windows comme cible de quota avec `user-mapping` réglez sur `on`, et créez la règle avec une limite de disque logiciel réalisable et une limite de disque dur.

Le mappage entre les utilisateurs UNIX et Windows doit être configuré plus tôt à l'aide de `vserver name-mapping create` commande.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target rdavis -qtree "" -disk-limit 1TB -soft
-disk-limit 800GB -user-mapping on
```

2. Vous pouvez afficher la règle de quotas :

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG
```

```
Vserver: vs0 Policy: default Volume: FG
```

| Type | Target | Qtree | User Mapping | Disk Limit | Soft Disk Limit | Files Limit | Soft Files Limit |
|------|--------|-------|--------------|------------|-----------------|-------------|------------------|
| user | rdavis | ""    | on           | 1TB        | 800GB           | -           | -                |

3. Pour activer la nouvelle règle de quota, vous initialisez les quotas sur le volume :

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. Vous pouvez vérifier que l'état du quota est actif :

```
cluster1::> volume quota show -vserver vs0 -volume FG
Vserver Name: vs0
Volume Name: FG
Quota State: on
Scan Status: -
Logging Messages: on
Logging Interval: 1h
Sub Quota Status: none
Last Quota Error Message: -
Collection of Quota Errors: -
```

5. Vous pouvez afficher les informations relatives à l'utilisation des disques et des fichiers du volume FlexGroup à l'aide du rapport de quota.

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0
```

| Volume      | Tree  | Type  | ID                         | ----Disk---- |       | ----Files----- |       | Quota |
|-------------|-------|-------|----------------------------|--------------|-------|----------------|-------|-------|
|             |       |       |                            | Used         | Limit | Used           | Limit |       |
| Specififier |       |       |                            |              |       |                |       |       |
| -----       | ----- | ----- | -----                      | -----        | ----- | -----          | ----- |       |
| FG          |       | user  | rdavis,ABCCORP\RobertDavis | 0B           | 1TB   | 0              | -     |       |
| rdavis      |       |       |                            |              |       |                |       |       |

La limite du quota est partagée entre l'utilisateur répertorié dans la cible du quota et l'utilisateur Windows ou UNIX correspondant.

Une fois la limite du disque dur atteinte, l'utilisateur répertorié dans la cible du quota et l'utilisateur Windows ou UNIX correspondant sont bloqués afin d'écrire plus de données dans les fichiers.

#### Exemple 4 : vérification de la taille du qtree lorsque le quota est activé

1. Vous devez créer une règle de quotas de type `tree` et où la règle a à la fois une limite de disque logiciel et une limite de disque dur réalisable.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type tree -target tree_4118314302 -qtree "" -disk-limit 48GB
-soft-disk-limit 30GB
```

2. Vous pouvez afficher la règle de quotas :

```
cluster1::> quota policy rule show -vserver vs0
```

| Vserver: vs0 |                 |       | Policy: default |       |       | Volume: FG |       |
|--------------|-----------------|-------|-----------------|-------|-------|------------|-------|
| Type         | Target          | Qtree | User            | Disk  | Soft  | Files      | Soft  |
| Threshold    |                 |       | Mapping         | Limit | Disk  | Limit      | Files |
|              |                 |       |                 |       | Limit |            | Limit |
| tree         | tree_4118314302 | ""    | -               | 48GB  | -     | 20         | -     |

3. Pour activer la nouvelle règle de quota, vous initialisez les quotas sur le volume :

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```



- a. Vous pouvez afficher les informations relatives à l'utilisation des disques et des fichiers du volume FlexGroup à l'aide du rapport de quota.

```
cluster1:> quota report -vserver vs0
Vserver: vs0
----Disk---- ----Files----- Quota
Volume Tree Type ID Used Limit Used Limit Specifier

FG tree_4118314302 tree 1 30.35GB 48GB 14 20 tree_4118314302
```

La limite du quota est partagée entre l'utilisateur répertorié dans la cible du quota et l'utilisateur Windows ou UNIX correspondant.

4. À partir d'un client NFS, utilisez `df` commande pour afficher l'utilisation de l'espace total, l'espace disponible et l'espace utilisé.

```
scsps0472342001# df -m /t/10.53.2.189/FG-3/tree_4118314302
Filesystem 1M-blocks Used Available Use% Mounted on
10.53.2.189/FG-3 49152 31078 18074 63% /t/10.53.2.189/FG-3
```

Avec la limite matérielle, l'utilisation de l'espace est calculée à partir d'un client NFS comme suit :

- Utilisation de l'espace total = limite stricte pour l'arborescence
- Espace libre = limite stricte moins utilisation de l'espace qtree  
Sans limitation stricte, l'utilisation de l'espace est calculée à partir d'un client NFS comme suit :
- Utilisation de l'espace = utilisation du quota
- Espace total = somme de l'utilisation des quotas et de l'espace libre physique dans le volume

5. À partir du partage SMB, utilisez l'Explorateur Windows pour afficher l'espace total utilisé, l'espace disponible et l'espace utilisé.

À partir d'un partage SMB, vous devez tenir compte des considérations suivantes pour calculer l'utilisation de l'espace :

- La limite matérielle du quota utilisateur pour l'utilisateur et le groupe est prise en compte pour le calcul de l'espace total disponible.
- La valeur minimale entre l'espace libre de la règle de quota Tree, la règle de quota utilisateur et la règle de quota groupe est considérée comme l'espace libre pour le partage SMB.
- L'utilisation de l'espace total est variable pour SMB et dépend de la limite matérielle qui correspond à l'espace libre minimum entre l'arborescence, l'utilisateur et le groupe.

## Application des règles et des limites au volume FlexGroups

### Étapes

1. Créer des règles de quota pour les cibles : `volume quota policy rule create -vserver vs0 -policy-name quota_policy_of_the_rule -volume flexgroup_vol -type {tree|user|group} -target target_for_rule -qtree qtree_name [-disk-limit`

```
hard_disk_limit_size] [-file-limit hard_limit_number_of_files] [-threshold threshold_disk_limit_size] [-soft-disk-limit soft_disk_limit_size] [-soft-file-limit soft_limit_number_of_files]
```

- Dans ONTAP 9.2 et ONTAP 9.1, le type de cible de quota ne peut être que `user` ou `group` Pour les volumes FlexGroup.

Le type de quota `Tree` n'est pas pris en charge pour les volumes FlexGroup dans ONTAP 9.2 et ONTAP 9.1.

- Dans ONTAP 9.3 et versions ultérieures, le type de cible de quota peut être `user`, `group`, ou `tree` Pour les volumes FlexGroup.
- Un chemin n'est pas pris en charge en tant que cible lors de la création de règles de quotas pour les volumes FlexGroup.
- Depuis ONTAP 9.5, vous pouvez spécifier la limite des disques durs, la limite des fichiers matériels, la limite soft disque, la limite soft fichiers et la limite de seuil des volumes FlexGroup.

Dans ONTAP 9.4 et versions antérieures, vous ne pouvez pas spécifier la limite des disques, la limite des fichiers, le seuil de la limite des disques, la limite soft disque ou la limite des fichiers logicielles lorsque vous créez des règles de quotas pour les volumes FlexGroup.

L'exemple suivant montre une règle de quota par défaut en cours de création pour le type cible utilisateur :

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name quota_policy_vs0_1 -volume fg1 -type user -target "" -qtree ""
```

L'exemple suivant montre une règle de quota `Tree` créée pour le `qtree` appelé `qtree1` :

```
cluster1::> volume quota policy rule create -policy-name default -vserver vs0 -volume fg1 -type tree -target "qtree1"
```

1. Activer les quotas du volume FlexGroup spécifié : `volume quota on -vserver svm_name -volume flexgroup_vol -foreground true`

```
cluster1::> volume quota on -vserver vs0 -volume fg1 -foreground true
```

1. Surveiller l'état de l'initialisation des quotas : `volume quota show -vserver svm_name`

Les volumes FlexGroup peuvent afficher le `mixed state`, ce qui indique que tous les volumes constitutifs ne sont pas encore dans le même état.

```
cluster1::> volume quota show -vserver vs0
```

| Vserver | Volume | State        | Scan Status |
|---------|--------|--------------|-------------|
| vs0     | fg1    | initializing | 95%         |
| vs0     | vol1   | off          | -           |

2 entries were displayed.

1. Afficher le rapport de quota pour le volume FlexGroup avec quotas actifs : `volume quota report -vserver svm_name -volume flexgroup_vol`

Vous ne pouvez pas spécifier de chemin avec `volume quota report` Commande pour les volumes FlexGroup.

L'exemple suivant montre le quota utilisateur pour le volume FlexGroup fg1 :

```
cluster1::> volume quota report -vserver vs0 -volume fg1
```

Vserver: vs0

| Quota     |      |      |      | ----Disk---- |       | ----Files---- |       |   |
|-----------|------|------|------|--------------|-------|---------------|-------|---|
| Volume    | Tree | Type | ID   | Used         | Limit | Used          | Limit |   |
| Specifier |      |      |      |              |       |               |       |   |
| fg1       |      | user | *    | 0B           | -     | 0             | -     | * |
| fg1       |      | user | root | 1GB          | -     | 1             | -     | * |

2 entries were displayed.

L'exemple suivant montre le quota Tree pour le volume FlexGroup fg1 :

```
cluster1::> volume quota report -vserver vs0 -volume fg1
```

Vserver: vs0

| Quota     |        |      |    | ----Disk---- |       | ----Files---- |       | Quota |
|-----------|--------|------|----|--------------|-------|---------------|-------|-------|
| Volume    | Tree   | Type | ID | Used         | Limit | Used          | Limit |       |
| Specifier |        |      |    |              |       |               |       |       |
| fg1       | qtree1 | tree | 1  | 68KB         | -     | 18            | -     |       |
| qtree1    |        |      |    |              |       |               |       |       |
| fg1       |        | tree | *  | 0B           | -     | 0             | -     | *     |

2 entries were displayed.

## Résultats

Les règles et limites de quota sont appliquées sur le volume FlexGroups.

L'utilisation peut atteindre jusqu'à 5 % de plus qu'une limite matérielle configurée avant que ONTAP n'applique le quota en rejetant le trafic supplémentaire.

#### Informations associées

- ["Référence de commande ONTAP"](#)

### Activer l'efficacité du stockage sur un volume FlexGroup

Vous pouvez exécuter la déduplication et la compression des données de manière indépendante ou simultanément sur un volume FlexGroup afin de réaliser des économies d'espace optimales.

#### Ce dont vous avez besoin

Le volume FlexGroup doit être en ligne.

#### Étapes

1. Efficacité du stockage sur le volume FlexGroup : `volume efficiency on -vserver svm_name -volume volume_name`

Les opérations d'efficacité du stockage sont activées sur l'ensemble des composants du volume FlexGroup.

Si un volume FlexGroup est étendu une fois l'efficacité du stockage activée sur le volume, l'efficacité du stockage est automatiquement activée sur les nouveaux composants.

2. Activez l'efficacité du stockage requise sur le volume FlexGroup à l'aide de `volume efficiency modify` commande.

Vous pouvez activer la déduplication à la volée, la déduplication post-traitement, la compression à la volée et la compression post-traitement sur les volumes FlexGroup. Vous pouvez également définir le type de compression (secondaire ou adaptative) et spécifier un planning ou une règle d'efficacité pour le volume FlexGroup.

3. Si vous n'utilisez pas les plannings ou les stratégies d'efficacité pour l'exécution des opérations de stockage, démarrez l'opération d'efficacité : `volume efficiency start -vserver svm_name -volume volume_name`

Si la déduplication et la compression des données sont activées sur un volume, la compression des données est exécutée initialement avant la déduplication. Cette commande échoue si une opération d'efficacité est déjà active sur le volume FlexGroup.

4. Vérifiez les opérations d'efficacité activées sur le volume FlexGroup : `volume efficiency show -vserver svm_name -volume volume_name`

```
cluster1::> volume efficiency show -vserver vs1 -volume fg1
 Vserver Name: vs1
 Volume Name: fg1
 Volume Path: /vol/fg1
 State: Enabled
 Status: Idle
 Progress: Idle for 17:07:25
 Type: Regular
 Schedule: sun-sat@0

...

 Compression: true
 Inline Compression: true
 Incompressible Data Detection: false
 Constituent Volume: false
 Compression Quick Check File Size: 524288000
 Inline Dedupe: true
 Data Compaction: false
```

## Protection des volumes FlexGroup à l'aide de copies Snapshot

Vous pouvez créer des règles Snapshot qui gèrent automatiquement la création de copies Snapshot ou créer manuellement des copies Snapshot pour les volumes FlexGroup. Une copie Snapshot valide est créée pour un volume FlexGroup uniquement après qu'ONTAP puisse créer une copie Snapshot pour chaque composant du volume FlexGroup.

### Description de la tâche

- Si plusieurs volumes FlexGroup sont associés à une règle Snapshot, assurez-vous que la planification des volumes FlexGroup ne se chevauchent pas.
- Depuis ONTAP 9.8, le nombre maximal de copies Snapshot prises en charge sur un volume FlexGroup est de 15 1023.





Avec ONTAP 9.8, le volume snapshot show La commande pour les volumes FlexGroup indique la taille de la copie Snapshot à l'aide de blocs logiques, plutôt que de calculer les blocs les plus jeunes. Cette nouvelle méthode de calcul de la taille peut rendre la taille de la copie Snapshot plus importante que les calculs dans les versions précédentes de ONTAP.

### Étapes

1. Créer une règle Snapshot ou créer manuellement une copie Snapshot :

Si vous souhaitez créer un...

Entrez cette commande...

|                             |                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Règle Snapshot              | <p>volume snapshot policy create</p> <div>  <p>Les planifications associées à la politique Snapshot d'un volume FlexGroup doivent avoir un intervalle supérieur à 30 minutes.</p> </div> <p>Lorsque vous créez un volume FlexGroup, le default La politique Snapshot s'applique au volume FlexGroup.</p> |
| Copie Snapshot manuellement | <p>volume snapshot create</p> <div>  <p>Une fois que vous avez créé une copie Snapshot d'un volume FlexGroup, vous ne pouvez pas modifier les attributs de cette copie. Si vous souhaitez modifier les attributs, vous devez supprimer, puis recréer la copie Snapshot.</p> </div>                       |

L'accès du client au volume FlexGroup est brièvement suspendu lors de la création d'une copie Snapshot.

1. Vérifiez qu'une copie Snapshot valide est créée pour le volume FlexGroup : `volume snapshot show -volume volume_name -fields state`

```
cluster1::> volume snapshot show -volume fg -fields state
vserver volume snapshot state

fg_vs fg hourly.2016-08-23_0505 valid
```

2. Afficher les copies Snapshot pour les composants du volume FlexGroup : `volume snapshot show -is -constituent true`

```
cluster1::> volume snapshot show -is-constituent true
```

| ---Blocks--- |          |                        |       |        |
|--------------|----------|------------------------|-------|--------|
| Vserver      | Volume   | Snapshot               | Size  | Total% |
| Used%        |          |                        |       |        |
| -----        | -----    | -----                  | ----- | -----  |
| fg_vs        | fg__0001 | hourly.2016-08-23_0505 | 72MB  | 0%     |
| 27%          |          |                        |       |        |
|              | fg__0002 | hourly.2016-08-23_0505 | 72MB  | 0%     |
| 27%          |          |                        |       |        |
|              | fg__0003 | hourly.2016-08-23_0505 | 72MB  | 0%     |
| 27%          |          |                        |       |        |
| ...          |          |                        |       |        |
|              | fg__0016 | hourly.2016-08-23_0505 | 72MB  | 0%     |
| 27%          |          |                        |       |        |

## Déplacer les composants d'un volume FlexGroup

Vous pouvez déplacer les composants d'un volume FlexGroup d'un agrégat à un autre afin d'équilibrer la charge lorsque certains composants subissent davantage de trafic. Le déplacement des composants permet également de libérer de l'espace sur un agrégat pour le redimensionnement des composants existants.

### Ce dont vous avez besoin

Pour déplacer un composant de volume FlexGroup dans une relation SnapMirror, vous devez avoir initialisé la relation SnapMirror.

### Description de la tâche

Vous ne pouvez pas effectuer de déplacement de volumes pendant l'extension des composants du volume FlexGroup.

### Étapes

1. Identifiez les composants du volume FlexGroup que vous souhaitez déplacer :

```
volume show -vserver svm_name -is-constituent true
```

```
cluster1::> volume show -vserver vs2 -is-constituent true
```

| Vserver | Volume    | Aggregate | State  | Type | Size  |
|---------|-----------|-----------|--------|------|-------|
| vs2     | fg1       | -         | online | RW   | 400TB |
| vs2     | fg1__0001 | aggr1     | online | RW   | 25TB  |
| vs2     | fg1__0002 | aggr2     | online | RW   | 25TB  |

...

- Identifiez un agrégat dans lequel vous pouvez déplacer le composant de volume FlexGroup :

```
volume move target-aggr show -vserver svm_name -volume vol_constituent_name
```

L'espace disponible dans l'agrégat que vous sélectionnez doit être supérieur à la taille du composant de volume FlexGroup que vous déplacez.

```
cluster1::> volume move target-aggr show -vserver vs2 -volume fg1_0002
```

| Aggregate Name | Available Size | Storage Type |
|----------------|----------------|--------------|
| aggr2          | 467.9TB        | hdd          |
| node12a_aggr3  | 100.34TB       | hdd          |
| node12a_aggr2  | 100.36TB       | hdd          |
| node12a_aggr1  | 100.36TB       | hdd          |
| node12a_aggr4  | 100.36TB       | hdd          |

5 entries were displayed.

- Vérifier que le composant de volume FlexGroup peut être déplacé vers l'agrégat prévu :

```
volume move start -vserver svm_name -volume vol_constituent_name -destination
-aggregate aggr_name -perform-validation-only true
```

```
cluster1::> volume move start -vserver vs2 -volume fg1_0002 -destination
-aggregate node12a_aggr3 -perform-validation-only true
Validation succeeded.
```

- Déplacez le composant de volume FlexGroup :

```
volume move start -vserver svm_name -volume vol_constituent_name -destination
-aggregate aggr_name [-allow-mixed-aggr-types {true|false}]
```

L'opération de déplacement de volume s'exécute en arrière-plan.



Depuis ONTAP 9.5, il est possible de déplacer des composants de volumes FlexGroup d'un FabricPool vers un pool non Fabric, ou inversement en paramétrant le `-allow-mixed-aggr-types` paramètre à `true`. Par défaut, le `-allow-mixed-aggr-types` l'option est définie sur `false`.



Vous ne pouvez pas utiliser `volume move` Commande pour activer le chiffrement sur les volumes FlexGroup.

```
cluster1::> volume move start -vserver vs2 -volume fg1_002 -destination
-aggregate node12a_aggr3
```



Si l'opération de déplacement de volume échoue en raison d'une opération SnapMirror active, vous devez abandonner l'opération SnapMirror à l'aide du `snapmirror abort -h` commande. Dans certains cas, l'opération d'abandon de SnapMirror peut également échouer. Dans ce cas, vous devez abandonner l'opération de déplacement de volume et réessayer ultérieurement.

#### 5. Vérifiez l'état de l'opération de déplacement de volume :

```
volume move show -volume vol_constituent_name
```

L'exemple suivant montre l'état d'un volume composant FlexGroup qui a terminé la phase de réplication et est en phase de mise en service de l'opération de déplacement de volume :

```
cluster1::> volume move show -volume fg1_002
Vserver Volume State Move Phase Percent-Complete Time-To-
Complete

vs2 fg1_002 healthy cutover - -
```

### Utilisation d'agrégats dans FabricPool pour les volumes FlexGroup existants

FabricPool est pris en charge par les volumes FlexGroup depuis la version ONTAP 9.5. Si vous souhaitez utiliser les agrégats du FabricPool pour vos volumes FlexGroup existants, vous pouvez soit convertir les agrégats sur lesquels réside le volume FlexGroup en agrégats du FabricPool, soit migrer les composants de volume FlexGroup vers des agrégats du FabricPool.

#### Ce dont vous avez besoin

- Le volume FlexGroup doit être défini sur avec la garantie d'espace `none`.
- Si vous souhaitez convertir les agrégats sur lesquels réside le volume FlexGroup en agrégats du FabricPool, tous les agrégats doivent utiliser des disques SSD.

#### Description de la tâche

Si un volume FlexGroup existant se trouve sur des agrégats non SSD, vous devez migrer les composants de volume FlexGroup vers des agrégats dans FabricPool.

## Choix

- Pour convertir les agrégats sur lesquels se trouve le volume FlexGroup vers des agrégats dans FabricPool, effectuez la procédure suivante :
  - a. Définissez la règle de Tiering sur le volume FlexGroup existant : `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

```
cluster-2::> volume modify -volume fg1 -tiering-policy auto
```

- b. Identifiez les agrégats sur lesquels réside le volume FlexGroup : `volume show -volume flexgroup_name -fields aggr-list`

```
cluster-2::> volume show -volume fg1 -fields aggr-list
vserver volume aggr-list

vs1 fg1 aggr1,aggr3
```

- c. Reliez un magasin d'objets à chaque agrégat répertorié dans la liste agrégat : `storage aggregate object-store attach -aggregate aggregate name -name object-store-name -allow-flexgroup true`

Vous devez attacher tous les agrégats à un magasin d'objets.

```
cluster-2::> storage aggregate object-store attach -aggregate aggr1
-object-store-name Amazon01B1
```

- Pour migrer les composants de volume FlexGroup vers des agrégats dans FabricPool, effectuez les opérations suivantes :

- a. Définissez la règle de Tiering sur le volume FlexGroup existant : `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

```
cluster-2::> volume modify -volume fg1 -tiering-policy auto
```

- b. Déplacer chaque composant du volume FlexGroup vers un agrégat d'FabricPool dans le même cluster : `volume move start -volume constituent-volume -destination-aggregate FabricPool_aggregate -allow-mixed-aggr-types true`

Vous devez déplacer tous les composants de volume FlexGroup vers des agrégats dans FabricPool (si les composants du volume FlexGroup se trouvent sur des types d'agrégats mixtes) et assurer l'équilibrage de l'ensemble des composants sur les nœuds du cluster.

```
cluster-2::> volume move start -volume fg1_001 -destination-aggregate
FP_aggr1 -allow-mixed-aggr-types true
```

## Rééquilibrer les volumes FlexGroup

Depuis ONTAP 9.12.1, vous pouvez rééquilibrer les volumes FlexGroup en déplaçant les fichiers d'un composant d'un FlexGroup vers un autre composant sans interruption.

Le rééquilibrage FlexGroup permet de redistribuer les capacités lorsque les déséquilibres se développent au fil du temps en raison de l'ajout de nouveaux fichiers et de la croissance des fichiers. Une fois que vous avez démarré manuellement l'opération de rééquilibrage, ONTAP sélectionne les fichiers et les déplace automatiquement et sans interruption.



Notez que le rééquilibrage FlexGroup dégrade les performances système lorsque de nombreux fichiers sont déplacés dans le cadre d'un seul rééquilibrage ou lors d'événements de rééquilibrage multiples en raison de la création d'inodes en plusieurs parties. Chaque fichier déplacé dans le cadre d'un événement de rééquilibrage a 2 inodes à pièces multiples associées à ce fichier. Plus le nombre de fichiers avec des inodes en plusieurs parties est élevé en pourcentage du nombre total de fichiers dans une FlexGroup, plus l'impact sur les performances est important. Certains cas d'utilisation, comme la conversion FlexVol en FlexGroup, peuvent entraîner la création d'inodes multiples.

Le rééquilibrage est disponible uniquement lorsque tous les nœuds du cluster exécutent ONTAP 9.12.1 ou une version ultérieure. Vous devez activer la fonctionnalité de données granulaires sur tous les volumes FlexGroup qui exécutent l'opération de rééquilibrage. Une fois cette fonctionnalité activée, vous ne pouvez pas revenir à ONTAP 9.11.1 et aux versions antérieures sauf si vous supprimez ce volume ou restaurez-le à partir d'une copie Snapshot créée avant l'activation du paramètre.

Depuis ONTAP 9.14.1, ONTAP introduit un algorithme qui déplace les fichiers de manière proactive et sans interruption dans des volumes pour lesquels les données granulaires sont activées sans interaction de l'utilisateur. L'algorithme fonctionne dans des scénarios très spécifiques et ciblés afin d'atténuer les goulots d'étranglement des performances. Les scénarios dans lesquels cet algorithme peut agir incluent une charge d'écriture très élevée sur un ensemble de fichiers particulier sur un nœud du cluster ou un fichier en constante expansion dans un répertoire parent très actif.

### Considérations relatives au rééquilibrage FlexGroup

Il est important de connaître le fonctionnement du rééquilibrage FlexGroup et son interaction avec d'autres fonctionnalités de ONTAP.

- Conversion FlexVol en FlexGroup

Il est recommandé de *pas* utiliser le rééquilibrage automatique FlexGroup après une conversion FlexVol en FlexGroup. Vous pouvez utiliser la fonctionnalité de déplacement de fichier avec effet rétroactif disruptive disponible dans ONTAP 9.10.1 et versions ultérieures, en entrant le volume `rebalance file-move` commande. Pour la syntaxe de commande, voir `volume rebalance file-move start` page de manuel.

Le rééquilibrage avec la fonction de rééquilibrage automatique des FlexGroup peut dégrader les performances lors du déplacement d'un grand nombre de fichiers, par exemple lorsque vous effectuez une conversion FlexVol vers FlexGroup, et jusqu'à 50 à 85 % des données du volume FlexVol sont déplacées vers un nouveau composant.

- Taille minimale et maximale du fichier

La sélection de fichiers pour le rééquilibrage automatique est basée sur les blocs enregistrés. La taille de fichier minimale prise en compte pour le rééquilibrage est de 100 Mo par défaut (elle peut être configurée à 20 Mo à l'aide du paramètre de taille de fichier min illustré ci-dessous) et la taille de fichier maximale est de 100 Go.

- Fichiers dans des copies Snapshot

Vous pouvez configurer le rééquilibrage FlexGroup pour tenir compte uniquement des fichiers qui ne sont actuellement présents dans aucune copie Snapshot. Au démarrage du rééquilibrage, une notification s'affiche si une opération de copie Snapshot est planifiée à tout moment au cours d'une opération de rééquilibrage.

Les copies snapshot sont restreintes si un fichier est en cours de déplacement et est en cours de cadrage au niveau de la destination. Une opération de restauration de copie Snapshot n'est pas autorisée tant que le rééquilibrage des fichiers est en cours.

Toute copie Snapshot créée après l'activation de l' `granular-data` option ne peut pas être répliquée sur un système exécutant ONTAP 9.11.1 et les versions antérieures, car ONTAP 9.11.1 et les versions antérieures ne prennent pas en charge les inodes en plusieurs parties.

- Opérations SnapMirror

Le rééquilibrage de la FlexGroup doit avoir lieu entre les opérations SnapMirror planifiées. Une opération SnapMirror peut échouer si un fichier est déplacé avant une opération SnapMirror démarre si ce déplacement de fichier ne se termine pas dans une période de 24 minutes. Tout nouveau déplacement de fichier qui commence après le démarrage du transfert SnapMirror n'échoue pas.

- Efficacité du stockage par compression basée sur des fichiers

Avec l'efficacité du stockage en compression basée sur les fichiers, le fichier est décompressé avant son déplacement vers la destination, ce qui entraîne une perte des économies en termes de compression. Les économies de compression sont reobtenues après l'exécution d'un scanner en arrière-plan manuel sur le volume FlexGroup après le rééquilibrage. Cependant, si un fichier est associé à une copie Snapshot sur un volume, ce fichier est ignoré pour la compression.

- Déduplication

Le déplacement des fichiers dédupliqués peut augmenter l'utilisation globale du volume FlexGroup. Lors du rééquilibrage des fichiers, seuls les blocs uniques sont déplacés vers la destination, ce qui libère cette capacité sur la source. Les blocs partagés restent à la source et sont copiés vers la destination. Cela permet de réduire la capacité utilisée sur un composant à source presque complète. Cependant, cela peut également entraîner une augmentation de l'utilisation globale du volume FlexGroup grâce à des copies de blocs partagés sur les nouvelles destinations. Cela est également possible lorsque les fichiers qui font partie d'une copie Snapshot sont déplacés. Les économies d'espace ne sont pas entièrement reconnues avant le recyclage des copies Snapshot et l'absence de copie des fichiers dans des copies Snapshot.

- Volumes FlexClone

Si un rééquilibrage des fichiers est en cours lors de la création d'un volume FlexClone, le rééquilibrage ne sera pas effectué sur le volume FlexClone. Le rééquilibrage du volume FlexClone doit être effectué après sa création.

- Déplacement de fichier

Lorsqu'un fichier est déplacé au cours d'une opération de rééquilibrage FlexGroup, la taille de fichier est indiquée dans le cadre de quotas comptables des composants source et de destination. Une fois le déplacement terminé, la comptabilisation des quotas revient à normal et la taille du fichier est uniquement signalée sur la nouvelle destination.

- Protection autonome contre les ransomwares

Depuis la version ONTAP 9.13.1, la protection anti-ransomware autonome est prise en charge lors des opérations de rééquilibrage fluide et sans interruption.

- Volumes de magasin d'objets

Le rééquilibrage de la capacité des volumes n'est pas pris en charge sur les volumes de magasin d'objets tels que les compartiments S3.

### Activez le rééquilibrage FlexGroup

À partir de ONTAP 9.12.1, vous pouvez activer le rééquilibrage automatique des volumes FlexGroup sans interruption pour redistribuer les fichiers entre les composants FlexGroup.

À partir de ONTAP 9.13.1, vous pouvez planifier une seule opération de rééquilibrage FlexGroup pour commencer à une date et une heure à l'avenir.

### Avant de commencer


Vous devez avoir activé `granular-data` Option sur le volume FlexGroup avant l'activation du rééquilibrage FlexGroup. Vous pouvez l'activer en utilisant l'une des méthodes suivantes :

- Lorsque vous créez un volume FlexGroup à l'aide de `volume create` commande
- En modifiant un volume FlexGroup existant pour activer le paramètre à l'aide de `volume modify` commande
- Configuration automatique du système lorsque le rééquilibrage FlexGroup est lancé à l'aide du `volume rebalance` commande

### Étapes

Vous pouvez gérer le rééquilibrage des FlexGroup à l'aide de ONTAP System Manager ou de l'interface de ligne de commande ONTAP.

## System Manager

1. Naviguez jusqu'à **stockage > volumes** et localisez le volume FlexGroup à rééquilibrer.
2. Sélectionnez  pour afficher les détails du volume.
3. Sous **État solde FlexGroup**, sélectionnez **rééquilibrage**.



L'option **rééquilibrage** n'est disponible que lorsque l'état FlexGroup est hors solde.

4. Dans la fenêtre **Rebalance Volume**, modifiez les paramètres par défaut selon vos besoins.
5. Pour planifier l'opération de rééquilibrage, sélectionnez **rééquilibrer plus tard** et entrez la date et l'heure.

## CLI

1. Démarrer le rééquilibrage automatique : `volume rebalance start -vserver SVM_name -volume volume_name`

Vous pouvez également spécifier les options suivantes :

`[[ -max-runtime <time interval> ]` exécution maximale

`[ -max-Threshold <percent> ]` seuil de déséquilibre maximum par constituant

`[ -<percent>-seuil-min ]` Seuil de déséquilibre minimal par composant

`[ -max-file-Moves <integer> ]` nombre maximal de déplacements simultanés de fichiers par composant

`[ -min-file-size {<integer>[KB|MB|GB|TB|PB]} ]` taille minimale du fichier

`[ -START-Time <mm/dd/yyyy-00:00:00> ]` Date et heure de début du rééquilibrage de la planification

`[ -exclude-snapshots {true|false} ]` exclure les fichiers bloqués dans les copies Snapshot


Exemple :

```
volume rebalance start -vserver vs0 -volume fg1
```

## Modifier les configurations FlexGroup rééquilibrées

Vous pouvez modifier une configuration de rééquilibrage FlexGroup pour mettre à jour le seuil de déséquilibre, la quantité de fichiers simultanés ayant la taille minimale, l'exécution maximale et pour inclure ou exclure des copies Snapshot. Des options pour modifier votre calendrier de rééquilibrage FlexGroup sont disponibles à partir de ONTAP 9.13.1.

### System Manager

1. Naviguez jusqu'à **stockage > volumes** et localisez le volume FlexGroup à rééquilibrer.
2. Sélectionnez  pour afficher les détails du volume.
3. Sous **État solde FlexGroup**, sélectionnez **rééquilibrage**.



L'option **rééquilibrage** n'est disponible que lorsque l'état FlexGroup est hors solde.

4. Dans la fenêtre **Rebalance Volume**, modifiez les paramètres par défaut selon vos besoins.

### CLI

1. Modifier le rééquilibrage automatique : `volume rebalance modify -vserver SVM_name -volume volume_name`

Vous pouvez spécifier une ou plusieurs des options suivantes :

`[-max-runtime] <time interval>` exécution maximale

`[-max-Threshold <percent>]` seuil de déséquilibre maximum par constituant

`[-<percent>-seuil-min]` Seuil de déséquilibre minimal par composant

`[-max-file-Moves <integer>]` nombre maximal de déplacements simultanés de fichiers par composant

`[-min-file-size {<integer>[KB|MB|GB|TB|PB]}]` taille minimale du fichier


`[-START-Time <mm/dd/yyyy-00:00:00>]` Date et heure de début du rééquilibrage de la planification

`[-exclude-snapshots {true|false}]` exclure les fichiers bloqués dans les copies Snapshot

### Arrêter le rééquilibrage FlexGroup

Une fois le rééquilibrage FlexGroup activé ou planifié, vous pouvez l'arrêter à tout moment.

### System Manager

1. Accédez à **stockage > volumes** et recherchez le volume FlexGroup.
2. Sélectionnez  pour afficher les détails du volume.
3. Sélectionnez **Arrêter le rééquilibrage**.


### CLI

1. Arrêter le rééquilibrage FlexGroup : `volume rebalance stop -vserver SVM_name -volume volume_name`

### Afficher l'état de rééquilibrage FlexGroup

Vous pouvez afficher le statut d'une opération FlexGroup Rérééquilibrage, la configuration FlexGroup Rérééquilibrage, le temps d'opération Rérééquilibrage et les détails de l'instance de rééquilibrage.

## System Manager

1. Accédez à **stockage > volumes** et recherchez le volume FlexGroup.
2. Sélectionnez  pour afficher les détails de FlexGroup.
3. **Statut solde FlexGroup** s'affiche en bas du volet de détails.
4. Pour afficher des informations sur la dernière opération de rééquilibrage, sélectionnez **Etat du dernier rééquilibrage de volume**.

## CLI

1. Afficher le statut d'une opération de rééquilibrage FlexGroup : `volume rebalance show`

Exemple d'état de rééquilibrage :

```
> volume rebalance show
Vserver: vs0

Imbalance
Volume State Total Used Target
Size %

fg1 idle 4GB 115.3MB -
8KB 0%
```

Exemple de détails de configuration du rééquilibrage :

```
> volume rebalance show -config
Vserver: vs0

Min Max Threshold Max
Volume Exclude Runtime Min Max File Moves
File Size Snapshot

fg1 6h0m0s 5% 20% 25
4KB true
```

Exemple de détails de l'heure de rééquilibrage :



```
> volume rebalance show -time
Vserver: vs0
Volume Start Time Runtime
Max Runtime

fgl Wed Jul 20 16:06:11 2022 0h1m16s
6h0m0s
```

Exemple de détails d'instance de rééquilibrage :

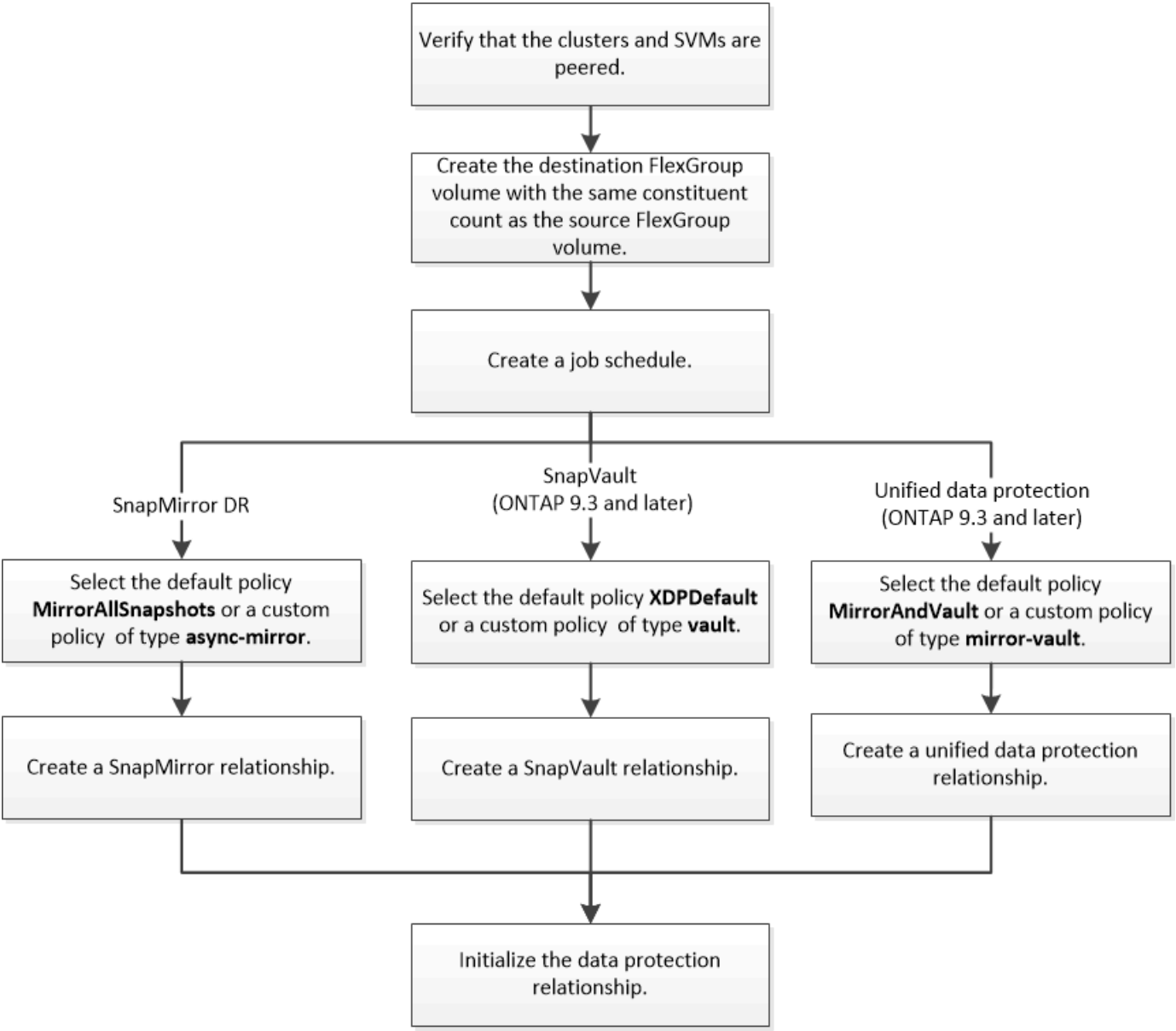
```
> volume rebalance show -instance
Vserver Name: vs0
Volume Name: fgl
Is Constituent: false
Rebalance State: idle
Rebalance Notice Messages: -
Total Size: 4GB
AFS Used Size: 115.3MB
Constituent Target Used Size: -
Imbalance Size: 8KB
Imbalance Percentage: 0%
Moved Data Size: -
Maximum Constituent Imbalance Percentage: 1%
Rebalance Start Time: Wed Jul 20 16:06:11 2022
Rebalance Stop Time: -
Rebalance Runtime: 0h1m32s
Rebalance Maximum Runtime: 6h0m0s
Maximum Imbalance Threshold per Constituent: 20%
Minimum Imbalance Threshold per Constituent: 5%
Maximum Concurrent File Moves per Constituent: 25
Minimum File Size: 4KB
Exclude Files Stuck in Snapshot Copies: true
```

## Protection des données pour les volumes FlexGroup

### Workflow de protection des données pour les volumes FlexGroup

Vous pouvez créer des relations SnapMirror de reprise après incident pour les volumes FlexGroup. Depuis ONTAP 9.3, vous pouvez aussi sauvegarder et restaurer des volumes FlexGroup à l'aide de la technologie SnapVault. De plus, vous pouvez créer une relation unifiée de protection des données qui utilise la même destination pour la sauvegarde et la reprise après incident.

Le workflow de protection des données consiste à vérifier les relations entre le cluster et le SVM peer, à créer un volume de destination, à créer une planification des tâches, à spécifier une politique, à créer une relation de protection des données et à initialiser la relation.



**Description de la tâche**

Le type de relation SnapMirror est toujours XDP Pour les volumes FlexGroup. Le type de protection des données fourni par une relation SnapMirror est déterminé par la règle de réplication que vous utilisez. Vous pouvez utiliser la règle par défaut ou une règle personnalisée du type requis pour la relation de réplication que vous souhaitez créer. Le tableau ci-dessous présente les types de règles par défaut et les types de règles personnalisées pris en charge pour différents types de relations de protection des données.

| Type de relation                | Stratégie par défaut | Type de règle personnalisée |
|---------------------------------|----------------------|-----------------------------|
| Reprise sur incident SnapMirror | MirrorAllsnapshots   | mise en miroir asynchrone   |
| Sauvegarde SnapVault            | XDPDefault           | coffre-fort                 |

|                                |                |             |
|--------------------------------|----------------|-------------|
| Protection unifiée des données | MirrorAndVault | coffre-fort |
|--------------------------------|----------------|-------------|

La stratégie MirrorLeste n'est pas prise en charge avec les volumes FlexGroup.

### Créer une relation SnapMirror pour les volumes FlexGroup

Vous pouvez créer une relation SnapMirror entre le volume FlexGroup source et le volume FlexGroup de destination sur un SVM peering pour la réplication des données en vue de la reprise sur incident. Vous pouvez utiliser les copies en miroir du volume FlexGroup pour restaurer des données en cas d'incident.

#### Ce dont vous avez besoin

Vous devez avoir créé la relation de peering de cluster et la relation de SVM peering.

#### ["Cluster et SVM peering"](#)

#### Description de la tâche

- Vous pouvez créer à la fois des relations SnapMirror intercluster et des relations SnapMirror intracluster pour les volumes FlexGroup.
- Depuis ONTAP 9.3, vous pouvez étendre les volumes FlexGroup faisant partie d'une relation SnapMirror.

Si vous utilisez une version d'ONTAP antérieure à ONTAP 9.3, vous ne devez pas étendre les volumes FlexGroup après l'établissement d'une relation SnapMirror. Toutefois, vous pouvez augmenter la capacité des volumes FlexGroup après avoir établi une relation SnapMirror. Si vous développez le volume FlexGroup source après avoir rompu la relation SnapMirror dans des versions antérieures à ONTAP 9.3, vous devez effectuer un transfert de base vers le volume FlexGroup de destination.

#### Étapes

1. Créer un volume FlexGroup de type destination DP Avec le même nombre de composants que celui du volume FlexGroup source :
  - a. Depuis le cluster source, déterminer le nombre de composants du volume FlexGroup source : `volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show -volume srcFG* -is-constituent true
```

| Vserver   | Volume      | Aggregate  | State  | Type | Size  |
|-----------|-------------|------------|--------|------|-------|
| Available | Used%       |            |        |      |       |
| vss       | srcFG       | -          | online | RW   | 400TB |
| 172.86GB  | 56%         |            |        |      |       |
| vss       | srcFG__0001 | Aggr_cmode | online | RW   | 25GB  |
| 10.86TB   | 56%         |            |        |      |       |
| vss       | srcFG__0002 | aggr1      | online | RW   | 25TB  |
| 10.86TB   | 56%         |            |        |      |       |
| vss       | srcFG__0003 | Aggr_cmode | online | RW   | 25TB  |
| 10.72TB   | 57%         |            |        |      |       |
| vss       | srcFG__0004 | aggr1      | online | RW   | 25TB  |
| 10.73TB   | 57%         |            |        |      |       |
| vss       | srcFG__0005 | Aggr_cmode | online | RW   | 25TB  |
| 10.67TB   | 57%         |            |        |      |       |
| vss       | srcFG__0006 | aggr1      | online | RW   | 25TB  |
| 10.64TB   | 57%         |            |        |      |       |
| vss       | srcFG__0007 | Aggr_cmode | online | RW   | 25TB  |
| 10.63TB   | 57%         |            |        |      |       |
| ...       |             |            |        |      |       |

- b. Depuis le cluster de destination, créez un volume FlexGroup de type destination DP Avec le même nombre de composants que celui du volume FlexGroup source.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG
```

Warning: The FlexGroup volume "dstFG" will be created with the following number of constituents of size 25TB: 16.

Do you want to continue? {y|n}: y

[Job 766] Job succeeded: Successful

- c. Depuis le cluster de destination, vérifiez le nombre de composants du volume FlexGroup de destination :
- ```
volume show -volume volume_name* -is-constituent true
```

```
cluster2::> volume show -volume dstFG* -is-constituent true
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
-----	-----	-----	-----	----	-----
-----	-----				
vsd	dstFG	-	online	DP	400TB
172.86GB	56%				
vsd	dstFG__0001	Aggr_cmode	online	DP	25GB
10.86TB	56%				
vsd	dstFG__0002	aggr1	online	DP	25TB
10.86TB	56%				
vsd	dstFG__0003	Aggr_cmode	online	DP	25TB
10.72TB	57%				
vsd	dstFG__0004	aggr1	online	DP	25TB
10.73TB	57%				
vsd	dstFG__0005	Aggr_cmode	online	DP	25TB
10.67TB	57%				
vsd	dstFG__0006	aggr1	online	DP	25TB
10.64TB	57%				
vsd	dstFG__0007	Aggr_cmode	online	DP	25TB
10.63TB	57%				
...					

2. Création d'un programme de travail : `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

Pour le `-month`, `-dayofweek`, et `-hour` vous pouvez spécifier des options `all` pour exécuter le travail tous les mois, tous les jours de la semaine et toutes les heures, respectivement.

L'exemple suivant crée un programme de travail nommé `my_weekly` Le samedi à 3:00 :

```
cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

3. Création d'une règle de type personnalisée `async-mirror` Pour la relation `SnapMirror` : `snapmirror policy create -vserver SVM -policy snapmirror_policy -type async-mirror`

Si vous ne créez pas de stratégie personnalisée, vous devez spécifier le `MirrorAllSnapshots` Règle pour les relations `SnapMirror`.

4. Depuis le cluster de destination, créer une relation `SnapMirror` entre le volume `FlexGroup` source et le volume `FlexGroup` de destination : `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -policy snapmirror_policy -schedule sched_name`

Les relations `SnapMirror` pour les volumes `FlexGroup` doivent être de type `XDP`.

Si vous spécifiez une valeur de papillon pour la relation SnapMirror pour le volume FlexGroup, chaque composant utilise la même valeur de papillon. La valeur de l'accélérateur n'est pas divisée entre les constituants.



Vous ne pouvez pas utiliser les étiquettes SnapMirror des copies Snapshot pour les volumes FlexGroup.

Dans ONTAP 9.4 et versions antérieures, si la politique n'est pas spécifiée avec le `snapmirror create` commande, le `MirrorAllSnapshots` la règle est utilisée par défaut. Dans ONTAP 9.5, si la politique n'est pas spécifiée avec le `snapmirror create` commande, le `MirrorAndVault` la règle est utilisée par défaut.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path  
vsd:dstFG -type XDP -policy MirrorAllSnapshots -schedule hourly  
Operation succeeded: snapmirror create for the relationship with  
destination "vsd:dstFG".
```

5. Depuis le cluster destination, initialiser la relation SnapMirror en effectuant un transfert de base :

```
snapmirror initialize -destination-path dest_svm:dest_flexgroup
```

Une fois le transfert de base terminé, le volume FlexGroup de destination est mis à jour régulièrement en fonction du calendrier de la relation SnapMirror.

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG  
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```



Si vous avez créé une relation SnapMirror entre des volumes FlexGroup avec le cluster source exécutant ONTAP 9.3 et le cluster de destination exécutant ONTAP 9.2 ou version antérieure, et si vous créez des qtrees sur le volume FlexGroup source, la mise à jour de SnapMirror échoue. Pour effectuer une restauration à partir de cette situation, vous devez supprimer tous les qtrees non par défaut du volume FlexGroup, désactiver la fonctionnalité qtree sur le volume FlexGroup, puis supprimer toutes les copies Snapshot activées avec la fonctionnalité qtree. Vous devez également effectuer ces étapes avant de restaurer de ONTAP 9.3 vers une version antérieure de ONTAP, si la fonctionnalité qtree est activée sur les volumes FlexGroup. ["Désactivez la fonctionnalité qtree dans les volumes FlexGroup avant de procéder au rétablissement"](#).

Une fois que vous avez terminé

Il est important de configurer le SVM de destination pour l'accès aux données en configurant les configurations requises telles que les LIF et les export policy.

Créer une relation SnapVault pour les volumes FlexGroup

Vous pouvez configurer une relation SnapVault et attribuer une policy SnapVault à cette relation pour créer une sauvegarde SnapVault.

Ce dont vous avez besoin

Notez les éléments à prendre en compte lors de la création d'une relation SnapVault pour les volumes

FlexGroup.

Étapes

1. Créer un volume FlexGroup de type destination DP Avec le même nombre de composants que celui du volume FlexGroup source :
 - a. Depuis le cluster source, déterminer le nombre de composants du volume FlexGroup source : `volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show -volume src* -is-constituent true
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
-----	-----	-----	-----	----	-----
-----	-----				
vss	src	-	online	RW	400TB
172.86GB	56%				
vss	src__0001	Aggr_cmode	online	RW	25GB
10.86TB	56%				
vss	src__0002	aggr1	online	RW	25TB
10.86TB	56%				
vss	src__0003	Aggr_cmode	online	RW	25TB
10.72TB	57%				
vss	src__0004	aggr1	online	RW	25TB
10.73TB	57%				
vss	src__0005	Aggr_cmode	online	RW	25TB
10.67TB	57%				
vss	src__0006	aggr1	online	RW	25TB
10.64TB	57%				
vss	src__0007	Aggr_cmode	online	RW	25TB
10.63TB	57%				
...					

- b. Depuis le cluster de destination, créez un volume FlexGroup de type destination DP Avec le même nombre de composants que celui du volume FlexGroup source.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dst

Warning: The FlexGroup volume "dst" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful
```

- c. Depuis le cluster de destination, vérifiez le nombre de composants du volume FlexGroup de destination : `volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show -volume dst* -is-constituent true
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
vsd	dst	-	online	RW	400TB
172.86GB	56%				
vsd	dst__0001	Aggr_cmode	online	RW	25GB
10.86TB	56%				
vsd	dst__0002	aggr1	online	RW	25TB
10.86TB	56%				
vsd	dst__0003	Aggr_cmode	online	RW	25TB
10.72TB	57%				
vsd	dst__0004	aggr1	online	RW	25TB
10.73TB	57%				
vsd	dst__0005	Aggr_cmode	online	RW	25TB
10.67TB	57%				
vsd	dst__0006	aggr1	online	RW	25TB
10.64TB	57%				
vsd	dst__0007	Aggr_cmode	online	RW	25TB
10.63TB	57%				
...					

2. Création d'un programme de travail : `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

Pour `-month`, `-dayofweek`, et `-hour`, vous pouvez spécifier `all` pour exécuter le travail chaque mois, jour de la semaine et heure, respectivement.

L'exemple suivant crée un programme de travail nommé `my_weekly` Le samedi à 3:00 :

```
cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

3. Création d'une policy SnapVault, puis définition d'une règle pour la policy SnapVault :

- a. Création d'une règle de type personnalisée `vault` Pour la relation SnapVault : `snapmirror policy create -vserver svm_name -policy policy_name -type vault`
- b. Définissez une règle pour la politique de SnapVault qui détermine les copies Snapshot transférées pendant les opérations d'initialisation et de mise à jour : `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

Si vous ne créez pas de stratégie personnalisée, vous devez spécifier le `XDPDefault` Règle pour les relations SnapVault.

4. Création d'une relation SnapVault : `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name -policy XDPDefault`

Dans ONTAP 9.4 et versions antérieures, si la politique n'est pas spécifiée avec le `snapmirror create` commande, le `MirrorAllSnapshots` la règle est utilisée par défaut. Dans ONTAP 9.5, si la politique n'est pas spécifiée avec le `snapmirror create` commande, le `MirrorAndVault` la règle est utilisée par défaut.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path  
vsd:dstFG -type XDP -schedule Daily -policy XDPDefault
```

5. Depuis le cluster destination, initialiser la relation SnapVault en effectuant un transfert de base :
`snapmirror initialize -destination-path dest_svm:dest_flexgroup`

```
cluster2::> snapmirror initialize -destination-path vsd:dst  
Operation is queued: snapmirror initialize of destination "vsd:dst".
```

Créez une relation unifiée de protection des données pour les volumes FlexGroup

Depuis ONTAP 9.3, vous pouvez créer et configurer des relations de protection des données unifiées SnapMirror pour configurer la reprise après incident et l'archivage sur le même volume de destination.

Ce dont vous avez besoin

Il est à prendre en compte les considérations relatives à la création de relations unifiées de protection des données pour les volumes FlexGroup.

["Considérations relatives à la création d'une relation de sauvegarde SnapVault et d'une relation unifiée de protection des données pour les volumes FlexGroup"](#)

Étapes

1. Créer un volume FlexGroup de type destination `DP` Avec le même nombre de composants que celui du volume FlexGroup source :
 - a. Depuis le cluster source, déterminer le nombre de composants du volume FlexGroup source : `volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show -volume srcFG* -is-constituent true
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
vss	srcFG	-	online	RW	400TB
172.86GB	56%				
vss	srcFG__0001	Aggr_cmode	online	RW	25GB
10.86TB	56%				
vss	srcFG__0002	aggr1	online	RW	25TB
10.86TB	56%				
vss	srcFG__0003	Aggr_cmode	online	RW	25TB
10.72TB	57%				
vss	srcFG__0004	aggr1	online	RW	25TB
10.73TB	57%				
vss	srcFG__0005	Aggr_cmode	online	RW	25TB
10.67TB	57%				
vss	srcFG__0006	aggr1	online	RW	25TB
10.64TB	57%				
vss	srcFG__0007	Aggr_cmode	online	RW	25TB
10.63TB	57%				
...					

- b. Depuis le cluster de destination, créez un volume FlexGroup de type destination DP Avec le même nombre de composants que celui du volume FlexGroup source.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG
```

Warning: The FlexGroup volume "dstFG" will be created with the following number of constituents of size 25TB: 16.

Do you want to continue? {y|n}: y

[Job 766] Job succeeded: Successful

- c. Depuis le cluster de destination, vérifiez le nombre de composants du volume FlexGroup de destination :
- ```
volume show -volume volume_name* -is-constituent true
```

```
cluster2::> volume show -volume dstFG* -is-constituent true
```

| Vserver   | Volume      | Aggregate  | State  | Type  | Size  |
|-----------|-------------|------------|--------|-------|-------|
| Available | Used%       |            |        |       |       |
| -----     | -----       | -----      | -----  | ----- | ----- |
| vsd       | dstFG       | -          | online | RW    | 400TB |
| 172.86GB  | 56%         |            |        |       |       |
| vsd       | dstFG__0001 | Aggr_cmode | online | RW    | 25GB  |
| 10.86TB   | 56%         |            |        |       |       |
| vsd       | dstFG__0002 | aggr1      | online | RW    | 25TB  |
| 10.86TB   | 56%         |            |        |       |       |
| vsd       | dstFG__0003 | Aggr_cmode | online | RW    | 25TB  |
| 10.72TB   | 57%         |            |        |       |       |
| vsd       | dstFG__0004 | aggr1      | online | RW    | 25TB  |
| 10.73TB   | 57%         |            |        |       |       |
| vsd       | dstFG__0005 | Aggr_cmode | online | RW    | 25TB  |
| 10.67TB   | 57%         |            |        |       |       |
| vsd       | dstFG__0006 | aggr1      | online | RW    | 25TB  |
| 10.64TB   | 57%         |            |        |       |       |
| vsd       | dstFG__0007 | Aggr_cmode | online | RW    | 25TB  |
| 10.63TB   | 57%         |            |        |       |       |
| ...       |             |            |        |       |       |

2. Création d'un programme de travail : `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

Pour le `-month`, `-dayofweek`, et `-hour` vous pouvez spécifier des options `all` pour exécuter le travail tous les mois, tous les jours de la semaine et toutes les heures, respectivement.

L'exemple suivant crée un programme de travail nommé `my_weekly` Le samedi à 3:00 :

```
cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

3. Création d'une règle de type personnalisée `mirror-vault`, puis définissez une règle pour la stratégie de miroir et de coffre-fort:

- a. Création d'une règle de type personnalisée `mirror-vault` pour la relation unifiée de protection des données : `snapmirror policy create -vserver svm_name -policy policy_name -type mirror-vault`
- b. Définissez une règle pour la stratégie de mise en miroir et de copie à distance qui détermine les copies Snapshot transférées pendant les opérations d'initialisation et de mise à jour : `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

Si vous ne spécifiez pas de stratégie personnalisée, le `MirrorAndVault` il est utilisé pour les relations de

protection des données unifiées,

4. Créer une relation unifiée de protection des données : `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name -policy MirrorAndVault`

Dans ONTAP 9.4 et versions antérieures, si la politique n'est pas spécifiée avec le `snapmirror create` commande, le `MirrorAllSnapshots` la règle est utilisée par défaut. Dans ONTAP 9.5, si la politique n'est pas spécifiée avec le `snapmirror create` commande, le `MirrorAndVault` la règle est utilisée par défaut.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path
vsd:dstFG -type XDP -schedule Daily -policy MirrorAndVault
```

5. Depuis le cluster destination, initialiser la relation de protection des données unifiée en effectuant un transfert de base : `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```

## Création d'une relation de reprise après incident de SVM pour les volumes FlexGroup

Depuis la version ONTAP 9.9.1, vous pouvez créer des relations SVM de reprise après incident à l'aide de volumes FlexGroup. Une relation SVM DR assure la redondance et la restauration de FlexGroups en cas d'incident via la synchronisation et la réplication de la configuration du SVM et de ses données. Une licence SnapMirror est requise pour SVM DR.

### Avant de commencer

Vous *ne pouvez pas* créer une relation de SVM DR FlexGroup avec les appliquer suivantes.

- Une configuration FlexGroup FlexClone existe
- Le volume FlexGroup fait partie d'une relation en cascade
- Le volume FlexGroup fait partie d'une relation de type « éventail » et votre cluster exécute une version ONTAP antérieure à ONTAP 9.12.1. (À partir de ONTAP 9.13.1, les relations de type « éventail » sont prises en charge.)

### Description de la tâche

- Tous les nœuds des deux clusters doivent exécuter la même version de ONTAP que le nœud sur lequel la prise en charge SVM DR a été ajoutée (ONTAP 9.9.1 ou version ultérieure).
- La relation de SVM DR entre les sites primaire et secondaire doit être saine et disposer d'un espace suffisant pour prendre en charge les volumes FlexGroup sur les SVM principal et secondaire.
- À partir de ONTAP 9.12.1, FabricPool, FlexGroup et SVM DR peuvent fonctionner conjointement. Dans les versions antérieures à ONTAP 9.12.1, chacune de ces fonctionnalités fonctionnait ensemble, mais les trois n'en ont pas toutes ensemble.
- Lorsque vous créez une relation SVM DR FlexGroup dans laquelle le volume FlexGroup fait partie d'une

relation de type « out », vous devez connaître les conditions suivantes :

- Le cluster source et le cluster destination doivent exécuter ONTAP 9.13.1 ou une version ultérieure.
- SVM DR avec volumes FlexGroup prend en charge les relations de ventilateur SnapMirror vers huit sites.

Pour plus d'informations sur la création d'une relation de SVM DR, reportez-vous à ["Gérer la réplication de SVM SnapMirror"](#) la section .

### Étapes

1. Créez une relation de SVM DR ou utilisez une relation existante.

["Réplication de l'ensemble d'une configuration de SVM"](#)

2. Créez un volume FlexGroup sur le site principal avec le nombre de composants requis.

["Création d'un volume FlexGroup"](#).

Attendez que FlexGroup et tous ses composants soient créés avant de continuer.

3. Pour répliquer le volume FlexGroup, mettez à jour le SVM sur le site secondaire : `snapmirror update -destination-path destination_svm_name: -source-path source_svm_name:`

Vous pouvez également vérifier si une mise à jour SnapMirror planifiée existe déjà en saisissant `snapmirror show -fields schedule`

4. Depuis le site secondaire, vérifiez que la relation SnapMirror fonctionne correctement : `snapmirror show`

```
cluster2::> snapmirror show
```

| Progress |      |             |              |              |          |         |   |
|----------|------|-------------|--------------|--------------|----------|---------|---|
| Source   |      | Destination | Mirror       | Relationship | Total    |         |   |
| Last     |      |             |              |              |          |         |   |
| Path     | Type | Path        | State        | Status       | Progress | Healthy |   |
| Updated  |      |             |              |              |          |         |   |
| -----    | ---- | -----       | -----        | -----        | -----    | -----   |   |
| -----    |      |             |              |              |          |         |   |
| vs1:     | XDP  | vs1_dst:    | Snapmirrored |              |          |         |   |
|          |      |             | Idle         |              | -        | true    | - |

5. Depuis le site secondaire, vérifiez que le nouveau volume FlexGroup et ses composants sont présents : `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

| Source           | Destination              | Mirror       | Relationship | Total | Progress | Healthy |
|------------------|--------------------------|--------------|--------------|-------|----------|---------|
| Last Path        | Type Path                | State        | Status       |       |          |         |
| vs1:             | XDP vs1_dst:             | Snapmirrored | Idle         | -     | true     | -       |
| vs1:fg_src       | XDP vs1_dst:fg_src       | Snapmirrored | Idle         | -     | true     | -       |
| vs1:fg_src__0001 | XDP vs1_dst:fg_src__0001 | Snapmirrored | Idle         | -     | true     | -       |
| vs1:fg_src__0002 | XDP vs1_dst:fg_src__0002 | Snapmirrored | Idle         | -     | true     | -       |
| vs1:fg_src__0003 | XDP vs1_dst:fg_src__0003 | Snapmirrored | Idle         | -     | true     | -       |
| vs1:fg_src__0004 | XDP vs1_dst:fg_src__0004 | Snapmirrored | Idle         | -     | true     | -       |

6 entries were displayed.

## Effectuer la transition d'une relation FlexGroup SnapMirror existante vers une reprise après incident de SVM

Vous pouvez créer une relation de FlexGroup SVM DR en migrant une relation SnapMirror volume FlexGroup existante.

### Ce dont vous avez besoin

- La relation SnapMirror volume FlexGroup est en état de santé.
- Les volumes FlexGroup source et destination ont le même nom.

### Étapes

1. Depuis la destination SnapMirror, resynchroniser la relation SnapMirror de niveau FlexGroup :  

```
snapmirror resync
```

2. Création de la relation SnapMirror SVM DR FlexGroup Utilisez la même règle SnapMirror que celle configurée sur les relations FlexGroup volume SnapMirror : `snapmirror create -destination -path dest_svm: -source-path src_svm: -identity-preserve true -policy MirrorAllSnapshots`



Vous devez utiliser le `-identity-preserve true` de la `snapmirror create` commande lorsque vous créez votre relation de réplication.

3. Vérifiez que la relation est rompue : `snapmirror show -destination-path dest_svm: -source-path src_svm:`

```
snapmirror show -destination-path fg_vs_renamed: -source-path fg_vs:
```

Progress

| Source  |      | Destination     | Mirror | Relationship | Total    |         |
|---------|------|-----------------|--------|--------------|----------|---------|
| Last    |      |                 |        |              |          |         |
| Path    | Type | Path            | State  | Status       | Progress | Healthy |
| Updated |      |                 |        |              |          |         |
| -----   | ---- | -----           | -----  | -----        | -----    | -----   |
| -----   |      |                 |        |              |          |         |
| fg_vs:  | XDP  | fg_vs1_renamed: |        | Broken-off   |          |         |
|         |      |                 |        | Idle         | -        | true -  |

4. Arrêter le SVM de destination : `vserver stop -vserver vs_name`

```
vserver stop -vserver fg_vs_renamed
[Job 245] Job is queued: Vserver Stop fg_vs_renamed.
[Job 245] Done
```

5. Resynchroniser la relation SVM SnapMirror : `snapmirror resync -destination-path dest_svm: -source-path src_svm:`

```
snapmirror resync -destination-path fg_vs_renamed: -source-path fg_vs:
Warning: This Vserver has volumes which are the destination of FlexVol
or FlexGroup SnapMirror relationships. A resync on the Vserver
SnapMirror relationship will cause disruptions in data access
```

6. Vérifier que la relation SnapMirror au niveau du SVM DR atteint un état inactif sain : `snapmirror show -expand`
7. Vérifier que la relation de FlexGroup SnapMirror est bien en état : `snapmirror show`

## Conversion d'un volume FlexVol en volume FlexGroup au sein d'une relation SVM-DR

Depuis ONTAP 9.10.1, vous pouvez convertir un volume FlexVol en volume FlexGroup sur une source SVM-DR.

### Ce dont vous avez besoin

- Le volume FlexVol en cours de conversion doit être en ligne.
- Les opérations et les configurations du volume FlexVol doivent être compatibles avec le processus de conversion.

Un message d'erreur est généré si le volume FlexVol est incompatible et que la conversion de volume est annulée. Vous pouvez effectuer des actions correctives et recommencer la conversion.

Pour plus de détails, voir ["Considérations relatives à la conversion de volumes FlexVol en volumes FlexGroup"](#)

### Étapes

1. Connexion en mode privilèges avancés : `set -privilege advanced`
2. Depuis la destination, mettre à jour la relation SVM-DR :

```
snapmirror update -destination-path <destination_svm_name>: -source-path <source_svm_name>:
```



Vous devez entrer deux-points (:) après le nom du SVM dans l' `-destination-path` option.

3. S'assurer que la relation SVM-DR est dans un état sous SnapMirror et qu'elle n'est pas supprimée :

```
snapmirror show
```

4. Depuis le SVM de destination, vérifier que le volume FlexVol est prêt pour la conversion :

```
volume conversion start -vserver <svm_name> -volume <vol_name> -check -only true
```

Si cette commande génère des erreurs autres que « il s'agit d'un volume SVMDR de destination », vous pouvez prendre l'action corrective appropriée, exécuter de nouveau la commande et poursuivre la conversion.

5. Depuis la destination, désactiver les transferts sur la relation SVM-DR :

```
snapmirror quiesce -destination-path <dest_svm>:
```



Vous devez entrer deux-points (:) après le nom du SVM dans l' `-destination-path` option.



6. Depuis le cluster source, démarrer la conversion :

```
volume conversion start -vserver <svm_name> -volume <vol_name>
```

7. Vérifiez que la conversion est réussie :

```
volume show <vol_name> -fields volume-style-extended,state
```

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state
```

| vserver | volume    | state  | volume-style-extended |
|---------|-----------|--------|-----------------------|
| -----   | -----     | -----  | -----                 |
| vs0     | my_volume | online | flexgroup             |

8. Depuis le cluster destination, reprendre les transferts pour la relation :

```
snapmirror resume -destination-path <dest_svm>:
```



Vous devez entrer deux-points (:) après le nom du SVM dans l'option `-destination-path`.

9. Depuis le cluster de destination, effectuer une mise à jour pour propager la conversion à la destination :

```
snapmirror update -destination-path <dest_svm>:
```



Vous devez entrer deux-points (:) après le nom du SVM dans l'option `-destination-path`.

10. S'assurer que la relation SVM-DR est dans un état sous SnapMirror et qu'elle n'est pas supprimée :

```
snapmirror show
```

11. Assurez-vous que la conversion s'est produite sur la destination :

```
volume show <vol_name> -fields volume-style-extended,state
```

```
cluster-2::*> volume show my_volume -fields volume-style-extended,state
```

| vserver | volume    | state  | volume-style-extended |
|---------|-----------|--------|-----------------------|
| -----   | -----     | -----  | -----                 |
| vs0_dst | my_volume | online | flexgroup             |

## Considérations relatives à la création de relations SnapMirror en cascade et avec fanout pour FlexGroups

Considérations et restrictions de prise en charge à prendre en compte lors de la création de relations SnapMirror en cascade et avec fanout pour les volumes FlexGroup.

### Considérations relatives à la création de relations en cascade

- Chaque relation peut être une relation entre clusters ou intra cluster.
- Tous les types de règles asynchrones, y compris les mises en miroir, les miroirs et les coffres-forts, sont pris en charge pour les deux relations.
- Seules les stratégies async-mirror « MirrorAlsnapshots », et non « MirrorLatest », sont prises en charge.
- Les mises à jour simultanées des relations XDP en cascade sont prises en charge.
- Prend en charge la suppression de A à B et de B à C et la resynchronisation de A à C ou la resynchronisation de C à A.
- Les volumes FlexGroup a et B prennent également en charge la mise en service lorsque tous les nœuds exécutent ONTAP 9.9.1 ou une version ultérieure.
- Les opérations de restauration à partir des volumes FlexGroup B ou C sont prises en charge.
- Les transferts sur les relations FlexGroup ne sont pas pris en charge, tandis que la destination est la source d'une relation de restauration.
- La destination d'une restauration FlexGroup ne peut pas être la destination d'une autre relation FlexGroup.
- Les opérations de restauration de fichiers FlexGroup ont les mêmes restrictions que les opérations régulières de restauration de FlexGroup.
- Tous les nœuds du cluster dans lequel résident les volumes FlexGroup B et C doivent exécuter ONTAP 9.9.1 ou une version ultérieure.
- Toutes les fonctionnalités d'expansion et d'expansion automatique sont prises en charge.
- Dans une configuration en cascade telle Que A à B à C, si Les Relations SnapMirror entre A et B et C ont un nombre différent de relations SnapMirror composants, une opération d'abandon de la source n'est pas prise en charge pour la relation SnapMirror entre B et C.
- System Manager ne prend pas en charge les relations en cascade dans ONTAP 9.9.1.
- Lors de la conversion d'un ensemble A à B en C de la relation FlexVol en une relation FlexGroup, vous devez d'abord convertir le B en C hop.
- Toutes les configurations en cascade FlexGroup pour les relations avec les types de règles pris en charge par LE PROTOCOLE REST sont également prises en charge par les API REST dans des configurations FlexGroup en cascade.
- À l'instar des relations FlexVol, la cascade FlexGroup n'est pas prise en charge par le système `snapmirror protect` commande.

### Considérations relatives à la création de relations de fanout

- Deux ou plusieurs relations de fanout FlexGroup sont prises en charge ; par exemple, A à B, A à C, avec un maximum de 8 pieds de fanout.
- Chaque relation peut être intercluster ou intracluster.
- Les mises à jour simultanées sont prises en charge pour les deux relations.
- Toutes les fonctionnalités d'expansion et d'expansion automatique sont prises en charge.
- Si les segments « fan out » de la relation comportent différents nombres de relations SnapMirror constitutifs, une opération d'abandon de la source n'est pas prise en charge pour les relations A à B et A à C.
- Tous les nœuds du cluster où résident la source et la destination FlexGroups doivent exécuter ONTAP 9.9.1 ou une version ultérieure.
- Tous les types de règles asynchrones actuellement pris en charge pour FlexGroup SnapMirror sont pris en charge dans les relations de type « fan out ».
- Vous pouvez effectuer les opérations de restauration de B à C FlexGroups.
- Toutes les configurations en mode « fan out » avec types de règles pris en charge par le REST sont également prises en charge pour les API REST dans les configurations en mode « fan out » de FlexGroup.

### Considérations relatives à la création d'une relation de sauvegarde SnapVault et d'une relation unifiée de protection des données pour les volumes FlexGroup

Il est à prendre en compte les considérations relatives à la création d'une relation de sauvegarde SnapVault et d'une relation de protection unifiée des données pour les volumes FlexGroup.

- Vous pouvez resynchroniser une relation de sauvegarde SnapVault et une relation de protection des données unifiée à l'aide de `-preserve`. Vous pouvez conserver les copies Snapshot sur le volume de destination plus récent que la dernière copie Snapshot commune.
- La conservation à long terme n'est pas prise en charge par les volumes FlexGroup.

La conservation à long terme permet de créer des copies Snapshot directement sur le volume de destination sans avoir besoin de stocker les copies Snapshot sur le volume source.

- Le `snapshot` commande `expiry-time` Option non prise en charge pour les volumes FlexGroup.
- L'efficacité du stockage ne peut pas être configurée sur le volume FlexGroup de destination d'une relation de sauvegarde SnapVault et d'une relation de protection unifiée des données.
- Vous ne pouvez pas renommer les copies Snapshot d'une relation de sauvegarde SnapVault et une relation unifiée de protection des données pour les volumes FlexGroup.
- Un volume FlexGroup peut être le volume source d'une seule relation de sauvegarde ou de restauration.

Un volume FlexGroup ne peut pas être à l'origine de deux relations SnapVault, de deux relations de restauration, ou d'une relation de sauvegarde SnapVault et de restauration.

- Si vous supprimez une copie Snapshot du volume FlexGroup source et que vous créez à nouveau une copie Snapshot du même nom, le prochain transfert de la mise à jour vers le volume FlexGroup de destination échoue si le volume de destination possède une copie Snapshot du même nom.

Cela est dû au fait que les copies Snapshot ne peuvent pas être renommées pour les volumes FlexGroup.

**Surveiller les transferts de données SnapMirror pour les volumes FlexGroup**

Vous devez régulièrement surveiller l'état des relations FlexGroup volume SnapMirror afin de vérifier que le volume FlexGroup de destination est mis à jour régulièrement conformément au planning spécifié.

**Description de la tâche**

Vous devez effectuer cette tâche à partir du cluster de destination.

**Étapes**

- 1. Afficher l'état de la relation SnapMirror de toutes les relations de volume FlexGroup : `snapmirror show -relationship-group-type flexgroup`

```
cluster2::> snapmirror show -relationship-group-type flexgroup

Progress
Source Destination Mirror Relationship Total
Last
Path Type Path State Status Progress Healthy
Updated

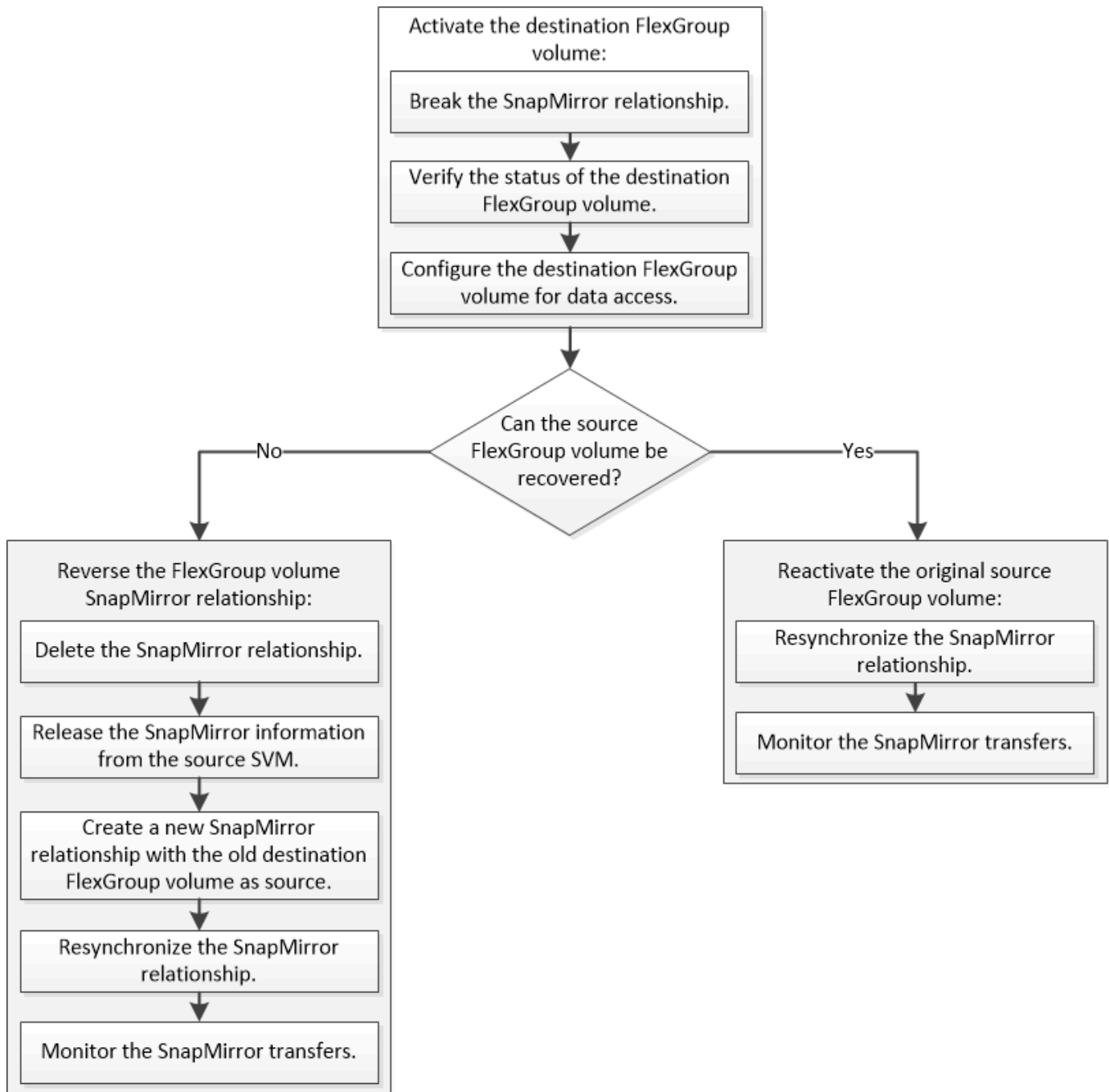
vss:s XDP vsd:d Snapmirrored
 Idle - true -
vss:s2 XDP vsd:d2 Uninitialized
 Idle - true -
2 entries were displayed.
```

**Gérer les opérations de protection des données pour les volumes FlexGroup**

**Reprise d'activité pour les volumes FlexGroup**

**Workflow de reprise d'activité pour les volumes FlexGroup**

Lorsqu'un incident survient sur le volume FlexGroup source, vous devez activer le volume FlexGroup de destination et rediriger l'accès client. Selon que le volume FlexGroup source peut être restauré ou non, il est recommandé de réactiver le volume FlexGroup source ou d'inverser la relation SnapMirror.



### Description de la tâche

L'accès client au volume FlexGroup de destination est bloqué pendant une courte période lors de l'exécution de certaines opérations SnapMirror, telles que l'arrêt et la resynchronisation de SnapMirror. En cas d'échec de l'opération SnapMirror, il est possible que certains composants restent dans cet état et que l'accès au volume FlexGroup soit refusé. Dans ce cas, vous devez refaire l'opération SnapMirror.

### Activer le volume FlexGroup de destination

Lorsque le volume FlexGroup source ne peut pas transmettre les données en raison d'événements tels que la corruption des données, la suppression accidentelle ou un état hors ligne, vous devez activer le volume FlexGroup de destination pour autoriser l'accès aux données jusqu'à ce que vous les restaurez sur le volume FlexGroup source. L'activation implique l'arrêt des futurs transferts de données SnapMirror et l'établissement

d'une relation plus étroit avec SnapMirror.

### Description de la tâche

Vous devez effectuer cette tâche à partir du cluster de destination.

### Étapes

1. Désactiver les transferts futurs pour la relation FlexGroup volume SnapMirror : `snapmirror quiesce dest_svm:dest_flexgroup`

```
cluster2::> snapmirror quiesce -destination-path vsd:dst
```

2. Interrompre la relation FlexGroup Volume SnapMirror : `snapmirror break dest_svm:dest_flexgroup`

```
cluster2::> snapmirror break -destination-path vsd:dst
```

3. Afficher l'état de la relation SnapMirror : `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

| Progress    | Source | Destination   | Mirror     | Relationship | Total  |          |         |
|-------------|--------|---------------|------------|--------------|--------|----------|---------|
| Last        | Path   | Type          | Path       | State        | Status | Progress | Healthy |
| Updated     |        |               |            |              |        |          |         |
| -----       | -----  | -----         | -----      | -----        | -----  | -----    | -----   |
| -----       |        |               |            |              |        |          |         |
| vss:s       | XDP    | vsd:dst       | Broken-off |              |        |          |         |
|             |        |               | Idle       |              | -      | true     | -       |
| vss:s__0001 | XDP    | vsd:dst__0001 | Broken-off |              |        |          |         |
|             |        |               | Idle       |              | -      | true     | -       |
| vss:s__0002 | XDP    | vsd:dst__0002 | Broken-off |              |        |          |         |
|             |        |               | Idle       |              | -      | true     | -       |
| vss:s__0003 | XDP    | vsd:dst__0003 | Broken-off |              |        |          |         |
|             |        |               | Idle       |              | -      | true     | -       |
| vss:s__0004 | XDP    | vsd:dst__0004 | Broken-off |              |        |          |         |
|             |        |               | Idle       |              | -      | true     | -       |
| vss:s__0005 | XDP    | vsd:dst__0005 | Broken-off |              |        |          |         |
|             |        |               | Idle       |              | -      | true     | -       |
| vss:s__0006 | XDP    | vsd:dst__0006 | Broken-off |              |        |          |         |
|             |        |               | Idle       |              | -      | true     | -       |
| vss:s__0007 | XDP    | vsd:dst__0007 | Broken-off |              |        |          |         |
|             |        |               | Idle       |              | -      | true     | -       |
| vss:s__0008 | XDP    | vsd:dst__0008 | Broken-off |              |        |          |         |
|             |        |               | Idle       |              | -      | true     | -       |
| ...         |        |               |            |              |        |          |         |

L'état de la relation SnapMirror de chaque composant est Broken-off.

4. Vérifier que le volume FlexGroup de destination est en lecture/écriture : `volume show -vserver svm_name`

```
cluster2::> volume show -vserver vsd
Vserver Volume Aggregate State Type Size
Available Used%

vsd dst - online **RW** 2GB
1.54GB 22%
vsd d2 - online DP 2GB
1.55GB 22%
vsd root_vs0 aggr1 online RW 100MB
94.02MB 5%
3 entries were displayed.
```

5. Redirection des clients vers le volume FlexGroup de destination.

#### Réactiver le volume FlexGroup source d'origine après un incident

Lorsque le volume FlexGroup source est disponible, vous pouvez resynchroniser les volumes FlexGroup source et de destination d'origine. Toutes les nouvelles données présentes sur le volume FlexGroup de destination sont perdues.

#### Description de la tâche

Toutes les règles de quota actives sur le volume de destination sont désactivées et les règles de quota sont supprimées avant d'effectuer une resynchronisation.

Vous pouvez utiliser le `volume quota policy rule create` et `volume quota modify` commandes permettant de créer et de réactiver des règles de quota une fois l'opération de resynchronisation terminée.

#### Étapes

1. Depuis le cluster de destination, faire une resynchronisation de la relation de FlexGroup volume  
`SnapMirror: snapmirror resync -destination-path dst_svm:dest_flexgroup`
2. Afficher l'état de la relation SnapMirror : `snapmirror show -expand`



```
cluster2::> snapmirror show -expand
```

| Progress | Source      | Destination | Mirror        | Relationship | Total  |          |         |
|----------|-------------|-------------|---------------|--------------|--------|----------|---------|
| Last     | Path        | Type        | Path          | State        | Status | Progress | Healthy |
| Updated  |             |             |               |              |        |          |         |
| -----    | -----       | -----       | -----         | -----        | -----  | -----    | -----   |
| -----    | vss:s       | XDP         | vsd:dst       | Snapmirrored |        |          |         |
|          |             |             |               | Idle         | -      | true     | -       |
|          | vss:s__0001 | XDP         | vsd:dst__0001 | Snapmirrored |        |          |         |
|          |             |             |               | Idle         | -      | true     | -       |
|          | vss:s__0002 | XDP         | vsd:dst__0002 | Snapmirrored |        |          |         |
|          |             |             |               | Idle         | -      | true     | -       |
|          | vss:s__0003 | XDP         | vsd:dst__0003 | Snapmirrored |        |          |         |
|          |             |             |               | Idle         | -      | true     | -       |
|          | vss:s__0004 | XDP         | vsd:dst__0004 | Snapmirrored |        |          |         |
|          |             |             |               | Idle         | -      | true     | -       |
|          | vss:s__0005 | XDP         | vsd:dst__0005 | Snapmirrored |        |          |         |
|          |             |             |               | Idle         | -      | true     | -       |
|          | vss:s__0006 | XDP         | vsd:dst__0006 | Snapmirrored |        |          |         |
|          |             |             |               | Idle         | -      | true     | -       |
|          | vss:s__0007 | XDP         | vsd:dst__0007 | Snapmirrored |        |          |         |
|          |             |             |               | Idle         | -      | true     | -       |
|          | vss:s__0008 | XDP         | vsd:dst__0008 | Snapmirrored |        |          |         |
|          |             |             |               | Idle         | -      | true     | -       |
| ...      |             |             |               |              |        |          |         |

L'état de la relation SnapMirror de chaque composant est Snapmirrored.

#### Inverser une relation SnapMirror entre des volumes FlexGroup pendant la reprise d'activité

Lorsqu'un incident désactive le volume FlexGroup source d'une relation SnapMirror, vous pouvez utiliser le volume FlexGroup de destination pour transmettre des données pendant que vous réparez ou remplacez le volume FlexGroup source. Une fois le volume FlexGroup source en ligne, vous pouvez faire du volume FlexGroup source d'origine une destination en lecture seule et inverser la relation SnapMirror.

#### Description de la tâche

Toutes les règles de quota actives sur le volume de destination sont désactivées et les règles de quota sont supprimées avant d'effectuer une resynchronisation.

Vous pouvez utiliser le `volume quota policy rule create` et `volume quota modify` commandes permettant de créer et de réactiver des règles de quota une fois l'opération de resynchronisation terminée.

## Étapes

1. Sur le volume FlexGroup de destination d'origine, supprimez la relation miroir de protection des données entre le volume FlexGroup source et le volume FlexGroup de destination : `snapmirror delete -destination-path svm_name:volume_name`

```
cluster2::> snapmirror delete -destination-path vsd:dst
```

2. Sur le volume FlexGroup source d'origine, supprimez les informations de relation du volume FlexGroup source : `snapmirror release -destination-path svm_name:volume_name -relationship -info-only`

Après la suppression d'une relation SnapMirror, vous devez supprimer les informations de relation du volume FlexGroup source avant de tenter une opération de resynchronisation.

```
cluster1::> snapmirror release -destination-path vsd:dst -relationship
-info-only true
```

3. Sur le nouveau volume FlexGroup de destination, créez la relation miroir : `snapmirror create -source-path src_svm_name:volume_name -destination-path dst_svm_name:volume_name -type XDP -policy MirrorAllSnapshots`

```
cluster1::> snapmirror create -source-path vsd:dst -destination-path
vss:src -type XDP -policy MirrorAllSnapshots
```

4. Sur le nouveau volume FlexGroup de destination, resynchroniser la FlexGroup source : `snapmirror resync -source-path svm_name:volume_name`

```
cluster1::> snapmirror resync -source-path vsd:dst
```

5. Surveiller les transferts SnapMirror : `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

| Progress | Source        | Destination | Mirror        | Relationship | Total  |          |         |
|----------|---------------|-------------|---------------|--------------|--------|----------|---------|
| Last     | Path          | Type        | Path          | State        | Status | Progress | Healthy |
| Updated  |               |             |               |              |        |          |         |
| -----    | -----         | -----       | -----         | -----        | -----  | -----    | -----   |
| -----    | vsd:dst       | XDP         | vss:src       | Snapmirrored |        |          |         |
|          |               |             |               | Idle         | -      | true     | -       |
|          | vss:dst__0001 | XDP         | vss:src__0001 | Snapmirrored |        |          |         |
|          |               |             |               | Idle         | -      | true     | -       |
|          | vsd:dst__0002 | XDP         | vss:src__0002 | Snapmirrored |        |          |         |
|          |               |             |               | Idle         | -      | true     | -       |
|          | vsd:dst__0003 | XDP         | vss:src__0003 | Snapmirrored |        |          |         |
|          |               |             |               | Idle         | -      | true     | -       |
|          | vsd:dst__0004 | XDP         | vss:src__0004 | Snapmirrored |        |          |         |
|          |               |             |               | Idle         | -      | true     | -       |
|          | vsd:dst__0005 | XDP         | vss:src__0005 | Snapmirrored |        |          |         |
|          |               |             |               | Idle         | -      | true     | -       |
|          | vsd:dst__0006 | XDP         | vss:src__0006 | Snapmirrored |        |          |         |
|          |               |             |               | Idle         | -      | true     | -       |
|          | vsd:dst__0007 | XDP         | vss:src__0007 | Snapmirrored |        |          |         |
|          |               |             |               | Idle         | -      | true     | -       |
|          | vsd:dst__0008 | XDP         | vss:src__0008 | Snapmirrored |        |          |         |
|          |               |             |               | Idle         | -      | true     | -       |
| ...      |               |             |               |              |        |          |         |

L'état de la relation SnapMirror de chaque composant apparaît comme `Snapmirrored` cela indique que la resynchronisation a réussi.

## Développement de volumes FlexGroup dans une relation SnapMirror

### Développement de volumes FlexGroup dans une relation SnapMirror

Depuis ONTAP 9.3, vous pouvez développer le volume FlexGroup source et le volume FlexGroup de destination dans une relation SnapMirror en ajoutant de nouveaux composants aux volumes. Vous pouvez développer les volumes de destination manuellement ou automatiquement.

#### Description de la tâche

- Après l'extension, le nombre de composants dans le volume FlexGroup source et le volume FlexGroup de destination d'une relation SnapMirror doit correspondre.

Si le nombre de composants des volumes ne correspond pas, les transferts SnapMirror échouent.

- Vous ne devez pas effectuer d'opération SnapMirror lorsque le processus d'extension est en cours.
- Si un incident survient avant la fin du processus d'extension, vous devez interrompre la relation SnapMirror et attendre la réussite de l'opération.



Vous devez interrompre la relation SnapMirror lorsque le processus d'extension est en cours uniquement en cas d'incident. Dans le cas d'un incident, cette opération peut prendre un certain temps. Vous devez attendre que l'opération de pause soit terminée avec succès avant d'effectuer une resynchronisation. En cas d'échec de l'opération de pause, vous devez recommencer l'opération. En cas d'échec de l'opération de pause, certains des nouveaux composants peuvent rester dans le volume FlexGroup de destination après l'opération de pause. Il est préférable de supprimer ces composants manuellement avant de poursuivre.

#### Développez le volume FlexGroup source d'une relation SnapMirror

Depuis ONTAP 9.3, vous pouvez étendre le volume FlexGroup source d'une relation SnapMirror en ajoutant de nouveaux composants au volume source. Vous pouvez développer le volume source de la même manière que vous développez un volume FlexGroup standard (volume read-write).

#### Étapes

1. Développez le volume FlexGroup source : `volume expand -vserver vs_server_name -volume fg_src -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster1::> volume expand -volume src_fg -aggr-list aggr1 -aggr-list
-multiplier 2 -vserver vs_src
```

```
Warning: The following number of constituents of size 50GB will be added
to FlexGroup "src_fg": 2.
```

```
Expanding the FlexGroup will cause the state of all Snapshot copies to
be set to "partial".
```

```
Partial Snapshot copies cannot be restored.
```

```
Do you want to continue? {y|n}: Y
```

```
[Job 146] Job succeeded: Successful
```

L'état de toutes les copies Snapshot qui sont effectuées avant l'extension partielle du volume

#### Développer le volume FlexGroup de destination d'une relation SnapMirror

Vous pouvez développer le volume FlexGroup de destination et rétablir la relation SnapMirror automatiquement ou manuellement. Par défaut, la relation SnapMirror est définie pour l'extension automatique et le volume FlexGroup de destination augmente automatiquement si le volume source se développe.

#### Ce dont vous avez besoin

- Le volume FlexGroup source doit avoir été étendu.

- La relation SnapMirror doit être dans le `SnapMirrored` état.

La relation SnapMirror ne doit pas être rompue ou supprimée.

### Description de la tâche

- Lorsque le volume FlexGroup de destination est créé, le volume est configuré par défaut pour une extension automatique.

Vous pouvez modifier le volume FlexGroup de destination pour une extension manuelle, si nécessaire.



La meilleure pratique consiste à étendre automatiquement le volume FlexGroup de destination.

- Toutes les opérations de SnapMirror échouent jusqu'à ce que les volumes FlexGroup source et FlexGroup de destination soient étendus et possèdent le même nombre de composants.
- Si vous développez le volume FlexGroup de destination une fois la relation SnapMirror rompue ou supprimée, vous ne pouvez pas resynchroniser la relation d'origine.

Si vous prévoyez de réutiliser le volume FlexGroup de destination, vous ne devez pas étendre le volume après avoir supprimé la relation SnapMirror.

### Choix

- Effectuer un transfert de mise à jour pour développer automatiquement le volume FlexGroup de destination :
  - a. Effectuer un transfert de mise à jour SnapMirror : `snapmirror update -destination-path svm:vol_name`
  - b. Vérifier que l'état de la relation SnapMirror se trouve dans `SnapMirrored` état : `snapmirror show`

```
cluster2::> snapmirror show
```

```
Progress
Source Destination Mirror Relationship Total
Last
Path Type Path State Status Progress
Healthy Updated

vs_src:src_fg
 XDP vs_dst:dst_fg
 Snapmirrored
 Idle - true
-
```

En fonction de la taille et de la disponibilité des agrégats, les agrégats sont sélectionnés automatiquement. De nouveaux composants correspondant aux composants du volume FlexGroup source sont ajoutés au volume FlexGroup de destination. Après l'extension, une opération de resynchronisation est

automatiquement déclenchée.

- Développez manuellement le volume FlexGroup de destination :
  - a. Si la relation SnapMirror est en mode d'expansion automatique, définir la relation SnapMirror en mode d'expansion manuelle : `snapmirror modify -destination-path svm:vol_name -is-auto-expand-enabled false`

```
cluster2::> snapmirror modify -destination-path vs_dst:dst_fg -is
-auto-expand-enabled false
Operation succeeded: snapmirror modify for the relationship with
destination "vs_dst:dst_fg".
```

- b. Mettre au repos la relation SnapMirror : `snapmirror quiesce -destination-path svm:vol_name`

```
cluster2::> snapmirror quiesce -destination-path vs_dst:dst_fg
Operation succeeded: snapmirror quiesce for destination
"vs_dst:dst_fg".
```

- c. Développez le volume FlexGroup de destination : `volume expand -vserver vs_server_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster2::> volume expand -volume dst_fg -aggr-list aggr1 -aggr-list
-multiplier 2 -vserver vs_dst

Warning: The following number of constituents of size 50GB will be
added to FlexGroup "dst_fg": 2.
Do you want to continue? {y|n}: y
[Job 68] Job succeeded: Successful
```

- d. Resynchroniser la relation SnapMirror : `snapmirror resync -destination-path svm:vol_name`

```
cluster2::> snapmirror resync -destination-path vs_dst:dst_fg
Operation is queued: snapmirror resync to destination
"vs_dst:dst_fg".
```

- e. Vérifier que l'état de la relation SnapMirror est bien SnapMirrored: `snapmirror show`

```
cluster2::> snapmirror show
```

| Progress      | Source  | Destination | Mirror        | Relationship | Total  |          |
|---------------|---------|-------------|---------------|--------------|--------|----------|
| Last          | Path    | Type        | Path          | State        | Status | Progress |
| Healthy       | Updated |             |               |              |        |          |
| -----         | -----   | -----       | -----         | -----        | -----  | -----    |
| -----         | -----   |             |               |              |        |          |
| vs_src:src_fg |         | XDP         | vs_dst:dst_fg |              |        |          |
|               |         |             |               | Snapmirrored |        |          |
|               |         |             |               | Idle         |        |          |
| -             |         |             |               |              | -      | true     |

## Effectuez la restauration SnapMirror des fichiers uniques à partir d'un volume FlexGroup

Depuis ONTAP 9.8, vous pouvez restaurer un seul fichier à partir d'un coffre-fort FlexGroup SnapMirror ou d'une destination UDP.

### Description de la tâche

- Vous pouvez restaurer à partir d'un volume FlexGroup de n'importe quelle géométrie vers un volume FlexGroup de n'importe quelle géométrie
- Un seul fichier par opération de restauration est pris en charge
- Vous pouvez restaurer le système vers le volume FlexGroup source d'origine ou vers un nouveau volume FlexGroup
- La recherche de fichiers verrouillés à distance n'est pas prise en charge.

La restauration d'un seul fichier échoue si le fichier source est clôturé.

- Vous pouvez redémarrer ou nettoyer une restauration de fichier unique abandonnée
- Vous devez nettoyer un transfert de restauration de fichier unique ayant échoué à l'aide du `clean-up-failure` de la `snapmirror restore` commande
- L'extension des volumes FlexGroup est prise en charge lorsqu'une restauration de fichiers uniques FlexGroup est en cours ou est en cours d'abandon

### Étapes

1. Restaurer un fichier depuis un volume FlexGroup :  
`snapmirror restore -destination-path destination_path -source-path source_path -file-list /f1 -throttle throttle -source-snapshot snapshot`

Voici un exemple d'opération de restauration de fichier unique pour un volume FlexGroup.

```
vserverA::> snapmirror restore -destination-path vs0:fg2 -source-path vs0:fgd -file-list /f1 -throttle 5 -source-snapshot snapmirror.81072cel-
```

d57b-11e9-94c0-005056a7e422\_2159190496.2019-09-19\_062631

[Job 135] Job is queued: snapmirror restore from source "vs0:fgd" for the snapshot snapmirror.81072ce1-d57b-11e9-94c0-005056a7e422\_2159190496.2019-09-19\_062631.

vserverA::> snapmirror show

| Source  | Destination    | Mirror | Relationship |              |              |
|---------|----------------|--------|--------------|--------------|--------------|
| Total   | Last           |        |              |              |              |
| Path    | Type           | Path   | State        | Status       | Progress     |
| Healthy | Updated        |        |              |              |              |
| -----   | ----           | -----  | -----        | -----        | -----        |
| -----   | -----          | -----  |              |              |              |
| vs0:v1d | RST            | vs0:v2 | -            | Transferring | Idle 83.12KB |
| true    | 09/19 11:38:42 |        |              |              |              |

vserverA::\*> snapmirror show vs0:fg2

Source Path: vs0:fgd  
Source Cluster: -  
Source Vserver: vs0  
Source Volume: fgd  
Destination Path: vs0:fg2  
Destination Cluster: -  
Destination Vserver: vs0  
Destination Volume: fg2  
Relationship Type: RST  
Relationship Group Type: none  
Managing Vserver: vs0  
SnapMirror Schedule: -  
SnapMirror Policy Type: -  
SnapMirror Policy: -  
Tries Limit: -  
Throttle (KB/sec): unlimited  
Current Transfer Throttle (KB/sec): 2  
Mirror State: -  
Relationship Status: Transferring  
File Restore File Count: 1  
File Restore File List: f1  
Transfer Snapshot: snapmirror.81072ce1-d57b-11e9-94c0-005056a7e422\_2159190496.2019-09-19\_062631  
Snapshot Progress: 2.87MB  
Total Progress: 2.87MB  
Network Compression Ratio: 1:1  
Snapshot Checkpoint: 2.97KB  
Newest Snapshot: -  
Newest Snapshot Timestamp: -



```
Exported Snapshot: -
Exported Snapshot Timestamp: -
Healthy: true
Physical Replica: -
Relationship ID: e6081667-dacb-11e9-94c0-005056a7e422
Source Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Destination Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Current Operation ID: 138f12e6-dacc-11e9-94c0-005056a7e422
Transfer Type: cg_file_restore
Transfer Error: -
Last Transfer Type: -
Last Transfer Error: -
Last Transfer Error Codes: -
Last Transfer Size: -
Last Transfer Network Compression Ratio: -
Last Transfer Duration: -
Last Transfer From: -
Last Transfer End Timestamp: -
Unhealthy Reason: -
Progress Last Updated: 09/19 07:07:36
Relationship Capability: 8.2 and above
Lag Time: -
Current Transfer Priority: normal
SMTape Operation: -
Constituent Relationship: false
Destination Volume Node Name: vserverA
Identity Preserve Vserver DR: -
Number of Successful Updates: 0
Number of Failed Updates: 0
Number of Successful Resyncs: 0
Number of Failed Resyncs: 0
Number of Successful Breaks: 0
Number of Failed Breaks: 0
Total Transfer Bytes: 0
Total Transfer Time in Seconds: 0
Source Volume MSIDs Preserved: -
OpMask: ffffffffffffffff
Is Auto Expand Enabled: -
Source Endpoint UUID: -
Destination Endpoint UUID: -
Is Catalog Enabled: false
```

## Restaurez un volume FlexGroup à partir d'une sauvegarde SnapVault

Vous pouvez effectuer une opération de restauration de volume complet des volumes

FlexGroup à partir d'une copie Snapshot sur le volume secondaire SnapVault. Vous pouvez restaurer le volume FlexGroup sur le volume source d'origine ou sur un nouveau volume FlexGroup.

### Avant de commencer

Vous devez prendre en compte certaines considérations relatives à la restauration à partir des sauvegardes SnapVault pour les volumes FlexGroup.

- Seule la restauration de base est prise en charge avec des copies Snapshot partielles à partir d'une sauvegarde SnapVault.  
Le nombre de composants du volume de destination doit correspondre au nombre de composants du volume source lors de la copie Snapshot effectuée.
- Si une opération de restauration échoue, aucune autre opération n'est autorisée tant que l'opération de restauration n'est pas terminée.  
Vous pouvez soit relancer l'opération de restauration, soit exécuter l'opération de restauration avec `cleanup` paramètre.
- Un volume FlexGroup peut être le volume source d'une seule relation de sauvegarde ou de restauration. Un volume FlexGroup ne peut pas être à l'origine de deux relations SnapVault, de deux relations de restauration, ou d'une relation SnapVault et de restauration.
- Les opérations de sauvegarde et de restauration de SnapVault ne peuvent pas être exécutées en parallèle. Lorsqu'une opération de restauration de base ou une opération de restauration incrémentielle est en cours, vous devez arrêter les opérations de sauvegarde.
- Vous devez annuler l'opération de restauration d'une copie Snapshot partielle du volume FlexGroup de destination.  
Vous ne pouvez pas abandonner l'opération de restauration d'une copie Snapshot partielle du volume source.
- Si vous abandonnez une opération de restauration, vous devez redémarrer l'opération avec la même copie Snapshot utilisée pour la précédente opération de restauration.

### Description de la tâche

Toutes les règles de quota actives sur le volume FlexGroup de destination sont désactivées avant l'exécution de la restauration.

Vous pouvez utiliser le volume `quota modify` commande permettant de réactiver les règles de quota une fois l'opération de restauration terminée.

### Étapes

1. Restaurez le volume FlexGroup : `snapmirror restore -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -snapshot snapshot_name`  
`snapshot_name` Est la copie Snapshot à restaurer depuis le volume source vers le volume de destination. Si la copie Snapshot n'est pas spécifiée, le volume de destination est restauré à partir de la dernière copie Snapshot.

```
vserverA::> snapmirror restore -source-path vserverB:dstFG -destination
-path vserverA:newFG -snapshot daily.2016-07-15_0010
Warning: This is a disruptive operation and the volume vserverA:newFG
will be read-only until the operation completes
Do you want to continue? {y|n}: y
```

## Désactiver la protection des SVM sur un volume FlexGroup

Lorsque l'indicateur SVM DR est défini sur `protected` Sur un volume FlexGroup, vous pouvez définir l'indicateur sur non protégé pour désactiver la SVM DR `protection` Sur un volume FlexGroup.

### Ce dont vous avez besoin

- La relation de SVM DR entre le stockage primaire et le stockage secondaire fonctionne correctement.
- Le paramètre de protection SVM DR est défini sur `protected`.

### Étapes

1. Désactiver la protection à l'aide de `volume modify` pour modifier la commande `vserver-dr-protection` Paramètre du volume FlexGroup à `unprotected`.

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection unprotected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. Mettre à jour le SVM sur le site secondaire : `snapmirror update -destination-path destination_svm_name: -source-path Source_svm_name:`
3. Vérifier que la relation SnapMirror est saine : `snapmirror show`
4. Vérifier que la relation SnapMirror FlexGroup a été supprimée : `snapmirror show -expand`

## Activer la protection des SVM sur un volume FlexGroup

Lorsque l'indicateur de protection SVM DR est défini sur `unprotected` Sur un volume FlexGroup, vous pouvez définir l'indicateur sur `protected` Pour activer la protection SVM DR

### Ce dont vous avez besoin

- La relation de SVM DR entre le stockage primaire et le stockage secondaire fonctionne correctement.
- Le paramètre de protection SVM DR est défini sur `unprotected`.

### Étapes

1. Activez la protection à l'aide du `volume modify` pour modifier le `vserver-dr-protection` Paramètre du volume FlexGroup à `protected`.

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection protected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. Mettre à jour le SVM sur le site secondaire : `snapmirror update -destination-path destination_svm_name -source-path source_svm_name`

```
snapmirror update -destination-path vs1_dst: -source-path vs1:
```

3. Vérifier que la relation SnapMirror est saine : `snapmirror show`

```
cluster2::> snapmirror show
```

| Progress | Source | Destination | Mirror   | Relationship | Total  |          |
|----------|--------|-------------|----------|--------------|--------|----------|
| Last     | Path   | Type        | Path     | State        | Status | Progress |
| Updated  |        |             |          |              |        | Healthy  |
|          |        |             |          |              |        |          |
|          |        |             |          |              |        |          |
|          | vs1:   | XDP         | vs1_dst: | Snapmirrored |        |          |
|          |        |             |          | Idle         | -      | true     |
|          |        |             |          |              |        | -        |

4. Vérifier que la relation de FlexGroup SnapMirror est saine : `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

```
Progress
Source Destination Mirror Relationship Total
Last
Path Type Path State Status Progress Healthy
Updated

vs1: XDP vs1_dst: Snapmirrored
 Idle - true -
vs1:fg_src XDP vs1_dst:fg_src Snapmirrored
 Idle - true -
vs1:fg_src__0001 XDP vs1_dst:fg_src__0001 Snapmirrored
 Idle - true -
vs1:fg_src__0002 XDP vs1_dst:fg_src__0002 Snapmirrored
 Idle - true -
vs1:fg_src__0003 XDP vs1_dst:fg_src__0003 Snapmirrored
 Idle - true -
vs1:fg_src__0004 XDP vs1_dst:fg_src__0004 Snapmirrored
 Idle - true -
6 entries were displayed.
```

## Conversion de volumes FlexVol en volumes FlexGroup

### Présentation de la conversion de volumes FlexVol en volumes FlexGroup

Si vous souhaitez étendre un volume FlexVol au-delà de sa limite d'espace, vous pouvez convertir le volume FlexVol en volume FlexGroup. Depuis ONTAP 9.7, vous pouvez convertir des volumes FlexVol autonomes ou FlexVol dans une relation SnapMirror avec des volumes FlexGroup.

### Considérations relatives à la conversion de volumes FlexVol en volumes FlexGroup

Avant de décider de convertir des volumes FlexVol en volumes FlexGroup, prenez connaissance des fonctionnalités et des opérations prises en charge.

À partir de ONTAP 9.13.1, la protection anti-ransomware autonome peut rester activée pendant les conversions. Si la protection est active, le FlexVol d'origine deviendra le composant racine du FlexGroup après la conversion. Si la protection est inactive, un nouveau FlexGroup sera créé pendant la conversion et le FlexVol d'origine prendra le rôle de composant racine.

#### **Opérations non prises en charge pendant la conversion**

Les opérations suivantes ne sont pas autorisées lorsque la conversion de volume est en cours :

- Déplacement de volumes
- L'auto-obalance agrégée
- Transfert d'agrégats
- Le basculement et le retour planifiés dans une configuration haute disponibilité
- Rétablissement manuel et automatique en configuration haute disponibilité
- Mise à niveau ou restauration du cluster
- Fractionnement du volume FlexClone
- Réhébergement de volumes
- Modification du volume et dimensionnement automatique
- Renommer le volume
- Association d'un magasin d'objets à un agrégat
- Basculement négocié dans la configuration MetroCluster
- Opérations SnapMirror
- Restaurer un objet à partir d'une copie Snapshot
- Opérations de quotas
- Opérations d'efficacité du stockage

Ces opérations peuvent être réalisées sur le volume FlexGroup une fois la conversion terminée.

#### **Configurations non prises en charge par les volumes FlexGroup**

- Mise hors ligne ou volume restreint
- Root volume SVM
- SAN
- SMB 1.0
- Espaces de noms NVMe
- Service VSS (Remote Volume Shadow Copy Service)

#### **Conversion d'un volume FlexVol en volume FlexGroup**

Depuis ONTAP 9.7, vous pouvez effectuer une conversion sans déplacement des données d'un volume FlexVol en volume FlexGroup sans nécessiter de copie des données ni d'espace disque supplémentaire.

#### **Avant de commencer**

- Les volumes transférés peuvent être convertis en volumes FlexGroup à partir de ONTAP 9.8.
- Le volume FlexVol en cours de conversion doit être en ligne.
- Les opérations et les configurations du volume FlexVol doivent être compatibles avec le processus de conversion.

Vérifier les conditions suivantes qui peuvent empêcher la conversion de réussir :

- Un volume FlexVol a été migré de 7-mode à l'aide de 7MTT (ONTAP 9.7).

Les volumes transférés peuvent être convertis à partir de ONTAP 9.8.

- Un élément est activé sur le volume qui n'est pas encore pris en charge avec le volume FlexGroup ; par exemple, les LUN SAN, Windows NFS, SMB1, dénomination des snapshots/suppression automatique, jeu de règles, SnapLock, objectif de niveau de service de l'espace ou application/reporting de l'espace logique. Pour plus d'informations, voir "[Configurations prises en charge et non prises en charge pour les volumes FlexGroup](#)".
- Le SVM où se trouve le volume FlexVol à convertir utilise actuellement le SVM DR.
- Des volumes FlexClone NetApp sont présents et le volume FlexVol est le volume parent. Le volume en cours de conversion ne peut pas être un parent ou un clone.
- Le volume est un volume d'origine NetApp FlexCache.
- Pour ONTAP 9.7 et les versions antérieures, les copies Snapshot NetApp ne doivent pas dépasser 255. Pour ONTAP 9.8 et versions ultérieures, les copies Snapshot 1023 sont prises en charge.
- Les fonctionnalités d'efficacité du stockage sont activées. Ceux-ci doivent être désactivés et peuvent être réactivés après la conversion.
- Le volume est la source d'une relation SnapMirror et la destination n'a pas encore été convertie.
- Le volume fait partie d'une relation SnapMirror active (non mise en veille).
- Les quotas sont activés. Ceux-ci doivent être désactivés et peuvent être réactivés après la conversion.
- Les noms de volume comportent plus de 197 caractères.
- Le volume est associé à une application.

Ceci s'applique uniquement à ONTAP 9.7. Cette limitation a été supprimée dans ONTAP 9.8.

- Les processus ONTAP sont en cours d'exécution, tels que la mise en miroir, les tâches, le serveur, la sauvegarde NDMP, et la conversion des inodes en cours.
- Le volume est un volume root SVM.
- Le volume est trop plein.

Si l'une de ces incompatibilités existe, un message d'erreur est généré si le volume FlexVol et la conversion du volume sont abandonnées. Vous pouvez effectuer des actions correctives et recommencer la conversion.

- Si un volume FlexVol atteint actuellement une capacité maximale de 80 % ou plus, envisagez de copier les données vers un volume FlexGroup nouvellement créé au lieu d'effectuer une conversion sans déplacement des données. Bien que les volumes de membres FlexGroup se rééquilibrent naturellement au fil du temps, la conversion d'un volume FlexVol de grande capacité en volume FlexGroup peut créer des problèmes de performance ou d'équilibrage qui ne seront pas rapidement rééquilibrés entre les volumes de membres.



La conversion d'un très grand volume FlexGroup entraîne l'saturation du composant du volume FlexGroup, ce qui engendre des problèmes de performances. Pour plus d'informations, reportez-vous à la section intitulée « quand ne pas créer de volume FlexGroup » dans le rapport technique TR ["Volumes FlexGroup - Guide des meilleures pratiques et de mise en œuvre"](#).

## Étapes

1. Vérifier que le volume FlexVol est en ligne : `volume show vol_name volume-style-extended,state`

```
cluster-1::> volume show my_volume -fields volume-style-extended,state
vserver volume state volume-style-extended

vs0 my_volume online flexvol
```

2. Vérifiez si le volume FlexVol peut être converti sans problème :

- a. Connectez-vous au mode de privilège avancé : `set -privilege advanced`
- b. Vérifiez le processus de conversion : `volume conversion start -vserver vs1 -volume flexvol -check-only true`

Vous devez corriger toutes les erreurs avant de convertir le volume.



Vous ne pouvez pas reconverter un volume FlexGroup en volume FlexVol.

3. Lancer la conversion : `volume conversion start -vserver svm_name -volume vol_name`

```
cluster-1::*> volume conversion start -vserver vs0 -volume my_volume

Warning: Converting flexible volume "my_volume" in Vserver "vs0" to a
FlexGroup
 will cause the state of all Snapshot copies from the volume to
be set
 to "pre-conversion". Pre-conversion Snapshot copies cannot be
 restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

4. Vérifiez que la conversion a réussi : `volume show vol_name -fields volume-style-extended,state`



```
cluster-1::*> volume show my_volume -fields volume-style-extended,state
vserver volume state volume-style-extended

vs0 my_volume online flexgroup
```

## Résultats

Le volume FlexVol est converti en volume FlexGroup à un seul membre.

## Une fois que vous avez terminé

Il est possible de développer le volume FlexGroup, si nécessaire.

## Conversion d'une relation SnapMirror volume FlexVol en une relation SnapMirror volume FlexGroup

Pour convertir une relation SnapMirror volume FlexVol en une relation SnapMirror volume FlexGroup dans ONTAP, vous devez d'abord convertir le volume FlexVol de destination suivi du volume FlexVol source.

### Description de la tâche

- La conversion FlexGroup n'est prise en charge que pour les relations SnapMirror asynchrones.
- Le temps de conversion dépend de plusieurs variables. Voici quelques-unes des variables :
  - CPU du contrôleur
  - Utilisation du CPU par d'autres applications
  - Volume de données dans la copie Snapshot initiale
  - La bande passante du réseau
  - Bande passante utilisée par d'autres applications

### Avant de commencer

- Le volume FlexVol en cours de conversion doit être en ligne.
- Le volume FlexVol source dans la relation SnapMirror ne doit pas être le volume source pour plusieurs relations SnapMirror.

Depuis la version ONTAP 9.9.1, les relations SnapMirror « fan out » sont prises en charge pour les volumes FlexGroup. Pour plus d'informations, voir "[Considérations relatives à la création de relations SnapMirror en cascade et avec fanout pour FlexGroups](#)".

- Les opérations et les configurations du volume FlexVol doivent être compatibles avec le processus de conversion.

Un message d'erreur est généré si le volume FlexVol présente une incompatibilité et que la conversion de volume est abandonnée. Vous pouvez effectuer des actions correctives et recommencer la conversion.

## Étapes

1. Vérifier que la relation SnapMirror est saine :

```
snapmirror show
```

Seules les relations miroir de type XDP peuvent être converties.

Exemple :

```
cluster2::> snapmirror show
```

| Progress | Source      | Destination | Mirror      | Relationship | Total  |          |         |
|----------|-------------|-------------|-------------|--------------|--------|----------|---------|
| Last     | Path        | Type        | Path        | State        | Status | Progress | Healthy |
| Updated  |             |             |             |              |        |          |         |
| -----    | -----       | -----       | -----       | -----        | -----  | -----    | -----   |
| -----    | vs0:src_dpv | DP          | vs2:dst_dpv | Snapmirrored |        |          |         |
|          |             |             |             | Idle         | -      | true     | -       |
|          | vs0:src_xdp | XDP         | vs2:dst_xdp | Snapmirrored |        |          |         |
|          |             |             |             | Idle         | -      | true     | -       |

## 2. Vérifiez si le volume source est compatible pour la conversion :

### a. Connectez-vous au mode de privilège avancé :

```
set -privilege advanced
```

### b. Vérifiez le processus de conversion :

```
volume conversion start -vserver <src_svm_name> -volume <src_vol>
-check-only true
```

Exemple :

```
volume conversion start -vserver vs1 -volume src_vol -check-only true
```

+

Vous devez corriger toutes les erreurs avant de convertir le volume.

## 3. Conversion du volume FlexVol de destination en volume FlexGroup

### a. Suspendre la relation FlexVol SnapMirror :

```
snapmirror quiesce -destination-path <dest_svm:dest_volume>
```

Exemple :

```
cluster2::> snapmirror quiesce -destination-path vs2:dst_xdp
```

b. Lancer la conversion :

```
volume conversion start -vserver <dest_svm> -volume <dest_volume>
```

Exemple :

```
cluster-1::> volume conversion start -vserver vs2 -volume dst_xdp
```

Warning: After the volume is converted to a FlexGroup, it will not be possible

to change it back to a flexible volume.

Do you want to continue? {y|n}: y

[Job 510] Job succeeded: SnapMirror destination volume "dst\_xdp" has been successfully converted to a FlexGroup volume.

You must now convert the relationship's source volume, "vs0:src\_xdp", to a FlexGroup.

Then, re-establish the SnapMirror relationship using the "snapmirror resync" command.

4. Convertissez le volume FlexVol source en volume FlexGroup :`

```
volume conversion start -vserver <src_svm_name> -volume <src_vol_name>
```

Exemple :

```
cluster-1::> volume conversion start -vserver vs0 -volume src_xdp

Warning: Converting flexible volume "src_xdp" in Vserver "vs0" to a
FlexGroup
 will cause the state of all Snapshot copies from the volume to
be set
 to "pre-conversion". Pre-conversion Snapshot copies cannot be
 restored.

Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

## 5. Resynchroniser la relation :

```
snapmirror resync -destination-path dest_svm_name:dest_volume
```

Exemple :

```
cluster2::> snapmirror resync -destination-path vs2:dst_xdp
```

### Une fois que vous avez terminé

Lorsque le volume FlexGroup source est étendu de manière à inclure davantage de composants, le volume de destination doit également être étendu.

## Gestion des volumes FlexCache

### Présentation de FlexCache

La technologie NetApp FlexCache accélère l'accès aux données, réduit la latence des réseaux WAN et diminue les coûts de bande passante WAN pour les charges de travail intensives en lecture, notamment lorsque les clients doivent accéder aux mêmes données de manière répétée. Lorsque vous créez un volume FlexCache, vous créez un cache distant d'un volume (d'origine) existant qui ne contient que les données fréquemment utilisées (données actives) du volume d'origine.

Lorsqu'un volume FlexCache reçoit une demande de lecture des données actives qu'il contient, il peut répondre plus rapidement que le volume d'origine, car il n'est pas nécessaire de se déplacer aussi loin pour atteindre le client. Lorsqu'un volume FlexCache reçoit une demande de lecture de données rarement lues (données inactives), il récupère les données requises depuis le volume d'origine, puis les stocke avant de répondre à la demande du client. Les demandes de lecture suivantes pour ces données sont ensuite envoyées directement depuis le volume FlexCache. Après la première demande, les données n'ont plus besoin de traverser le réseau ou d'être servies à partir d'un système fortement chargé. Supposons, par exemple, que vous rencontrez des goulots d'étranglement au sein de votre cluster au niveau d'un point d'accès unique pour les données fréquemment demandées. Vous pouvez utiliser les volumes FlexCache au sein du cluster pour fournir plusieurs points de montage aux données actives, ce qui réduit les goulots d'étranglement et améliore

les performances. Prenons un autre exemple : supposons que vous deviez réduire le trafic réseau vers un volume accessible depuis plusieurs clusters. Vous pouvez utiliser des volumes FlexCache pour distribuer les données actives du volume d'origine sur les clusters de votre réseau. Cela réduit le trafic WAN en offrant aux utilisateurs des points d'accès plus étroits.

Vous pouvez également utiliser la technologie FlexCache pour améliorer les performances dans les environnements cloud et de cloud hybride. Un volume FlexCache vous aide à migrer vos workloads vers le cloud hybride en mettant en cache des données depuis un data Center sur site vers le cloud. Vous pouvez également utiliser les volumes FlexCache pour supprimer les silos de clouds en mettant en cache les données d'un fournisseur cloud à un autre ou dans deux régions du même fournisseur de cloud.

Avec ONTAP 9.10.1, c'est possible "[activer le verrouillage global des fichiers](#)" Sur tous les volumes FlexCache. Le verrouillage global des fichiers empêche un utilisateur d'accéder à un fichier déjà ouvert par un autre utilisateur. Les mises à jour du volume d'origine sont ensuite distribuées simultanément à tous les volumes FlexCache.

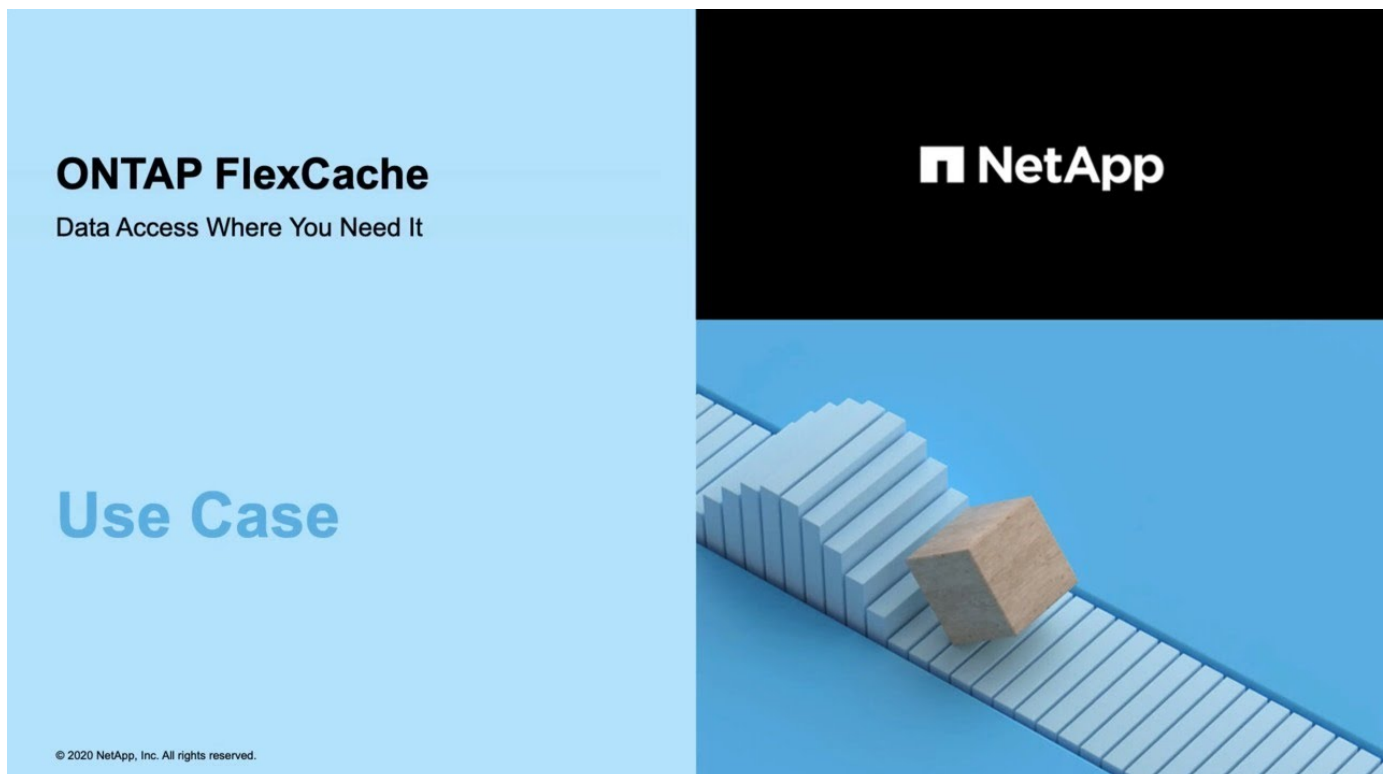
Depuis ONTAP 9.9.1, les volumes FlexCache conservent une liste de fichiers introuvables. Cela permet de réduire le trafic réseau en supprimant la nécessité d'envoyer plusieurs appels vers l'origine lorsque les clients recherchent des fichiers inexistantes.

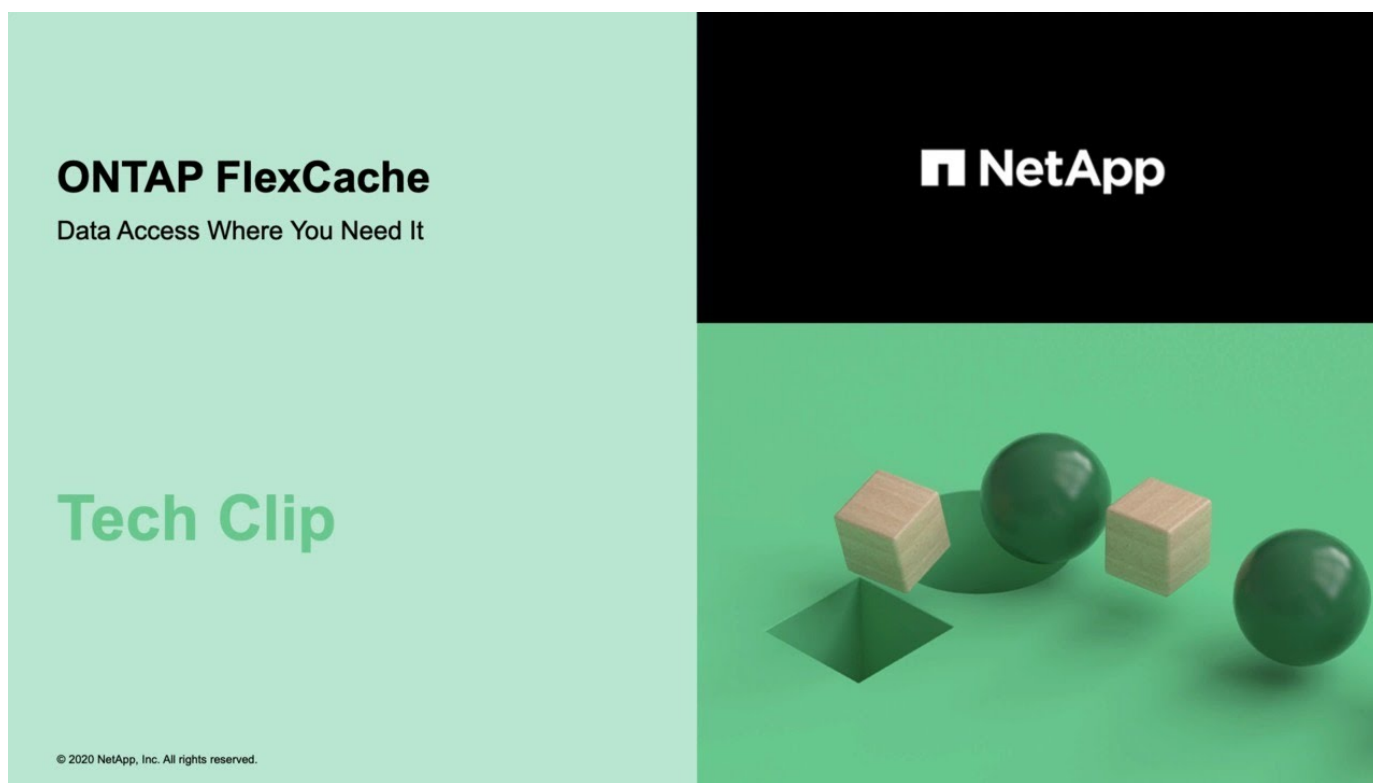
Une liste de suppléments "[Fonctionnalités prises en charge pour les volumes FlexCache et leurs volumes d'origine](#)", Comprenant une liste des protocoles pris en charge par la version ONTAP, est également disponible.

Pour en savoir plus sur l'architecture de la technologie ONTAP FlexCache, consultez le "[Tr-4743 : FlexCache dans ONTAP](#)".

## Vidéos

**Comment FlexCache peut réduire la latence des réseaux WAN et les temps de lecture des données globales**





## Fonctionnalités prises en charge et non prises en charge pour les volumes FlexCache

À partir de ONTAP 9.5, vous pouvez configurer des volumes FlexCache. Les volumes FlexVol sont pris en charge en tant que volumes d'origine et les volumes FlexGroup en tant que volumes FlexCache. Depuis ONTAP 9.7, les volumes FlexVol et FlexGroup sont pris en charge en tant que volumes d'origine. Les fonctionnalités et les protocoles pris en charge pour le volume d'origine et le volume FlexCache varient.

Les volumes en cache et les volumes d'origine peuvent interagir tant que les deux s'exécutent sur une version prise en charge de ONTAP. Gardez à l'esprit que les fonctionnalités ne sont prises en charge que lorsque le cache et l'origine exécutent au moins la version ONTAP où le support a été introduit ou une version ONTAP ultérieure.

### Protocoles pris en charge

| Protocole | Prise en charge sur le volume d'origine ? | Prise en charge par le volume FlexCache ? |
|-----------|-------------------------------------------|-------------------------------------------|
| NFSv3     | Oui.                                      | Oui.                                      |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NFSv4   | Oui.<br><br>Pour accéder aux volumes en cache à l'aide du protocole NFSv4.x, les clusters d'origine et de cache doivent utiliser ONTAP 9.10.1 ou version ultérieure. Le cluster d'origine et le cluster FlexCache peuvent avoir différentes versions de ONTAP, mais il doit s'agir de ONTAP 9.10.1 et versions ultérieures. Par exemple, l'origine peut avoir ONTAP 9.10.1 et le cache peut avoir ONTAP 9.11.1. | Oui.<br><br>Pris en charge à partir de ONTAP 9.10.1.<br><br>Pour accéder aux volumes en cache à l'aide du protocole NFSv4.x, les clusters d'origine et de cache doivent utiliser ONTAP 9.10.1 ou version ultérieure. Le cluster d'origine et le cluster FlexCache peuvent avoir différentes versions de ONTAP, mais il doit s'agir de ONTAP 9.10.1 et versions ultérieures. Par exemple, l'origine peut avoir ONTAP 9.10.1 et le cache peut avoir ONTAP 9.11.1. |
| NFSv4.2 | Oui.                                                                                                                                                                                                                                                                                                                                                                                                            | Non                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| PME     | Oui.                                                                                                                                                                                                                                                                                                                                                                                                            | Oui.<br><br>Pris en charge à partir de ONTAP 9.8.                                                                                                                                                                                                                                                                                                                                                                                                               |



### Fonctionnalités prises en charge

| Fonction                            | Prise en charge sur le volume d'origine ?                                                                                                                                                                                                                                         | Prise en charge par le volume FlexCache ? |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| Protection anti-ransomware autonome | Oui.<br><br>Pris en charge pour les volumes d'origine FlexVol à partir de ONTAP 9.10.1, et pour les volumes d'origine FlexGroup à partir de ONTAP 9.13.1. Voir " <a href="#">Cas d'utilisation et considérations relatives à la protection autonome contre les ransomwares</a> ". | Non                                       |

|                     |                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Antivirus           | <p>Oui.</p> <p>Pris en charge à partir de ONTAP 9.7.</p>                                                                                                                                                                                                                                         | <p>Sans objet</p> <p>Si vous configurez l'analyse antivirus à l'origine, elle n'est pas requise sur le cache. L'analyse antivirus d'origine détecte les fichiers infectés par des virus avant la validation des écritures, quelle que soit la source d'écriture. Pour plus d'informations sur l'utilisation de l'analyse antivirus avec FlexCache, reportez-vous au <a href="#">"Rapport technique FlexCache with ONTAP"</a>.</p> |
| Audit               | <p>Oui.</p> <p>Pris en charge à partir de ONTAP 9.7.</p> <p>Vous pouvez auditer les événements d'accès aux fichiers NFS dans des relations FlexCache à l'aide d'audits ONTAP natifs. Pour plus d'informations, voir <a href="#">Considérations relatives à l'audit des volumes FlexCache</a></p> | <p>Oui.</p> <p>Pris en charge à partir de ONTAP 9.7.</p> <p>Vous pouvez auditer les événements d'accès aux fichiers NFS dans des relations FlexCache à l'aide d'audits ONTAP natifs. Pour plus d'informations, voir <a href="#">Considérations relatives à l'audit des volumes FlexCache</a></p>                                                                                                                                  |
| Cloud Volumes ONTAP | <p>Oui.</p> <p>Pris en charge à partir de ONTAP 9.6</p>                                                                                                                                                                                                                                          | <p>Oui.</p> <p>Pris en charge à partir de ONTAP 9.6</p>                                                                                                                                                                                                                                                                                                                                                                           |
| Compaction          | <p>Oui.</p> <p>Pris en charge à partir de ONTAP 9.6</p>                                                                                                                                                                                                                                          | <p>Oui.</p> <p>Pris en charge à partir de ONTAP 9.7</p>                                                                                                                                                                                                                                                                                                                                                                           |
| Compression         | <p>Oui.</p> <p>Pris en charge à partir de ONTAP 9.6</p>                                                                                                                                                                                                                                          | <p>Oui.</p> <p>Pris en charge à partir de ONTAP 9.6</p>                                                                                                                                                                                                                                                                                                                                                                           |
| Déduplication       | <p>Oui.</p>                                                                                                                                                                                                                                                                                      | <p>Oui.</p> <p>La déduplication à la volée est prise en charge sur les volumes FlexCache depuis ONTAP 9.6. La déduplication entre les volumes est prise en charge sur les volumes FlexCache à partir de ONTAP 9.7.</p>                                                                                                                                                                                                            |



|                                         |                                                     |                                                                                                                                                                                         |
|-----------------------------------------|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FabricPool                              | Oui.<br><br>Pris en charge à partir de ONTAP 9.7    | Oui.<br><br>Pris en charge à partir de ONTAP 9.7                                                                                                                                        |
| Reprise après incident FlexCache        | Oui.<br><br>Pris en charge à partir de ONTAP 9.7    | Oui.<br><br>Pris en charge à partir de ONTAP 9.9.1, avec le protocole NFSv3 uniquement. Les volumes FlexCache doivent se trouver dans des SVM distincts ou dans des clusters distincts. |
| Volume FlexGroup                        | Oui.<br><br>Pris en charge à partir de ONTAP 9.7    | Oui.                                                                                                                                                                                    |
| Volume FlexVol                          | Oui.                                                | Non                                                                                                                                                                                     |
| FPolicy                                 | Oui.<br><br>Pris en charge à partir de ONTAP 9.7    | Oui.<br><br>Pris en charge pour NFS à partir de ONTAP 9.7.<br>Pris en charge pour SMB à partir de ONTAP 9.14.1.                                                                         |
| Configuration MetroCluster              | Oui.<br><br>Pris en charge à partir de ONTAP 9.7    | Oui.<br><br>Pris en charge à partir de ONTAP 9.7                                                                                                                                        |
| Microsoft Offloaded Data Transfer (ODX) | Oui.                                                | Non                                                                                                                                                                                     |
| Chiffrement d'agrégat NetApp (NAE)      | Oui.<br><br>Pris en charge à partir de ONTAP 9.6    | Oui.<br><br>Pris en charge à partir de ONTAP 9.6                                                                                                                                        |
| NVE (NetApp Volume Encryption)          | Oui.<br><br>Pris en charge à partir de ONTAP 9.6    | Oui.<br><br>Pris en charge à partir de ONTAP 9.6                                                                                                                                        |
| Compartiment NAS ONTAP S3               | Oui.<br><br>Pris en charge à partir de ONTAP 9.12.1 | Non                                                                                                                                                                                     |

|                                    |                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| La QoS                             | Oui.                                                                                                                                                                       | Oui.<br><br><br>La qualité de service au niveau des fichiers n'est pas prise en charge pour les volumes FlexCache.                                                                                                                                                            |
| Qtrees                             | Oui.<br><br>À partir de ONTAP 9.6, vous pouvez créer et modifier des qtrees. Les qtrees créés sur la source sont accessibles sur le cache.                                 | Non                                                                                                                                                                                                                                                                                                                                                              |
| Quotas                             | Oui.<br><br>Depuis la version ONTAP 9.6, l'application de quotas sur les volumes d'origine FlexCache est prise en charge pour les utilisateurs, les groupes et les qtrees. | Non<br><br>En mode FlexCache writeound (mode par défaut), les écritures sur le cache sont transmises au volume d'origine. Les quotas sont appliqués à l'origine.<br><br><br>Depuis ONTAP 9.6, le quota distant (rquota) est pris en charge au niveau des volumes FlexCache. |
| Notification des modifications SMB | Oui.                                                                                                                                                                       | Oui.<br><br>Depuis ONTAP 9.14.1, SMB change Notify est pris en charge au niveau du cache.                                                                                                                                                                                                                                                                        |
| Volumes SnapLock                   | Non                                                                                                                                                                        | Non                                                                                                                                                                                                                                                                                                                                                              |
| Relations asynchrones SnapMirror*  | Oui.                                                                                                                                                                       | Non                                                                                                                                                                                                                                                                                                                                                              |

|                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
|                                                                                                                                                                                                                                                                   | <p>*FlexCache origines :</p> <ul style="list-style-type: none"> <li>• Vous pouvez disposer d'un volume FlexCache issu d'une FlexVol d'origine</li> <li>• Vous pouvez disposer d'un volume FlexCache issu d'une FlexGroup d'origine</li> <li>• Vous pouvez avoir un volume FlexCache depuis un volume primaire d'origine dans la relation SnapMirror.</li> <li>• Depuis ONTAP 9.8, un volume secondaire SnapMirror peut être un volume d'origine FlexCache. Le volume secondaire SnapMirror doit être inactif sans mise à jour SnapMirror active ; dans le cas contraire, la création de FlexCache échoue.</li> </ul> | Relations synchrones SnapMirror                    |
| Non                                                                                                                                                                                                                                                               | Non                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | SnapRestore                                        |
| Oui.                                                                                                                                                                                                                                                              | Non                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Copies Snapshot                                    |
| Oui.                                                                                                                                                                                                                                                              | Non                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Configuration de SVM DR                            |
| <p>Oui.</p> <p>Pris en charge à partir de avecONTAP 9.5. Le SVM principal d'une relation de SVM DR peut avoir le volume d'origine. Cependant, si la relation de SVM DR est rompue, la relation FlexCache doit être recréeée avec un nouveau volume d'origine.</p> | <p>Non</p> <p>Les volumes FlexCache peuvent être répartis sur des SVM primaires, mais pas dans des SVM secondaires. Tout volume FlexCache au sein du SVM principal n'est pas répliqué dans le cadre de la relation de SVM DR.</p>                                                                                                                                                                                                                                                                                                                                                                                    | Protection d'accès au niveau du stockage (SCORIES) |
| Non                                                                                                                                                                                                                                                               | Non                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Provisionnement fin                                |
| Oui.                                                                                                                                                                                                                                                              | <p>Oui.</p> <p>Pris en charge à partir de ONTAP 9.7</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Clonage de volumes                                 |

|                                                                                                                       |                                                                                                                                                                                   |                                                 |
|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| Oui.<br><br>Le clonage d'un volume d'origine et des fichiers du volume d'origine est pris en charge depuis ONTAP 9.6. | Non                                                                                                                                                                               | Déplacement de volumes                          |
| Oui.                                                                                                                  | Oui (uniquement pour les composants de volume)<br><br>Le déplacement des composants de volume d'un volume FlexCache est pris en charge par ONTAP 9.6 et les versions ultérieures. | Réhébergement de volumes                        |
| Non                                                                                                                   | Non                                                                                                                                                                               | API vStorage pour l'intégration de baies (VAAL) |



Dans les versions ONTAP 9 antérieures à 9.5, les volumes FlexVol d'origine ne peuvent transmettre que les données aux volumes FlexCache créés sur des systèmes exécutant Data ONTAP 8.2.x en 7-mode. Depuis ONTAP 9.5, les volumes FlexVol d'origine peuvent également transmettre des données vers des volumes FlexCache sur les systèmes ONTAP 9. Pour plus d'informations sur la migration de 7-mode FlexCache vers ONTAP 9 FlexCache, reportez-vous à la section "[Rapport technique NetApp 4743 : FlexCache in ONTAP](#)".

## Instructions de dimensionnement d'un volume FlexCache

Avant de commencer le provisionnement des volumes, vous devez connaître les limites des volumes FlexCache.

La taille limite d'un volume FlexVol s'applique à un volume d'origine. La taille d'un volume FlexCache peut être inférieure ou égale au volume d'origine. La meilleure pratique pour la taille d'un volume FlexCache consiste à correspondre à au moins 10 % de la taille du volume d'origine.

Vous devez également connaître les limites supplémentaires suivantes sur les volumes FlexCache :

| Limite                                                                                   | ONTAP 9.5-9.6 | ONTAP 9.7 | ONTAP 9.8 et versions ultérieures |
|------------------------------------------------------------------------------------------|---------------|-----------|-----------------------------------|
| Nombre maximal de volumes FlexCache que vous pouvez créer à partir d'un volume d'origine | 10            | 10        | 100                               |
| Nombre maximal recommandé de volumes d'origine par nœud                                  | 10            | 100       | 100                               |
| Nombre maximal recommandé de volumes FlexCache par nœud                                  | 10            | 100       | 100                               |
| Nombre maximal recommandé de composants FlexGroup dans un volume FlexCache par nœud      | 40            | 800       | 800                               |
| Nombre maximal de composants par volume FlexCache par nœud                               | 32            | 32        | 32                                |

## Créer un volume FlexCache

Vous pouvez créer un volume FlexCache dans le même cluster pour améliorer les performances lors de l'accès à un objet à chaud. Si des data centers sont implantés sur différents sites, vous pouvez créer des volumes FlexCache sur des clusters distants pour accélérer l'accès aux données.

### Description de la tâche

- À partir de ONTAP 9.5, FlexCache prend en charge les volumes FlexVol en tant que volumes d'origine et les volumes FlexGroup en tant que volumes FlexCache.
- Depuis ONTAP 9.7, les volumes FlexVol et FlexGroup sont pris en charge en tant que volumes d'origine.
- Depuis ONTAP 9.14.0, vous pouvez créer un volume FlexCache non chiffré à partir d'une source chiffrée.

### Avant de commencer

- Vous devez exécuter ONTAP 9.5 ou une version ultérieure.
- Si vous utilisez ONTAP 9.6 ou une version antérieure, vous devez ["Ajoutez une licence FlexCache"](#).


Aucune licence FlexCache n'est requise pour ONTAP 9.7 ou version ultérieure. À partir de ONTAP 9.7, la fonctionnalité FlexCache est incluse dans ONTAP et ne nécessite plus de licence ni d'activation.




Si une paire haute disponibilité est utilisée ["Cryptage SAS ou disques NVMe \(SED, NSE, FIPS\)"](#), vous devez suivre les instructions de la rubrique ["Retour d'un lecteur FIPS ou SED en mode non protégé"](#) Pour tous les disques de la paire HA avant d'initialiser le système (options de démarrage 4 ou 9). Si vous ne le faites pas, vous risquez de subir des pertes de données si les disques sont requalifiés.

## Exemple 4. Étapes

### System Manager

1. Si le volume FlexCache se trouve sur un autre cluster que le volume d'origine, créez une relation entre clusters :
  - a. Dans le cluster local, cliquez sur **protection > Présentation**.
  - b. Développez **intercluster Settings**, cliquez sur **Add Network interfaces** et ajoutez les interfaces réseau intercluster du cluster.Répétez cette étape sur le cluster distant.
  - c. Dans le cluster distant, cliquez sur **protection > Présentation**. Cliquez sur  dans la section homologues du cluster et cliquez sur **générer une phrase de passe**.
  - d. Copiez la phrase secrète générée et collez-la dans le cluster local.
  - e. Dans le cluster local, sous pairs de cluster, cliquez sur **clusters homologues** et créez des clusters locaux et distants.
2. Créer une relation de SVM entre pairs :

Sous Storage VM homologues, cliquez sur, puis sur  **Peer Storage VMs** pour homologuer les machines virtuelles de stockage.

3. Sélectionnez **stockage > volumes**.
4. Sélectionnez **Ajouter**.
5. Sélectionnez **plus d'options**, puis sélectionnez **Ajouter en tant que cache pour un volume distant**.



Si vous exécutez ONTAP 9.8 ou une version ultérieure et que vous souhaitez désactiver QoS ou choisir une stratégie QoS personnalisée, cliquez sur **plus d'options**, puis sous **stockage et optimisation**, sélectionnez **niveau de service de performances**.

### CLI

1. Si le volume FlexCache à créer se trouve dans un autre cluster, créez une relation entre clusters :
  - a. Sur le cluster destination, créez une relation entre pairs avec le cluster source de protection des données :

```
cluster peer create -generate-passphrase -offer-expiration
MM/DD/YYYY HH:MM:SS|1...7days|1...168hours -peer-addr
<peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name>,...|*
-ipospace <ipospace_name>
```

Depuis ONTAP 9.6, le chiffrement TLS est activé par défaut lors de la création d'une relation cluster peer-to-peer. Le chiffrement TLS est pris en charge pour la communication intercluster entre les volumes d'origine et FlexCache. Vous pouvez également désactiver le chiffrement TLS pour la relation cluster peer, si nécessaire.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers *
```

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR  
Expiration Time: 6/7/2017 08:16:10 EST  
Initial Allowed Vserver Peers: \*  
Intercluster LIF IP: 192.140.112.101  
Peer Cluster Name: Clus\_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed again.

- a. Sur le cluster source, authentifier le cluster source sur le cluster destination :

```
cluster peer create -peer-addr <peer_LIF_IPs> -ipspace <ipspace>
```

```
cluster01::> cluster peer create -peer-addr
192.140.112.101,192.140.112.102
```

Notice: Use a generated passphrase or choose a passphrase of 8 or more characters.

To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:  
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.

2. Si le volume FlexCache se trouve dans un SVM différent de celui du volume d'origine, créer une relation de SVM peer-to-peer flexcache en tant qu'application :

- a. Si la SVM se trouve dans un autre cluster, créer une autorisation SVM pour les SVM de peering :

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

L'exemple suivant illustre la création d'une autorisation de pairs SVM qui s'applique à tous les SVM locaux :

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache
```

Warning: This Vserver peer permission applies to all local Vservers.  
After that no explicit  
"vserver peer accept" command required for Vserver peer relationship  
creation request  
from peer cluster "cluster2" with any of the local Vservers. Do you  
want to continue? {y|n}: y

a. Créer la relation entre SVM :

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. Créer un volume FlexCache :

```
volume flexcache create -vserver <cache_svm> -volume
<cache_vol_name> -auto-provision-as flexgroup -size <vol_size>
-origin-vserver <origin_svm> -origin-volume <origin_vol_name>
```

L'exemple suivant illustre la création d'un volume FlexCache et sélectionne automatiquement les agrégats existants pour le provisionnement :

```
cluster1::> volume flexcache create -vserver vs_1 -volume fc1 -auto
-provision-as flexgroup -origin-volume vol_1 -size 160MB -origin
-vserver vs_1
[Job 443] Job succeeded: Successful
```

L'exemple suivant illustre la création d'un volume FlexCache et définit la Junction path :

```
cluster1::> flexcache create -vserver vs34 -volume fc4 -aggr-list
aggr34,aggr43 -origin-volume origin1 -size 400m -junction-path /fc4
[Job 903] Job succeeded: Successful
```

4. Vérifier la relation FlexCache depuis le volume FlexCache et le volume d'origine

a. Afficher la relation FlexCache dans le cluster :

```
volume flexcache show
```



```
cluster1::> volume flexcache show
```

| Vserver        | Volume | Size  | Origin-Vserver | Origin-Volume |
|----------------|--------|-------|----------------|---------------|
| Origin-Cluster |        |       |                |               |
| vs_1           | fc1    | 160MB | vs_1           | vol_1         |
| cluster1       |        |       |                |               |

- b. Afficher toutes les relations FlexCache dans le cluster d'origine :

```
volume flexcache origin show-caches
```

```
cluster::> volume flexcache origin show-caches
```

| Origin-Vserver | Origin-Volume | Cache-Vserver | Cache-Volume |
|----------------|---------------|---------------|--------------|
| Cache-Cluster  |               |               |              |
| vs0            | ovol1         | vs1           | cfg1         |
| clusA          |               |               |              |
| vs0            | ovol1         | vs2           | cfg2         |
| clusB          |               |               |              |
| vs_1           | vol_1         | vs_1          | fc1          |
| cluster1       |               |               |              |

## Résultat

Le volume FlexCache a été créé avec succès. Les clients peuvent monter le volume en utilisant la Junction path du volume FlexCache.

## Informations associées

["Cluster et SVM peering"](#)

## Réécriture FlexCache

### Présentation de la réécriture de FlexCache

Introduit dans ONTAP 9.15.1, l'écriture différée FlexCache est un autre mode de fonctionnement pour l'écriture au niveau du cache. La réécriture permet de valider l'écriture sur un stockage stable au niveau du cache et d'en accuser réception au client sans attendre que les données soient à l'origine. Les données sont transférées de manière asynchrone vers l'origine. Le résultat est un système de fichiers distribué à l'échelle mondiale qui permet aux écritures d'effectuer des opérations à des vitesses proches de celles locales pour des charges de travail et des environnements spécifiques, et qui offre des avantages considérables en termes de performances.



ONTAP 9.12.1 a présenté une fonctionnalité de réécriture sous forme de préversion publique. Il s'agit de la version à écriture différée 1 (wbv1) et ne doit pas être considéré comme la version à écriture différée dans ONTAP 9.15.1, qui est appelée la version à écriture différée 2 (wbv2).

### Écriture différée contre écriture immédiate

Depuis son lancement dans ONTAP 9.5, FlexCache est un cache en lecture-écriture, mais il fonctionne en mode d'écriture immédiate. Les écritures du cache ont été envoyées à l'origine pour être stockées dans un stockage stable. Une fois que l'origine a validé l'écriture sur un stockage stable, elle a reconnu l'écriture dans le cache. Le cache accuse alors réception de l'écriture sur le client. Ainsi, chaque écriture a des frais de déplacement du réseau entre le cache et l'origine. La réécriture de FlexCache change cela.



Après la mise à niveau vers ONTAP 9.15.1, vous pouvez convertir un cache d'écriture immédiate classique en cache à écriture différée et, si nécessaire, revenir à l'écriture immédiate. Cela peut cependant compliquer la lecture des journaux de diagnostic en cas de problème.

|                    | Ecrivez                                | Réécriture                               |
|--------------------|----------------------------------------|------------------------------------------|
| Version ONTAP      | 9.6+                                   | 9.15.1+                                  |
| Cas d'utilisation  | Charge de travail exigeante en lecture | Charge de travail exigeante en écritures |
| Données validées à | Origine                                | Cache                                    |
| Expérience client  | De type WAN                            | LAN-Ike                                  |
| Limites            | 100 par origine                        | 10 par origine                           |
| "CAP Theorem"      | Disponible et tolérant à la partition  | Disponibilité et cohérence               |

### Terminologie de réécriture FlexCache

Comprendre les concepts et les termes clés qui travaillent avec la réécriture FlexCache.

| Durée                                       | Définition                                                                                                                                                                                                                                       |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>données corrompues</b>                   | Données qui ont été validées pour un stockage stable au niveau du cache, mais qui n'ont pas été transférées vers l'origine.                                                                                                                      |
| <b>Exclusive Lock délégation (XLD)</b>      | Autorité de verrouillage au niveau du protocole accordée par fichier à un cache. Cette autorité permet au cache de distribuer des verrous d'écriture exclusifs aux clients sans contacter l'origine.                                             |
| <b>Délégation de verrous partagés (SLD)</b> | Autorité de verrouillage au niveau du protocole accordée par fichier à un cache. Cette autorité permet au cache de distribuer des verrous de lecture partagés aux clients sans contacter l'origine.                                              |
| <b>Réécriture</b>                           | Mode de fonctionnement FlexCache dans lequel les écritures dans un cache sont validées sur un stockage stable au niveau de ce cache et immédiatement réceptionnées sur le client. Les données sont écrites de manière asynchrone vers l'origine. |

| Durée                                                  | Définition                                                                                                                                                                                                                                                 |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Écrit</b>                                           | Mode de fonctionnement FlexCache dans lequel les écritures dans un cache sont transmises à l'origine pour être validées dans un stockage stable. Une fois validé, l'origine reconnaît l'écriture dans le cache et le cache reconnaît l'écriture au client. |
| <b>Système d'enregistrement de données (DDRS) sale</b> | Mécanisme propriétaire qui assure le suivi des données corrompues dans un cache à écriture différée par fichier.                                                                                                                                           |
| <b>Origine</b>                                         | FlexGroup ou FlexVol contenant les données source de tous les volumes FlexCache cache. Il s'agit de la source unique de vérité, orchestre le verrouillage et assure 100 % de cohérence des données, de devise et de cohérence.                             |
| <b>Cache</b>                                           | FlexGroup qui est un volume de cache fragmenté de l'origine FlexCache.                                                                                                                                                                                     |

### Cohérent, actuel et cohérent

FlexCache est la solution de NetApp pour disposer des bonnes données, partout et à tout moment. FlexCache est 100 % cohérent, actuel et cohérent 100 % du temps :

- **Cohérent:** les données sont les mêmes partout où elles sont consultées.
- **Actuel:** les données sont toujours à jour.
- **Cohérent:** les données sont correctes/non corrompues.

### Architecture de réécriture de FlexCache

FlexCache a été conçu dans un souci de cohérence, avec notamment les deux modes de fonctionnement en écriture : écriture différée et écriture immédiate. Le mode de fonctionnement classique avec écriture immédiate et le nouveau mode de fonctionnement avec écriture différée introduit dans ONTAP 9.15.1 garantissent que les données accédées seront toujours cohérentes à 100 %, actuelles et cohérentes.

Les concepts suivants décrivent en détail le fonctionnement de l'écriture différée FlexCache.

#### Délégations

Les délégations de verrouillage et les délégations de données permettent à FlexCache de conserver des caches d'écriture différée et d'écriture immédiate, cohérents et à jour. L'origine orchestre les deux délégations.

#### Verrouiller les délégations

Une délégation de verrouillage est une autorité de verrouillage au niveau du protocole que l'origine accorde à chaque fichier à un cache pour émettre des verrous de protocole aux clients selon les besoins. Ceux-ci incluent [Délégations de verrous exclusives \(XLD\)](#) et [Délégations de verrous partagés \(SLD\)](#).

#### XLD et réécriture

Pour s'assurer que ONTAP n'a jamais à réconcilier une écriture en conflit, un XLD est accordé à un cache où un client demande d'écrire dans un fichier. Il est important de noter qu'un seul XLD peut exister pour n'importe quel fichier à tout moment, ce qui signifie qu'il n'y aura jamais plus d'un rédacteur dans un fichier à la fois.

Lorsque la demande d'écriture dans un fichier arrive dans un cache activé pour l'écriture différée, les étapes suivantes sont effectuées :

1. Le cache vérifie s'il possède déjà un XLD pour le fichier demandé. Si c'est le cas, il accordera le verrouillage en écriture au client tant qu'un autre client n'écrit pas dans le fichier au niveau du cache. Si le cache n'a pas de XLD pour le fichier demandé, il en demandera un à l'origine. Il s'agit d'un appel propriétaire qui traverse le réseau intercluster.
2. Lors de la réception de la demande XLD du cache, l'origine vérifie s'il existe un XLD en attente pour le fichier dans un autre cache. Si c'est le cas, il se souviendra de la XLD de ce fichier, qui déclenche un vidage de tout de [données corrompues](#) ce cache à l'origine.
3. Une fois que les données corrompues de ce cache sont vidées et validées dans un stockage stable à l'origine, l'origine accorde le fichier XLD au cache demandeur.
4. Une fois le fichier XLD reçu, le cache accorde le verrouillage au client et l'écriture commence.

Un schéma de séquence de haut niveau couvrant certaines de ces étapes est décrit dans le [\[write-back-sequence-diagram\]](#) schéma de séquence.

Du point de vue du client, tout verrouillage fonctionnera comme s'il s'agissait d'écrire dans un FlexVol ou un FlexGroup standard avec un petit délai potentiel lorsque le verrouillage en écriture est demandé.

Dans son itération actuelle, si un cache activé pour l'écriture différée contient le XLD pour un fichier, ONTAP bloquera l'accès **any** à ce fichier dans d'autres caches, y compris les READ opérations.



Il y a une limite de 170 XLD par composant d'origine.

## Délégations de données

Une délégation de données est une garantie par fichier donnée à un cache par l'origine que les données mises en cache pour ce fichier sont à jour. Tant que le cache dispose d'une délégation de données pour un fichier, il peut transmettre les données en cache pour ce fichier au client sans avoir à contacter l'origine. Si le cache n'a pas de délégation de données pour le fichier, il doit contacter l'origine pour recevoir les données demandées par le client.

En mode écriture différée, la délégation de données d'un fichier est révoquée si un XLD est pris pour ce fichier dans un autre cache ou à l'origine. Cela permet de débloquer efficacement le fichier des clients de tous les autres caches et de l'origine, même pour les lectures. Il s'agit d'un compromis à effectuer pour s'assurer que les anciennes données ne sont jamais utilisées.

Les lectures effectuées sur un cache avec écriture différée fonctionnent généralement de la même manière que les lectures effectuées sur un cache avec écriture immédiate. Dans les caches à écriture immédiate et à écriture différée, il peut y avoir un impact initial `READ` sur les performances lorsque le fichier demandé dispose d'un verrouillage en écriture exclusif dans un cache à écriture différée autre que celui où la lecture est émise. La XLD doit être révoquée et les données corrompues doivent être validées à l'origine avant que la lecture sur l'autre cache puisse être traitée.

## Suivi des données corrompues

L'écriture différée du cache à l'origine se produit de manière asynchrone. Cela signifie que les données corrompues ne sont pas immédiatement réécrites à l'origine. ONTAP utilise un système d'enregistrement des données corrompues pour assurer le suivi des données corrompues par fichier. Chaque enregistrement de données corrompues (DDR) représente environ 20 Mo de données corrompues pour un fichier particulier. Lorsqu'un fichier est en cours d'écriture, ONTAP commence à vider les données corrompues une fois que deux DDRs ont été remplis et que le troisième DDR est en cours d'écriture. Il en résulte qu'environ 40 Mo de

données corrompues restent dans un cache pendant les écritures. Pour les protocoles avec état (NFSv4.x, SMB), les 40 Mo de données restantes seront retransmis à l'origine lorsque le fichier est fermé. Pour les protocoles sans état (NFSv3), les 40 Mo de données sont réappliqués lorsque l'accès au fichier est demandé dans un autre cache ou lorsque le fichier est inactif pendant deux minutes ou plus, jusqu'à cinq minutes maximum. Pour plus d'informations sur le vidage des données corrompues déclenché par un temporisateur ou déclenché par un espace, reportez-vous à la section [Épureurs de cache](#).

Outre les DDRs et les épureurs, certaines opérations NAS front-end déclenchent également le vidage de toutes les données corrompues d'un fichier :

- SETATTR
  - 'stETATTR' qui ne modifie que mtime, atime et/ou ctime peut être traité au niveau du cache, évitant ainsi la pénalité du WAN.
- CLOSE
- OPEN dans un autre cache
- READ dans un autre cache
- REaddir dans un autre cache
- REaddirplus dans un autre cache
- WRITE dans un autre cache

### Mode déconnecté

Lorsqu'un XLD pour un fichier est conservé dans un cache d'écriture et que ce cache est déconnecté de l'origine, les lectures pour ce fichier sont toujours autorisées sur les autres caches et à l'origine. Ce comportement est différent lorsqu'un XLD est conservé par un cache activé pour l'écriture différée. Dans ce cas, si le cache est déconnecté, les lectures dans le fichier se suspendent partout. Cela permet d'assurer une cohérence de 100 %, le maintien de la monnaie et de la cohérence. Les lectures sont autorisées en mode d'écriture immédiate car l'origine est garantie que toutes les données disponibles ont été acquittées en écriture sur le client. En mode écriture différée pendant une déconnexion, l'origine ne peut pas garantir que toutes les données écrites et reconnues par le cache activé pour l'écriture différée ont été transmises à l'origine avant la déconnexion.

Si un cache avec un XLD pour un fichier est déconnecté pendant une période prolongée, un administrateur système peut révoquer manuellement le XLD à l'origine. Cela permettra aux E/S du fichier de reprendre au niveau des caches survivants et de l'origine.



La révocation manuelle du XLD entraîne la perte de toutes les données corrompues du fichier au niveau du cache déconnecté. La révocation manuelle d'un XLD ne doit être effectuée qu'en cas d'interruption catastrophique entre le cache et l'origine.

### Épureurs de cache

Des épureurs dans ONTAP s'exécutent en réponse à des événements spécifiques, tels qu'une temporisation arrivant à expiration ou un dépassement des seuils d'espace. Les épureurs prennent un verrou exclusif sur le fichier en cours de nettoyage, gelant efficacement les E/S dans ce fichier jusqu'à la fin du nettoyage.

Les épureurs comprennent :

- **Nettoyage à base de mtime sur le cache:** ce nettoyage démarre toutes les cinq minutes et nettoie tout fichier restant non modifié pendant deux minutes. Si des données corrompues du fichier sont toujours dans

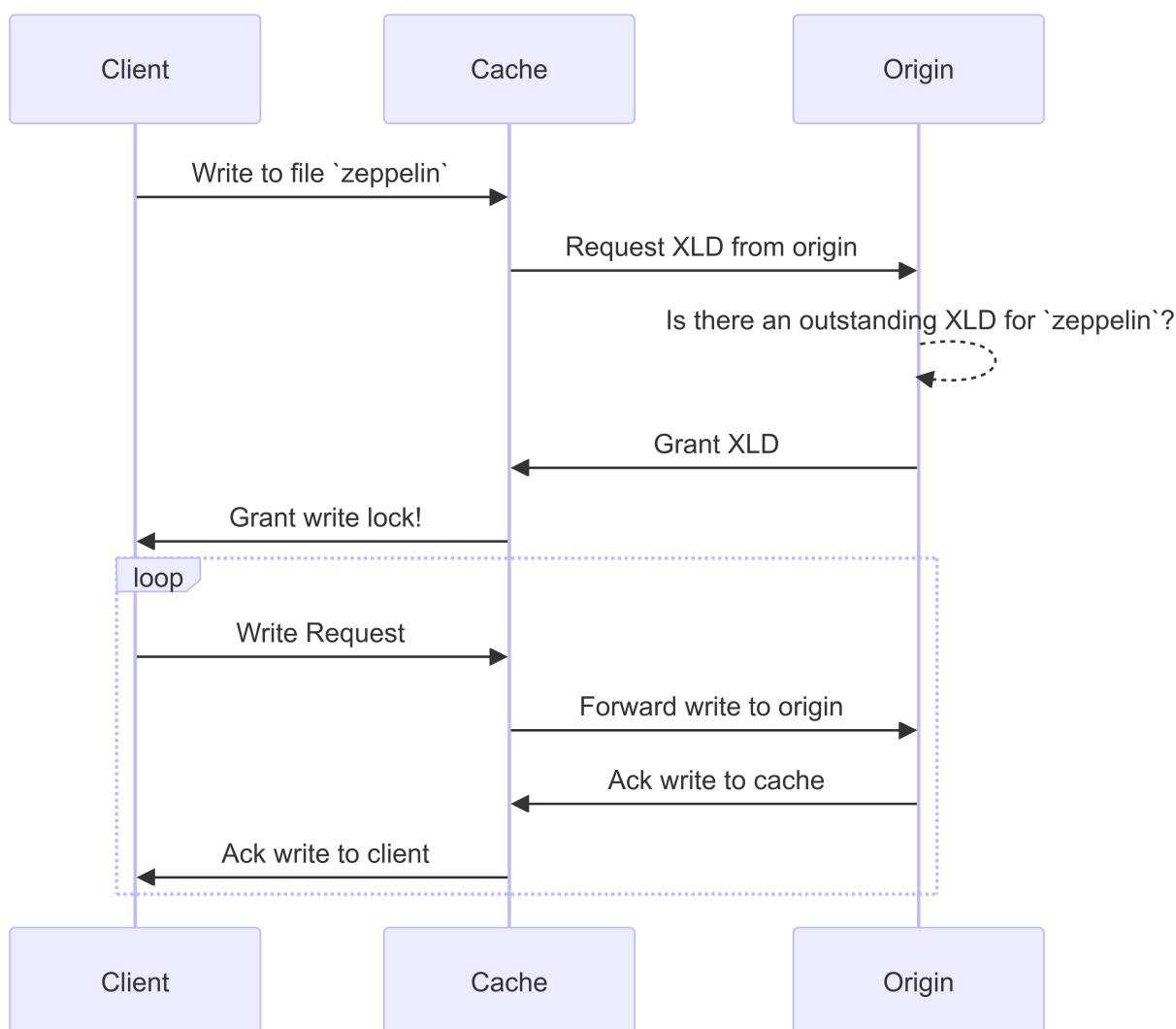
le cache, les E/S vers ce fichier sont suspendues et une réécriture est déclenchée. L'E/S reprendra une fois l'écriture différée terminée.

- **Mtime-based scrubber on origin:** tout comme le scrubber mtime-based au niveau du cache, il s'exécute également toutes les cinq minutes. Cependant, il élimine tout fichier assis non modifié pendant 15 minutes, rappelant la délégation de l'inode. Cette épurateur ne lance pas de réécriture.
- **RW base de la limite de l'épurateur à l'origine:** ONTAP surveille le nombre de délégations de verrous RW qui sont distribuées par constituant d'origine. Si ce nombre dépasse 170, ONTAP commence à nettoyer les délégations de verrouillage d'écriture sur une base au moins récemment utilisée (LRU).
- **Nettoyage basé sur l'espace sur le cache:** si un volume FlexCache atteint 90% plein, le cache est vidé, et il est supprimé sur une base LRU.
- **Scrubber à l'origine :** si un volume d'origine FlexCache atteint 90% plein, le cache est vidé, ce qui l'expulse sur une base LRU.

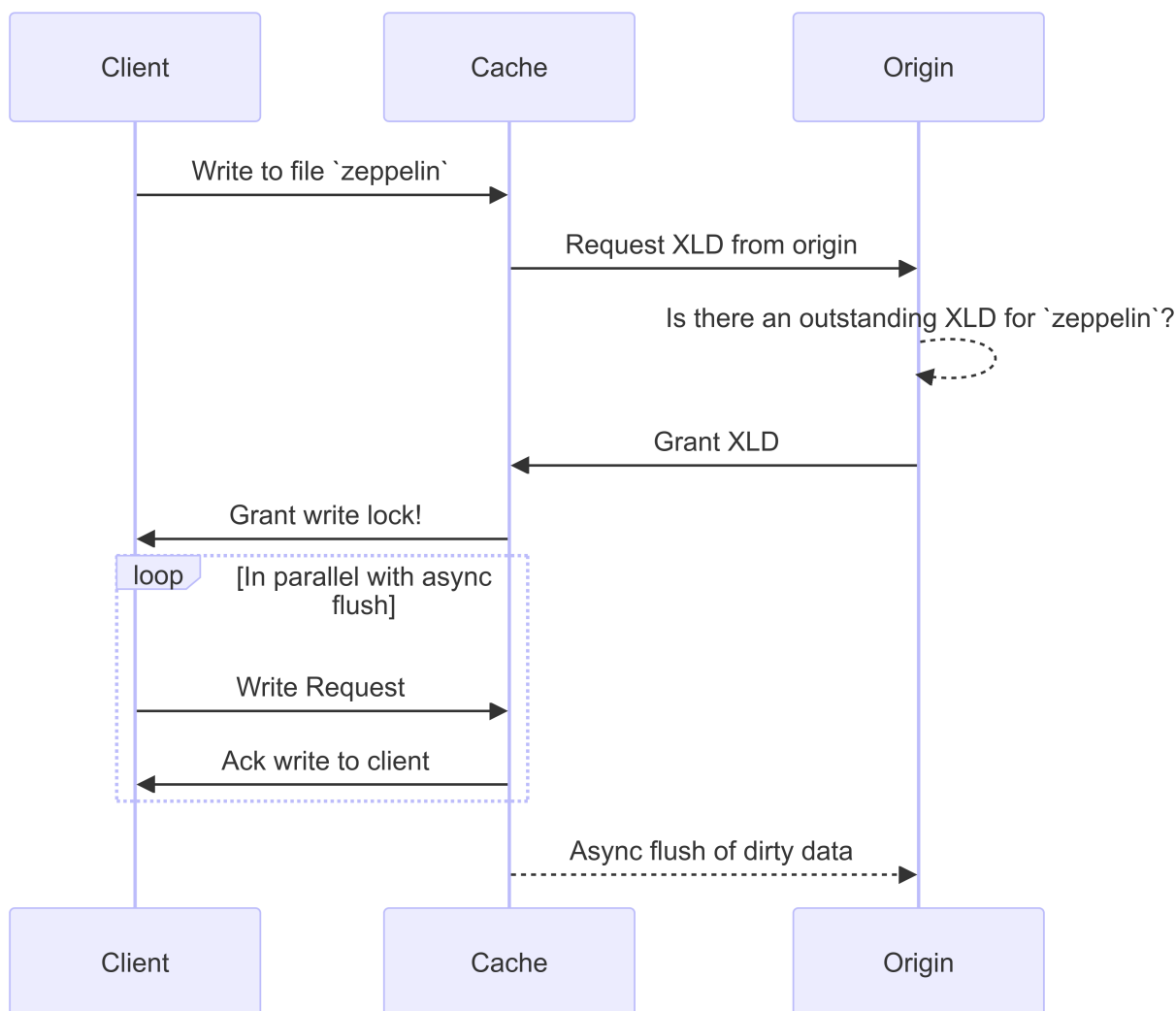
## Diagrammes de séquence

Ces diagrammes de séquence décrivent la différence entre les accusés de réception d'écriture et les modes de réécriture.

### Ecrivez



## Réécriture



### Cas d'utilisation d'écriture différée FlexCache

Il s'agit de profils d'écriture mieux adaptés à un FlexCache à écriture différée. Vous devez tester votre charge de travail pour vérifier si l'écriture différée ou l'annulation fournit les meilleures performances.



La réécriture ne remplace pas la réinscription. Bien que la réécriture soit conçue avec des charges de travail intensives en écriture, la réinscription demeure le meilleur choix pour de nombreuses charges de travail.

### Workloads cibles

#### Taille du fichier

La taille du fichier est moins importante que le nombre d'écritures émises entre `OPEN` le et les `CLOSE` appels pour un fichier. Les petits fichiers ont par nature moins d' `WRITE` appels, ce qui les rend moins idéaux pour les réécritures. Les fichiers volumineux peuvent avoir plus d'écritures entre `OPEN` les appels et `CLOSE` , mais cela n'est pas garanti.

#### Taille d'écriture

Lors de l'écriture à partir d'un client, d'autres appels NAS sont impliqués autres que des appels d'écriture :

- CREATE
- OPEN
- CLOSE
- REaddir/REaddirPLUS
- SETATTR: SETATTR les appels qui ne modifient que `mtime`, `atime` ou `ctime` sont traités dans le cache.

Ces appels doivent être traités à l'origine et déclencher une réécriture de toutes les données corrompues accumulées au niveau du cache activé pour l'écriture différée pour le fichier en cours d'exécution. Les E/S vers le fichier seront suspendues jusqu'à ce que l'écriture différée soit terminée.

En sachant que ces appels doivent traverser le WAN, vous pouvez identifier les charges de travail adaptées à la réécriture. En général, plus le nombre d'écritures pouvant être effectuées entre OPEN les CLOSE appels et sans que l'un des autres appels répertoriés ci-dessus ne soit émis est élevé, plus le gain de performances est élevé.

### Lecture après écriture

Dans le passé, les workloads de lecture après écriture ont des performances médiocres chez FlexCache. Ceci est dû au mode de fonctionnement de la réécriture avant 9.15.1. L' `WRITE` appel au fichier doit être validé à l'origine et l'appel suivant `READ` devra renvoyer les données dans le cache. Les deux opérations sont donc pénalisées par le WAN. Par conséquent, les charges de travail de lecture après écriture sont déconseillées pour FlexCache en mode d'écriture immédiate. Avec l'introduction de la fonctionnalité de réécriture dans la version 9.15.1, les données sont désormais validées au niveau du cache et peuvent être immédiatement lues à partir du cache, éliminant ainsi les pénalités liées au WAN. Si votre charge de travail inclut la lecture après écriture sur les volumes FlexCache, vous devez configurer le cache pour qu'il fonctionne en mode écriture différée.



Si la lecture après écriture est un élément critique de votre charge de travail, vous devez configurer votre cache pour qu'il fonctionne en mode écriture différée.

### Écriture après écriture

Lorsqu'un fichier accumule des données corrompues dans un cache, le cache réécrit les données de manière asynchrone vers l'origine. Cela se traduit naturellement par des moments où le client ferme le fichier avec des données corrompues en attendant toujours d'être retransférées vers l'origine. Si un autre fichier ouvert ou en écriture vient d'être enregistré pour le fichier qui vient d'être fermé et qui contient toujours des données corrompues, l'écriture sera suspendue jusqu'à ce que toutes les données corrompues aient été vidées à l'origine.

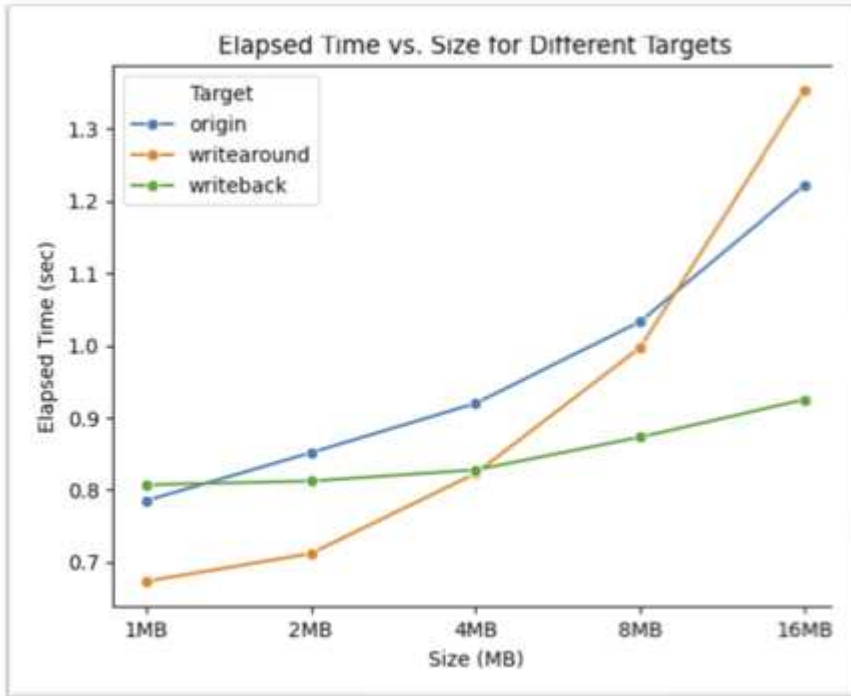
### Considérations relatives à la latence

Lorsque FlexCache fonctionne en mode de réécriture, les clients NAS bénéficient d'avantages à mesure que la latence augmente. Il est toutefois important de noter que la surcharge liée à l'écriture différée est supérieure aux avantages obtenus dans les environnements à faible latence. Dans certains tests NetApp, les bénéfices de l'écriture différée ont commencé autour d'une latence minimale entre le cache et l'origine de 8 ms. Cette latence varie en fonction des charges de travail. Assurez-vous donc de tester pour en savoir plus sur les avantages.

Le graphique suivant montre le point de retour pour l'écriture différée dans les tests de laboratoire NetApp. L' `x` axe est la taille du fichier et l' `y` axe est le temps écoulé. Le test a utilisé NFSv3, à monter avec une et de 256 Ko, et une `rsizewsize` latence WAN de 64 ms. Ce test a été réalisé en utilisant une petite instance ONTAP



Select pour le cache et l'origine, ainsi qu'une seule opération d'écriture par thread. Vos résultats peuvent varier.



L'écriture différée ne doit pas être utilisée pour la mise en cache intracluster. La mise en cache intracluster se produit lorsque l'origine et le cache se trouvent dans le même cluster.

### Conditions préalables à la réécriture de FlexCache

Avant de déployer FlexCache en mode écriture différée, assurez-vous que vous avez satisfait aux conditions requises pour le logiciel, la licence et la configuration du système.

#### Version ONTAP

- L'origine **must** exécute ONTAP 9.15.1 ou une version ultérieure.
- Tout cluster de cache devant fonctionner en mode de réécriture **must** exécute ONTAP 9.15.1 ou une version ultérieure.
- Tout cluster de cache qui n'a pas besoin d'opérer en mode de réécriture peut exécuter n'importe quelle version de ONTAP prise en charge.

#### Licences

FlexCache, y compris le mode d'opération de réécriture, est inclus avec votre achat de ONTAP. Aucune licence supplémentaire n'est requise.

#### Peering

- Les clusters d'origine et de cache doivent être ["peering de cluster"](#)
- Les serveurs virtuels (SVM) sur le cluster d'origine et cache doivent ["peering de vservers"](#) utiliser l'option FlexCache.



Vous n'avez pas besoin de transférer un cluster de cache vers un autre cluster de cache. Il n'est pas non plus nécessaire de placer un SVM en cache sur une autre SVM en cache.

## Interopérabilité de réécriture FlexCache

Prenez en compte ces considérations d'interopérabilité lors du déploiement de FlexCache en mode de réécriture.

### Version ONTAP

Pour utiliser le mode de fonctionnement écriture différée, le cache et l'origine **doivent** exécuter ONTAP 9.15.1 ou une version ultérieure.



Les clusters qui ne sont pas dotés d'un cache avec écriture différée peuvent exécuter des versions antérieures de ONTAP, mais ce cluster ne peut fonctionner qu'en mode d'écriture différée.

Vous pouvez avoir plusieurs versions de ONTAP dans votre environnement.

| Cluster   | Version ONTAP | Écriture différée prise en charge ? |
|-----------|---------------|-------------------------------------|
| Origine   | ONTAP 9.15.1  | S/O †                               |
| Cluster 1 | ONTAP 9.15.1  | Oui.                                |
| Cluster 2 | ONTAP 9.14.1  | Non                                 |

| Cluster   | Version ONTAP | Écriture différée prise en charge ? |
|-----------|---------------|-------------------------------------|
| Origine   | ONTAP 9.14.1  | S/O †                               |
| Cluster 1 | ONTAP 9.15.1  | Non                                 |
| Cluster 2 | ONTAP 9.15.1  | Non                                 |

† Les origines ne sont pas un cache, donc ni la prise en charge de l'écriture différée ni de l'écriture immédiate n'est applicable.



Dans [\[exemple2-table\]](#), aucun cluster ne peut activer le mode de réécriture car l'origine n'exécute pas ONTAP 9.15.1 ou une version ultérieure, ce qui est une exigence stricte.

### Interopérabilité avec les clients

Tout client généralement pris en charge par ONTAP peut accéder à un volume FlexCache, qu'il fonctionne en mode Write-Around ou Write-back. Pour obtenir la liste à jour des clients pris en charge, consultez la page NetApp "[matrice d'interopérabilité](#)".

Bien que la version du client n'ait pas d'importance particulière, le client doit être suffisamment nouveau pour prendre en charge NFSv3, NFSv4.0, NFSv4.1, SMB2.x ou SMB3.x. SMB1 et NFSv2 sont des protocoles obsolètes et ne sont pas pris en charge.

## Réécriture et réinscription

Comme le montre la [\[exemple1-table\]](#), FlexCache fonctionnant en mode écriture différée peut coexister avec les caches fonctionnant en mode écriture immédiate. Il est conseillé de comparer la réinscription à la réécriture à votre charge de travail spécifique.



Si les performances d'une charge de travail sont identiques entre la réécriture et la réinscription, utilisez la réinscription.

## Interopérabilité des fonctionnalités ONTAP

Pour obtenir la liste la plus récente d'interopérabilité des fonctionnalités FlexCache, reportez-vous à la section "[Fonctionnalités prises en charge et non prises en charge pour les volumes FlexCache](#)".

## Activez et gérez l'écriture différée FlexCache

À partir de ONTAP 9.15.1, vous pouvez activer le mode de réécriture de code FlexCache sur les volumes FlexCache afin d'améliorer les performances des environnements de périphérie et du cache avec des charges de travail intensives en écriture. Vous pouvez également déterminer si l'écriture différée est activée sur un volume FlexCache ou désactiver l'écriture différée sur le volume si nécessaire.

Lorsque l'écriture différée est activée sur le volume du cache, les demandes d'écriture sont envoyées au cache local plutôt qu'au volume d'origine.

### Avant de commencer

Vous devez être en mode privilèges avancés.

### Créez un volume FlexCache dont l'écriture différée est activée


#### Étapes


Vous pouvez créer un volume FlexCache dont l'écriture différée est activée via ONTAP System Manager ou l'interface de ligne de commande ONTAP.

## System Manager

1. Si le volume FlexCache se trouve sur un autre cluster que le volume d'origine, créez une relation entre clusters :
  - a. Sur le cluster local, cliquez sur **protection > vue d'ensemble**.
  - b. Développez **intercluster Settings**, cliquez sur **Add Network interfaces** et ajoutez les interfaces intercluster au cluster.

Répétez cette opération sur le cluster distant.

  - c. Sur le cluster distant, cliquez sur **protection > Présentation**. Cliquez sur  dans la section homologues du cluster et cliquez sur **générer une phrase de passe**.
  - d. Copiez la phrase secrète générée et collez-la dans le cluster local.
  - e. Sur le cluster local, sous homologues du cluster, cliquez sur **clusters homologues** et homologue les clusters locaux et distants.
2. Si le volume FlexCache se trouve sur un cluster différent du volume d'origine, créer une relation entre pairs SVM :

Sous **Storage VM homologues**, cliquez sur, puis sur  **Peer Storage VMs** pour faire la distinction entre les machines virtuelles de stockage.

Si le volume FlexCache se trouve sur le même cluster, vous ne pouvez pas créer de relation de pairs SVM à l'aide de System Manager.

3. Sélectionnez **stockage > volumes**.
4. Sélectionnez **Ajouter**.
5. Sélectionnez **plus d'options**, puis sélectionnez **Ajouter en tant que cache pour un volume distant**.
6. Sélectionnez **Activer la réécriture FlexCache**.

## CLI

1. Si le volume FlexCache à créer se trouve dans un autre cluster, créez une relation entre clusters :
  - a. Sur le cluster destination, créez une relation entre pairs avec le cluster source de protection des données :

```
cluster peer create -generate-passphrase -offer-expiration
MM/DD/YYYY HH:MM:SS|1...7days|1...168hours -peer-addr
<peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name>,...|*
-ipospace <ipospace_name>
```

Depuis ONTAP 9.6, le chiffrement TLS est activé par défaut lors de la création d'une relation cluster peer-to-peer. Le chiffrement TLS est pris en charge pour la communication intercluster entre les volumes d'origine et FlexCache. Vous pouvez également désactiver le chiffrement TLS pour la relation cluster peer, si nécessaire.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers *
```

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR  
Expiration Time: 6/7/2017 08:16:10 EST  
Initial Allowed Vserver Peers: \*  
Intercluster LIF IP: 192.140.112.101  
Peer Cluster Name: Clus\_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed again.

- a. Sur le cluster source, authentifier le cluster source sur le cluster destination :

```
cluster peer create -peer-addr <peer_LIF_IPs> -ipspace <ipspace>
```

```
cluster01::> cluster peer create -peer-addr
192.140.112.101,192.140.112.102
```

Notice: Use a generated passphrase or choose a passphrase of 8 or more characters.

To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:  
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.

2. Si le volume FlexCache se trouve dans un SVM différent de celui du volume d'origine, créer une relation de SVM peer-to-peer flexcache en tant qu'application :

- a. Si la SVM se trouve dans un autre cluster, créer une autorisation SVM pour les SVM de peering :

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

L'exemple suivant illustre la création d'une autorisation de pairs SVM qui s'applique à tous les SVM locaux :

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache
```

Warning: This Vserver peer permission applies to all local Vservers. After that no explicit "vserver peer accept" command required for Vserver peer relationship creation request from peer cluster "cluster2" with any of the local Vservers. Do you want to continue? {y|n}: y

a. Créer la relation entre SVM :

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. Créer un volume FlexCache avec l'écriture différée activée :

```
volume flexcache create -vserver <cache_vserver_name> -volume
<cache_flexgroup_name> -aggr-list <list_of_aggregates> -origin
-volume <origin_flexgroup> -origin-vserver <origin_vserver name>
-junction-path <junction_path> -is-writeback-enabled true
```

### Activez l'écriture différée FlexCache sur un volume FlexCache existant

Vous pouvez activer la réécriture de code FlexCache sur un volume FlexCache existant à l'aide de ONTAP System Manager ou de l'interface de ligne de commande ONTAP.

#### System Manager

1. Sélectionnez **stockage > volumes** et sélectionnez un volume FlexCache existant.
2. Sur la page vue d'ensemble du volume, cliquez sur **Modifier** dans le coin supérieur droit.
3. Dans la fenêtre **Edit Volume**, sélectionnez **Enable FlexCache write-back**.

#### CLI

1. Activer la réécriture sur un volume FlexCache existant :

```
volume flexcache config modify -volume <cache_flexgroup_name> -is
-writeback-enabled true
```

## Vérifiez si l'écriture FlexCache est activée

### Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour déterminer si l'écriture différée FlexCache est activée.

#### System Manager

1. Sélectionnez **stockage > volumes** et sélectionnez un volume.
2. Dans le volume **vue d'ensemble**, localisez **détails FlexCache** et vérifiez si l'écriture différée FlexCache est définie sur **activée** sur le volume FlexCache.

#### CLI

1. Vérifiez si l'écriture différée FlexCache est activée :

```
volume flexcache config show -volume cache -fields is-writeback-enabled
```

## Désactiver l'écriture différée sur un volume FlexCache

Avant de pouvoir supprimer un volume FlexCache, vous devez désactiver l'écriture différée FlexCache.

### Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour désactiver l'écriture différée FlexCache.

#### System Manager

1. Sélectionnez **stockage > volumes** et sélectionnez un volume FlexCache existant sur lequel la réécriture FlexCache est activée.
2. Sur la page vue d'ensemble du volume, cliquez sur **Modifier** dans le coin supérieur droit.
3. Dans la fenêtre **Edit Volume**, désélectionnez **Enable FlexCache write-back**.

#### CLI

1. Désactiver l'écriture différée :

```
volume flexcache config modify -volume <cache_vol_name> -is-writeback-enabled false
```

## Gestion des volumes FlexCache

### Considérations relatives à l'audit des volumes FlexCache

Depuis ONTAP 9.7, vous pouvez auditer les événements d'accès aux fichiers NFS dans les relations FlexCache à l'aide de l'audit natif du ONTAP et de la gestion des règles de

## fichiers avec FPolicy.

À partir de ONTAP 9.14.1, FPolicy est pris en charge pour les volumes FlexCache avec NFS ou SMB. Auparavant, FPolicy n'était pas pris en charge pour les volumes FlexCache avec SMB.

Les opérations d'audit natives et FPolicy sont configurées et gérées avec les mêmes commandes d'interface de ligne de commande utilisées pour les volumes FlexVol. Il existe cependant un comportement différent avec les volumes FlexCache.

### • **Audit natif**

- Un volume FlexCache ne peut pas être utilisé comme destination pour les journaux d'audit.
- Si vous souhaitez auditer les lectures et écritures sur les volumes FlexCache, vous devez configurer l'audit sur le SVM cache ainsi que sur le SVM d'origine.

En effet, les opérations du système de fichiers sont vérifiées à l'endroit où elles sont traitées. En d'autres lieux, les lectures sont auditées sur la SVM cache et les écritures sont vérifiées sur la SVM d'origine.

- Pour suivre l'origine des opérations d'écriture, l'UUID et le MSID du SVM sont ajoutés dans le journal d'audit afin d'identifier le volume FlexCache à partir duquel l'écriture est créée.
- Bien que les listes de contrôle d'accès système (CLS) puissent être définies sur un fichier en utilisant les protocoles NFSv4 ou SMB, les volumes FlexCache ne prennent en charge que NFSv3. Par conséquent, les CLS ne peuvent être définies que sur le volume d'origine.

### • **FPolicy**

- Bien que les écritures sur un volume FlexCache soient effectuées sur le volume d'origine, les configurations FPolicy surveillent les écritures sur le volume du cache. Ce n'est pas le cas des audits natifs, dans lesquels les écritures sont auditées sur le volume d'origine.
- Même si ONTAP ne nécessite pas la même configuration FPolicy sur le cache et les SVM d'origine, il est recommandé de déployer deux configurations similaires. Pour ce faire, il est possible de créer une nouvelle politique FPolicy pour le cache, configurée comme celle de la SVM d'origine, mais avec le périmètre de la nouvelle règle limitée au SVM cache.

## **Synchronisation des propriétés d'un volume FlexCache depuis un volume d'origine**

Certaines propriétés de volume du volume FlexCache doivent toujours être synchronisées avec celles du volume d'origine. Si la synchronisation des propriétés du volume d'un volume FlexCache échoue après la modification des propriétés au niveau du volume d'origine, vous pouvez synchroniser manuellement les propriétés.

### **Description de la tâche**

Les propriétés de volume suivantes d'un volume FlexCache doivent toujours être synchronisées avec celles du volume d'origine :

- Style de sécurité (`-security-style`)
- Nom du volume (`-volume-name`)
- Taille maximale du répertoire (`-maxdir-size`)
- Lecture minimum à l'avance (`-min-readahead`)

### **Étape**



1. Depuis le volume FlexCache, synchroniser les propriétés du volume :

```
volume flexcache sync-properties -vserver svm_name -volume flexcache_volume
```

```
cluster1::> volume flexcache sync-properties -vserver vs1 -volume fc1
```

### Mettre à jour les configurations d'une relation FlexCache

Après un déplacement de volumes, un transfert d'agrégats ou un basculement du stockage, les informations de configuration du volume sur le volume d'origine et le volume FlexCache sont mises à jour automatiquement. En cas d'échec des mises à jour automatiques, un message EMS est généré et vous devez mettre à jour manuellement la configuration de la relation FlexCache.

Si le volume d'origine et le volume FlexCache sont en mode déconnecté, vous devrez peut-être effectuer des opérations supplémentaires pour mettre à jour une relation FlexCache manuellement.

#### Description de la tâche

Pour mettre à jour les configurations d'un volume FlexCache, vous devez exécuter la commande à partir du volume d'origine. Pour mettre à jour les configurations d'un volume d'origine, vous devez exécuter la commande à partir du volume FlexCache.

#### Étape

1. Mettre à jour la configuration de la relation FlexCache :

```
volume flexcache config-refresh -peer-vserver peer_svm -peer-volume
peer_volume_to_update -peer-endpoint-type [origin | cache]
```

### Activer les mises à jour des temps d'accès aux fichiers

Depuis ONTAP 9.11.1, vous pouvez activer le `-atime-update` Champ du volume FlexCache pour permettre la mise à jour des temps d'accès aux fichiers. Vous pouvez également définir une période de mise à jour de l'heure d'accès à l'aide du `-atime-update-period` attribut. Le `-atime-update-period` les attributs contrôlent la fréquence des mises à jour du temps d'accès et la fréquence de leur propagation au volume d'origine.

#### Présentation

ONTAP fournit un champ appelé de niveau volume `-atime-update`, Pour gérer les mises à jour de temps d'accès sur les fichiers et les répertoires lus à l'aide DE READ, READLINK et READDIR. Atime est utilisé pour les décisions de cycle de vie des données pour les fichiers et les répertoires rarement utilisés. Les fichiers rarement utilisés sont ensuite transférés vers le stockage d'archivage et sont souvent transférés vers les bandes.

Le champ `atime-update` est désactivé par défaut sur les volumes FlexCache existants et nouvellement créés. Si vous utilisez des volumes FlexCache avec des versions antérieures à 9.11.1 de ONTAP, vous devez laisser le champ `atime-update` désactivé afin que les caches ne soient pas inutilement supprimés lors d'une opération

de lecture sur le volume d'origine. Toutefois, avec les grands caches FlexCache, les administrateurs utilisent des outils spéciaux pour gérer les données. Ils peuvent ainsi veiller à ce que les données actives restent dans le cache et que les données inactives sont supprimées. Cette opération n'est pas possible si `atime-update` est désactivé. Toutefois, vous pouvez l'activer à partir de ONTAP 9.11.1 `-atime-update` et `-atime-update -period`, et utiliser les outils requis pour gérer les données mises en cache.

### Avant de commencer

Tous les volumes FlexCache doivent exécuter ONTAP 9.11.1 ou une version ultérieure.

### Description de la tâche

Réglage `-atime-update-period` une mise à jour de 86400 secondes n'autorise pas plus d'une durée d'accès par période de 24 heures, quel que soit le nombre d'opérations de lecture effectuées sur un fichier.

Réglage du `-atime-update-period 0` envoie des messages à l'origine pour chaque accès en lecture. L'origine informe ensuite chaque volume FlexCache que son heure est dépassée, ce qui affecte les performances.

### Étapes

1. Activer les mises à jour des temps d'accès aux fichiers et définir la fréquence de mise à jour :

```
volume modify -volume vol_name -vserver SVM_name -atime-update true -atime-update-period seconds
```

L'exemple suivant active `-atime-update` et `-atime-update-period` à 86400 secondes ou 24 heures :

```
c1: volume modify -volume origin1 vs1_c1 -atime-update true -atime-update-period 86400
```

2. Vérifiez-le `-atime-update` est activé :

```
volume show -volume vol_name -fields atime-update,atime-update-period
```

```
c1::*> volume show -volume cache1_origin1 -fields atime-update,atime-update-period
vserver volume atime-update atime-update-period

vs2_c1 cache1_origin1 true 86400
```

### Activer le verrouillage global des fichiers

Depuis ONTAP 9.10.1, le verrouillage global des fichiers peut être appliqué pour empêcher les lectures de tous les fichiers mis en cache liés.

Lorsque le verrouillage global des fichiers est activé, les modifications du volume d'origine sont suspendues jusqu'à ce que tous les volumes FlexCache soient en ligne. Le verrouillage global des fichiers doit être activé uniquement lorsque vous avez le contrôle de la fiabilité des connexions entre le cache et l'origine du fait de la

suspension et des délais de modification possibles lorsque les volumes FlexCache sont hors ligne.

## Avant de commencer

- Le verrouillage global des fichiers requiert que les clusters contenant l'origine et tous les caches associés exécutent ONTAP 9.9.1 ou une version ultérieure. Le verrouillage global des fichiers peut être activé sur les volumes FlexCache nouveaux ou existants. La commande peut être exécutée sur un seul volume et s'applique à tous les volumes FlexCache associés.
- Vous devez être au niveau de privilège avancé pour activer le verrouillage global des fichiers.
- Si vous restaurez une version de ONTAP antérieure à la version 9.9.1, le verrouillage global des fichiers doit d'abord être désactivé sur les caches d'origine et associés. Pour désactiver, à partir du volume d'origine, exécutez : `volume flexcache prepare-to-downgrade -disable-feature-set 9.10.0`
- Le processus permettant d'activer le verrouillage global des fichiers dépend de la présence ou non de caches dans l'origine :
  - [\[enable-gfl-new\]](#)
  - [\[enable-gfl-existing\]](#)

## Activation du verrouillage global des fichiers sur les nouveaux volumes FlexCache

### Étapes

1. Création du volume FlexCache avec `-is-global-file-locking` défini sur vrai :

```
volume flexcache create volume volume_name -is-global-file-locking-enabled true
```



La valeur par défaut de `-is-global-file-locking` est « faux ». Lorsque c'est le cas `volume flexcache create` les commandes sont exécutées sur un volume, elles doivent être passées avec `-is-global-file-locking enabled` défini sur « vrai ».

## Activation du verrouillage global des fichiers sur les volumes FlexCache existants

### Étapes

1. Le verrouillage global des fichiers doit être défini à partir du volume d'origine.
2. L'origine ne peut avoir d'autres relations existantes (par exemple, SnapMirror). Toute relation existante doit être dissociée. Tous les caches et volumes doivent être connectés au moment de l'exécution de la commande. Pour vérifier l'état de la connexion, exécutez :

```
volume flexcache connection-status show
```

L'état de tous les volumes répertoriés doit s'afficher sous `connected`. Pour plus d'informations, voir ["Afficher l'état d'une relation FlexCache"](#) ou ["Synchronisation des propriétés d'un volume FlexCache depuis une origine"](#).

3. Activer le verrouillage global des fichiers sur les caches :

```
volume flexcache origin config show/modify -volume volume_name -is-global-file-locking-enabled true
```

## Préremplissage d'un volume FlexCache

Le volume FlexCache peut être prérempli afin de réduire le temps d'accès aux données en cache.

### Ce dont vous avez besoin

- Vous devez être un administrateur de cluster au niveau de privilège avancé
- Les chemins que vous transmettez pour la préremplissage doivent exister ou l'opération de préremplissage échoue.

### Description de la tâche

- Préremplissage lit uniquement les fichiers et parcourt les répertoires
- Le `-isRecursion` indicateur s'applique à la liste complète des répertoires transmis à préremplissage

### Étapes

#### 1. Préremplissage d'un volume FlexCache :

```
volume flexcache prepopulate -cache-vserver vs2 -cache-volume -path
-list path_list -isRecursion true|false
```

- Le `-path-list` paramètre indique le chemin du répertoire relatif que vous souhaitez préremplir à partir du répertoire racine d'origine. Par exemple, si le répertoire racine d'origine est nommé `/origine` et qu'il contient des répertoires `/origine/dir1` et `/origine/dir2`, vous pouvez spécifier la liste des chemins comme suit : `-path-list dir1, dir2` ou `-path-list /dir1, /dir2`.
- La valeur par défaut du `-isRecursion` Le paramètre est vrai.

Cet exemple préremplit un chemin de répertoire unique :

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list /dir1
(volume flexcache prepopulate start)
[JobId 207]: FlexCache prepopulate job queued.
```

Cet exemple préremplit les fichiers de plusieurs répertoires :

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list /dir1,/dir2,/dir3,/dir4
(volume flexcache prepopulate start)
[JobId 208]: FlexCache prepopulate job queued.
```

Cet exemple préremplit un seul fichier :

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list /dir1/file1.txt
(volume flexcache prepopulate start)
[JobId 209]: FlexCache prepopulate job queued.
```

Cet exemple prérenseigne tous les fichiers de l'origine :

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list / -isRecursion true
(volume flexcache prepopulate start)
[JobId 210]: FlexCache prepopulate job queued.
```

Cet exemple inclut un chemin non valide pour la prépopulation :

```
cluster1::*> flexcache prepopulate start -cache-volume
vol_cache2_vs3_c2_vol_origin1_vs1_c1 -cache-vserver vs3_c2 -path-list
/dir1, dir5, dir6
(volume flexcache prepopulate start)

Error: command failed: Path(s) "dir5, dir6" does not exist in origin
volume
 "vol_origin1_vs1_c1" in Vserver "vs1_c1".
```

2. Afficher le nombre de fichiers lus :

```
job show -id job_ID -ins
```

## Supprime une relation FlexCache

Si vous n'avez plus besoin du volume FlexCache, vous pouvez supprimer une relation FlexCache et le volume FlexCache.

### Étapes

1. Depuis le cluster qui dispose du volume FlexCache, mettre le volume FlexCache hors ligne :

```
volume offline -vserver svm_name -volume volume_name
```

2. Supprimez le volume FlexCache :

```
volume flexcache delete -vserver svm_name -volume volume_name
```

Les détails de la relation FlexCache sont supprimés du volume d'origine et du volume FlexCache.

# Gestion du réseau

## Commencez

### Présentation de la gestion du réseau

Vous pouvez utiliser les informations suivantes pour effectuer des opérations basiques d'administration du réseau de stockage via System Manager ou l'interface de ligne de commandes. Vous pouvez configurer des ports réseau physiques et virtuels (VLAN et groupes d'interface), créer des LIF à l'aide d'IPv4 et d'IPv6, gérer le routage et les services de résolution d'hôte dans les clusters, utiliser l'équilibrage de charge pour optimiser le trafic réseau et surveiller un cluster à l'aide de SNMP.

Sauf mention contraire, les procédures de l'interface de ligne de commandes s'appliquent à toutes les versions de ONTAP 9.

Pour en savoir plus sur l'impact des fonctionnalités réseau disponibles avec chaque version de ONTAP 9, consultez le ["Notes de version de ONTAP"](#).

Depuis ONTAP 9.8, vous pouvez utiliser System Manager pour afficher un graphique indiquant les composants et la configuration de votre réseau. Depuis la version ONTAP 9.12, vous pouvez afficher l'association de LIF et de sous-réseau sur la grille des interfaces réseau. Si vous utilisez le Gestionnaire système classique (disponible uniquement dans ONTAP 9.7 et versions antérieures), reportez-vous à la section ["Gestion du réseau"](#).

La nouvelle fonction de visualisation réseau permet aux utilisateurs de voir le chemin des connexions réseau entre les hôtes, ports, SVM, volumes, etc. Dans une interface graphique.

Le graphique s'affiche lorsque vous sélectionnez **réseau > vue d'ensemble** ou lorsque vous sélectionnez → dans la section **réseau** du tableau de bord.

Les catégories de composants suivantes sont indiquées sur le graphique :


- Hôtes
- Ports de stockage
- Interfaces réseau
- Machines virtuelles de stockage
- Composants d'accès aux données

Chaque section fournit des informations supplémentaires que vous pouvez placer le curseur de la souris sur ou sélectionner pour effectuer des tâches de gestion et de configuration du réseau.

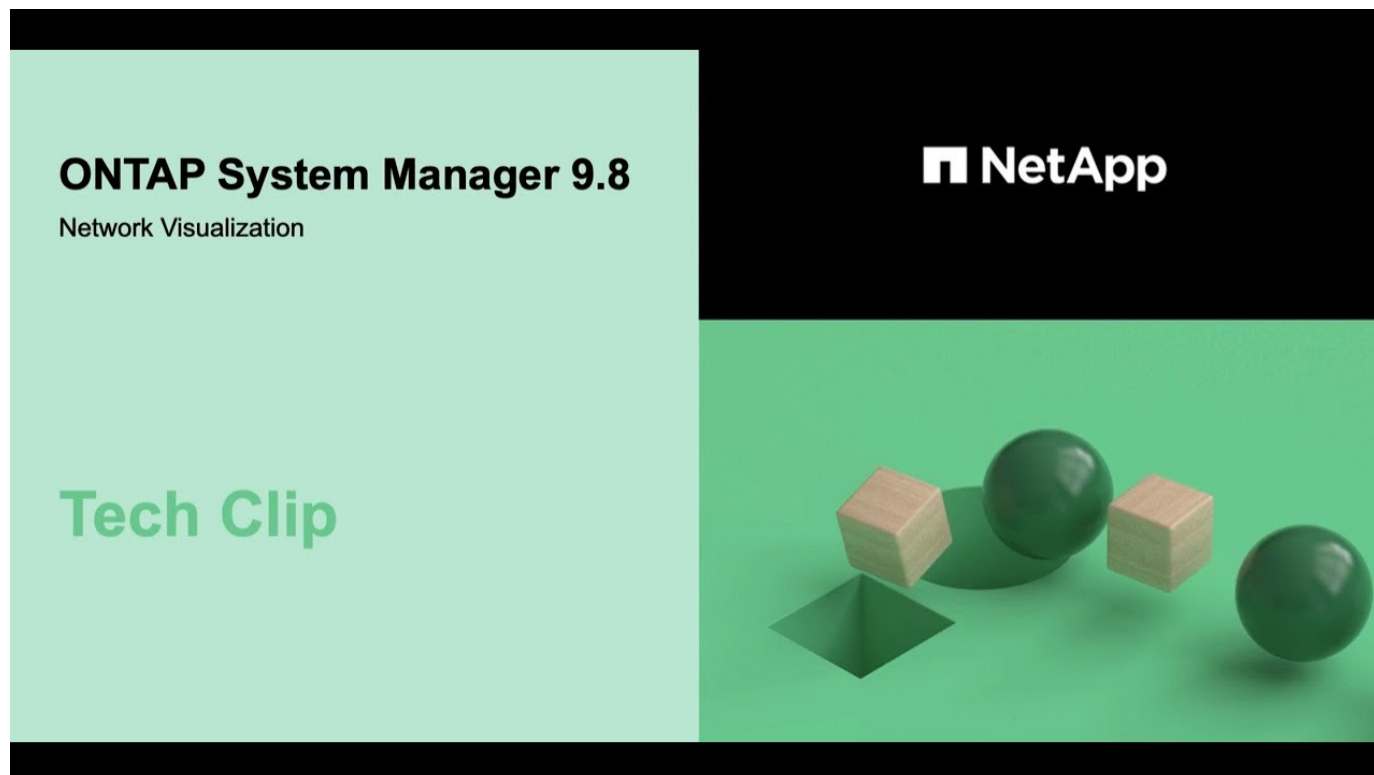
### Exemples

Voici quelques exemples des nombreuses façons dont vous pouvez interagir avec le graphique pour afficher des détails sur chaque composant ou lancer des actions pour gérer votre réseau :

- Cliquez sur un hôte pour afficher sa configuration : les ports, les interfaces réseau, les machines virtuelles de stockage et les composants d'accès aux données qui lui sont associés.

- Passez la souris sur le nombre de volumes d'une VM de stockage pour sélectionner un volume pour en afficher les détails.
- Sélectionnez une interface iSCSI pour afficher ses performances la semaine dernière.
- Cliquez sur  en regard d'un composant pour lancer des actions de modification de ce composant.
- Déterminez rapidement l'emplacement des problèmes dans votre réseau, indiqué par un « X » à côté de composants défectueux.

### Vidéo de visualisation réseau de System Manager



### Vérifiez votre configuration réseau après une mise à niveau ONTAP à partir de ONTAP 9.7x ou version antérieure

Après avoir effectué la mise à niveau de ONTAP 9.7x ou une version antérieure vers ONTAP 9.8 ou une version ultérieure, vous devez vérifier la configuration de votre réseau. Après la mise à niveau, ONTAP surveille automatiquement l'accessibilité de la couche 2.

#### Étape

1. Vérifiez que chaque port est joignable par rapport au domaine de diffusion attendu :

```
network port reachability show -detail
```

La sortie de la commande contient les résultats de l'accessibilité. Utilisez l'arbre décisionnel et le tableau ci-dessous pour comprendre les résultats de l'accessibilité (état-accessibilité) et déterminer ce que, le cas échéant, faire ensuite.



| état-accessibilité | Description |
|--------------------|-------------|
|--------------------|-------------|



|                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ok                                                    | <p>Le port a une capacité de réachabilité de couche 2 à son domaine de diffusion attribué.</p> <p>Si l'état de la capacité d'accessibilité est « ok », mais qu'il y a des « ports inattendus », envisagez de fusionner un ou plusieurs domaines de diffusion. Pour plus d'informations, voir "<a href="#">Fusionner les domaines de diffusion</a>".</p> <p>Si le statut de la capacité d'accessibilité est « ok », mais qu'il y a des « ports inaccessibles », envisagez de diviser un ou plusieurs domaines de diffusion. Pour plus d'informations, voir "<a href="#">Séparer les domaines de diffusion</a>".</p> <p>Si l'état de la capacité de reprise est « ok » et qu'il n'y a pas de ports inattendus ou inaccessibles, votre configuration est correcte.</p> |
| mauvaise configuration de la capacité de réachabilité | <p>Le port n'a pas la capacité de reachcapacité de couche 2 à son domaine de diffusion affecté ; cependant, le port a une capacité de reachcapacité de couche 2 à un domaine de diffusion différent.</p> <p>Vous pouvez réparer l'accessibilité du port. Lorsque vous exécutez la commande suivante, le système affecte le port au broadcast domain auquel il a la capacité de reachcapacité :</p> <pre>network port reachability repair -node -port</pre> <p>Pour plus d'informations, voir "<a href="#">Réparation de l'accessibilité de l'orifice</a>".</p>                                                                                                                                                                                                      |
| sans trabilité                                        | <p>Le port n'a pas la possibilité de reachcapacité de couche 2 à un domaine de diffusion existant.</p> <p>Vous pouvez réparer l'accessibilité du port. Lorsque vous exécutez la commande suivante, le système affecte le port à un nouveau domaine de diffusion créé automatiquement dans l'IPspace par défaut :</p> <pre>network port reachability repair -node -port</pre> <p>Pour plus d'informations, voir "<a href="#">Réparation de l'accessibilité de l'orifice</a>".</p>                                                                                                                                                                                                                                                                                    |
| accessibilité multi-domaines                          | <p>Le port a une capacité de réachabilité de couche 2 à son domaine de diffusion attribué ; cependant, il a également la possibilité de reachcapacité de couche 2 à au moins un autre domaine de broadcast.</p> <p>Examinez la connectivité physique et la configuration du commutateur pour déterminer si elle est incorrecte ou si le domaine de diffusion attribué au port doit être fusionné avec un ou plusieurs domaines de diffusion.</p> <p>Pour plus d'informations, voir "<a href="#">Fusionner les domaines de diffusion</a>" ou "<a href="#">Réparation de l'accessibilité de l'orifice</a>".</p>                                                                                                                                                       |
| inconnu                                               | <p>Si l'état de la capacité d'accessibilité est « inconnu », attendez quelques minutes et essayez à nouveau la commande.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

Une fois que vous avez réparé un port, vous devez vérifier et résoudre les LIFs et les VLAN déplacés. Si le port faisait partie d'un groupe d'interfaces, vous devez également connaître ce qui s'est passé pour ce groupe.

# Composants réseau

## Composants réseau d'une vue d'ensemble d'un cluster

Vous devez vous familiariser avec les composants réseau d'un cluster avant de configurer ce dernier. La configuration des composants de mise en réseau physique d'un cluster en composants logiques offre la flexibilité et la fonctionnalité de colocation d'ONTAP.

Les différents composants réseau d'un cluster sont les suivants :

- Ports physiques

Les cartes réseau (NIC) et les adaptateurs de bus hôte (HBA) fournissent des connexions physiques (Ethernet et Fibre Channel) de chaque nœud aux réseaux physiques (gestion et réseaux de données).

Pour connaître la configuration requise du site, les informations de switch, le câblage des ports et le câblage du port intégré du contrôleur, consultez le Hardware Universe à l'adresse ["hwu.netapp.com"](http://hwu.netapp.com).

- Ports logiques

Les réseaux locaux virtuels (VLAN) et les groupes d'interfaces constituent les ports logiques. Les groupes d'interfaces traitent plusieurs ports physiques comme un seul port, tandis que les VLAN divisent un port physique en plusieurs ports distincts.

- Les IPspaces

Les IPspaces permettent de créer un espace d'adresse IP distinct pour chaque SVM dans un cluster. Ainsi, les clients se trouvant dans des domaines réseau distincts d'un point de vue administratif peuvent accéder aux données du cluster tout en utilisant des adresses IP redondantes à partir de la même plage de sous-réseaux.

- Les domaines de diffusion

Un broadcast domain resgrand dans un IPspace et contient un groupe de ports réseau, potentiellement depuis plusieurs nœuds du cluster, qui appartiennent au même réseau de couche 2. Les ports du groupe sont utilisés dans un SVM pour le trafic de données.

- Sous-réseaux

Un sous-réseau est créé au sein d'un domaine de diffusion et contient un pool d'adresses IP appartenant au même sous-réseau de couche 3. Ce pool d'adresses IP simplifie l'allocation d'adresses IP lors de la création de LIF.

- Interfaces logiques

Une interface logique (LIF) est une adresse IP ou un WWPN (World port Name) associé à un port. Il est associé à des attributs tels que les groupes de basculement, les règles de basculement et les règles de pare-feu. Une LIF communique sur le réseau par l'intermédiaire du port (physique ou logique) auquel elle est actuellement liée.

Les différents types de LIF d'un cluster sont des LIFs de données, des LIFs de management du cluster-

scoped, des LIFs de management du nœud-scoped, des LIFs intercluster et des LIFs de cluster. La propriété des LIFs dépend du SVM où réside la LIF. Les LIF de données sont détenues par des SVM de données, des LIF de gestion « node-scoped », un système de gestion Cluster-scoped et des LIF intercluster sont au sein des SVM admin, et des LIF de cluster appartiennent au SVM.

- Zones DNS

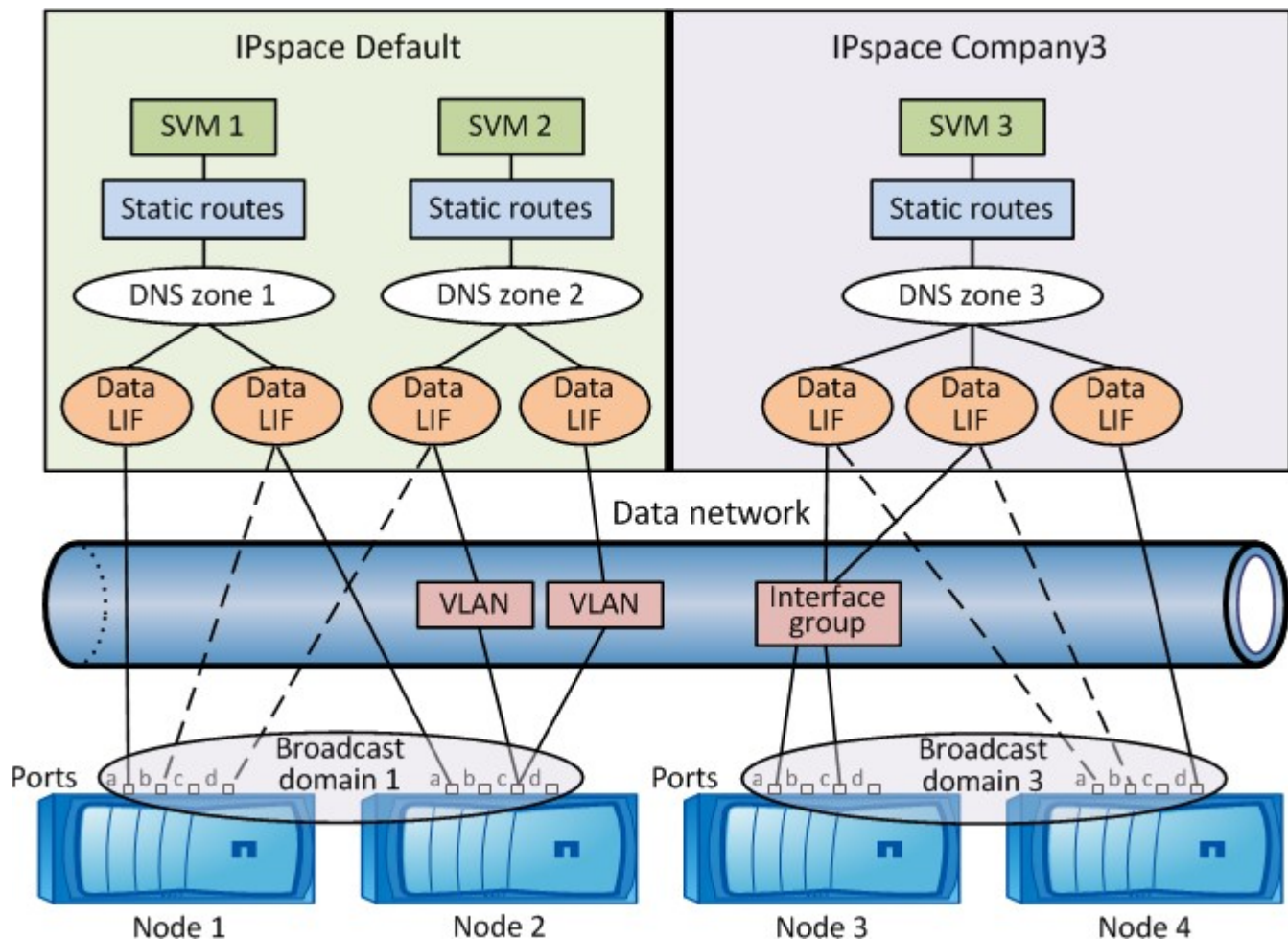
La zone DNS peut être spécifiée lors de la création de la LIF, ce qui fournit un nom à exporter via le serveur DNS du cluster. Plusieurs LIF peuvent partager le même nom, ce qui permet à la fonctionnalité d'équilibrage de la charge DNS de distribuer les adresses IP pour le nom en fonction du chargement.

Les SVM peuvent avoir plusieurs zones DNS.

- Routage

Chaque SVM est autonome en matière de mise en réseau. Un SVM possède des LIFs et des routes qui peuvent atteindre chacun des serveurs externes configurés.

La figure suivante montre comment les différents composants réseau sont associés dans un cluster à quatre nœuds :



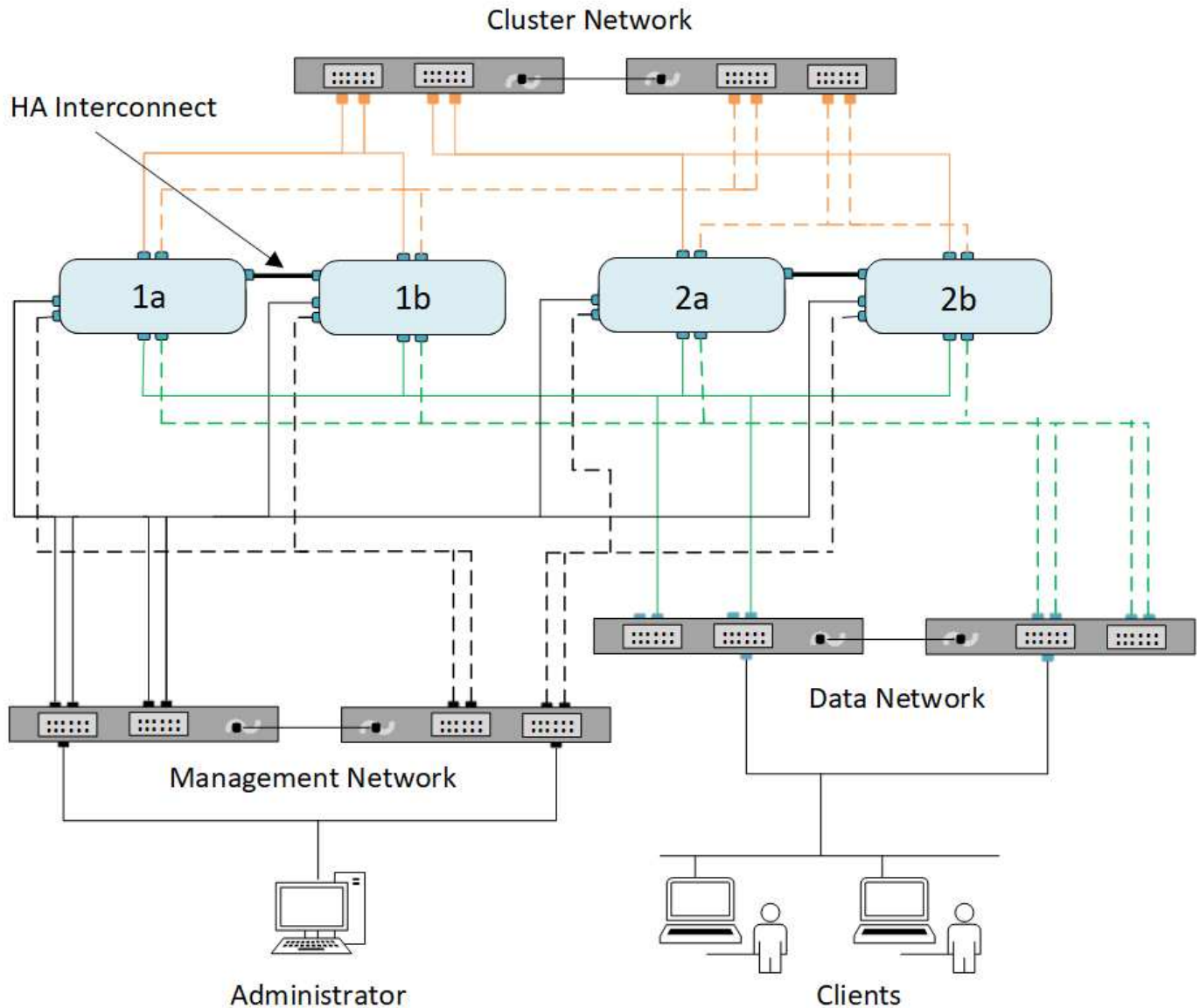
## Instructions de câblage réseau

Les meilleures pratiques en matière de câblage réseau séparent le trafic sur les réseaux

suivants : cluster, gestion et données.

Vous devez câbler un cluster de manière à ce que le trafic du cluster se trouve sur un réseau distinct de tout autre trafic. Le trafic de gestion de réseau est séparé du trafic de données et du trafic intracluster, mais cette pratique est facultative. La maintenance de réseaux distincts permet d'obtenir de meilleures performances, une administration simplifiée et une meilleure sécurité et gestion de l'accès aux nœuds.

Le schéma suivant illustre le câblage réseau d'un cluster HA à quatre nœuds qui comprend trois réseaux distincts :



Vous devez suivre certaines directives lors du câblage des connexions réseau :

- Chaque nœud doit être connecté à trois réseaux distincts.

Un réseau est destiné à la gestion, un autre à l'accès aux données et une autre à la communication intracluster. Les réseaux de données et de gestion peuvent être séparés de façon logique.

- Vous pouvez disposer de plusieurs connexions réseau de données à chaque nœud pour améliorer le flux

de trafic client (données).

- Un cluster peut être créé sans connexions réseau de données, mais il doit inclure une connexion d'interconnexion de cluster.
- Il doit toujours y avoir deux connexions de cluster ou plus à chaque nœud.

Pour plus d'informations sur le câblage réseau, reportez-vous au ["Centre de documentation du système AFF et FAS"](#) et le ["Hardware Universe"](#).

## Relations entre les domaines de diffusion, les groupes de basculement et les règles de basculement

Les domaines de diffusion, les groupes de basculement et les règles de basculement fonctionnent ensemble afin de déterminer quel port reprendre le contrôle lorsque le nœud ou le port sur lequel une LIF est configurée tombe en panne.

Un broadcast domain répertorie tous les ports accessibles sur le même réseau Ethernet de couche 2. Un paquet de diffusion Ethernet envoyé à partir de l'un des ports est visible par tous les autres ports du domaine de diffusion. Cette caractéristique de reachabilité commune d'un broadcast domain est importante pour les LIFs car si une LIF devait basculer vers n'importe quel autre port du broadcast, elle pourrait toujours atteindre tous les hôtes locaux et distants accessibles depuis le port d'origine.

Les Failover Groups regroupent les ports d'un broadcast domain capable de procurer le failover de LIF les uns pour les autres. Chaque broadcast domain dispose d'un failover group qui inclut tous ses ports. Ce failover group contenant l'ensemble des ports du broadcast domain est le Default et recommandé pour le LIF. Vous pouvez créer des groupes de basculement avec des sous-ensembles plus petits que vous définissez, par exemple un groupe de ports de basculement dont la vitesse de liaison est identique au sein d'un domaine de diffusion.

Une politique de basculement détermine la façon dont une LIF utilise les ports d'un failover group lorsqu'un nœud ou un port tombe en panne. Considérez la stratégie de basculement comme un type de filtre appliqué à un groupe de basculement. Les cibles de basculement d'une LIF (l'ensemble des ports vers lesquels une LIF peut basculer) sont déterminées en appliquant la politique de basculement de la LIF au failover group de la LIF dans le broadcast domain.

Vous pouvez afficher les cibles de basculement d'une LIF à l'aide de la commande CLI suivante :

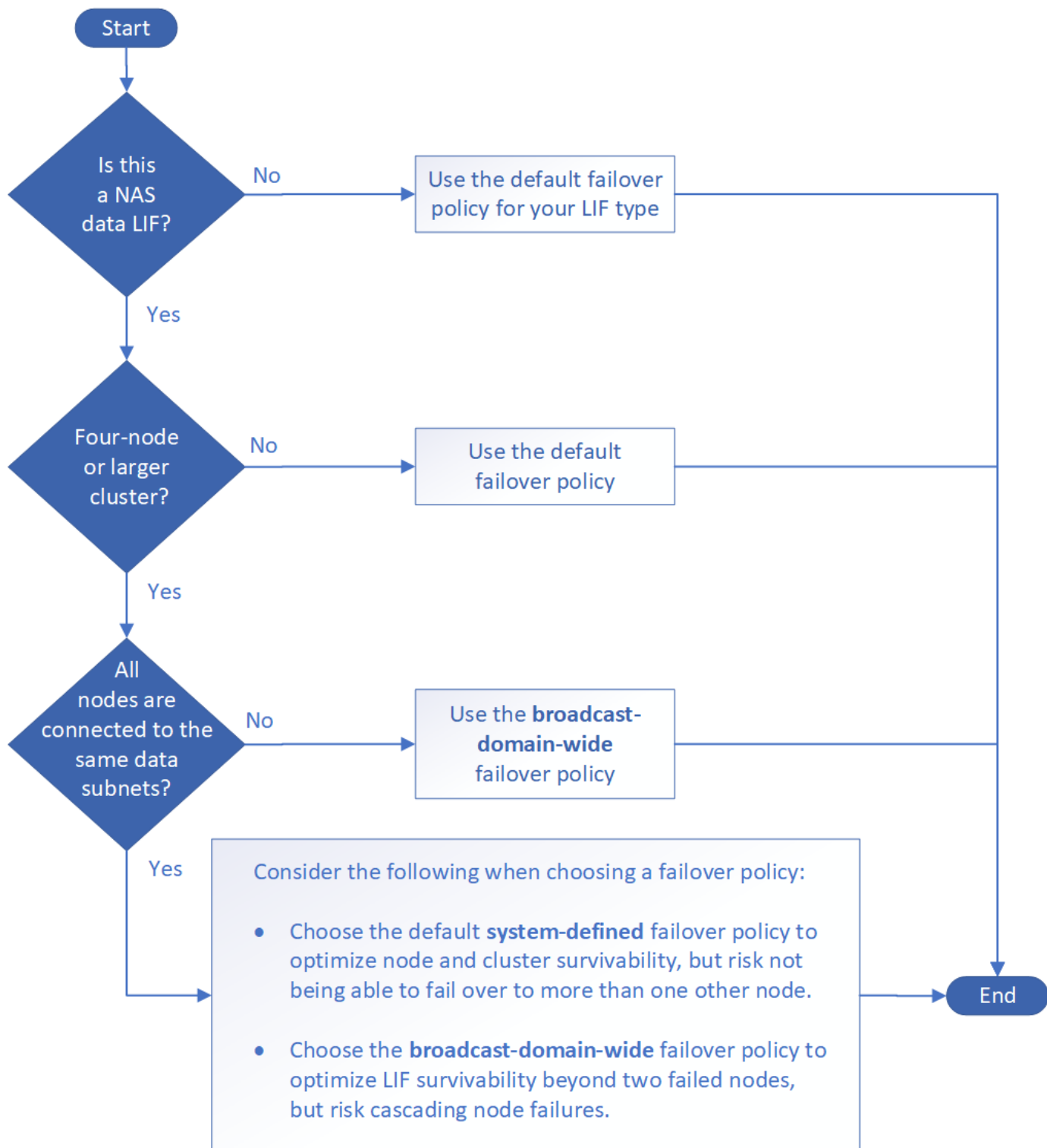
```
network interface show -failover
```

NetApp recommande fortement d'utiliser la stratégie de basculement par défaut pour votre type de LIF.

### Décider de la règle de basculement LIF à utiliser

Vous pouvez choisir d'utiliser la stratégie de basculement par défaut recommandée ou de la modifier en fonction de votre type et de votre environnement LIF.

#### Arbre de décision de stratégie de basculement



#### Stratégies de basculement par défaut par type de LIF

| Type de LIF    | Règle de basculement par défaut | Description                                            |
|----------------|---------------------------------|--------------------------------------------------------|
| Les LIF BGP    | désactivé                       | La LIF ne bascule pas vers un autre port.              |
| LIF de cluster | local uniquement                | La LIF bascule vers les ports du même nœud uniquement. |

|                     |                        |                                                                                             |
|---------------------|------------------------|---------------------------------------------------------------------------------------------|
| LIF Cluster-mgmt    | broadcast-domain-large | La LIF bascule vers les ports du même broadcast domain, sur n'importe quel nœud du cluster. |
| LIF intercluster    | local uniquement       | La LIF bascule vers les ports du même nœud uniquement.                                      |
| LIF de données NAS  | défini par le système  | LIF bascule vers un autre nœud qui n'est pas le partenaire de haute disponibilité.          |
| LIF node management | local uniquement       | La LIF bascule vers les ports du même nœud uniquement.                                      |
| LIF de données SAN  | désactivé              | La LIF ne bascule pas vers un autre port.                                                   |

La règle de basculement « sfo-partenaire uniquement » n'est pas une valeur par défaut, mais elle peut être utilisée pour le basculement de la LIF vers un port du nœud de rattachement ou du partenaire SFO uniquement.

## Workflow de basculement de chemin NAS (ONTAP 9.8 et versions ultérieures)

### À propos du basculement de chemin NAS (ONTAP 9.8 et versions ultérieures)

Ce flux de travail vous guide tout au long des étapes de configuration réseau pour configurer le basculement de chemin NAS pour ONTAP 9.8 et versions ultérieures. Ce flux de travail suppose les éléments suivants :

- Vous souhaitez appliquer les bonnes pratiques de basculement de chemin NAS dans un workflow qui simplifie la configuration du réseau.
- Vous souhaitez utiliser l'interface de ligne de commandes, pas System Manager.
- Vous configurez la mise en réseau sur un nouveau système exécutant ONTAP 9.8 ou version ultérieure.

Si vous exécutez une version ONTAP antérieure à la version 9.8, vous devez utiliser la procédure de basculement de chemin NAS suivante pour ONTAP 9.0 à 9.7 :

- ["Flux de production de basculement de chemin NAS ONTAP 9.0-9.7"](#)

Si vous souhaitez obtenir des informations sur la gestion du réseau, vous devez utiliser le matériel de référence de gestion du réseau :

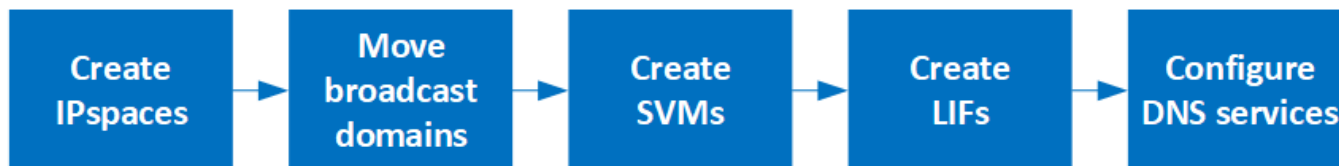
- [Présentation de la gestion du réseau](#)

### Workflow (ONTAP 9.8 et versions ultérieures)

Si vous connaissez déjà les concepts de base de la mise en réseau, vous pourrez peut-être gagner du temps en configurant votre réseau en consultant ce flux de travail pratique pour la configuration du basculement de chemin NAS.

Une LIF NAS migre automatiquement vers un port réseau survivant après une panne de liaison sur son port actuel. Vous pouvez utiliser les valeurs par défaut de ONTAP pour gérer le basculement de chemin.





Une LIF SAN ne migre pas (sauf si vous la déplacez manuellement après l'échec de la liaison). La technologie de chemins d'accès multiples sur l'hôte achemine le trafic vers une autre LIF. Pour plus d'informations, voir ["Administration SAN"](#).

1

### "Remplissez la feuille de travail"

Utilisez la fiche pour planifier le basculement de chemin NAS.

2

### "Créez les IPspaces"

Créer un espace d'adresse IP distinct pour chaque SVM d'un cluster.

3

### "Déplacez les domaines de diffusion vers les IPspaces"

Déplacer les domaines de diffusion dans les IPspaces.

4

### "Créer des SVM"

Création des SVM pour le service de données aux clients.

5

### "Créez des LIF"

Créez des LIF sur les ports que vous souhaitez utiliser pour accéder à des données.

6

### "Configurer les services DNS pour le SVM"

Configurer les services DNS pour le SVM avant de créer un serveur NFS ou SMB.

## Fiche technique de configuration du basculement de chemin NAS (ONTAP 9.8 et versions ultérieures)

Avant de configurer le basculement du chemin NAS, vous devez remplir toutes les sections de la fiche technique.

### Configuration IPspace

Les IPspaces permettent de créer un espace d'adresse IP distinct pour chaque SVM dans un cluster. Ainsi, les clients se trouvant dans des domaines réseau distincts d'un point de vue administratif peuvent accéder aux données du cluster tout en utilisant des adresses IP redondantes à partir de la même plage de sous-réseaux.

| Informations | Obligatoire ? | Vos valeurs |
|--------------|---------------|-------------|
|--------------|---------------|-------------|



|                                                 |      |  |
|-------------------------------------------------|------|--|
| Nom IPspace<br>Identifiant unique de l'IPspace. | Oui. |  |
|-------------------------------------------------|------|--|

### Configuration broadcast domain

Un domaine de diffusion regroupe les ports qui appartiennent au même réseau de couche 2 et définit la MTU pour les ports de domaine de diffusion.

Les domaines de diffusion sont affectés à un IPspace. Un IPspace peut contenir un ou plusieurs domaines de diffusion.



Le port vers lequel une LIF échoue doit être membre du failover group pour le LIF. Pour chaque broadcast domain créé par ONTAP, un failover group avec le même nom est également créé qui contient tous les ports du broadcast domain.

| Informations                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Obligatoire ? | Vos valeurs |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-------------|
| Nom IPspace<br>L'IPspace à lequel le domaine de diffusion est affecté.<br><br>Cet IPspace doit exister.                                                                                                                                                                                                                                                                                                                                                                                                           | Oui.          |             |
| Nom du domaine de diffusion<br>Nom du domaine de diffusion.<br><br>Ce nom doit être unique dans l'IPspace.                                                                                                                                                                                                                                                                                                                                                                                                        | Oui.          |             |
| MTU<br>La valeur maximale de l'unité de transmission pour le domaine de diffusion, généralement définie sur <b>1500</b> ou <b>9000</b> .<br><br>La valeur MTU est appliquée à tous les ports du domaine de diffusion et à tous les ports ajoutés ultérieurement au domaine de diffusion.<br><br>La valeur MTU doit correspondre à tous les périphériques connectés à ce réseau. Notez que le MTU doit être défini sur 1500 octets au maximum pour la gestion des ports e0M et le trafic du processeur de service. | Oui.          |             |

|                                                                                                                                                                                                                                                                                                                                          |      |  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--|
| <p>Ports</p> <p>Les ports sont affectés à des domaines de diffusion en fonction de l'accessibilité. Une fois l'affectation du port terminée, vérifiez l'accessibilité en exécutant le <code>network port reachability show</code> commande.</p> <p>Ces ports peuvent être des ports physiques, des VLAN ou des groupes d'interfaces.</p> | Oui. |  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--|

## Configuration de sous-réseau

Un sous-réseau contient des pools d'adresses IP et une passerelle par défaut qui peuvent être affectés aux LIF utilisées par des SVM résidant dans l'IPspace.

- Lors de la création d'une LIF sur un SVM, vous pouvez spécifier le nom du sous-réseau au lieu de fournir une adresse IP et un sous-réseau.
- Étant donné qu'un sous-réseau peut être configuré avec une passerelle par défaut, il n'est pas nécessaire de créer la passerelle par défaut dans une étape distincte lors de la création d'un SVM.
- Un domaine de diffusion peut contenir un ou plusieurs sous-réseaux.
- Vous pouvez configurer des LIF SVM qui se trouvent sur des sous-réseaux différents en associant plusieurs sous-réseaux au domaine de diffusion de l'IPspace.
- Chaque sous-réseau doit contenir des adresses IP qui ne se chevauchent pas avec les adresses IP attribuées à d'autres sous-réseaux dans le même IPspace.
- Vous pouvez attribuer des adresses IP spécifiques aux LIF de données d'un SVM et créer une passerelle par défaut pour la SVM au lieu d'utiliser un sous-réseau.

| Informations                                                                                                                                                            | Obligatoire ? | Vos valeurs |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-------------|
| <p>Nom IPspace</p> <p>L'IPspace à lequel le sous-réseau sera affecté.</p> <p>Cet IPspace doit exister.</p>                                                              | Oui.          |             |
| <p>Nom du sous-réseau</p> <p>Nom du sous-réseau.</p> <p>Ce nom doit être unique dans l'IPspace.</p>                                                                     | Oui.          |             |
| <p>Nom du domaine de diffusion</p> <p>Domaine de diffusion auquel le sous-réseau sera affecté.</p> <p>Ce domaine de diffusion doit résider dans l'IPspace spécifié.</p> | Oui.          |             |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                |      |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--|
| Nom et masque de sous-réseau<br>Sous-réseau et masque dans lequel les adresses IP résident.                                                                                                                                                                                                                                                                                                                                                                    | Oui. |  |
| <p>Passerelle<br/>Vous pouvez spécifier une passerelle par défaut pour le sous-réseau.</p> <p>Si vous n'attribuez pas de passerelle lors de la création du sous-réseau, vous pouvez en affecter une ultérieurement.</p>                                                                                                                                                                                                                                        | Non  |  |
| <p>Plages d'adresses IP<br/>Vous pouvez spécifier une plage d'adresses IP ou des adresses IP spécifiques.</p> <p>Par exemple, vous pouvez spécifier une plage telle que :</p> <p>192.168.1.1-192.168.1.100,<br/>192.168.1.112, 192.168.1.145</p> <p>Si vous ne spécifiez pas de plage d'adresses IP, la plage complète d'adresses IP dans le sous-réseau spécifié est disponible pour l'attribuer aux LIF.</p>                                                 | Non  |  |
| <p>Forcer la mise à jour des associations LIF<br/>Spécifie s'il faut forcer la mise à jour des associations LIF existantes.</p> <p>Par défaut, la création de sous-réseau échoue si des interfaces de processeur de service ou des interfaces réseau utilisent les adresses IP dans les plages fournies.</p> <p>L'utilisation de ce paramètre associe toutes les interfaces adressées manuellement avec le sous-réseau et permet à la commande de réussir.</p> | Non  |  |

## Configuration d'un SVM

Vous utilisez des SVM pour fournir des données aux clients et aux hôtes.

Les valeurs que vous enregistrez servent à créer un SVM de données par défaut. Si vous créez un SVM source MetroCluster, consultez la ["Guide d'installation et de configuration de MetroCluster FAS-Attached"](#) ou le ["Guide d'installation et de configuration d'étirement MetroCluster"](#).

| Informations | Obligatoire ? | Vos valeurs |
|--------------|---------------|-------------|
|--------------|---------------|-------------|

|                                                                                                                                                                                                                                                                                                                                                                                                                                  |      |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--|
| Nom du SVM<br>Nom de domaine complet (FQDN) du SVM.<br><br>Ce nom doit être unique pour toutes les ligues de groupe.                                                                                                                                                                                                                                                                                                             | Oui. |  |
| Nom du volume root<br>Le nom du volume root du SVM.                                                                                                                                                                                                                                                                                                                                                                              | Oui. |  |
| Nom de l'agrégat<br>Nom de l'agrégat qui détient le volume root du SVM.<br><br>Cet agrégat doit exister.                                                                                                                                                                                                                                                                                                                         | Oui. |  |
| Style de sécurité<br>Le style de sécurité du volume root du SVM.<br><br>Les valeurs possibles sont <b>ntfs</b> , <b>unix</b> et <b>mixte</b> .                                                                                                                                                                                                                                                                                   | Oui. |  |
| Nom IPspace<br>L'IPspace à lequel la SVM est affectée.<br><br>Cet IPspace doit exister.                                                                                                                                                                                                                                                                                                                                          | Non  |  |
| Définition du langage SVM<br>Langue par défaut à utiliser pour le SVM et ses volumes.<br><br>Si vous ne spécifiez pas de langue par défaut, le langage SVM par défaut est défini sur <b>C.UTF-8</b> .<br><br>Le paramètre de langage SVM détermine le jeu de caractères utilisé pour afficher les noms de fichiers et les données de tous les volumes NAS de la SVM.<br><br>Vous pouvez modifier la langue une fois le SVM créé. | Non  |  |

## Configuration de LIF

Un SVM fournit des données aux clients et hôtes via une ou plusieurs interfaces logiques réseau (LIF).

| Informations                          | Obligatoire ? | Vos valeurs |
|---------------------------------------|---------------|-------------|
| Nom du SVM<br>Nom du SVM pour la LIF. | Oui.          |             |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |      |  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--|
| <p>Nom de LIF<br/>Nom de la LIF.</p> <p>Vous pouvez attribuer plusieurs LIF de données par nœud, et vous pouvez attribuer des LIF à n'importe quel nœud du cluster, pourvu que le nœud dispose de ports de données disponibles.</p> <p>Pour assurer la redondance, vous devez créer au moins deux LIF de données pour chaque sous-réseau de données, et les LIF attribuées à un sous-réseau particulier doivent recevoir des ports home-logiques sur différents nœuds.</p> <p><b>Important :</b> si vous configurez un serveur SMB afin d'héberger Hyper-V ou SQL Server sur SMB pour des solutions de continuité de l'activité, la SVM doit disposer d'au moins une LIF de données sur chaque nœud du cluster.</p> | Oui. |  |
| <p>Stratégie de service<br/>Politique de service pour la LIF.</p> <p>La politique de service définit les services réseau pouvant utiliser LIF. Les services et les règles de service intégrés sont disponibles pour la gestion du trafic de données et de gestion sur les SVM de données et de système.</p>                                                                                                                                                                                                                                                                                                                                                                                                         | Oui. |  |
| <p>Protocoles autorisés<br/>Les LIF basées sur IP ne nécessitent pas de protocoles autorisés. Utilisez plutôt la ligne de stratégie de service.</p> <p>Spécifier les protocoles autorisés pour les LIFs SAN sur les ports FibreChannel. Ce sont les protocoles qui peuvent utiliser cette LIF. Les protocoles qui utilisent la LIF ne peuvent pas être modifiés après la création de la LIF. Vous devez spécifier tous les protocoles lors de la configuration de la LIF.</p>                                                                                                                                                                                                                                       | Non  |  |
| <p>Nœud de départ<br/>Le nœud sur lequel la LIF renvoie lorsque la LIF est rétablie dans son home port.</p> <p>Vous devez enregistrer un home node pour chaque LIF de données.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Oui. |  |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                             |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|--|
| <p>Home port ou broadcast domain</p> <p>Choisissez l'une des options suivantes :</p> <p><b>Port</b> : spécifiez le port sur lequel l'interface logique renvoie lorsque la LIF est rétablie sur son port home. Cela n'est fait que pour la première LIF dans le sous-réseau d'un IPspace, sinon elle n'est pas requise.</p> <p><b>Broadcast Domain</b>: Préciser le broadcast domain, et le système sélectionne le port approprié auquel l'interface logique renvoie lorsque le LIF est rétabli sur son home port.</p> | Oui.                                        |  |
| <p>Nom du sous-réseau</p> <p>Sous-réseau à affecter à la SVM.</p> <p>Toutes les LIF de données utilisées pour créer des connexions SMB disponibles en continu avec les serveurs applicatifs doivent se trouver sur le même sous-réseau.</p>                                                                                                                                                                                                                                                                           | Oui (en cas d'utilisation d'un sous-réseau) |  |

## Configuration DNS

Vous devez configurer DNS sur le SVM avant de créer un serveur NFS ou SMB.

| Informations                                                                                                                                                                                                                                                  | Obligatoire ? | Vos valeurs |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-------------|
| <p>Nom du SVM</p> <p>Nom du SVM sur lequel vous souhaitez créer un serveur NFS ou SMB.</p>                                                                                                                                                                    | Oui.          |             |
| <p>Nom de domaine DNS</p> <p>Liste de noms de domaine à ajouter à un nom d'hôte lors de la résolution de nom hôte-IP.</p> <p>Indiquez d'abord le domaine local, suivi des noms de domaine pour lesquels les requêtes DNS sont le plus souvent effectuées.</p> | Oui.          |             |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |      |  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--|
| <p>Adresses IP des serveurs DNS</p> <p>Liste des adresses IP des serveurs DNS qui fourniront une résolution de nom pour le serveur NFS ou SMB.</p> <p>Les serveurs DNS répertoriés doivent contenir les enregistrements SRV nécessaires à la localisation des serveurs LDAP Active Directory et des contrôleurs de domaine du domaine auquel le serveur SMB sera rattaché.</p> <p>L'enregistrement SRV permet de mapper le nom d'un service au nom d'ordinateur DNS d'un serveur offrant ce service. La création du serveur SMB échoue si ONTAP ne parvient pas à obtenir les enregistrements d'emplacement de service par le biais de requêtes DNS locales.</p> <p>La façon la plus simple de s'assurer que ONTAP puisse localiser les enregistrements SRV Active Directory est de configurer des serveurs DNS intégrés à Active Directory en tant que serveurs DNS SVM.</p> <p>Vous pouvez utiliser des serveurs DNS non intégrés à Active Directory à condition que l'administrateur DNS ait ajouté manuellement les enregistrements SRV à la zone DNS qui contient des informations sur les contrôleurs de domaine Active Directory.</p> <p>Pour plus d'informations sur les enregistrements SRV intégrés à Active Directory, reportez-vous à la rubrique "<a href="#">Fonctionnement de la prise en charge DNS pour Active Directory sur Microsoft TechNet</a>".</p> | Oui. |  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--|

## Configuration DNS dynamique

Avant de pouvoir utiliser DNS dynamique pour ajouter automatiquement des entrées DNS à vos serveurs DNS intégrés à Active Directory, vous devez configurer DNS dynamique (DDNS) sur le SVM.

Des enregistrements DNS sont créés pour chaque LIF de données sur le SVM. En créant plusieurs LIF de données sur le SVM, vous pouvez établir des connexions client avec équilibrage de la charge aux adresses IP attribuées. La charge DNS équilibre les connexions effectuées à l'aide du nom d'hôte aux adresses IP attribuées selon une séquence périodique.

| Informations                                                                        | Obligatoire ? | Vos valeurs |
|-------------------------------------------------------------------------------------|---------------|-------------|
| <p>Nom du SVM</p> <p>SVM sur lequel vous souhaitez créer un serveur NFS ou SMB.</p> | Oui.          |             |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                               |      |  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--|
| Si vous souhaitez utiliser DDNS<br>Indique s'il faut utiliser DDNS.                                                                                                                                                                                                                                                                                                                                                                                           | Oui. |  |
| Les serveurs DNS configurés sur le SVM<br>doivent prendre en charge DDNS. Par défaut,<br>DDNS est désactivé.                                                                                                                                                                                                                                                                                                                                                  |      |  |
| Utilisation de DDNS sécurisé ou non<br>Secure DDNS est pris en charge uniquement<br>avec un DNS intégré à Active Directory.<br><br>Si votre DNS intégré à Active Directory<br>n'autorise que les mises à jour DDNS<br>sécurisées, la valeur de ce paramètre doit être<br>vraie.<br><br>Par défaut, Secure DDNS est désactivé.<br><br>Secure DDNS ne peut être activé qu'après la<br>création d'un serveur SMB ou d'un compte<br>Active Directory pour la SVM. | Non  |  |
| FQDN du domaine DNS<br>Le FQDN du domaine DNS.<br><br>Vous devez utiliser le même nom de domaine<br>configuré pour les services de nom DNS sur la<br>SVM.                                                                                                                                                                                                                                                                                                     | Non  |  |

## Workflow de basculement de chemin NAS (ONTAP 9.7 et versions antérieures)

### Configuration du basculement de chemin NAS (ONTAP 9.7 et versions antérieures)

Ce flux de travail vous guide tout au long des étapes de configuration réseau pour configurer le basculement de chemin NAS pour ONTAP 9.0 - 9.7. Ce flux de travail suppose les éléments suivants :

- Vous souhaitez appliquer les bonnes pratiques de basculement de chemin NAS qui simplifient la configuration du réseau.
- Vous souhaitez utiliser l'interface de ligne de commandes, pas System Manager.
- Vous configurez la mise en réseau sur un nouveau système exécutant ONTAP 9.0 à 9.7.

Si vous exécutez une version ONTAP ultérieure à la version 9.7, vous devez utiliser la procédure de basculement du chemin NAS pour ONTAP 9.8 ou version ultérieure :

- [Flux de travail de basculement de chemin NAS ONTAP 9.8 et versions ultérieures](#)

Si vous souhaitez obtenir des détails sur les composants et la gestion du réseau, vous devez utiliser le matériel de référence de gestion du réseau :

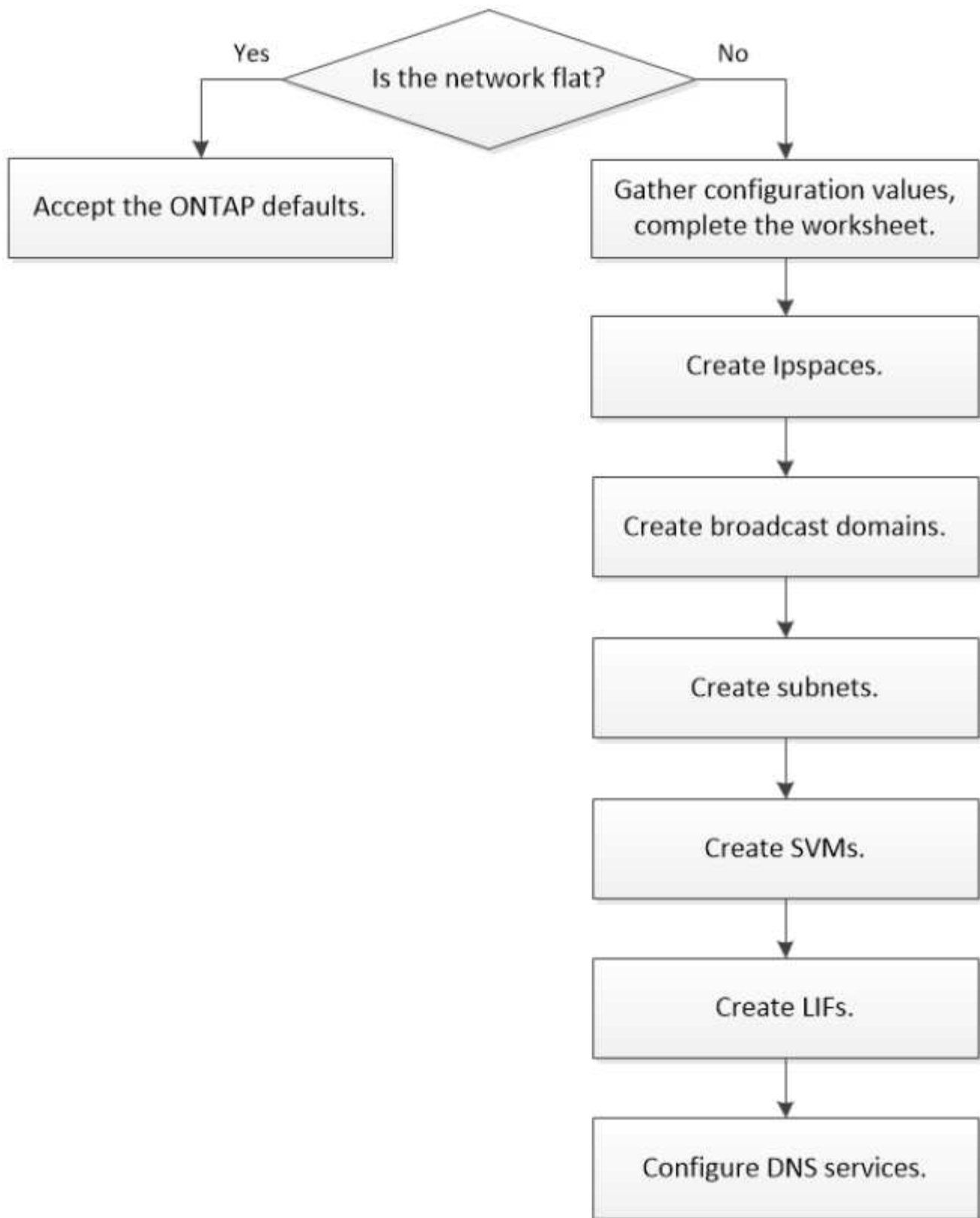


- [Présentation de la gestion du réseau](#)

## **Workflow (ONTAP 9.7 et versions antérieures)**

Si vous connaissez déjà les concepts de base de la mise en réseau, vous pourrez peut-être gagner du temps en configurant votre réseau en consultant ce flux de travail pratique pour la configuration du basculement de chemin NAS.

Une LIF NAS migre automatiquement vers un port réseau survivant après une panne de liaison sur son port actuel. Si votre réseau est plat, vous pouvez compter sur les valeurs par défaut de ONTAP pour gérer le basculement de chemin. Dans le cas contraire, vous devez configurer le basculement de chemin en suivant les étapes de ce flux de travail.



Une LIF SAN ne migre pas (sauf si vous la déplacez manuellement après l'échec de la liaison). La technologie de chemins d'accès multiples sur l'hôte achemine le trafic vers une autre LIF. Pour plus d'informations, voir "[Administration SAN](#)".

**1****"Remplissez la feuille de travail"**

Utilisez la fiche pour planifier le basculement de chemin NAS.

**2****"Créez les IPspaces"**

Créer un espace d'adresse IP distinct pour chaque SVM d'un cluster.

**3****"Créer des domaines de diffusion"**

Créer des domaines de diffusion.

**4****"Créer des sous-réseaux"**

Créer des sous-réseaux.

**5****"Créer des SVM"**

Création des SVM pour le service de données aux clients.

**6****"Créez des LIF"**

Créez des LIF sur les ports que vous souhaitez utiliser pour accéder à des données.

**7****"Configurer les services DNS pour le SVM"**

Configurer les services DNS pour le SVM avant de créer un serveur NFS ou SMB.

## Fiche technique pour la configuration de basculement de chemin NAS (ONTAP 9.7 et versions antérieures)

Avant de configurer le basculement du chemin NAS, vous devez remplir toutes les sections de la fiche technique.

### Configuration IPspace

Les IPspaces permettent de créer un espace d'adresse IP distinct pour chaque SVM dans un cluster. Ainsi, les clients se trouvant dans des domaines réseau distincts d'un point de vue administratif peuvent accéder aux données du cluster tout en utilisant des adresses IP redondantes à partir de la même plage de sous-réseaux.

| Informations | Obligatoire ? | Vos valeurs |
|--------------|---------------|-------------|
|--------------|---------------|-------------|

|                                                                                                                                                 |      |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------|------|--|
| <b>Nom IPspace</b> <ul style="list-style-type: none"> <li>• Le nom de l'IPspace.</li> <li>• Le nom doit être unique dans le cluster.</li> </ul> | Oui. |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------|------|--|

## Configuration broadcast domain


Un domaine de diffusion regroupe les ports qui appartiennent au même réseau de couche 2 et définit la MTU pour les ports de domaine de diffusion.

Les domaines de diffusion sont affectés à un IPspace. Un IPspace peut contenir un ou plusieurs domaines de diffusion.



Le port vers lequel une LIF échoue doit être membre du failover group pour le LIF. Lorsque vous créez un broadcast domain, ONTAP crée automatiquement un failover group avec le même nom. Le failover group contient tous les ports assignés au broadcast domain.

| Informations                                                                                                                                                           | Obligatoire ? | Vos valeurs |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-------------|
| <b>Nom IPspace</b> <ul style="list-style-type: none"> <li>• L'IPspace à lequel le domaine de diffusion est affecté.</li> <li>• L'IPspace doit exister.</li> </ul>      | Oui.          |             |
| <b>Nom du domaine de diffusion</b> <ul style="list-style-type: none"> <li>• Nom du domaine de diffusion.</li> <li>• Ce nom doit être unique dans l'IPspace.</li> </ul> | Oui.          |             |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |             |  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--|
| <p>MTU</p> <ul style="list-style-type: none"> <li>• MTU du domaine de diffusion.</li> <li>• Généralement réglé sur <b>1500</b> ou <b>9000</b>.</li> <li>• La valeur MTU est appliquée à tous les ports du domaine de diffusion et à tous les ports ajoutés ultérieurement au domaine de diffusion.</li> </ul> <div>  <p>La valeur MTU doit correspondre à tous les périphériques connectés à ce réseau. Notez que le MTU doit être défini sur 1500 octets au maximum pour la gestion des ports e0M et le trafic du processeur de service.</p> </div> | <p>Oui.</p> |  |
| <p>Ports</p> <ul style="list-style-type: none"> <li>• Les ports réseau à ajouter au broadcast domain.</li> <li>• Les ports affectés au domaine de diffusion peuvent être des ports physiques, des VLAN ou des groupes d'interfaces (ifgroups).</li> <li>• Si un port se trouve dans un autre broadcast domain, il doit être supprimé avant de pouvoir être ajouté au broadcast domain.</li> <li>• Les ports sont attribués en spécifiant le nom du nœud et le port : par exemple, node1:e0d.</li> </ul>                                                                                                                               | <p>Oui.</p> |  |

## Configuration de sous-réseau

Un sous-réseau contient des pools d'adresses IP et une passerelle par défaut qui peuvent être affectés aux LIF utilisées par des SVM résidant dans l'IPspace.

- Lors de la création d'une LIF sur un SVM, vous pouvez spécifier le nom du sous-réseau au lieu de fournir une adresse IP et un sous-réseau.

- Étant donné qu'un sous-réseau peut être configuré avec une passerelle par défaut, il n'est pas nécessaire de créer la passerelle par défaut dans une étape distincte lors de la création d'un SVM.
- Un domaine de diffusion peut contenir un ou plusieurs sous-réseaux.  
Vous pouvez configurer des LIF SVM qui se trouvent sur des sous-réseaux différents en associant plusieurs sous-réseaux au domaine de diffusion de l'IPspace.
- Chaque sous-réseau doit contenir des adresses IP qui ne se chevauchent pas avec les adresses IP attribuées à d'autres sous-réseaux dans le même IPspace.
- Vous pouvez attribuer des adresses IP spécifiques aux LIF de données d'un SVM et créer une passerelle par défaut pour la SVM au lieu d'utiliser un sous-réseau.

| Informations                                                                                                                                                                                                                                                                               | Obligatoire ? | Vos valeurs |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-------------|
| <b>Nom IPspace</b> <ul style="list-style-type: none"> <li>• L'IPspace à lequel le sous-réseau sera affecté.</li> <li>• L'IPspace doit exister.</li> </ul>                                                                                                                                  | Oui.          |             |
| <b>Nom du sous-réseau</b> <ul style="list-style-type: none"> <li>• Nom du sous-réseau.</li> <li>• Le nom doit être unique dans l'IPspace.</li> </ul>                                                                                                                                       | Oui.          |             |
| <b>Nom du domaine de diffusion</b> <ul style="list-style-type: none"> <li>• Domaine de diffusion auquel le sous-réseau sera affecté.</li> <li>• Le domaine de diffusion doit résider dans l'IPspace spécifié.</li> </ul>                                                                   | Oui.          |             |
| <b>Nom et masque de sous-réseau</b> <ul style="list-style-type: none"> <li>• Sous-réseau et masque dans lequel les adresses IP résident.</li> </ul>                                                                                                                                        | Oui.          |             |
| <b>Passerelle</b> <ul style="list-style-type: none"> <li>• Vous pouvez spécifier une passerelle par défaut pour le sous-réseau.</li> <li>• Si vous n'attribuez pas de passerelle lors de la création du sous-réseau, vous pouvez en attribuer une à tout moment au sous-réseau.</li> </ul> | Non           |             |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |     |  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|--|
| <b>Plages d'adresses IP</b> <ul style="list-style-type: none"> <li>• Vous pouvez spécifier une plage d'adresses IP ou des adresses IP spécifiques.<br/>Par exemple, vous pouvez spécifier une plage telle que :<br/>192.168.1.1–<br/>192.168.1.100,<br/>192.168.1.112,<br/>192.168.1.145</li> <li>• Si vous ne spécifiez pas de plage d'adresses IP, la plage complète d'adresses IP dans le sous-réseau spécifié est disponible pour l'attribuer aux LIF.</li> </ul>                                                  | Non |  |
| <b>Forcer la mise à jour des associations LIF</b> <ul style="list-style-type: none"> <li>• Spécifie s'il faut forcer la mise à jour des associations LIF existantes.</li> <li>• Par défaut, la création de sous-réseau échoue si des interfaces de processeur de service ou des interfaces réseau utilisent les adresses IP dans les plages fournies.</li> <li>• L'utilisation de ce paramètre associe toutes les interfaces adressées manuellement avec le sous-réseau et permet à la commande de réussir.</li> </ul> | Non |  |

## Configuration d'un SVM

Vous utilisez des SVM pour fournir des données aux clients et aux hôtes.

Les valeurs que vous enregistrez servent à créer un SVM de données par défaut. Si vous créez un SVM source MetroCluster, consultez la ["Installez un MetroCluster connecté à un fabric"](#) ou le ["Installez un MetroCluster extensible"](#).

| Informations | Obligatoire ? | Vos valeurs |
|--------------|---------------|-------------|
|--------------|---------------|-------------|


|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |      |  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--|
| <p>Nom du SVM</p> <ul style="list-style-type: none"> <li>• Nom du SVM.</li> <li>• Vous devez utiliser un nom de domaine complet pour garantir des noms de SVM uniques à travers les ligues de cluster.</li> </ul>                                                                                                                                                                                                                                                                        | Oui. |  |
| <p>Nom du volume root</p> <ul style="list-style-type: none"> <li>• Le nom du volume root du SVM.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                              | Oui. |  |
| <p>Nom de l'agrégat</p> <ul style="list-style-type: none"> <li>• Nom de l'agrégat qui détient le volume root du SVM.</li> <li>• Cet agrégat doit exister.</li> </ul>                                                                                                                                                                                                                                                                                                                     | Oui. |  |
| <p>Style de sécurité</p> <ul style="list-style-type: none"> <li>• Le style de sécurité du volume root du SVM.</li> <li>• Les valeurs possibles sont <b>ntfs</b>, <b>unix</b> et <b>mixte</b>.</li> </ul>                                                                                                                                                                                                                                                                                 | Oui. |  |
| <p>Nom IPspace</p> <ul style="list-style-type: none"> <li>• L'IPspace à lequel la SVM est affectée.</li> <li>• Cet IPspace doit exister.</li> </ul>                                                                                                                                                                                                                                                                                                                                      | Non  |  |
| <p>Définition du langage SVM</p> <ul style="list-style-type: none"> <li>• Langue par défaut à utiliser pour le SVM et ses volumes.</li> <li>• Si vous ne spécifiez pas de langue par défaut, le langage SVM par défaut est défini sur <b>C.UTF-8</b>.</li> <li>• Le paramètre de langage SVM détermine le jeu de caractères utilisé pour afficher les noms de fichiers et les données de tous les volumes NAS de la SVM. Vous pouvez modifier la langue une fois le SVM créé.</li> </ul> | Non  |  |



## Configuration de LIF

Un SVM fournit des données aux clients et hôtes via une ou plusieurs interfaces logiques réseau (LIF).

| Informations                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Obligatoire ?                   | Vos valeurs |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-------------|
| Nom du SVM <ul style="list-style-type: none"><li>Nom du SVM pour la LIF.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Oui.                            |             |
| Nom de LIF <ul style="list-style-type: none"><li>Nom de la LIF.</li><li>Vous pouvez attribuer plusieurs LIF de données par nœud, et vous pouvez attribuer des LIF à n'importe quel nœud du cluster, pourvu que le nœud dispose de ports de données disponibles.</li><li>Pour assurer la redondance, vous devez créer au moins deux LIF de données pour chaque sous-réseau de données, et les LIF attribuées à un sous-réseau particulier doivent recevoir des ports home-logiques sur différents nœuds.<br/><b>Important</b> : si vous configurez un serveur SMB afin d'héberger Hyper-V ou SQL Server sur SMB pour des solutions de continuité de l'activité, la SVM doit disposer d'au moins une LIF de données sur chaque nœud du cluster.</li></ul> | Oui.                            |             |
| Rôle LIF <ul style="list-style-type: none"><li>Le rôle de la LIF.</li><li>Le rôle des LIF de données est attribué</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Oui.<br>Obsolète dans ONTAP 9.6 | les données |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                          |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|--|
| <p>Stratégie de service</p> <p>Politique de service pour la LIF.</p> <p>La politique de service définit les services réseau pouvant utiliser LIF. Les services et les règles de service intégrés sont disponibles pour la gestion du trafic de données et de gestion sur les SVM de données et de système.</p>                                                                                                                                                                                                                                                                                                           | <p>Oui.</p> <p>À partir de ONTAP 9.6</p> |  |
| <p>Protocoles autorisés</p> <ul style="list-style-type: none"> <li>• Protocoles pouvant utiliser le LIF.</li> <li>• Par défaut, SMB, NFS et FlexCache sont autorisés. Le protocole FlexCache permet d'utiliser un volume en tant que volume d'origine pour un volume FlexCache sur un système exécutant Data ONTAP 7-mode.</li> </ul> <div>  <p>Les protocoles qui utilisent la LIF ne peuvent pas être modifiés après la création de la LIF. Vous devez spécifier tous les protocoles lors de la configuration de la LIF.</p> </div> | <p>Non</p>                               |  |
| <p>Nœud de départ</p> <ul style="list-style-type: none"> <li>• Le nœud sur lequel la LIF renvoie lorsque la LIF est rétablie dans son home port.</li> <li>• Vous devez enregistrer un home node pour chaque LIF de données.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                   | <p>Oui.</p>                              |  |

|                                                                                                                                                                                                                                                                                   |                                             |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|--|
| Home port ou broadcast domain <ul style="list-style-type: none"> <li>Le port sur lequel l'interface logique renvoie lorsque la LIF est rétablie dans son port home port.</li> <li>Vous devez enregistrer un port d'origine pour chaque LIF de données.</li> </ul>                 | Oui.                                        |  |
| Nom du sous-réseau <ul style="list-style-type: none"> <li>Sous-réseau à affecter à la SVM.</li> <li>Toutes les LIF de données utilisées pour créer des connexions SMB disponibles en continu avec les serveurs applicatifs doivent se trouver sur le même sous-réseau.</li> </ul> | Oui (en cas d'utilisation d'un sous-réseau) |  |

## Configuration DNS

Vous devez configurer DNS sur le SVM avant de créer un serveur NFS ou SMB.

| Informations                                                                                                                                                                                                                                                                                        | Obligatoire ? | Vos valeurs |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-------------|
| Nom du SVM <ul style="list-style-type: none"> <li>Nom du SVM sur lequel vous souhaitez créer un serveur NFS ou SMB.</li> </ul>                                                                                                                                                                      | Oui.          |             |
| Nom de domaine DNS <ul style="list-style-type: none"> <li>Liste de noms de domaine à ajouter à un nom d'hôte lors de la résolution de nom hôte-IP.</li> <li>Indiquez d'abord le domaine local, suivi des noms de domaine pour lesquels les requêtes DNS sont le plus souvent effectuées.</li> </ul> | Oui.          |             |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |             |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--|
| <p>Adresses IP des serveurs DNS</p> <ul style="list-style-type: none"> <li>• Liste des adresses IP des serveurs DNS qui fourniront une résolution de nom pour le serveur NFS ou SMB.</li> <li>• Les serveurs DNS répertoriés doivent contenir les enregistrements SRV nécessaires à la localisation des serveurs LDAP Active Directory et des contrôleurs de domaine du domaine auquel le serveur SMB sera rattaché. L'enregistrement SRV permet de mapper le nom d'un service au nom d'ordinateur DNS d'un serveur offrant ce service. La création du serveur SMB échoue si ONTAP ne parvient pas à obtenir les enregistrements d'emplacement de service par le biais de requêtes DNS locales. La façon la plus simple de s'assurer que ONTAP puisse localiser les enregistrements SRV Active Directory est de configurer des serveurs DNS intégrés à Active Directory en tant que serveurs DNS SVM. Vous pouvez utiliser des serveurs DNS non intégrés à Active Directory à condition que l'administrateur DNS ait ajouté manuellement les enregistrements SRV à la zone DNS qui contient des informations sur les contrôleurs de domaine Active Directory.</li> <li>• Pour plus d'informations sur les enregistrements SRV intégrés à Active Directory, reportez-vous à la rubrique <a href="#">"Fonctionnement de la prise en charge DNS pour Active Directory sur Microsoft TechNet"</a>.</li> </ul> | <p>Oui.</p> |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--|

## Configuration DNS dynamique

Avant de pouvoir utiliser DNS dynamique pour ajouter automatiquement des entrées DNS à vos serveurs DNS intégrés à Active Directory, vous devez configurer DNS dynamique (DDNS) sur le SVM.

Des enregistrements DNS sont créés pour chaque LIF de données sur le SVM. En créant plusieurs LIF de données sur le SVM, vous pouvez établir des connexions client avec équilibrage de la charge aux adresses IP attribuées. La charge DNS équilibre les connexions effectuées à l'aide du nom d'hôte aux adresses IP attribuées selon une séquence périodique.

| Informations                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Obligatoire ? | Vos valeurs |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-------------|
| <b>Nom du SVM</b> <ul style="list-style-type: none"><li>• SVM sur lequel vous souhaitez créer un serveur NFS ou SMB.</li></ul>                                                                                                                                                                                                                                                                                                                                                                             | Oui.          |             |
| <b>Si vous souhaitez utiliser DDNS</b> <ul style="list-style-type: none"><li>• Indique s'il faut utiliser DDNS.</li><li>• Les serveurs DNS configurés sur le SVM doivent prendre en charge DDNS. Par défaut, DDNS est désactivé.</li></ul>                                                                                                                                                                                                                                                                 | Oui.          |             |
| <b>Utilisation de DDNS sécurisé ou non</b> <ul style="list-style-type: none"><li>• Secure DDNS est pris en charge uniquement avec un DNS intégré à Active Directory.</li><li>• Si votre DNS intégré à Active Directory n'autorise que les mises à jour DDNS sécurisées, la valeur de ce paramètre doit être vraie.</li><li>• Par défaut, Secure DDNS est désactivé.</li><li>• Secure DDNS ne peut être activé qu'après la création d'un serveur SMB ou d'un compte Active Directory pour la SVM.</li></ul> | Non           |             |
| <b>FQDN du domaine DNS</b> <ul style="list-style-type: none"><li>• Le FQDN du domaine DNS.</li><li>• Vous devez utiliser le même nom de domaine configuré pour les services de nom DNS sur la SVM.</li></ul>                                                                                                                                                                                                                                                                                               | Non           |             |

# Ports réseau

## Configuration des ports réseau

Les ports sont des ports physiques (NIC) ou virtualisés, comme des groupes d'interfaces ou des VLAN.

Les réseaux locaux virtuels (VLAN) et les groupes d'interfaces constituent les ports virtuels. Les groupes d'interfaces traitent plusieurs ports physiques comme un seul port, tandis que les VLAN subdivisent un port physique en plusieurs ports logiques distincts.

- Ports physiques : les LIFs peuvent être configurées directement sur des ports physiques.
- Groupe d'interface : agrégat de ports contenant au moins deux ports physiques qui agissent comme un seul port de jonction. Un groupe d'interface peut être multimode ou dynamique en mode unique.
- VLAN : port logique qui reçoit et envoie le trafic VLAN-balisé (norme IEEE 802.1Q). Les caractéristiques du port VLAN incluent l'ID VLAN du port. Les ports physiques sous-jacents ou les ports de groupe d'interfaces sont considérés comme des ports de jonction VLAN et les ports de commutateur connectés doivent être configurés pour faire le lien entre les ID VLAN.

Les ports physiques sous-jacents ou les ports d'interface group d'un port VLAN peuvent continuer à héberger les LIFs, qui transmettent et reçoivent du trafic non balisé.

- Port IP virtuel (VIP) : port logique utilisé comme port de home port pour une LIF VIP. Les ports VIP sont créés automatiquement par le système et ne prennent en charge qu'un nombre limité d'opérations. Les ports VIP sont pris en charge à partir de ONTAP 9.5.

la convention d'appellation des ports est *énuméberLetter* :

- Le premier caractère décrit le type de port.  
« e » représente Ethernet.
- Le second caractère indique l'emplacement numéroté de l'adaptateur de port.
- Le troisième caractère indique la position du port sur un adaptateur multiport.  
« a » indique le premier port, « b » indique le second port, etc.

Par exemple : e0b Indique qu'un port Ethernet est le second port sur la carte mère du nœud.

Les VLAN doivent être nommés à l'aide de la syntaxe `port_name-vlan-id`.

`port_name` spécifie le port physique ou le groupe d'interface.

`vlan-id` Spécifie l'identification VLAN sur le réseau. Par exemple : e1c-80 Est un nom de VLAN valide.

## Configurez les ports réseau

### Combinaison de ports physiques pour créer des groupes d'interfaces

Un groupe d'interface, également appelé Groupe d'agrégation de liens (LAG), est créé en combinant deux ports physiques ou plus sur le même nœud en un seul port logique. Le port logique offre une résilience accrue, une disponibilité accrue et un partage de charge accru.

## Types de groupe d'interface

Le système de stockage prend en charge trois types de groupes d'interfaces : mode unique, multimode statique et multimode dynamique. Chaque groupe d'interface fournit différents niveaux de tolérance aux pannes. Les groupes d'interfaces multimode fournissent des méthodes pour équilibrer la charge du trafic réseau.

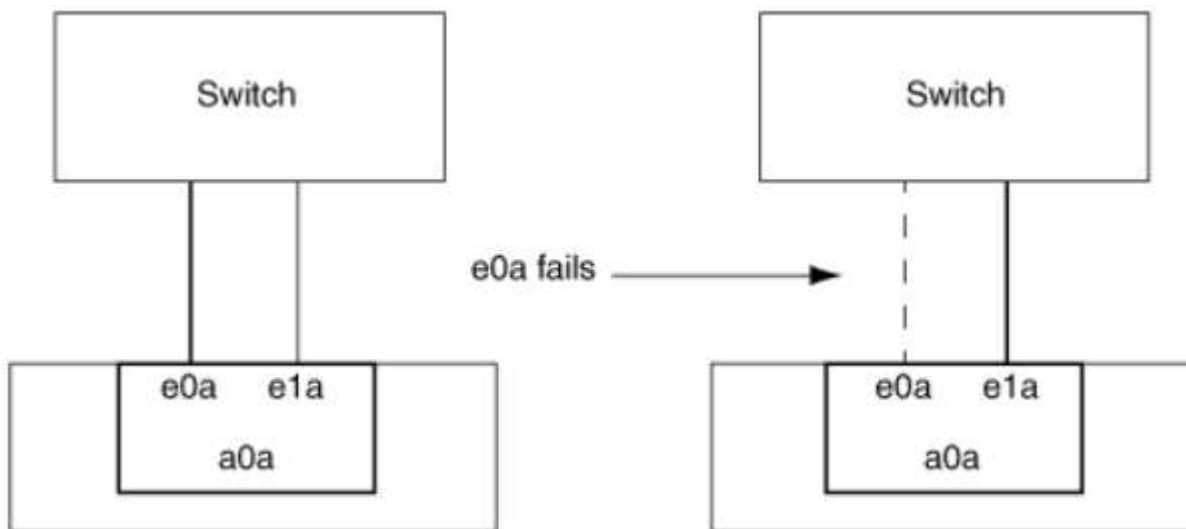
### Caractéristiques des groupes d'interfaces monomode

Dans un groupe d'interface à mode unique, une seule des interfaces du groupe d'interface est active. Les autres interfaces sont en veille, prêtes à prendre le relais en cas de défaillance de l'interface active.

Caractéristiques des groupes d'interfaces monomode :

- Pour le basculement, le cluster surveille la liaison active et contrôle le basculement. Comme le cluster surveille la liaison active, aucune configuration de commutateur n'est requise.
- Il peut y avoir plusieurs interfaces en veille dans un groupe d'interface à mode unique.
- Si un groupe d'interface à mode unique couvre plusieurs commutateurs, vous devez connecter les switches à l'aide d'une liaison ISL (Inter-Switch Link).
- Pour un groupe d'interface à mode unique, les ports switchs doivent être situés dans le même domaine de diffusion.
- Les paquets ARP de contrôle de liaison, dont l'adresse source est 0.0.0.0, sont envoyés sur les ports pour vérifier que les ports se trouvent dans le même domaine de diffusion.

La figure suivante illustre un exemple de groupe d'interfaces monomode. Dans la figure, e0a et e1a font partie du groupe d'interface a0a mode unique. Si l'interface active e0a, tombe en panne, l'interface e1a de secours prend le relais et maintient la connexion au commutateur.



Pour profiter de la fonctionnalité Single-mode, l'approche recommandée consiste à utiliser des groupes de basculement. L'utilisation d'un failover group permet de continuer à utiliser le second port pour d'autres LIFs et de ne pas avoir à le conserver. En outre, les groupes de basculement peuvent couvrir plus de deux ports et couvrir plusieurs nœuds.

## Caractéristiques des groupes d'interfaces multimode statiques

La mise en œuvre du groupe d'interfaces multimode statique dans ONTAP est conforme à la norme IEEE 802.3ad (statique). Tout switch qui prend en charge les agrégats, mais qui ne dispose pas d'échange de paquets de contrôle pour la configuration d'un agrégat, peut être utilisé avec des groupes d'interfaces multimode statiques.

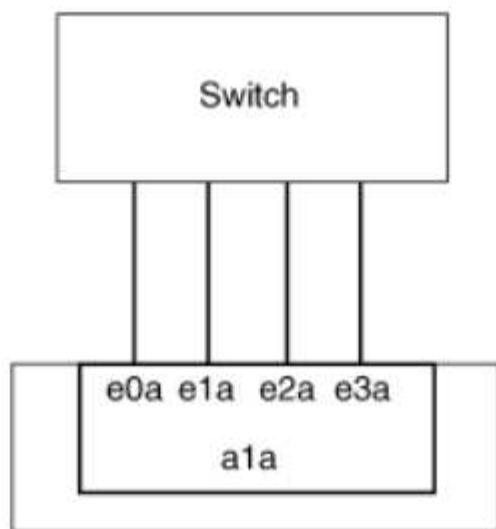
Les groupes d'interfaces multimode statiques ne sont pas conformes à la norme IEEE 802.3ad (dynamique), également appelée protocole LACP (Link Aggregation Control Protocol). Le protocole LACP est l'équivalent du protocole PAgP (Port Aggregation Protocol), le protocole propriétaire d'agrégation de liens de Cisco.

Les caractéristiques d'un groupe d'interfaces multimode statique sont les suivantes :

- Toutes les interfaces du groupe d'interface sont actives et partagent une seule adresse MAC.
  - Plusieurs connexions individuelles sont distribuées sur les interfaces du groupe d'interface.
  - Chaque connexion ou session utilise une interface au sein du groupe d'interface.  
Lorsque vous utilisez le schéma d'équilibrage de charge séquentiel, toutes les sessions sont distribuées sur les liaisons disponibles par paquet et ne sont pas liées à une interface particulière du groupe d'interfaces.
- Les groupes d'interfaces multimode statiques peuvent effectuer une restauration en cas de défaillance d'une interface jusqu'à « n-1 », où n est le nombre total d'interfaces qui forment le groupe d'interface.
- Si un port tombe en panne ou est débranché, le trafic qui traverserait la liaison défaillante est automatiquement redistribué à l'une des interfaces restantes.
- Les groupes d'interfaces multimode statiques peuvent détecter une perte de liaison, mais ils ne peuvent pas détecter une perte de connectivité au client ou les erreurs de configuration de commutateur qui pourraient affecter la connectivité et les performances.
- Un groupe d'interfaces multimode statiques nécessite un commutateur qui prend en charge l'agrégation de liens sur plusieurs ports de commutateur.  
Le commutateur est configuré de sorte que tous les ports auxquels sont connectées les liaisons d'un groupe d'interfaces font partie d'un seul port logique. Certains commutateurs ne prennent pas en charge l'agrégation de liens des ports configurés pour les trames Jumbo. Pour plus d'informations, consultez la documentation du fournisseur de votre commutateur.
- Plusieurs options d'équilibrage de charge sont disponibles pour distribuer le trafic entre les interfaces d'un groupe d'interfaces multimode statique.

La figure suivante illustre un exemple de groupe d'interfaces multimode statiques. Les interfaces e0a, e1a, e2a et e3a font partie du groupe d'interface multimode a1a. Les quatre interfaces du groupe d'interfaces multimode a1a sont actives.





Il existe plusieurs technologies qui permettent de répartir le trafic dans un lien agrégé unique sur plusieurs commutateurs physiques. Les technologies utilisées pour activer cette fonctionnalité varient selon les produits de mise en réseau. Les groupes d'interfaces multimode statiques en ONTAP sont conformes à la norme IEEE 802.3. Si une technologie particulière d'agrégation de liens de commutateur multiple est dite compatible avec les normes IEEE 802.3 ou conforme à celles-ci, elle doit fonctionner avec ONTAP.

La norme IEEE 802.3 indique que le périphérique de transmission d'une liaison agrégée détermine l'interface physique pour la transmission. Par conséquent, ONTAP est uniquement responsable de la distribution du trafic sortant et ne peut pas contrôler l'arrivée des trames entrantes. Si vous souhaitez gérer ou contrôler la transmission du trafic entrant sur une liaison agrégée, cette transmission doit être modifiée sur le périphérique réseau directement connecté.

### Groupe d'interfaces multimode dynamique

Les groupes d'interfaces multimode dynamiques implémentent le protocole LACP (Link Aggregation Control Protocol) pour communiquer l'appartenance aux groupes au commutateur directement connecté. LACP vous permet de détecter la perte de l'état de liaison et l'incapacité du nœud à communiquer avec le port de switch DAS.

La mise en œuvre de groupes d'interfaces multimode dynamiques dans ONTAP est conforme à la norme IEEE 802.3 AD (802.1 AX). ONTAP ne prend pas en charge le protocole PAgP (Port Aggregation Protocol), qui est un protocole propriétaire d'agrégation de liens de Cisco.

Un groupe d'interfaces multimode dynamique requiert un switch qui prend en charge LACP.

ONTAP implémente un LACP en mode actif non configurable qui fonctionne bien avec les switches configurés en mode actif ou passif. ONTAP implémente les temporisateurs LACP longs et courts (pour une utilisation avec des valeurs non configurables 3 secondes et 90 secondes), comme spécifié dans IEEE 802.3 AD (802.1AX).

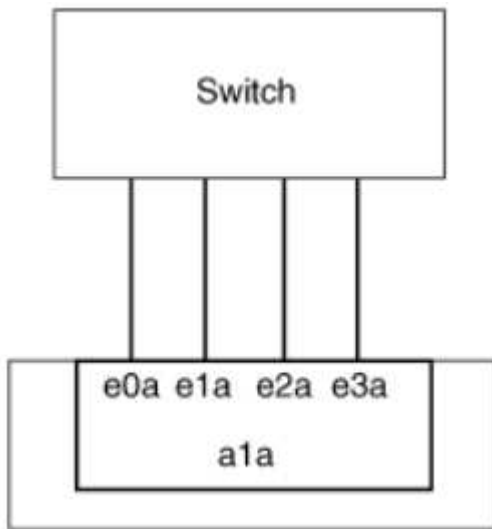
L'algorithme d'équilibrage de charge ONTAP détermine le port membre à utiliser pour transmettre le trafic sortant et ne contrôle pas la réception des trames entrantes. Le commutateur détermine le membre (port physique individuel) de son groupe de canaux de port à utiliser pour la transmission, en fonction de l'algorithme d'équilibrage de charge configuré dans le groupe de canaux de port du commutateur. Par conséquent, la configuration du commutateur détermine le port membre (port physique individuel) du système de stockage pour recevoir le trafic. Pour plus d'informations sur la configuration du commutateur, reportez-vous à la documentation fournie par votre fournisseur de commutateur.

Si une interface individuelle ne parvient pas à recevoir de paquets de protocole LACP successifs, cette interface individuelle est marquée comme « Lag\_inactive » dans la sortie de la commande « ifgrp status ». Le trafic existant est automatiquement redirigé vers les interfaces actives restantes.

Les règles suivantes s'appliquent lors de l'utilisation de groupes d'interfaces multimode dynamiques :

- Les groupes d'interfaces multimodes dynamiques doivent être configurés de manière à utiliser les méthodes d'équilibrage de charge basées sur les ports, les protocoles IP, MAC ou Round Robin.
- Dans un groupe d'interfaces multimode dynamiques, toutes les interfaces doivent être actives et partager une adresse MAC unique.

La figure suivante illustre un exemple de groupe d'interfaces multimode dynamiques. Les interfaces e0a, e1a, e2a et e3a font partie du groupe d'interface multimode a1a. Les quatre interfaces du groupe d'interfaces multimode dynamique a1a sont actives.



### Équilibrage de la charge dans les groupes d'interfaces multimode

Vous pouvez vous assurer que toutes les interfaces d'un groupe d'interfaces multimode sont utilisées de la même manière pour le trafic sortant à l'aide des méthodes d'équilibrage de charge basées sur l'adresse IP, l'adresse MAC, l'ordre séquentiel ou le port pour distribuer le trafic réseau de façon égale sur les ports réseau d'un groupe d'interfaces multimode.

La méthode d'équilibrage de charge d'un groupe d'interfaces multimode ne peut être spécifiée que lorsque le groupe d'interfaces est créé.

**Meilleure pratique** : l'équilibrage de charge basé sur les ports est recommandé chaque fois que possible. Utilisez l'équilibrage de charge basé sur les ports, sauf si le réseau a une raison ou une limitation spécifique qui l'empêche.

### Équilibrage de charge basé sur des ports

L'équilibrage de charge basé sur les ports est la méthode recommandée.

Vous pouvez égaliser le trafic sur un groupe d'interfaces multimode en fonction des ports de la couche de transport (TCP/UDP) en utilisant la méthode d'équilibrage de charge basée sur les ports.

La méthode d'équilibrage de charge basée sur le port utilise un algorithme de hachage rapide sur les adresses IP source et de destination, ainsi que le numéro de port de la couche de transport.

## Équilibrage de la charge des adresses IP et MAC

L'équilibrage de la charge des adresses IP et MAC est le moyen d'égaliser le trafic sur les groupes d'interfaces multimodes.

Ces méthodes d'équilibrage de charge utilisent un algorithme de hachage rapide sur les adresses source et de destination (adresse IP et adresse MAC). Si le résultat de l'algorithme de hachage est mappé à une interface qui n'est pas à l'état de la liaison ACTIVE, l'interface active suivante est utilisée.



Ne sélectionnez pas la méthode d'équilibrage de charge de l'adresse MAC lors de la création de groupes d'interfaces sur un système qui se connecte directement à un routeur. Dans une telle configuration, pour chaque trame IP sortante, l'adresse MAC de destination est l'adresse MAC du routeur. Par conséquent, une seule interface du groupe d'interface est utilisée.

L'équilibrage de charge d'adresse IP fonctionne de la même manière pour les adresses IPv4 et IPv6.

## Équilibrage séquentiel de la charge

Vous pouvez utiliser l'équilibrage séquentiel des charges pour distribuer de manière égale des paquets entre plusieurs liaisons à l'aide d'un algorithme de permutation circulaire. Vous pouvez utiliser l'option séquentielle pour équilibrer la charge du trafic d'une connexion unique sur plusieurs liaisons afin d'augmenter le débit de connexion unique.

Cependant, étant donné que l'équilibrage séquentiel de la charge peut causer une livraison de paquets hors de la commande, les performances peuvent être extrêmement faibles. Par conséquent, l'équilibrage séquentiel de la charge n'est généralement pas recommandé.

## Créez un groupe d'interfaces ou LAG

Vous pouvez créer un groupe d'interface ou LAG (monomode, multimode statique ou multimode dynamique) afin de présenter une interface unique aux clients en combinant les capacités des ports réseau agrégés.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## System Manager

### Utilisez System Manager pour créer un LAG

#### Étapes

1. Sélectionnez **réseau > port Ethernet > + Groupe d'agrégation de liens** pour créer un LAG.
2. Sélectionnez le nœud dans la liste déroulante.
3. Choisissez parmi les options suivantes :
  - a. ONTAP à **sélectionne automatiquement le domaine de diffusion (recommandé)**.
  - b. Pour sélectionner manuellement un domaine de diffusion.
4. Sélectionnez les ports pour former le LAG.
5. Sélectionnez le mode :
  - a. Unique : un seul port est utilisé à la fois.
  - b. Multiples : tous les ports peuvent être utilisés simultanément.
  - c. LACP : le protocole LACP détermine les ports qui peuvent être utilisés.
6. Sélectionner l'équilibrage de charge :
  - a. Sur IP
  - b. Basé SUR MAC
  - c. Port
  - d. Séquentiel
7. Enregistrez les modifications.

The screenshot shows the 'Add Link Aggregation Group' dialog box in the ONTAP System Manager interface. The dialog has a dark blue header with the title 'Add Link Aggregation Group' and a close button (X). Below the header, there are several sections for configuration:

- NODE:** A dropdown menu showing 'sti47-vs1m-ucs521e'.
- BROADCAST DOMAIN:** A dropdown menu showing 'Automatically select broadcast domain (Recommended)'. A red arrow points to this dropdown with a note: 'Note: Instead of a global switch or checkbox, what if we expose BD dropdown with "Automatic" as a default selection?'.
- PORTS TO INCLUDE:** Two checkboxes labeled 'e0e' and 'e0f', both of which are unchecked.
- MODE:** Three radio button options: 'Single' (selected), 'Multiple', and 'LACP'. Below 'Single' is the text 'Only one port is used at a time.' Below 'Multiple' is 'All ports can be used simultaneously.' Below 'LACP' is 'The LACP protocol determines the ports that can be used.'
- LOAD DISTRIBUTION:** Three radio button options: 'IP based' (selected), 'MAC based', and 'Port'. Below 'IP based' is the text 'Network traffic is distributed based on the destination IP address.' Below 'MAC based' is 'Network traffic is distributed based on the next-hop MAC addresses.'

At the bottom of the dialog, there are three small icons: a refresh icon, a save icon, and a cancel icon.

#### CLI

### Utilisez l'interface de ligne de commande pour créer un groupe d'interfaces

Pour obtenir la liste complète des restrictions de configuration qui s'appliquent aux groupes d'interfaces de port, reportez-vous à la section `network port ifgrp add-port` page de manuel.

Lors de la création d'un groupe d'interfaces multimode, vous pouvez spécifier l'une des méthodes d'équilibrage de charge suivantes :

- `port`: Le trafic réseau est distribué sur la base des ports de la couche de transport (TCP/UDP). Il s'agit de la méthode d'équilibrage de charge recommandée.
- `mac`: Le trafic réseau est distribué sur la base d'adresses MAC.
- `ip`: Le trafic réseau est distribué sur la base des adresses IP.
- `sequential`: Le trafic réseau est distribué au fur et à mesure qu'il est reçu.



L'adresse MAC d'un groupe d'interfaces est déterminée par l'ordre des ports sous-jacents et la façon dont ces ports s'initialisent au démarrage. Vous ne devez donc pas présumer que l'adresse MAC ifgrp est conservée entre les redémarrages ou les mises à niveau ONTAP.

### Étape

Utilisez le `network port ifgrp create` commande permettant de créer un groupe d'interface.

Vous devez nommer les groupes d'interface à l'aide de la syntaxe `a<number><letter>`. Par exemple, `a0A`, `a0b`, `a1c` et `a2a` sont des noms de groupes d'interfaces valides.

Pour plus d'informations sur cette commande, reportez-vous au ["Référence de commande ONTAP"](#).

L'exemple suivant montre comment créer un groupe d'interfaces nommé `a0a` avec une fonction de distribution de port et un mode multimode :

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode multimode
```

### Ajoutez un port à un groupe d'interfaces ou LAG

Vous pouvez ajouter jusqu'à 16 ports physiques à un groupe d'interfaces ou LAG pour toutes les vitesses de port.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## System Manager

### Utilisez System Manager pour ajouter un port à un LAG

#### Étapes

1. Sélectionnez **réseau > port Ethernet > LAG** pour modifier un LAG.
2. Sélectionnez des ports supplémentaires sur le même nœud à ajouter au LAG.
3. Enregistrez les modifications.

#### CLI

### Utilisez l'interface de ligne de commande pour ajouter des ports à un groupe d'interfaces

#### Étape

Ajout de ports réseau au groupe d'interface :

```
network port ifgrp add-port
```

Pour plus d'informations sur cette commande, reportez-vous au ["Référence de commande ONTAP"](#).

L'exemple suivant montre comment ajouter le port e0c à un groupe d'interfaces nommé a0a :

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

Depuis ONTAP 9.8, les groupes d'interface sont automatiquement placés dans un domaine de diffusion approprié environ une minute après l'ajout du premier port physique au groupe d'interface. Si vous ne souhaitez pas que ONTAP le fait, et préférez placer manuellement le ifgrp sur un domaine de broadcast, spécifiez ensuite le `-skip-broadcast-domain-placement` dans le cadre du `ifgrp add-port` commande.

### Supprimer un port d'un groupe d'interfaces ou LAG

Vous pouvez supprimer un port d'un groupe d'interface qui héberge les LIFs, tant qu'il ne s'agit pas du dernier port du groupe d'interfaces. Il n'y a pas d'exigence que le groupe d'interface ne doit pas héberger les LIFs d'hôtes, ni que le groupe d'interface ne doit pas être le home port d'une LIF compte tenu de ne pas supprimer le dernier port du groupe d'interface. Cependant, si vous supprimez le dernier port, vous devez d'abord migrer ou déplacer les LIF du groupe d'interface.

#### Description de la tâche

Vous pouvez supprimer jusqu'à 16 ports (interfaces physiques) d'un groupe d'interfaces ou LAG.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## System Manager

### Utilisez System Manager pour supprimer un port d'un LAG

#### Étapes

1. Sélectionnez **réseau > port Ethernet > LAG** pour modifier un LAG.
2. Sélectionnez les ports à supprimer du LAG.
3. Enregistrez les modifications.

#### CLI

### Utilisez l'interface de ligne de commande pour supprimer des ports d'un groupe d'interfaces

#### Étape

Suppression des ports réseau d'un groupe d'interfaces :

```
network port ifgrp remove-port
```

L'exemple suivant montre comment supprimer le port e0c d'un groupe d'interfaces nommé a0A :

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

### Supprimer un groupe d'interfaces ou LAG

Vous pouvez supprimer des groupes d'interfaces ou des groupes LAG si vous souhaitez configurer des LIF directement sur les ports physiques sous-jacents ou décider de modifier le groupe d'interfaces ou le mode LAG ou la fonction de distribution.

#### Avant de commencer

- Le groupe d'interface ou LAG ne doit pas héberger de LIF.
- Le groupe d'interface ou LAG ne doit pas être le port de départ, ni la cible de basculement d'une LIF.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## System Manager

### Utilisez System Manager pour supprimer un LAG

#### Étapes

1. Sélectionnez **réseau > port Ethernet > LAG** pour supprimer un LAG.
2. Sélectionnez le LAG à supprimer.
3. Supprimer le LAG.

#### CLI

### Utilisez l'interface de ligne de commande pour supprimer un groupe d'interfaces

#### Étape

Utilisez le `network port ifgrp delete` commande permettant de supprimer un groupe d'interface.

Pour plus d'informations sur cette commande, reportez-vous au "[Référence de commande ONTAP](#)".

L'exemple suivant montre comment supprimer un groupe d'interfaces nommé a0b :

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

## Configurez les VLAN sur des ports physiques

Vous pouvez utiliser des VLAN dans ONTAP pour assurer une segmentation logique des réseaux en créant des domaines de diffusion distincts, définis sur la base d'un port de commutateur, par opposition aux domaines de diffusion traditionnels, définis sur des limites physiques.

Un VLAN peut s'étendre sur plusieurs segments de réseau physique. Les stations terminales appartenant à un VLAN sont liés par fonction ou application.

Par exemple, les stations d'extrémité d'un VLAN peuvent être regroupées par des départements, tels que l'ingénierie et la comptabilité, ou par des projets, tels que la release1 et la rele2. Étant donné que la proximité physique des stations de fin n'est pas essentielle dans un VLAN, vous pouvez disperser géographiquement les stations de fin et encore contenir le domaine de diffusion dans un réseau commuté.

Dans ONTAP 9.13.1 et 9.14.1, les ports non balisés qui ne sont utilisés par aucune interface logique (LIF) et qui ne disposent pas d'une connectivité VLAN native sur le commutateur connecté sont marqués comme dégradés. Cela permet d'identifier les ports inutilisés et n'indique pas une panne. Les VLAN natifs autorisent le trafic non balisé sur le port de base ifgrp, tel que les diffusions CFM ONTAP. Configurez des VLAN natifs sur le commutateur pour empêcher le blocage du trafic non marqué.

Vous pouvez gérer des VLAN en créant, en supprimant ou en affichant des informations les concernant.



Vous ne devez pas créer de VLAN sur une interface réseau avec le même identifiant que le VLAN natif du commutateur. Par exemple, si l'interface réseau e0b est sur un VLAN 10 natif, vous ne devez pas créer de VLAN e0b-10 sur cette interface.



## Créez un VLAN

Vous pouvez créer un VLAN pour la maintenance de domaines de diffusion distincts au sein du même domaine réseau en utilisant System Manager ou le `network port vlan create` commande.

### Avant de commencer

Vérifiez que les exigences suivantes ont été respectées :

- Les commutateurs déployés sur le réseau doivent soit être conformes aux normes IEEE 802.1Q, soit disposer d'une implémentation spécifique au fournisseur de VLAN.
- Pour prendre en charge plusieurs VLAN, une station d'extrémité doit être configurée de manière statique pour appartenir à un ou plusieurs VLAN.
- Le VLAN n'est pas connecté à un port hébergeant une LIF de cluster.
- Le VLAN n'est pas connecté aux ports affectés à l'IPspace Cluster.
- Le VLAN n'est pas créé sur un port de groupe d'interfaces qui ne contient aucun port membre.

### Description de la tâche

La création d'un VLAN connecte le VLAN au port réseau d'un nœud spécifié d'un cluster.

Lorsque vous configurez un VLAN sur un port pour la première fois, le port risque de tomber en panne, entraînant une déconnexion temporaire du réseau. Les ajouts de VLAN ultérieurs au même port n'affectent pas l'état du port.



Vous ne devez pas créer de VLAN sur une interface réseau avec le même identifiant que le VLAN natif du commutateur. Par exemple, si l'interface réseau e0b est sur un VLAN 10 natif, vous ne devez pas créer de VLAN e0b-10 sur cette interface.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## System Manager

### Utilisez System Manager pour créer un VLAN

Depuis ONTAP 9.12.0, vous pouvez sélectionner automatiquement le domaine de diffusion ou manuellement dans la liste. Auparavant, les domaines de diffusion étaient toujours sélectionnés automatiquement en fonction de la connectivité de couche 2. Si vous sélectionnez manuellement un domaine de diffusion, un avertissement s'affiche pour indiquer que la sélection manuelle d'un domaine de diffusion peut entraîner une perte de connectivité.

#### Étapes

1. Sélectionnez **réseau > port Ethernet > + VLAN**.
2. Sélectionnez le nœud dans la liste déroulante.
3. Choisissez parmi les options suivantes :
  - a. ONTAP à **sélectionne automatiquement le domaine de diffusion (recommandé)**.
  - b. Pour sélectionner manuellement un domaine de diffusion dans la liste.
4. Sélectionnez les ports pour former le VLAN.
5. Spécifiez l'ID du VLAN.
6. Enregistrez les modifications.

#### CLI

### Utilisez l'interface de ligne de commande pour créer un VLAN

Dans certaines circonstances, si vous voulez créer le port VLAN sur un port dégradé sans corriger le problème matériel ou toute mauvaise configuration logicielle, alors vous pouvez définir le `-ignore-health-status` paramètre du `network port modify` commande en tant que `true`.

#### Étapes

1. Utilisez le `network port vlan create` Pour créer un VLAN.
2. Vous devez spécifier l' `vlan-name` ou le `port` et `vlan-id` Options lors de la création d'un VLAN. Le nom du VLAN est une combinaison du nom du port (ou du groupe d'interfaces) et de l'identificateur du VLAN du commutateur réseau, avec un tiret entre les deux. Par exemple : `e0c-24` et `e1c-80` Sont des noms de VLAN valides.

L'exemple suivant montre comment créer un VLAN `e1c-80` connecté au port réseau `e1c` sur le nœud `cluster-1-01`:

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

Depuis ONTAP 9.8, les VLAN sont automatiquement placés dans des domaines de diffusion appropriés environ une minute après leur création. Si vous ne souhaitez pas que ONTAP le fait, et préférez placer manuellement le VLAN dans un domaine de diffusion, spécifiez le `-skip-broadcast-domain-placement` dans le cadre du `vlan create` commande.

Pour plus d'informations sur cette commande, reportez-vous au ["Référence de commande ONTAP"](#).

## Modifiez un VLAN

Vous pouvez modifier le domaine de diffusion ou désactiver un VLAN.

### Utilisez System Manager pour modifier un VLAN

Depuis ONTAP 9.12.0, vous pouvez sélectionner automatiquement le domaine de diffusion ou manuellement sur dans la liste. Auparavant, les domaines de diffusion étaient toujours sélectionnés automatiquement en fonction de la connectivité de couche 2. Si vous sélectionnez manuellement un domaine de diffusion, un avertissement s'affiche pour indiquer que la sélection manuelle d'un domaine de diffusion peut entraîner une perte de connectivité.

### Étapes

1. Sélectionnez **réseau > port Ethernet > VLAN**.
2. Sélectionnez l'icône de modification.
3. Effectuez l'une des opérations suivantes :
  - Modifiez le domaine de diffusion en sélectionnant un autre domaine dans la liste.
  - Décochez la case **Enabled**.
4. Enregistrez les modifications.

### Supprimer un VLAN

Vous devrez peut-être supprimer un VLAN avant de retirer une carte réseau de son logement. Lorsque vous supprimez un VLAN, il est automatiquement supprimé de toutes les règles et groupes de basculement qui l'utilisent.

### Avant de commencer

Assurez-vous qu'il n'y a pas de LIFs associées au VLAN.

### Description de la tâche

La suppression du dernier VLAN d'un port peut provoquer une déconnexion temporaire du réseau du port.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## System Manager

### Utilisez System Manager pour supprimer un VLAN

#### Étapes

1. Sélectionnez **réseau > port Ethernet > VLAN**.
2. Sélectionnez le VLAN à supprimer.
3. Cliquez sur **Supprimer**.

#### CLI

### Utilisez l'interface de ligne de commande pour supprimer un VLAN

#### Étape

Utilisez le `network port vlan delete` Commande de suppression d'un VLAN.

L'exemple suivant montre comment supprimer un VLAN `e1c-80` dans le port réseau `e1c` sur le nœud `cluster-1-01`:

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

## Modifier les attributs de port réseau

Vous pouvez modifier les paramètres de négociation automatique, duplex, contrôle du flux, vitesse et état d'un port réseau physique.

### Avant de commencer

Le port que vous souhaitez modifier ne doit pas héberger les LIFs.

### Description de la tâche

- Il n'est pas recommandé de modifier les paramètres d'administration des interfaces réseau 100 GbE, 40 GbE, 10 GbE ou 1 GbE.

Les valeurs que vous définissez pour le mode duplex et la vitesse du port sont appelées paramètres administratifs. En fonction des limites du réseau, les paramètres d'administration peuvent différer des paramètres opérationnels (c'est-à-dire le mode duplex et la vitesse utilisés par le port).

- Il n'est pas recommandé de modifier les paramètres d'administration des ports physiques sous-jacents dans un groupe d'interfaces.

Le `-up-admin` paramètre (disponible au niveau des privilèges avancés) modifie les paramètres administratifs du port.

- Il n'est pas recommandé de régler le `-up-admin` Paramètre administratif sur `false` pour tous les ports d'un nœud, ou pour le port qui héberge la dernière LIF de cluster opérationnelle sur un nœud.
- Il n'est pas recommandé de modifier la taille MTU du port de gestion, `e0M`.
- La taille MTU d'un port dans un domaine de diffusion ne peut pas être modifiée à partir de la valeur MTU définie pour le domaine de diffusion.

- La taille MTU d'un VLAN ne peut pas dépasser la valeur de la taille MTU de son port de base.

## Étapes

1. Modifier les attributs d'un port réseau :

```
network port modify
```

2. Vous pouvez définir le `-ignore-health-status` champ à `true` pour spécifier que le système peut ignorer l'état de santé du port réseau d'un port spécifié.

Le statut de l'état de santé des ports réseau est automatiquement modifié et passe de dégradé à sain, et ce port peut désormais être utilisé pour héberger les LIFs. Vous devez définir le contrôle de flux des ports du cluster sur `none`. Par défaut, le contrôle de flux est défini sur `full`.

La commande suivante désactive le contrôle de flux sur le port `e0b` en définissant le contrôle de flux sur aucun :

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

## Convertissez les ports NIC 40 GbE en ports 10 GbE multiples pour assurer la connectivité 10 GbE

Vous pouvez convertir les cartes réseau X1144A-R6 et X91440A-R6 40GbE pour prendre en charge quatre ports 10GbE.

Si vous connectez une plateforme matérielle prenant en charge l'une de ces cartes réseau à un cluster prenant en charge l'interconnexion de cluster 10GbE et les connexions de données client, la carte réseau doit être convertie pour fournir les connexions 10GbE nécessaires.

### Avant de commencer

Vous devez utiliser un câble de dérivation pris en charge.

### Description de la tâche

Pour obtenir la liste complète des plates-formes prenant en charge les cartes réseau, reportez-vous au ["Hardware Universe"](#).



Sur la carte réseau X1144A-R6, seul le port A peut être converti pour prendre en charge les quatre connexions 10GbE. Une fois le port A converti, le port e n'est pas disponible pour utilisation.

## Étapes

1. Passez en mode maintenance.
2. Convertissez le NIC de la prise en charge de 40 GbE en prise en charge de 10 GbE.

```
nicadmin convert -m [40G | 10G] [port-name]
```

3. Après avoir utilisé la commande `convert`, arrêtez le nœud.
4. Installez ou remplacez le câble.

5. En fonction du modèle matériel, utilisez le processeur de service ou le contrôleur BMC (Baseboard Management Controller) pour mettre le nœud sous tension et mettre le nœud en marche pour que la conversion prenne effet.

### Suppression d'une carte réseau du nœud (ONTAP 9.8 et versions ultérieures)

Cette rubrique s'applique à ONTAP 9.8 et versions ultérieures. Vous devrez peut-être retirer une carte réseau défectueuse de son logement ou la déplacer vers un autre emplacement pour des raisons de maintenance.

#### Étapes

1. Mettez le nœud hors tension.
2. Retirez physiquement la carte réseau de son logement.
3. Mettez le nœud sous tension.
4. Vérifiez que le port a été supprimé :

```
network port show
```



ONTAP supprime automatiquement le port de n'importe quel groupe d'interfaces. Si le port était le seul membre d'un groupe d'interfaces, le groupe d'interfaces est supprimé.

5. Si des VLAN y sont configurés sur le port, ils sont déplacés. Vous pouvez afficher les VLAN déplacés à l'aide de la commande suivante :

```
cluster controller-replacement network displaced-vlans show
```



Le `displaced-interface show`, `displaced-vlans show`, et `displaced-vlans restore` les commandes sont uniques et ne nécessitent pas le nom de la commande entièrement qualifié, qui commence par `cluster controller-replacement network`.

6. Ces VLAN sont supprimés, mais peuvent être restaurés à l'aide de la commande suivante :

```
displaced-vlans restore
```

7. Si des LIFs de type port y sont configurées, ONTAP sélectionne automatiquement de nouveaux ports d'accueil pour ces LIFs sur un autre port du même broadcast domain. Si aucun port domestique approprié n'est trouvé sur le même filer, ces LIF sont considérées comme déplacées. Vous pouvez afficher les LIFs déplacées à l'aide de la commande suivante :

```
displaced-interface show
```

8. Lorsqu'un nouveau port est ajouté au broadcast domain sur le même node, les home ports des LIFs sont automatiquement restaurés. Vous pouvez également définir le port d'accueil à l'aide de `network interface modify -home-port -home-node` or use the `displaced-interface restore` commande.

## Suppression d'une carte réseau du nœud (ONTAP 9.7 ou version antérieure)

Cette rubrique s'applique à ONTAP 9.7 ou version antérieure. Vous devrez peut-être retirer une carte réseau défectueuse de son logement ou la déplacer vers un autre emplacement pour des raisons de maintenance.

### Avant de commencer

- Toutes les LIFs hébergées sur les ports NIC doivent avoir été migrées ou supprimées.
- Aucun des ports NIC ne peut être le home ports des LIFs.
- Vous devez disposer de privilèges avancés pour supprimer les ports d'une carte réseau.

### Étapes

1. Supprimez les ports de la carte réseau :

```
network port delete
```

2. Vérifier que les ports ont été supprimés :

```
network port show
```

3. Répétez l'étape 1 si la sortie de la commande network port show affiche toujours le port supprimé.

## Surveiller les ports réseau

### Contrôle de l'état de santé des ports réseau

La gestion ONTAP des ports réseau inclut un contrôle automatique de l'état de santé et un ensemble de moniteurs pour vous aider à identifier les ports réseau qui ne conviennent pas à l'hébergement des LIF.

### Description de la tâche

Si un contrôle de l'état détermine qu'un port réseau est défectueux, il avertit les administrateurs via un message EMS ou indique que le port est dégradé. ONTAP évite d'héberger les LIF sur des ports réseau dégradés si d'autres cibles de basculement sont présentes pour cette LIF. Un port peut se dégrader en raison d'un événement de panne logicielle, tel que le fait de sauter des liaisons (rebondissement rapide des liaisons entre le haut et le bas) ou le partitionnement réseau :

- Les ports réseaux du cluster IPspace sont marqués comme détériorées lorsqu'ils connaissent une liaison flipant ou une perte de la capacité de couche 2 (L2) à d'autres ports réseau du domaine de diffusion.
- Les ports réseau des IPspaces sans cluster sont marqués comme dégradés lorsqu'ils réalisent des liaisons téléphoniques.

Vous devez connaître les comportements suivants d'un port dégradé :

- Un port dégradé ne peut pas être inclus dans un VLAN ou dans un groupe d'interfaces.

Si un port membre d'un groupe d'interface est marqué comme dégradé, mais que le groupe d'interfaces est toujours marqué comme défectueux, les LIF peuvent être hébergées sur ce groupe d'interface.

- Les LIF sont automatiquement migrées depuis les ports dégradés vers les ports sains.
- Lors d'un événement de basculement, un port dégradé n'est pas considéré comme la cible de

basculement. Si aucun port défectueux n'est disponible, les ports LIF hôtes sont dégradés conformément à la politique de basculement normale.

- Vous ne pouvez ni créer, ni migrer, ni restaurer une LIF vers un port dégradé.

Vous pouvez modifier le `ignore-health-status` définition du port réseau sur `true`. Vous pouvez ensuite héberger une LIF sur les ports sains.

## Étapes

1. Connectez-vous au mode de privilège avancé :

```
set -privilege advanced
```

2. Vérifiez les moniteurs d'intégrité qui sont activés pour surveiller l'intégrité des ports du réseau :

```
network options port-health-monitor show
```

L'état de santé d'un port est déterminé par la valeur des moniteurs d'intégrité.

Les contrôles d'état suivants sont disponibles et activés par défaut dans ONTAP :

- Surveillance de l'état du cerclage : surveille le cerclage de liaison

Si la liaison d'un port est plus d'une fois dans cinq minutes, ce port est marqué comme dégradé.

- Moniteur d'intégrité de la capacité d'accessibilité L2 : surveille si tous les ports configurés dans le même domaine de diffusion ont une capacité d'accessibilité L2 entre eux

Ce contrôle de l'état signale les problèmes de réabilité L2 dans tous les IPspaces, mais il marque uniquement les ports du cluster IPspace comme étant dégradés.

- Contrôle CRC : surveille les statistiques CRC sur les ports

Ce contrôle de l'état ne marque pas un port comme dégradé mais génère un message EMS lorsqu'un taux de défaillance CRC très élevé est observé.

3. Activez ou désactivez tous les moniteurs de santé pour un IPspace comme vous le souhaitez en utilisant le `network options port-health-monitor modify` commande.
4. Pour afficher l'état de santé détaillé d'un port :

```
network port show -health
```

Le résultat de la commande affiche le statut d'état de santé du port, `ignore health status` paramètre et liste des raisons pour lesquelles le port est marqué comme dégradé.

Un état de santé du port peut être `healthy` ou `degraded`.

Si le `ignore health status` le paramètre est `true`, il indique que le statut de l'état de santé du port a été



modifié de `degraded` à `healthy` par l'administrateur.

Si le `ignore health status` le paramètre est `false`, l'état d'intégrité du port est déterminé automatiquement par le système.

#### Surveiller l'accessibilité des ports réseau (ONTAP 9.8 et versions ultérieures)

La surveillance de l'accessibilité est intégrée à ONTAP 9.8 et versions ultérieures. Utilisez cette surveillance pour identifier si la topologie de réseau physique ne correspond pas à la configuration ONTAP. Dans certains cas, ONTAP peut réparer l'accessibilité des ports. Dans d'autres cas, des étapes supplémentaires sont nécessaires.

#### Description de la tâche

Utilisez ces commandes pour vérifier, diagnostiquer et réparer les erreurs de configuration du réseau qui ne correspondent pas au câblage physique ou à la configuration du commutateur réseau.

#### Étape

1. Afficher la capacité de port :

```
network port reachability show
```

2. Utilisez l'arbre de décision et le tableau suivants pour déterminer l'étape suivante, le cas échéant.



| État-accessibilité | Description |
|--------------------|-------------|
|--------------------|-------------|

|                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ok                                                    | <p>Le port a une capacité de réachabilité de couche 2 à son domaine de diffusion attribué. Si l'état de la capacité d'accessibilité est « ok », mais qu'il y a des « ports inattendus », envisagez de fusionner un ou plusieurs domaines de diffusion. Pour plus d'informations, reportez-vous à la <i>Unexpected ports row</i> suivante.</p> <p>Si le statut de la capacité d'accessibilité est « ok », mais qu'il y a des « ports inaccessibles », envisagez de diviser un ou plusieurs domaines de diffusion. Pour plus d'informations, reportez-vous à la ligne <i>ports inaccessibles</i> suivante.</p> <p>Si l'état de la capacité de reprise est « ok » et qu'il n'y a pas de ports inattendus ou inaccessibles, votre configuration est correcte.</p> |
| Ports inattendus                                      | <p>Le port a une capacité de réachabilité de couche 2 à son domaine de diffusion attribué ; cependant, il a également la possibilité de reachcapacité de couche 2 à au moins un autre domaine de broadcast.</p> <p>Examinez la connectivité physique et la configuration du commutateur pour déterminer si elle est incorrecte ou si le domaine de diffusion attribué au port doit être fusionné avec un ou plusieurs domaines de diffusion.</p> <p>Pour plus d'informations, voir "<a href="#">Fusionner les domaines de diffusion</a>".</p>                                                                                                                                                                                                                 |
| Ports inaccessibles                                   | <p>Si un seul domaine de diffusion a été partitionné en deux ensembles de capacité d'accès différents, vous pouvez fractionner un domaine de diffusion pour synchroniser la configuration ONTAP avec la topologie de réseau physique.</p> <p>En général, la liste des ports inaccessibles définit l'ensemble des ports qui doivent être divisés en un autre domaine de diffusion après avoir vérifié que la configuration physique et du commutateur est exacte.</p> <p>Pour plus d'informations, voir "<a href="#">Séparer les domaines de diffusion</a>".</p>                                                                                                                                                                                               |
| mauvaise configuration de la capacité de réachabilité | <p>Le port n'a pas la capacité de reachcapacité de couche 2 à son domaine de diffusion affecté ; cependant, le port a une capacité de reachcapacité de couche 2 à un domaine de diffusion différent.</p> <p>Vous pouvez réparer l'accessibilité du port. Lorsque vous exécutez la commande suivante, le système affecte le port au broadcast domain auquel il a la capacité de reachcapacité :</p> <pre>network port reachability repair -node -port</pre> <p>Pour plus d'informations, voir "<a href="#">Réparation de l'accessibilité de l'orifice</a>".</p>                                                                                                                                                                                                |
| sans trabilité                                        | <p>Le port n'a pas la possibilité de reachcapacité de couche 2 à un domaine de diffusion existant.</p> <p>Vous pouvez réparer l'accessibilité du port. Lorsque vous exécutez la commande suivante, le système affecte le port à un nouveau domaine de diffusion créé automatiquement dans l'IPspace par défaut :</p> <pre>network port reachability repair -node -port</pre> <p>Pour plus d'informations, voir "<a href="#">Réparation de l'accessibilité de l'orifice</a>".</p>                                                                                                                                                                                                                                                                              |

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| accessibilité multi-domaines | <p>Le port a une capacité de réachabilité de couche 2 à son domaine de diffusion attribué ; cependant, il a également la possibilité de reachcapacité de couche 2 à au moins un autre domaine de broadcast.</p> <p>Examinez la connectivité physique et la configuration du commutateur pour déterminer si elle est incorrecte ou si le domaine de diffusion attribué au port doit être fusionné avec un ou plusieurs domaines de diffusion.</p> <p>Pour plus d'informations, voir <a href="#">"Fusionner les domaines de diffusion"</a> ou <a href="#">"Réparation de l'accessibilité de l'orifice"</a>.</p> |
| inconnu                      | <p>Si l'état de la capacité d'accessibilité est « inconnu », attendez quelques minutes et essayez à nouveau la commande.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

Une fois que vous avez réparé un port, vous devez vérifier et résoudre les LIFs et les VLAN déplacés. Si le port faisait partie d'un groupe d'interfaces, vous devez également connaître ce qui s'est passé pour ce groupe. Pour plus d'informations, voir ["Réparation de l'accessibilité de l'orifice"](#).

### Présentation des ports ONTAP

Un certain nombre de ports connus sont réservés pour les communications ONTAP avec des services spécifiques. Des conflits de ports se produisent si une valeur de port dans votre environnement de réseau de stockage est identique à celle du port ONTAP.

Le tableau suivant répertorie les ports TCP et UDP utilisés par ONTAP.

| Service       | Port/Protocole | Description                           |
|---------------|----------------|---------------------------------------|
| ssh           | 22/TCP         | Connexion au shell sécurisée          |
| telnet        | 23/TCP         | Connexion à distance                  |
| DNS           | 53/TCP         | DNS avec équilibrage de charge        |
| http          | 80/TCP         | Protocole de transfert de texte       |
| rpcbind       | 111/TCP        | Appel de procédure à distance         |
| rpcbind       | 111/UDP        | Appel de procédure à distance         |
| ntp           | 123/UDP        | Protocole de temps réseau             |
| msrpc         | 135/UDP        | MSRPC                                 |
| netbios-ssn   | 139/TCP        | Session de service NetBIOS            |
| snmp          | 161/UDP        | Protocole de gestion de réseau simple |
| https         | 443/TCP        | HTTP sur TLS                          |
| microsoft- ds | 445/TCP        | Microsoft- ds                         |
| montage       | 635/TCP        | Montage NFS                           |
| montage       | 635/UDP        | Montage NFS                           |
| nommé         | 953/UDP        | Nom démon                             |

|                                    |                   |                                                                       |
|------------------------------------|-------------------|-----------------------------------------------------------------------|
| nfs                                | 2049/UDP          | Démon du serveur NFS                                                  |
| nfs                                | 2049/TCP          | Démon du serveur NFS                                                  |
| nrv                                | 2050/TCP          | Protocole NetApp Remote Volume                                        |
| iscsi                              | 3260/TCP          | Port cible iSCSI                                                      |
| verrouillage                       | 4045/TCP          | Démon de verrouillage NFS                                             |
| verrouillage                       | 4045/UDP          | Démon de verrouillage NFS                                             |
| NSM                                | 4046/TCP          | Moniteur d'état du réseau                                             |
| NSM                                | 4046/UDP          | Moniteur d'état du réseau                                             |
| rquotad                            | 4049/UDP          | Protocole NFS rquotad                                                 |
| krb524                             | 4444/UDP          | Kerberos 524                                                          |
| mdns                               | 5353/UDP          | DNS multicast                                                         |
| HTTPS                              | 5986/UDP          | Port HTTPS : protocole binaire d'écoute                               |
| https                              | 8443/TCP          | Interface graphique 7MTT via https                                    |
| ndmp                               | 10000/TCP         | Protocole de gestion des données réseau                               |
| Peering de clusters                | 11104/TCP         | Peering de cluster, bidirectionnel                                    |
| Peering de cluster, bidirectionnel | 11105/TCP         | Peering de clusters                                                   |
| NDMP                               | 18600 - 18699/TCP | NDMP                                                                  |
| NDMP                               | 30000/TCP         | accepte les connexions de contrôle sur les prises femelles sécurisées |
| port témoin cifs                   | 40001/TCP         | port témoin cifs                                                      |
| tls                                | 50000/TCP         | Sécurité de la couche de transport                                    |
| iscsi                              | 65200/TCP         | Port iSCSI                                                            |

#### Ports internes ONTAP

Le tableau suivant répertorie les ports TCP et UDP utilisés en interne par ONTAP. Ces ports permettent d'établir une communication LIF intracluster :

| Port/Protocole | Description        |
|----------------|--------------------|
| 514            | Syslog             |
| 900            | RPC NetApp Cluster |
| 902            | RPC NetApp Cluster |
| 904            | RPC NetApp Cluster |
| 905            | RPC NetApp Cluster |
| 910            | RPC NetApp Cluster |
| 911            | RPC NetApp Cluster |

|      |                                            |
|------|--------------------------------------------|
| 913  | RPC NetApp Cluster                         |
| 914  | RPC NetApp Cluster                         |
| 915  | RPC NetApp Cluster                         |
| 918  | RPC NetApp Cluster                         |
| 920  | RPC NetApp Cluster                         |
| 921  | RPC NetApp Cluster                         |
| 924  | RPC NetApp Cluster                         |
| 925  | RPC NetApp Cluster                         |
| 927  | RPC NetApp Cluster                         |
| 928  | RPC NetApp Cluster                         |
| 929  | RPC NetApp Cluster                         |
| 931  | RPC NetApp Cluster                         |
| 932  | RPC NetApp Cluster                         |
| 933  | RPC NetApp Cluster                         |
| 934  | RPC NetApp Cluster                         |
| 935  | RPC NetApp Cluster                         |
| 936  | RPC NetApp Cluster                         |
| 937  | RPC NetApp Cluster                         |
| 939  | RPC NetApp Cluster                         |
| 940  | RPC NetApp Cluster                         |
| 951  | RPC NetApp Cluster                         |
| 954  | RPC NetApp Cluster                         |
| 955  | RPC NetApp Cluster                         |
| 956  | RPC NetApp Cluster                         |
| 958  | RPC NetApp Cluster                         |
| 961  | RPC NetApp Cluster                         |
| 963  | RPC NetApp Cluster                         |
| 964  | RPC NetApp Cluster                         |
| 966  | RPC NetApp Cluster                         |
| 967  | RPC NetApp Cluster                         |
| 982  | RPC NetApp Cluster                         |
| 983  | RPC NetApp Cluster                         |
| 5125 | Port de contrôle secondaire pour le disque |
| 5133 | Port de contrôle secondaire pour le disque |

|       |                                                  |
|-------|--------------------------------------------------|
| 5144  | Port de contrôle secondaire pour le disque       |
| 65502 | Étendue des nœuds SSH                            |
| 65503 | Partage de LIF                                   |
| 7810  | RPC NetApp Cluster                               |
| 7811  | RPC NetApp Cluster                               |
| 7812  | RPC NetApp Cluster                               |
| 7813  | RPC NetApp Cluster                               |
| 7814  | RPC NetApp Cluster                               |
| 7815  | RPC NetApp Cluster                               |
| 7816  | RPC NetApp Cluster                               |
| 7817  | RPC NetApp Cluster                               |
| 7818  | RPC NetApp Cluster                               |
| 7819  | RPC NetApp Cluster                               |
| 7820  | RPC NetApp Cluster                               |
| 7821  | RPC NetApp Cluster                               |
| 7822  | RPC NetApp Cluster                               |
| 7823  | RPC NetApp Cluster                               |
| 7824  | RPC NetApp Cluster                               |
| 8023  | Périmètre de nœud TELNET                         |
| 8514  | Étendue du nœud RSH                              |
| 9877  | Port client KMIP (hôte local interne uniquement) |

## Les IPspaces

### Configuration de l'aperçu des IPspaces

Les IPspaces permettent de configurer un cluster ONTAP unique afin d'y accéder aux clients à partir de plusieurs domaines réseau distincts d'un point de vue administratif, même si ces clients utilisent la même plage de sous-réseau d'adresses IP. Cela permet de séparer le trafic client pour des raisons de confidentialité et de sécurité.

Un IPspace définit un espace d'adresse IP distinct dans lequel les SVM (Storage Virtual machines) résident. Les ports et les adresses IP définis pour un IPspace ne sont applicables qu'au sein de cet IPspace. Une table de routage distincte est conservée pour chaque SVM au sein d'un IPspace. Par conséquent, aucun routage de trafic cross-SVM ou cross-IPspace n'a lieu.



Les IPspaces prennent en charge les adresses IPv4 et IPv6 sur leurs domaines de routage.

Si vous gérez le stockage pour une seule organisation, vous n'avez pas besoin de configurer les IPspaces. Si vous gérez le stockage de plusieurs entreprises sur un même cluster ONTAP, et qu'aucun de vos clients n'a de

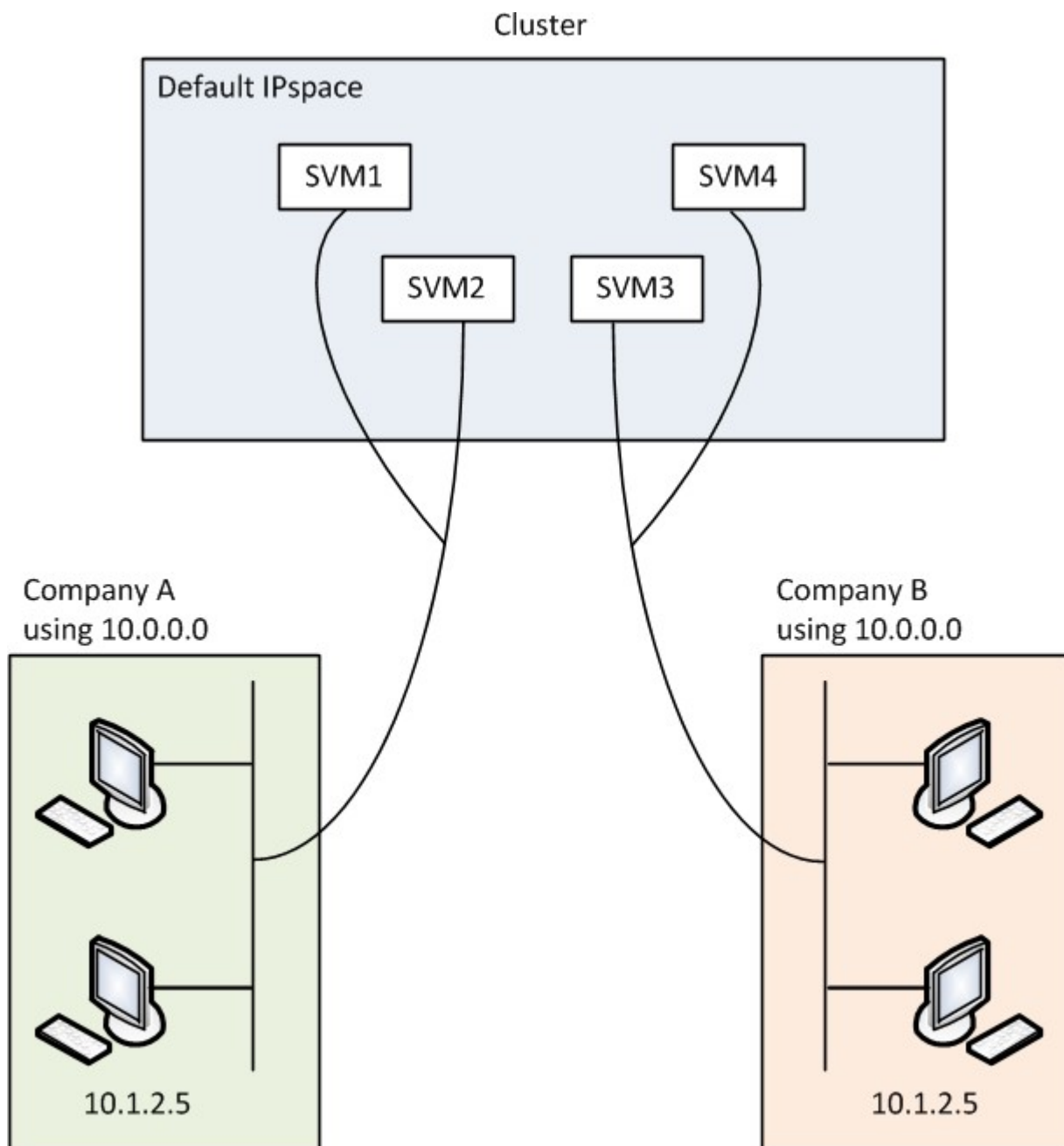
configurations réseau contradictoires, vous n'avez également besoin d'utiliser les IPspaces. Dans de nombreux cas, l'utilisation de machines virtuelles de stockage (SVM), avec leurs propres tables de routage IP distinctes, peut être utilisée pour isoler les configurations réseau uniques au lieu d'utiliser les IPspaces.

### Exemple d'utilisation des IPspaces

Une application commune pour l'utilisation des IPspaces est le besoin d'un fournisseur de services de stockage (SSP) pour connecter les clients des entreprises A et B à un cluster ONTAP sur site du SSP. Dans les deux cas, les deux entreprises utilisent les mêmes plages d'adresse IP privées.

Le SSP crée des SVM sur le cluster pour chaque client et fournit un chemin réseau dédié entre deux SVM et le réseau de l'entreprise A, et entre les deux autres SVM et le réseau de l'entreprise B.

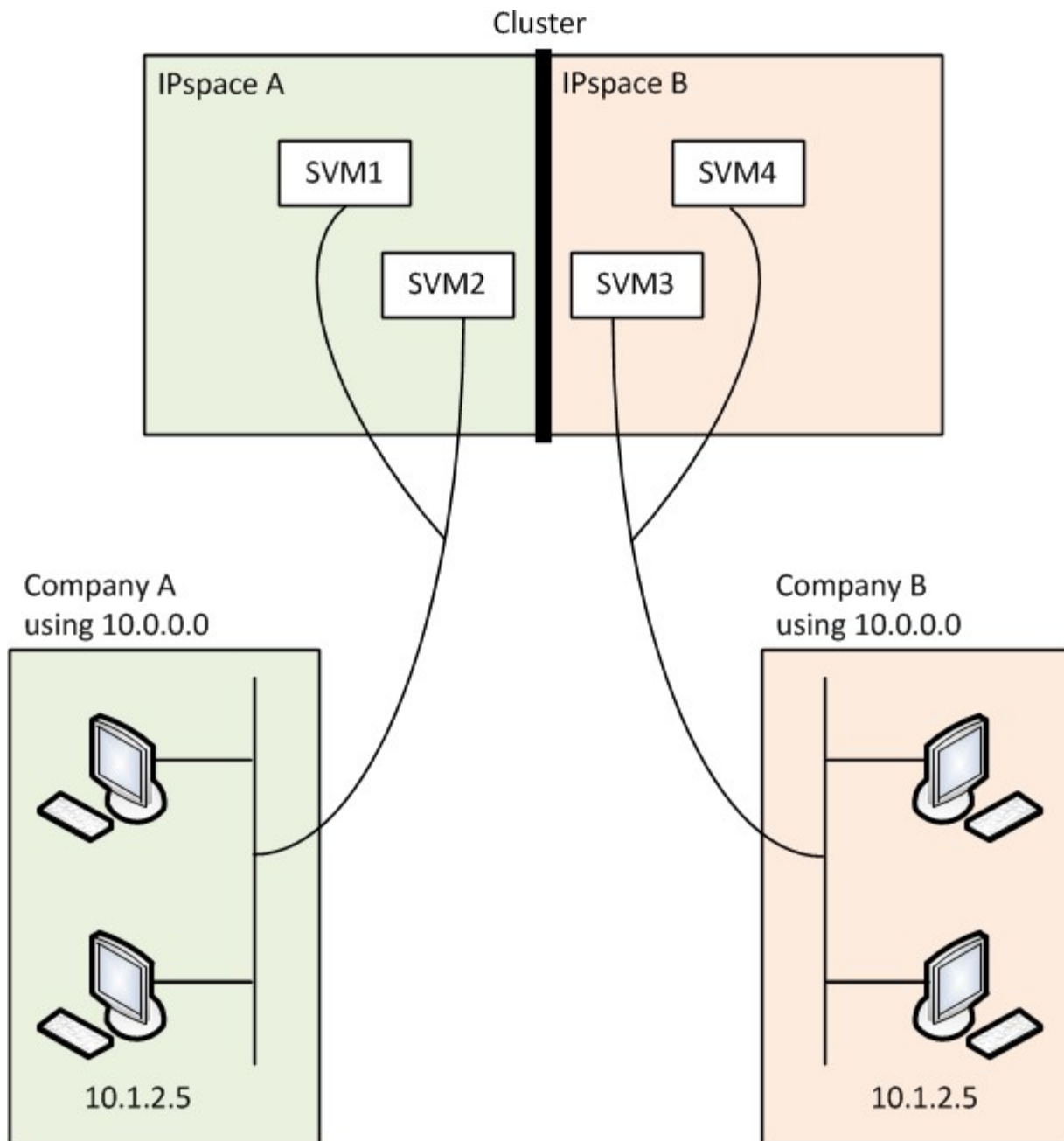
Ce type de déploiement est présenté dans l'illustration suivante et fonctionne si les deux sociétés utilisent des plages d'adresses IP non privées. Cependant, l'illustration montre que les deux sociétés utilisent les mêmes plages d'adresses IP privées, ce qui cause des problèmes.





Les deux entreprises utilisent le sous-réseau de l'adresse IP privée 10.0.0.0, ce qui entraîne les problèmes suivants :

- Les SVM du cluster sur le site SSP ont des adresses IP contradictoires si les deux entreprises décident d'utiliser la même adresse IP pour leurs SVM respectifs.
- Même si les deux entreprises conviennent d'utiliser différentes adresses IP pour leurs SVM, des problèmes peuvent survenir.
- Par exemple, si un client du réseau A possède la même adresse IP qu'un client du réseau B, les paquets destinés à un client de l'espace d'adresse A peuvent être routés vers un client dans l'espace d'adresse B, et vice versa.
- Si les deux sociétés décident d'utiliser des espaces d'adresse mutuellement exclusifs (par exemple, A utilise 10.0.0.0 avec un masque de réseau 255.128.0.0 et B utilise 10.128.0.0 avec un masque de réseau 255.128.0.0), Le SSP doit configurer des routes statiques sur le cluster pour acheminer le trafic de manière appropriée vers les réseaux A et B.
- Cette solution n'est ni évolutive (en raison des routes statiques), ni sécurisée (le trafic de diffusion est envoyé à toutes les interfaces du cluster). Pour résoudre ces problèmes, le SSP définit deux IPspaces sur le cluster : un pour chaque entreprise. Étant donné qu'aucun trafic cross-IPspace n'est routé, les données de chaque entreprise sont acheminées de manière sécurisée vers son réseau respectif même si tous les SVM sont configurés dans l'espace d'adresse 10.0.0.0, comme illustré ci-dessous :



De plus, les adresses IP mentionnées par les différents fichiers de configuration, tels que `/etc/hosts` fichier, le `/etc/hosts.equiv` fichier, et the `/etc/rc` Fichier, sont relatifs à cet IPspace. Les IPspaces permettent au SSP de configurer la même adresse IP pour plusieurs SVM, sans conflit.

### Propriétés standard des IPspaces

Les IPspaces spéciaux sont créés par défaut lors de la première création du cluster. De plus, des machines virtuelles de stockage spéciales sont créées pour chaque IPspace.

Deux IPspaces sont créés automatiquement lors de l'initialisation du cluster :

- IPspace par défaut

Cet IPspace est un conteneur pour les ports, les sous-réseaux et les SVM qui servent de données. Si votre configuration n'a pas besoin d'IPspaces distinctes pour les clients, tous les SVM peuvent être créés dans cet IPspace. Cet IPspace contient également les ports de gestion du cluster et des nœuds.

- IPspace « cluster »

Cet IPspace contient tous les ports de cluster de tous les nœuds du cluster. Il est créé automatiquement lors de la création du cluster. Il assure la connectivité au réseau interne privé du cluster. À mesure que les nœuds supplémentaires rejoignent le cluster, les ports de cluster à partir de ces nœuds sont ajoutés à l'IPspace « Cluster ».

Un SVM « système » existe pour chaque IPspace. Lorsque vous créez un IPspace, un SVM système par défaut du même nom est créé :

- Le SVM système pour le « Cluster » IPspace transmet le trafic du cluster entre les nœuds d'un cluster sur le réseau interne de cluster privé.

Il est géré par l'administrateur du cluster, et il porte le nom « Cluster ».

- Le SVM système pour l'IPspace « par défaut » transmet le trafic de gestion du cluster et des nœuds, y compris le trafic intercluster entre les clusters.

Il est géré par l'administrateur du cluster, et il utilise le même nom que le cluster.

- Le SVM système pour un IPspace personnalisé que vous créez implique le trafic de gestion pour ce SVM.

Il est géré par l'administrateur du cluster, et il utilise le même nom que l'IPspace.

Un ou plusieurs SVM pour les clients peuvent exister dans un IPspace. Chaque SVM client dispose de ses propres volumes et configurations de données, et il est administré indépendamment des autres SVM.

## Créez les IPspaces

Les IPspaces sont des espaces d'adresse IP distincts dans lesquels les serveurs de stockage virtuels (SVM) résident. Vous pouvez créer des IPspaces lorsque vos SVM ont besoin de leur propre stockage, administration et routage sécurisés. Les IPspaces permettent de créer un espace d'adresse IP distinct pour chaque SVM dans un cluster. Ainsi, les clients se trouvant dans des domaines réseau distincts d'un point de vue administratif peuvent accéder aux données du cluster tout en utilisant des adresses IP redondantes à partir de la même plage de sous-réseaux.

### Description de la tâche

Il existe une limite de 512 IPspaces au niveau du cluster. La limite à l'échelle du cluster est réduite à 256 IPspaces pour les clusters contenant des nœuds de 6 Go de RAM. Reportez-vous au Hardware Universe pour déterminer si des limites supplémentaires s'appliquent à votre plateforme.

["NetApp Hardware Universe"](#)



Un nom IPspace ne peut pas être « tous », car « tous » est un nom réservé au système.

### Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

### Étape

1. Création d'un IPspace :

```
network ipspace create -ipspace ipspace_name
```

`ipspace_name` Est le nom de l'IPspace que vous souhaitez créer. La commande suivante crée l'IPspace `ipspace1` sur un cluster :

```
network ipspace create -ipspace ipspace1
```

## 2. Afficher les IPspaces :

```
network ipspace show
```

| IPspace  | Vserver List | Broadcast Domains |
|----------|--------------|-------------------|
| Cluster  | Cluster      | Cluster           |
| Default  | Cluster1     | Default           |
| ipspace1 | ipspace1     | -                 |

L'IPspace est créé, ainsi que le système SVM pour l'IPspace. Le SVM système transmet le trafic de gestion.

### Une fois que vous avez terminé

Si vous créez un IPspace dans un cluster avec une configuration MetroCluster, les objets IPspace doivent être répliqués manuellement sur les clusters partenaires. Tout SVM créé et affecté à un IPspace avant la réplication de l'IPspace ne sera pas répliqué sur les clusters partenaires.

Les domaines de diffusion sont créés automatiquement dans l'IPspace par défaut et peuvent être déplacés entre les IPspaces à l'aide de la commande suivante :

```
network port broadcast-domain move
```

Par exemple, si vous souhaitez déplacer un domaine de diffusion de « default » à « ips1 », à l'aide de la commande suivante :

```
network port broadcast-domain move -ipspace Default -broadcast-domain
Default -to-ipspace ips1
```

## Affichez les IPspaces

Vous pouvez afficher la liste des IPspaces qui existent dans un cluster et afficher les serveurs de stockage virtuels (SVM), les domaines de diffusion et les ports affectés à chaque IPspace.

### Étape

Affichage des IPspaces et des SVM dans un cluster :

```
network ipspace show [-ipspace ipspace_name]
```

La commande suivante affiche tous les IPspaces, le SVM et les domaines de diffusion dans le cluster :

```
network ipspace show
IPspace Vserver List Broadcast Domains
----- -
Cluster
Default Cluster Cluster
 vs1, cluster-1 Default
ipspace1 vs3, vs4, ipspace1 bcast1
```

La commande suivante affiche les nœuds et les ports faisant partie de l'IPspace ipspace1 :

```
network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

## Supprimez un IPspace

Si vous n'avez plus besoin d'un IPspace, vous pouvez le supprimer.

### Avant de commencer

Il ne doit y avoir aucun domaine de diffusion, aucune interface réseau ou SVM associé à l'IPspace que vous souhaitez supprimer.

Les IPspaces « Default » (Cluster-defined) et « Cluster » (Cluster-defined IPspaces) ne peuvent pas être supprimés.

### Étape

Suppression d'un IPspace :

```
network ipspace delete -ipspace ipspace_name
```

La commande suivante supprime IPspace ipspace1 du cluster :

```
network ipspace delete -ipspace ipspace1
```

## Les domaines de diffusion

### Broadcast domain (ONTAP 9.8 et versions ultérieures)

#### Présentation du broadcast domain (ONTAP 9.8 et versions ultérieures)

Les domaines de diffusion sont destinés à regrouper les ports réseau qui appartiennent au même réseau de couche 2. Les ports du groupe peuvent ensuite être utilisés par une machine virtuelle de stockage (SVM) pour le trafic de données ou de gestion.

Un domaine de diffusion réside dans un IPspace. Lors de l'initialisation du cluster, le système crée deux broadcast domain :

- Le broadcast domain « Default » contient les ports qui sont dans le « Default » IPspace.

Ces ports servent principalement à transmettre des données. Les ports de management des clusters et de management des nœuds sont également présents dans ce broadcast domain.

- Le broadcast domain « Cluster » contient les ports qui sont dans le « Cluster » IPspace.

Ces ports sont utilisés pour la communication de cluster et incluent tous les ports de cluster de tous les nœuds du cluster.

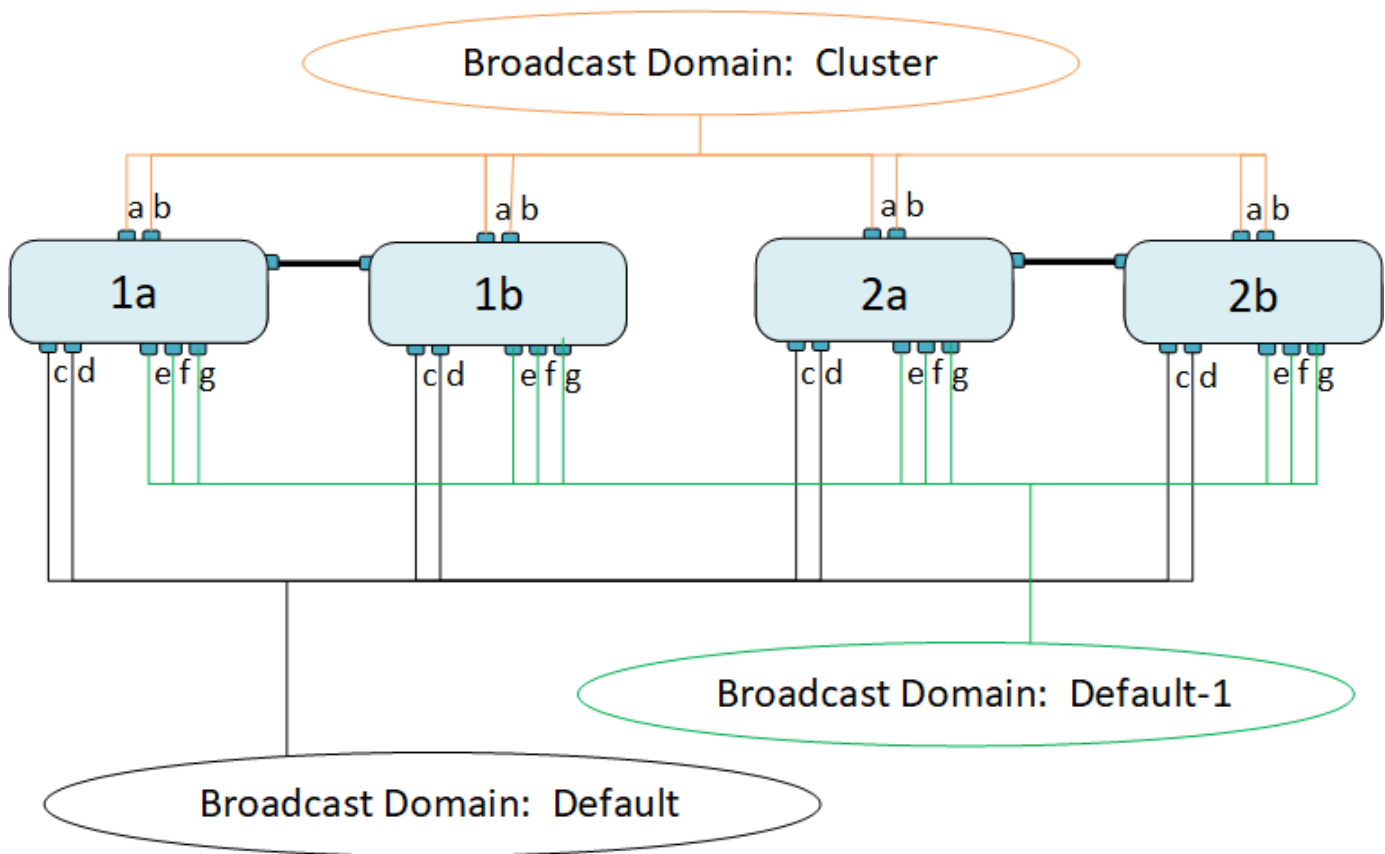
Le système crée des domaines de diffusion supplémentaires dans l'IPspace par défaut si nécessaire. Le broadcast domain « Default » contient le home-port de la LIF de gestion, ainsi que tous les autres ports qui ont une accessibilité de couche 2 à ce port. Les domaines de diffusion supplémentaires sont nommés « default-1 », « default-2 », etc.

#### Exemple d'utilisation de domaines de diffusion

Un broadcast domain est un ensemble de ports réseau dans le même IPspace qui peut également être réachstable au niveau de la couche 2, notamment les ports de nombreux nœuds du cluster.

L'illustration montre les ports assignés à trois broadcast domain dans un cluster à quatre nœuds :

- Le broadcast domain « Cluster » est créé automatiquement lors de l'initialisation du cluster et il contient les ports a et b de chaque nœud du cluster.
- Le broadcast domain est également créé automatiquement lors de l'initialisation du cluster et il contient les ports c et d de chaque nœud du cluster.
- Le système crée automatiquement tout domaine de diffusion supplémentaire lors de l'initialisation du cluster en fonction de la capacité d'accès au réseau de couche 2. Ces domaines de diffusion supplémentaires sont nommés default-1, default-2, etc.



Un failover group du même nom avec les mêmes ports réseau que chacun des domaines de broadcast est créé automatiquement. Ce failover group est automatiquement géré par le système, ce qui signifie qu'à mesure que des ports sont ajoutés ou supprimés du broadcast domain, ils sont automatiquement ajoutés ou supprimés de ce failover group.

### Ajouter un domaine de diffusion

Les domaines de diffusion regroupent des ports réseau dans le cluster qui appartiennent au même réseau de couche 2. Les ports peuvent ensuite être utilisés par les SVM.

Depuis ONTAP 9.8, les domaines de diffusion sont automatiquement créés lors de l'opération de création ou de jointure du cluster. Depuis ONTAP 9.12.0, outre les domaines de diffusion créés automatiquement, vous pouvez ajouter manuellement un domaine de diffusion dans System Manager.

### Avant de commencer

Les ports que vous prévoyez d'ajouter au broadcast domain ne doivent pas appartenir à un autre broadcast domain. Si les ports que vous souhaitez utiliser appartiennent à un autre domaine de diffusion mais sont inutilisés, supprimez ces ports du domaine de diffusion d'origine.

### Description de la tâche

- Tous les noms de domaine de diffusion doivent être uniques au sein d'un IPspace.
- Les ports ajoutés à un domaine de diffusion peuvent être des ports réseau physiques, des VLAN ou des groupes d'interfaces/groupes d'agrégation de liens (LAG/ifgrps).
- Si les ports que vous souhaitez utiliser appartiennent à un autre domaine de diffusion, mais sont inutilisés, supprimez-les du domaine de diffusion existant avant de les ajouter au nouveau.
- L'unité de transmission maximale (MTU) des ports ajoutés à un domaine de diffusion est mise à jour vers la valeur MTU définie dans le domaine de diffusion.

- La valeur MTU doit correspondre à tous les périphériques connectés à ce réseau de couche 2, à l'exception du trafic de gestion du port e0M.
- Si vous ne spécifiez pas de nom IPspace, le domaine de diffusion est créé dans l'IPspace « par défaut ».

Pour faciliter la configuration du système, un failover group du même nom est créé automatiquement contenant les mêmes ports.



## System Manager

### Étapes

1. Sélectionnez **réseau > Présentation > domaine de diffusion**.
2. Cliquez sur **+ Add**
3. Nommez le domaine de diffusion.
4. Définissez la MTU.
5. Sélectionner l'IPspace.
6. Enregistrez le domaine de diffusion.

Vous pouvez modifier ou supprimer un domaine de diffusion après son ajout.

### CLI

Dans ONTAP 9.7 ou version antérieure, vous pouvez créer manuellement un domaine de diffusion.

Si vous utilisez ONTAP 9.8 et les versions ultérieures, les domaines de diffusion sont créés automatiquement en fonction de l'accessibilité de couche 2. Pour plus d'informations, voir ["Réparation de l'accessibilité de l'orifice"](#).

### Étapes

1. Afficher les ports qui ne sont pas actuellement affectés à un broadcast domain :

```
network port show
```

Si l'affichage est grand, utilisez le `network port show -broadcast-domain` commande pour afficher uniquement les ports non assignés.

2. Créer un broadcast domain :

```
network port broadcast-domain create -broadcast-domain
broadcast_domain_name -mtu mtu_value [-ipSPACE ipSPACE_name] [-ports
ports_list]
```

a. `broadcast_domain_name` est le nom du domaine de diffusion que vous souhaitez créer.

b. `mtu_value` Est la taille de MTU des paquets IP ; 1500 et 9000 sont des valeurs types.

Cette valeur est appliquée à tous les ports ajoutés à ce broadcast domain.

c. `ipSPACE_name` Est le nom de l'IPspace à laquelle ce broadcast domain sera ajouté.

L'IPspace par défaut est utilisé sauf si vous spécifiez une valeur pour ce paramètre.

d. `ports_list` est la liste des ports qui seront ajoutés au broadcast domain.

Les ports sont ajoutés au format `node_name:port_number`, par exemple, `node1:e0c`.

3. Vérifiez que le domaine de diffusion a été créé comme vous le souhaitez :

```
network port show -instance -broadcast-domain new_domain
```

### Exemple

La commande suivante crée broadcast domain bcast1 dans l'IPspace par défaut, définit le MTU sur 1500 et ajoute quatre ports :

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

### Une fois que vous avez terminé

Vous pouvez définir le pool d'adresses IP qui seront disponibles dans le broadcast domain en créant un sous-réseau, ou encore attribuer des SVM et des interfaces au IPspace à ce moment. Pour plus d'informations, voir ["Cluster et SVM peering"](#).

Si vous devez modifier le nom d'un domaine de diffusion existant, utilisez le `network port broadcast-domain rename` commande.

### Ajouter ou supprimer des ports d'un domaine de diffusion (ONTAP 9.8 et versions ultérieures)

Les domaines de diffusion sont automatiquement créés lors de l'opération de création ou de jointure du cluster. Il n'est pas nécessaire de supprimer manuellement les ports des domaines de diffusion.

Si l'accessibilité du port réseau a changé, via la connectivité réseau physique ou la configuration du commutateur, et qu'un port réseau appartient à un autre domaine de diffusion, reportez-vous à la rubrique suivante :


["Réparation de l'accessibilité de l'orifice"](#)

## System Manager

À partir de ONTAP 9.14.1, vous pouvez utiliser System Manager pour réaffecter des ports Ethernet sur des domaines de diffusion. Il est recommandé d'attribuer chaque port Ethernet à un domaine de diffusion. Ainsi, si vous annulez l'attribution d'un port Ethernet à un domaine de diffusion, vous devez le réaffecter à un autre domaine de diffusion.

### Étapes

Pour réaffecter des ports Ethernet, effectuez les opérations suivantes :

1. Sélectionnez **réseau > vue d'ensemble**.
2. Dans la section **Broadcast Domains**, sélectionnez  en regard du nom de domaine.
3. Dans le menu déroulant, sélectionnez **Modifier**.
4. Sur la page **Edit Broadcast Domain**, désélectionnez les ports Ethernet que vous souhaitez réaffecter à un autre domaine.
5. Pour chaque port désélectionné, la fenêtre **réaffecter le port Ethernet** s'affiche. Sélectionnez le domaine de diffusion auquel vous souhaitez réaffecter le port, puis sélectionnez **réaffecter**.
6. Sélectionnez tous les ports que vous souhaitez affecter au domaine de diffusion actuel et enregistrez vos modifications.

### CLI

Si l'accessibilité du port réseau a changé, via la connectivité réseau physique ou la configuration du commutateur, et qu'un port réseau appartient à un autre domaine de diffusion, reportez-vous à la rubrique suivante :

#### "Réparation de l'accessibilité de l'orifice"

Vous pouvez également ajouter ou supprimer manuellement des ports de domaines de diffusion à l'aide du `network port broadcast-domain add-ports` ou le `network port broadcast-domain remove-ports` commande.

### Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Les ports que vous prévoyez d'ajouter à un broadcast domain ne doivent pas appartenir à un autre broadcast domain.
- Les ports qui appartiennent déjà à un groupe d'interface ne peuvent pas être ajoutés individuellement à un broadcast domain.

### Description de la tâche

Les règles suivantes s'appliquent lors de l'ajout et de la suppression de ports réseau :

| Lors de l'ajout de ports...                                                                | Lors de la suppression des ports...                                            |
|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Les ports peuvent être des ports réseau, des VLAN ou des groupes d'interfaces (ifgrps).    | S/O                                                                            |
| Les ports sont ajoutés au groupe de basculement défini par le système du broadcast domain. | Les ports sont supprimés de tous les failover groups dans le broadcast domain. |
| La MTU des ports est mise à jour vers la valeur MTU définie dans le domaine de diffusion.  | La MTU des ports est inchangée.                                                |

L'IPspace des ports est mis à jour vers la valeur IPspace du broadcast domain.

Les ports sont déplacés vers l'IPspace « par défaut » sans attribut de domaine de diffusion.



Si vous supprimez le dernier port membre d'un groupe d'interfaces à l'aide du `network port ifgrp remove-port` commande, il provoque la suppression du port group d'interface du broadcast domain, car un port group d'interface vide n'est pas autorisé dans un broadcast domain.

## Étapes

1. Affiche les ports actuellement affectés ou non affectés à un domaine de diffusion à l'aide de l'`network port show` commande.
2. Ajouter ou supprimer des ports réseau du broadcast domain :

| Les fonctions que vous recherchez...                 | Utiliser...                                             |
|------------------------------------------------------|---------------------------------------------------------|
| Permet d'ajouter des ports à un domaine de diffusion | <code>network port broadcast-domain add-ports</code>    |
| Supprime des ports d'un broadcast domain             | <code>network port broadcast-domain remove-ports</code> |

3. Vérifiez que les ports ont été ajoutés ou supprimés du broadcast domain :

```
network port show
```

Pour plus d'informations sur ces commandes, reportez-vous à la section ["Référence de commande ONTAP"](#)

### Exemples d'ajout et de suppression de ports

La commande suivante ajoute le port e0g sur le nœud cluster-1-01 et le port e0g sur le nœud cluster-1-02 au broadcast domain bcast1 dans l'IPspace par défaut :

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

La commande suivante ajoute deux ports de cluster à broadcast domain Cluster dans le Cluster IPspace :

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

La commande suivante supprime le port e0e sur le nœud cluster1-01 du broadcast domain bcast1 dans le Default IPspace :

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain
bcast1 -ports cluster-1-01:e0e
```

## Réparation de l'accessibilité de l'orifice

Les domaines de diffusion sont créés automatiquement. Cependant, si un port est

recâblage ou si la configuration du commutateur change, un port peut avoir besoin d'être réparé dans un domaine de diffusion différent (nouveau ou existant).

ONTAP peut détecter et recommander automatiquement des solutions aux problèmes de câblage réseau en fonction de la capacité de couche 2 d'un composant de domaine de diffusion (ports ethernet).

Un câblage incorrect pendant peut provoquer une affectation de port de domaine de diffusion inattendue. Depuis ONTAP 9.10.1, le cluster vérifie automatiquement la présence de problèmes de câblage réseau en vérifiant la capacité de port après la configuration du cluster ou lorsqu'un nouveau nœud rejoint un cluster existant.

## System Manager

Si un problème de capacité de port est détecté, System Manager recommande une opération de réparation pour résoudre le problème.

Une fois le cluster configuré, des problèmes de câblage réseau sont signalés sur le tableau de bord.

Après l'ajout d'un nouveau nœud à un cluster, des problèmes de câblage réseau apparaissent sur la page nœuds.

Vous pouvez également afficher l'état du câblage réseau sur le schéma de réseau. Les problèmes de capacité de port sont indiqués sur le schéma du réseau par une icône d'erreur rouge.

## Post-configuration du cluster

Une fois le cluster configuré, si le système détecte un problème de câblage réseau, un message s'affiche sur le tableau de bord.



## Étapes

1. Corriger le câblage comme indiqué dans le message.
2. Cliquez sur le lien pour lancer la boîte de dialogue mettre à jour les domaines de diffusion. La boîte de dialogue mettre à jour les domaines de diffusion s'ouvre.



3. Examinez les informations sur le port, y compris le nœud, les problèmes, le domaine de diffusion actuel et le domaine de diffusion attendu.
4. Sélectionnez les ports à réparer et cliquez sur **Fix**.  
Le système déplace les ports du domaine de diffusion actuel vers le domaine de diffusion attendu.

## Jointure post-nœud

Après l'ajout d'un nouveau nœud à un cluster, si le système détecte un problème de câblage réseau, un message s'affiche sur la page nœuds.

ONTAP System Manager

Search actions, objects, and pages

Overview

Overview

NAME: C1\_sti75-vsim-ucs179a-1620738189

VERSION: NetApp Release Storming\_9.10.0: Mon May 10 13:29:41 UTC 2021

UUID: 9957e052-b253-11eb-8094-005056ac85bc

LOCATION: sti

NTAP SERVERS: 10.235.48.111





DNS DOMAINS: cti.gdLenglab.netapp.com, gdLenglab.netapp.com, rtp.netapp.com, eng.netapp.com, netapp.com

NAME SERVERS: 10.224.223.131, 10.224.223.130

MANAGEMENT INTERFACES: 172.21.105.181, fd20:8b1e:b255:91b6:9d2, fd20:8b1e:b255:91b6:9da

DATE AND TIME: May 25, 2021, 7:51 AM America/New\_York

Nodes

| Nodes                                                                             | Name               | Serial Number | Up Time             | Utilization                                                                           | Management IP                           | Service Processor IP | System ID  |
|-----------------------------------------------------------------------------------|--------------------|---------------|---------------------|---------------------------------------------------------------------------------------|-----------------------------------------|----------------------|------------|
| sti75-vsim-ucs179b / sti75-vsim-ucs179a                                           |                    |               |                     |                                                                                       |                                         |                      |            |
|  | sti75-vsim-ucs179b | 4086630-01-3  | 13 day(s), 22:39:02 |  6%  | 172.21.138.127, fd20:8b1e:b255:91af:29c |                      | 4086630013 |
|  | sti75-vsim-ucs179a | 4086630-01-4  | 13 day(s), 22:39:02 |  19% | 172.21.138.125, fd20:8b1e:b255:91af:29a |                      | 4086630014 |

One port cannot be reached because the broadcast domain configuration is not correct. Make sure the port cabling and the switch configuration are correct and update broadcast domains.  
[Update Broadcast Domains](#)

## Étapes

1. Corriger le câblage comme indiqué dans le message.
2. Cliquez sur le lien pour lancer la boîte de dialogue mettre à jour les domaines de diffusion. La boîte de dialogue mettre à jour les domaines de diffusion s'ouvre.

Update Broadcast Domains

The broadcast domains for the following ports are not correctly configured

| Port | Node           | Issue         | Current Broadca... | Expected Broadc... |
|------|----------------|---------------|--------------------|--------------------|
| e0g  | sti75-vsim-... | Not reachable | mgmt_bd_1500       | Default            |

Cancel Fix

3. Examinez les informations sur le port, y compris le nœud, les problèmes, le domaine de diffusion actuel et le domaine de diffusion attendu.
4. Sélectionnez les ports à réparer et cliquez sur **Fix**.  
Le système déplace les ports du domaine de diffusion actuel vers le domaine de diffusion attendu.

## CLI

### Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

### Description de la tâche

Une commande est disponible pour réparer automatiquement la configuration du domaine de diffusion pour un port basé sur la capacité d'accessibilité de couche 2 détectée par ONTAP.

## Étapes

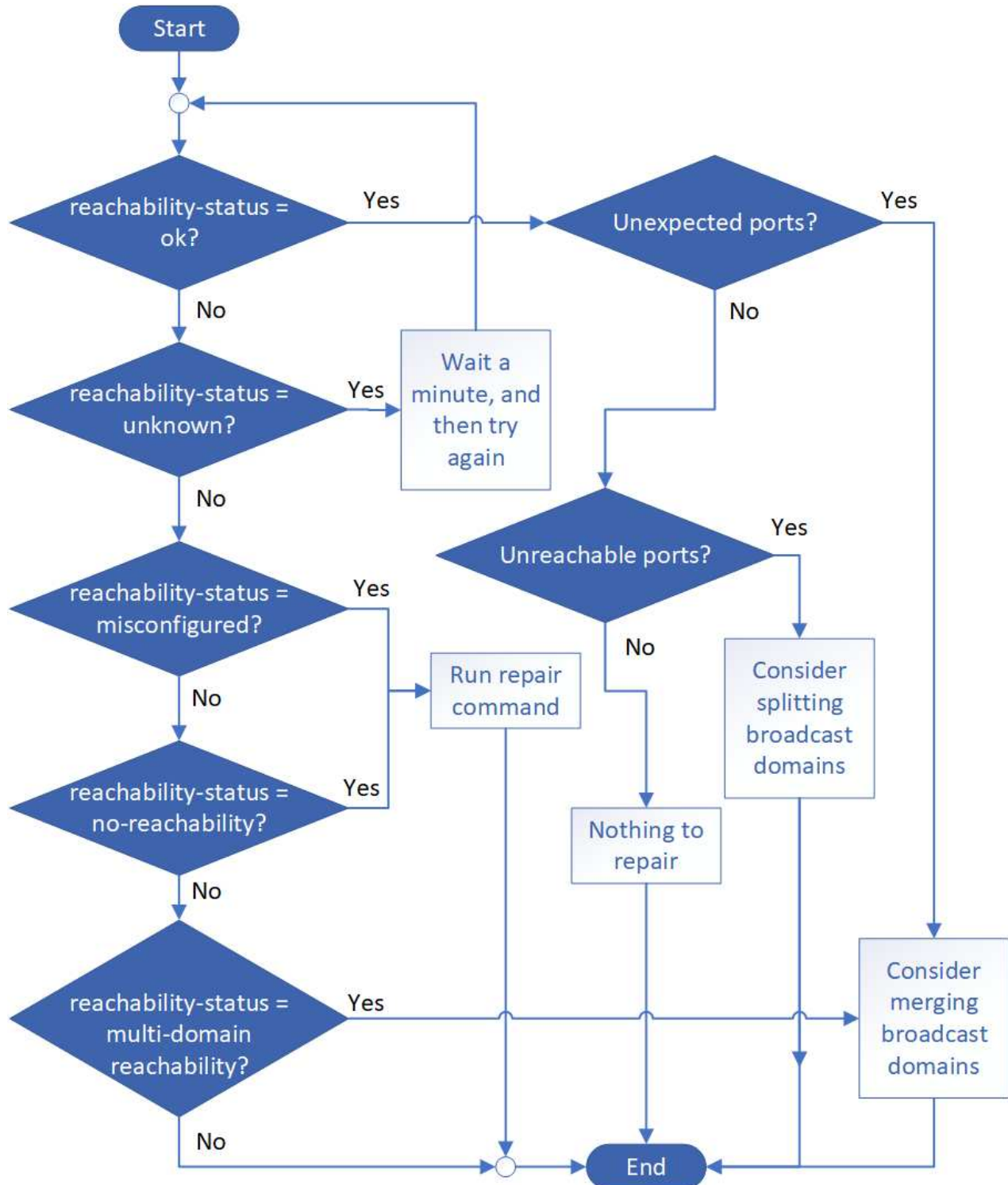
1. Vérifiez la configuration et le câblage de votre commutateur.

2. Vérifiez l'accessibilité du port :

```
network port reachability show -detail -node -port
```

La sortie de la commande contient les résultats de l'accessibilité.

3. Utilisez l'arbre décisionnel et le tableau ci-dessous pour comprendre les résultats de l'accessibilité et déterminer ce que, le cas échéant, faire ensuite.





| État-accessibilité                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ok                                                    | <p>Le port a une capacité de réachabilité de couche 2 à son domaine de diffusion attribué.</p> <p>Si l'état de la capacité d'accessibilité est « ok », mais qu'il y a des « ports inattendus », envisagez de fusionner un ou plusieurs domaines de diffusion. Pour plus d'informations, reportez-vous à la <i>Unexpected ports</i> row suivante.</p> <p>Si le statut de la capacité d'accessibilité est « ok », mais qu'il y a des « ports inaccessibles », envisagez de diviser un ou plusieurs domaines de diffusion. Pour plus d'informations, reportez-vous à la ligne <i>ports inaccessibles</i> suivante.</p> <p>Si l'état de la capacité de reprise est « ok » et qu'il n'y a pas de ports inattendus ou inaccessibles, votre configuration est correcte.</p> |
| Ports inattendus                                      | <p>Le port a une capacité de réachabilité de couche 2 à son domaine de diffusion attribué ; cependant, il a également la possibilité de reachcapacité de couche 2 à au moins un autre domaine de broadcast.</p> <p>Examinez la connectivité physique et la configuration du commutateur pour déterminer s'il est incorrect ou si le domaine de diffusion attribué au port doit être fusionné avec un ou plusieurs domaines de diffusion.</p> <p>Pour plus d'informations, voir "<a href="#">Fusionner les domaines de diffusion</a>".</p>                                                                                                                                                                                                                            |
| Ports inaccessibles                                   | <p>Si un seul domaine de diffusion a été partitionné en deux ensembles de capacité d'accès différents, vous pouvez fractionner un domaine de diffusion pour synchroniser la configuration ONTAP avec la topologie de réseau physique.</p> <p>En général, la liste des ports inaccessibles définit l'ensemble des ports qui doivent être divisés en un autre domaine de diffusion après avoir vérifié que la configuration physique et du commutateur est exacte.</p> <p>Pour plus d'informations, voir "<a href="#">Séparer les domaines de diffusion</a>".</p>                                                                                                                                                                                                      |
| mauvaise configuration de la capacité de réachabilité | <p>Le port n'a pas la capacité de reachcapacité de couche 2 à son domaine de diffusion affecté ; cependant, le port a une capacité de réachabilité de couche 2 à un domaine de diffusion différent.</p> <p>Vous pouvez réparer l'accessibilité du port. Lorsque vous exécutez la commande suivante, le système affecte le port au broadcast domain auquel il a la capacité de reachcapacité :</p> <pre>network port reachability repair -node -port</pre>                                                                                                                                                                                                                                                                                                            |

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sans trabilité               | <p>Le port n'a pas la possibilité de reachcapacité de couche 2 à un domaine de diffusion existant.</p> <p>Vous pouvez réparer l'accessibilité du port. Lorsque vous exécutez la commande suivante, le système affecte le port à un nouveau domaine de diffusion créé automatiquement dans l'IPspace par défaut :</p> <pre>network port reachability repair -node -port</pre> <p><b>Remarque :</b> si tous les ports membres du groupe d'interfaces (ifgrp) signalent no-reachability, exécutant le <code>network port reachability repair</code> sur chaque port membre, chaque port est supprimé de l'ifgrp et placé dans un nouveau domaine de diffusion, ce qui entraîne la suppression de l'ifgrp lui-même. Avant d'utiliser le <code>network port reachability repair</code> vérifiez que le domaine de diffusion accessible du port correspond à ce que vous attendez en fonction de la topologie de votre réseau physique.</p> |
| accessibilité multi-domaines | <p>Le port a une capacité de réachbilité de couche 2 à son domaine de diffusion attribué ; cependant, il a également la possibilité de reachcapacité de couche 2 à au moins un autre domaine de broadcast.</p> <p>Examinez la connectivité physique et la configuration du commutateur pour déterminer s'il est incorrect ou si le domaine de diffusion attribué au port doit être fusionné avec un ou plusieurs domaines de diffusion.</p> <p>Pour plus d'informations, voir "<a href="#">Fusionner les domaines de diffusion</a>".</p>                                                                                                                                                                                                                                                                                                                                                                                              |
| inconnu                      | <p>Si l'état de la capacité d'accessibilité est « inconnu », attendez quelques minutes et essayez à nouveau la commande.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Après avoir réparé un port, vérifiez s'il y a des LIFs et des VLAN déplacés. Si le port faisait partie d'un groupe d'interfaces, vous devez également connaître ce qui s'est passé pour ce groupe.

## LIF

Lorsqu'un port est réparé et déplacé dans un autre domaine de diffusion, tous les LIFs configurés sur le port réparé se voient automatiquement attribuer un nouveau port de base. Si possible, ce port home est sélectionné dans le même domaine de diffusion sur le même nœud. Vous pouvez également sélectionner un port home port à partir d'un autre nœud ou, s'il n'existe aucun port home approprié, celui-ci sera effacé.

Si le port de rattachement d'une LIF est déplacé vers un autre nœud ou est désactivé, la LIF est considérée comme ayant été « déplacée ». Vous pouvez afficher ces LIFs déplacées à l'aide de la commande suivante :

```
displaced-interface show
```

Si des LIF sont déplacées, il faut soit :

- Restaurer le domicile de la LIF déplacée :

```
displaced-interface restore
```

- Définir l'origine du LIF manuellement :

```
network interface modify -home-port -home-node
```

- Supprimer l'entrée de la table « déplacés-interface » si vous êtes satisfait du domicile actuellement configuré du LIF :

```
displaced-interface delete
```

## VLAN

Si le port réparé comporte des VLAN, ces derniers sont automatiquement supprimés mais sont également enregistrés comme ayant été « déplacés ». Vous pouvez afficher les VLAN déplacés suivants :

```
displaced-vlans show
```

En cas de déplacement de réseaux locaux virtuels, vous devez :

- Restaurez les VLAN sur un autre port :

```
displaced-vlans restore
```

- Supprimez l'entrée du tableau « déplacés-vlan » :

```
displaced-vlans delete
```

## Groupes d'interface

Si le port réparé faisait partie d'un groupe d'interfaces, il est retiré de ce groupe d'interfaces. S'il s'agissait du seul port membre attribué au groupe d'interface, le groupe d'interface lui-même est supprimé.

## Sections connexes

["Vérifiez votre configuration réseau après la mise à niveau"](#)

["Surveiller l'accessibilité des ports réseau"](#)

## Déplacer les domaines de diffusion dans les IPspaces (ONTAP 9.8 et versions ultérieures)

Déplacez les domaines de diffusion créés par le système en fonction de la réaccessibilité de couche 2 vers les IPspaces que vous avez créés.

Avant de déplacer le domaine de diffusion, vous devez vérifier l'accessibilité des ports de vos domaines de diffusion.

L'analyse automatique des ports peut déterminer quels ports peuvent se toucher et les placer dans le même domaine de diffusion, mais cette analyse ne peut pas déterminer l'IPspace approprié. Si le domaine de diffusion appartient à un IPspace non-défaut, vous devez le déplacer manuellement en suivant les étapes de cette section.

## Avant de commencer

Les domaines de diffusion sont automatiquement configurés dans le cadre des opérations de création et de jointure du cluster. ONTAP définit le broadcast domain « Default » comme l'ensemble des ports qui ont une connectivité de couche 2 vers le home port de l'interface de gestion sur le premier nœud créé dans le cluster.

D'autres domaines de diffusion sont créés, si nécessaire, et sont nommés **default-1**, **default-2**, etc.

Lorsqu'un nœud rejoint un cluster existant, ses ports réseau rejoignent automatiquement les domaines de diffusion existants en fonction de leur accessibilité de couche 2. S'ils n'ont pas la possibilité de reacher un domaine de diffusion existant, les ports sont placés dans un ou plusieurs nouveaux domaines de diffusion.

### Description de la tâche

- Les ports avec LIF de cluster sont automatiquement placés dans l'IPspace « Cluster ».
- Les ports qui reachcapacité au home port de la LIF node-management sont placés dans le broadcast « default ».
- Les autres domaines de diffusion sont automatiquement créés par ONTAP dans le cadre de l'opération de création ou de jointure du cluster.
- Au fur et à mesure de l'ajout de VLAN et de groupes d'interface, ils sont automatiquement placés dans le domaine de diffusion approprié une minute après leur création.

### Étapes

1. Vérifiez l'accessibilité des ports de vos domaines de diffusion. ONTAP surveille automatiquement l'accessibilité de couche 2. Utilisez la commande suivante pour vérifier que chaque port a été ajouté à un broadcast domain et a la capacité de reachable « ok ».

```
network port reachability show -detail
```

2. Si nécessaire, déplacez les domaines de diffusion vers d'autres IPspaces :

```
network port broadcast-domain move
```

Par exemple, si vous souhaitez déplacer un domaine de diffusion de « Default » à « ips1 » :

```
network port broadcast-domain move -ipspace Default -broadcast-domain Default
-to-ipspace ips1
```

### Domaines de diffusion divisés (ONTAP 9.8 et versions ultérieures)

Si l'accessibilité des ports réseau a changé, via la connectivité réseau physique ou la configuration du commutateur, De plus, un groupe de ports réseau précédemment configurés dans un domaine de diffusion unique est désormais partitionné en deux ensembles de capacité d'accès différents, vous pouvez fractionner un domaine de diffusion pour synchroniser la configuration ONTAP avec la topologie de réseau physique.

Pour déterminer si un domaine de diffusion de port réseau est partitionné en plusieurs ensembles de capacité d'accès, utilisez le `network port reachability show -details` Commande et attention à quels ports ne sont pas connectabilité les uns aux autres (« ports inaccessibles »). En général, la liste des ports inaccessibles définit l'ensemble des ports qui doivent être répartis dans un autre broadcast domain, après avoir vérifié que la configuration physique et celle du switch est exacte.

### Étape

Diviser un domaine de diffusion en deux domaines de diffusion :

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` est le nom de l'ipspace où réside le domaine de diffusion.
- `-broadcast-domain` est le nom du domaine de diffusion qui sera partagé.
- `-new-broadcast-domain` est le nom du nouveau domaine de diffusion qui sera créé.
- `-ports` est le nom du nœud et le port à ajouter au nouveau broadcast domain.

### Fusionner les domaines de diffusion (ONTAP 9.8 et versions ultérieures)

Si la capacité d'accessibilité des ports réseau a changé, soit par le biais de la connectivité réseau physique, soit par la configuration des commutateurs, et si deux groupes de ports réseau précédemment configurés dans plusieurs domaines de diffusion sont désormais tous des domaines de partage, la fusion de deux domaines de diffusion peut être utilisée pour synchroniser la configuration ONTAP avec la topologie du réseau physique.

Pour déterminer si plusieurs domaines de diffusion appartiennent à un ensemble de capacité d'accès, utilisez la commande « `Network port reachability show -details` » et prêtez attention aux ports configurés dans un autre domaine de diffusion ayant une connectivité l'un avec l'autre (« ports imprévus »). En général, la liste des ports inattendus définit l'ensemble des ports qui doivent être fusionnés dans le domaine de diffusion après avoir vérifié que la configuration physique et de commutateur est exacte.

#### Étape

Fusionner les ports d'un domaine de diffusion dans un domaine de diffusion existant :

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` est le nom de l'ipspace où résident les domaines de diffusion.
- `-broadcast-domain` est le nom du domaine de diffusion qui sera fusionné.
- `-into-broadcast-domain` est le nom du domaine de diffusion qui recevra des ports supplémentaires.

### Modification de la valeur MTU pour les ports d'un domaine de diffusion (ONTAP 9.8 et versions ultérieures)

Vous pouvez modifier la valeur MTU d'un domaine de diffusion pour modifier la valeur MTU de tous les ports de ce domaine de diffusion. Cela peut être fait pour prendre en charge les modifications de topologie effectuées sur le réseau.

#### Avant de commencer

La valeur MTU doit correspondre à tous les périphériques connectés à ce réseau de couche 2, à l'exception du

trafic de gestion du port e0M.

### Description de la tâche

La modification de la valeur MTU entraîne une brève interruption du trafic sur les ports affectés. Le système affiche une invite vous demandant de répondre par y pour effectuer la modification de la MTU.

### Étape

Modifier la valeur MTU pour tous les ports d'un domaine de diffusion :

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

- `broadcast_domain` est le nom du domaine de diffusion.
- `mtu` Est la taille de MTU des paquets IP ; 1500 et 9000 sont des valeurs types.
- `ipspace` Est le nom de l'IPspace dans lequel réside ce domaine de diffusion. L'IPspace par défaut est utilisé sauf si vous spécifiez une valeur pour cette option. La commande suivante remplace la MTU sur 9000 pour tous les ports du broadcast domain `bcast1` :

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <
9000 >
Warning: Changing broadcast domain settings will cause a momentary data-
serving interruption.
Do you want to continue? {y|n}: <y>
```

### Afficher les domaines de diffusion (ONTAP 9.8 et versions ultérieures)

Vous pouvez afficher la liste des domaines de broadcast au sein de chaque IPspace dans un cluster. La sortie affiche également la liste des ports et la valeur MTU pour chaque domaine de diffusion.

### Étape

Afficher les broadcast domain et les ports associés dans le cluster :

```
network port broadcast-domain show
```

La commande suivante affiche tous les broadcast domain et les ports associés du cluster :

```

network port broadcast-domain show
IPspace Broadcast
Name Domain Name MTU Port List

Cluster Cluster 9000
 cluster-1-01:e0a complete
 cluster-1-01:e0b complete
 cluster-1-02:e0a complete
 cluster-1-02:e0b complete
Default Default 1500
 cluster-1-01:e0c complete
 cluster-1-01:e0d complete
 cluster-1-02:e0c complete
 cluster-1-02:e0d complete
 Default-1 1500
 cluster-1-01:e0e complete
 cluster-1-01:e0f complete
 cluster-1-01:e0g complete
 cluster-1-02:e0e complete
 cluster-1-02:e0f complete
 cluster-1-02:e0g complete

```

La commande suivante affiche les ports du broadcast domain default-1 qui ont un statut de mise à jour de l'erreur, ce qui indique que le port n'a pas pu être mis à jour correctement :

```

network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error

IPspace Broadcast
Name Domain Name MTU Port List

Default Default-1 1500
 cluster-1-02:e0g error

```

Pour plus d'informations, voir ["Référence de commande ONTAP"](#).

### Supprimer un domaine de diffusion

Si vous n'avez plus besoin d'un domaine de diffusion, vous pouvez le supprimer. Cela déplace les ports associés à ce broadcast domain vers le « Default » IPspace.

#### Avant de commencer

Il ne doit y avoir aucun sous-réseau, aucune interface réseau ou SVM associé au broadcast domain que vous souhaitez supprimer.

## Description de la tâche

- Le domaine de diffusion « Cluster » créé par le système ne peut pas être supprimé.
- Tous les Failover Groups liés au broadcast domain sont supprimés lorsque vous supprimez le broadcast domain.


La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

### System Manager

#### À partir de ONTAP 9.12.0, vous pouvez utiliser System Manager pour supprimer un domaine de diffusion

L'option de suppression n'est pas affichée lorsque le broadcast domain contient des ports ou est associé à un sous-réseau.

#### Étapes

1. Sélectionnez **réseau > Présentation > domaine de diffusion**.
2. Sélectionnez  > **Supprimer** en regard du domaine de diffusion que vous souhaitez supprimer.

### CLI

#### Utilisez l'interface de ligne de commande pour supprimer un domaine de diffusion

#### Étape

Supprimer un broadcast domain :

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

La commande suivante supprime le domaine de diffusion default-1 dans IPspace ipspace1 :

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

## Broadcast domain (ONTAP 9.7 et versions antérieures)

### Présentation du domaine de diffusion (ONTAP 9.7 et versions antérieures)

Les domaines de diffusion sont destinés à regrouper les ports réseau qui appartiennent au même réseau de couche 2. Les ports du groupe peuvent ensuite être utilisés par une machine virtuelle de stockage (SVM) pour le trafic de données ou de gestion.

Un domaine de diffusion réside dans un IPspace. Lors de l'initialisation du cluster, le système crée deux broadcast domain :

- Le broadcast domain contient des ports qui sont dans le Default IPspace.  
Ces ports servent principalement à transmettre des données. Les ports de management des clusters et de management des nœuds sont également présents dans ce broadcast domain.
- Le broadcast domain Cluster broadcast domain contient des ports qui sont dans le Cluster IPspace.  
Ces ports sont utilisés pour la communication de cluster et incluent tous les ports de cluster de tous les



nœuds du cluster.

Si vous avez créé des IPspaces uniques pour séparer le trafic client, créez un domaine de diffusion dans chacun de ces IPspaces.



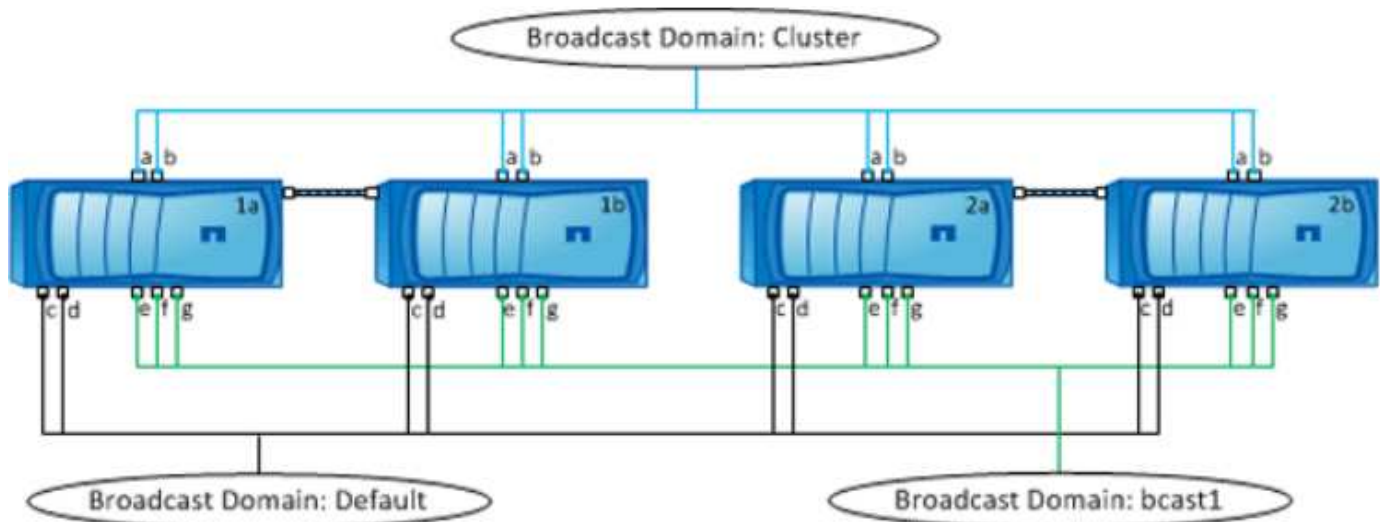
Créez un broadcast domain pour regrouper les ports réseau du cluster qui appartiennent au même réseau de couche 2. Les ports peuvent ensuite être utilisés par les SVM.

#### Exemple d'utilisation de domaines de diffusion

Un broadcast domain est un ensemble de ports réseau dans le même IPspace qui peut également être réachstable au niveau de la couche 2, notamment les ports de nombreux nœuds du cluster.

L'illustration montre les ports assignés à trois broadcast domain dans un cluster à quatre nœuds :

- Le Cluster broadcast domain est créé automatiquement lors de l'initialisation du cluster et il contient les ports a et b de chaque nœud du cluster.
  - Le broadcast domain est également créé automatiquement lors de l'initialisation du cluster et il contient les ports c et d de chaque nœud du cluster.
  - Le broadcast domain bcast1 a été créé manuellement et il contient les ports e, f et g de chaque nœud du cluster.
- Ce broadcast domain a été créé par l'administrateur système spécifiquement pour un nouveau client afin de pouvoir accéder aux données via un nouveau SVM.



Un failover group du même nom avec les mêmes ports réseau que chacun des domaines de broadcast est créé automatiquement. Ce failover group est automatiquement géré par le système, ce qui signifie qu'à mesure que des ports sont ajoutés ou supprimés du broadcast domain, ils sont automatiquement ajoutés ou supprimés de ce failover group.

#### Détermination des ports pouvant être utilisés pour un domaine de diffusion (ONTAP 9.7 et versions antérieures)

Avant de pouvoir configurer un broadcast domain afin de le ajouter au nouveau IPspace, vous devez déterminer les ports disponibles pour le broadcast domain.



Cette tâche est pertinente pour ONTAP 9.0 - 9.7, et non pour ONTAP 9.8.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Description de la tâche

- Les ports peuvent être des ports physiques, des VLAN ou des groupes d'interfaces (ifgroups).
- Les ports que vous souhaitez ajouter au nouveau domaine de diffusion ne peuvent pas être attribués à un domaine de diffusion existant.
- Si les ports que vous souhaitez ajouter au broadcast domain se trouvent déjà dans un autre broadcast domain (par exemple le broadcast domain par défaut dans le Default IPspace), vous devez supprimer les ports de ce broadcast domain avant de les attribuer au nouveau broadcast domain.
- Les ports sur lesquels des LIFs leur sont attribuées ne peuvent pas être supprimés d'un broadcast domain.
- Étant donné que les LIFs de cluster management et node management sont attribuées au broadcast domain par défaut dans l'IPspace par défaut, les ports attribués à ces LIFs ne peuvent pas être supprimés du broadcast domain par défaut.

Étapes

1. Déterminez les affectations de port actuelles.

```
network port show
```

| Node  | Port | IPspace | Broadcast Domain | Link  | MTU  | Admin/Oper |
|-------|------|---------|------------------|-------|------|------------|
| ----- | ---- | -----   | -----            | ----- | ---- | -----      |
| node1 |      |         |                  |       |      |            |
|       | e0a  | Cluster | Cluster          | up    | 9000 | auto/1000  |
|       | e0b  | Cluster | Cluster          | up    | 9000 | auto/1000  |
|       | e0c  | Default | Default          | up    | 1500 | auto/1000  |
|       | e0d  | Default | Default          | up    | 1500 | auto/1000  |
|       | e0e  | Default | Default          | up    | 1500 | auto/1000  |
|       | e0f  | Default | Default          | up    | 1500 | auto/1000  |
|       | e0g  | Default | Default          | up    | 1500 | auto/1000  |
| node2 |      |         |                  |       |      |            |
|       | e0a  | Cluster | Cluster          | up    | 9000 | auto/1000  |
|       | e0b  | Cluster | Cluster          | up    | 9000 | auto/1000  |
|       | e0c  | Default | Default          | up    | 1500 | auto/1000  |
|       | e0d  | Default | Default          | up    | 1500 | auto/1000  |
|       | e0e  | Default | Default          | up    | 1500 | auto/1000  |
|       | e0f  | Default | Default          | up    | 1500 | auto/1000  |
|       | e0g  | Default | Default          | up    | 1500 | auto/1000  |

Dans cet exemple, la sortie de la commande fournit les informations suivantes :

- Ports e0c, e0d, e0e, e0f, et e0g Sur chaque nœud sont affectés au domaine de diffusion par défaut.
  - Ces ports sont potentiellement disponibles pour être utilisés dans le domaine de broadcast de l'IPspace que vous souhaitez créer.
2. Déterminez les ports du broadcast domain par défaut qui sont attribués aux interfaces LIF, et ne peuvent donc pas être déplacés vers un nouveau broadcast domain.

```
network interface show
```

| Vserver  | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is Home |
|----------|-------------------|-------------------|----------------------|--------------|--------------|---------|
| Cluster  |                   |                   |                      |              |              |         |
|          | node1_clus1       | up/up             | 10.0.2.40/24         | node1        | e0a          | true    |
|          | node1_clus2       | up/up             | 10.0.2.41/24         | node1        | e0b          | true    |
|          | node2_clus1       | up/up             | 10.0.2.42/24         | node2        | e0a          | true    |
|          | node2_clus2       | up/up             | 10.0.2.43/24         | node2        | e0b          | true    |
| cluster1 |                   |                   |                      |              |              |         |
|          | cluster_mgmt      | up/up             | 10.0.1.41/24         | node1        | e0c          | true    |
|          | node1_mgmt        | up/up             | 10.0.1.42/24         | node1        | e0c          | true    |
|          | node2_mgmt        | up/up             | 10.0.1.43/24         | node2        | e0c          | true    |

Dans l'exemple suivant, le résultat de la commande fournit les informations suivantes :

- Les ports de nœud sont affectés au port e0c Sur chaque nœud et sur le home node de la LIF d'administration du cluster est on e0c marche node1.
- Ports e0d, e0e, e0f, et e0g Sur chaque nœud ne hébergent pas les LIFs et peuvent être supprimées du broadcast domain par défaut, puis ajoutés à un nouveau broadcast domain pour le nouveau IPspace.

### Créer un domaine de diffusion (ONTAP 9.7 et versions antérieures)

Dans la version ONTAP 9.7 et antérieure, vous créez un broadcast domain pour regrouper les ports réseau du cluster qui appartiennent au même réseau de couche 2. Les ports peuvent ensuite être utilisés par les SVM. Vous devez créer un domaine de diffusion pour un IPspace personnalisé. Les SVM créés dans l'IPspace utilisent les ports du broadcast domain.



Cette tâche est pertinente pour ONTAP 9.0 - 9.7, et non pour ONTAP 9.8.

#### Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Depuis ONTAP 9.8, les domaines de diffusion sont automatiquement créés lors de l'opération de création ou de jointure du cluster. Si vous exécutez ONTAP 9.8 ou une version ultérieure, ces étapes ne sont pas nécessaires.

Dans ONTAP 9.7 et les versions antérieures, les ports que vous prévoyez d'ajouter au broadcast domain ne doivent pas appartenir à un autre broadcast domain.

#### Description de la tâche

Le port vers lequel une LIF échoue doit être membre du failover group pour le LIF. Lorsque vous créez un broadcast domain, ONTAP crée automatiquement un failover group avec le même nom. Le failover group contient tous les ports assignés au broadcast domain.

- Tous les noms de domaine de diffusion doivent être uniques au sein d'un IPspace.
- Les ports ajoutés à un domaine de diffusion peuvent être des ports réseau physiques, des VLAN ou des groupes d'interfaces (ifgrps).
- Si les ports que vous souhaitez utiliser appartiennent à un autre domaine de diffusion, mais sont inutilisés, vous utilisez le `network port broadcast-domain remove-ports` commande pour supprimer les ports du broadcast domain existant.
- Le MTU des ports ajoutés à un domaine de diffusion est mis à jour en fonction de la valeur MTU définie dans le domaine de diffusion.
- La valeur MTU doit correspondre à tous les périphériques connectés à ce réseau de couche 2, à l'exception du trafic de gestion du port e0M.
- Si vous ne spécifiez pas de nom IPspace, le domaine de diffusion est créé dans l'IPspace « par défaut ».

Pour faciliter la configuration du système, un failover group du même nom est créé automatiquement contenant les mêmes ports.

## Étapes

1. Afficher les ports qui ne sont pas actuellement affectés à un broadcast domain :

```
network port show
```

Si l'affichage est grand, utilisez le `network port show -broadcast-domain` commande pour afficher uniquement les ports non assignés.

2. Créer un broadcast domain :

```
network port broadcast-domain create -broadcast-domain broadcast_domain_name
-mtu mtu_value [-ipspace ipspace_name] [-ports ports_list]
```

° *broadcast\_domain\_name* est le nom du domaine de diffusion que vous souhaitez créer.

° *mtu\_value* Est la taille de MTU des paquets IP ; 1500 et 9000 sont des valeurs types.

Cette valeur est appliquée à tous les ports ajoutés à ce broadcast domain.

° *ipspace\_name* Est le nom de l'IPspace à laquelle ce broadcast domain sera ajouté.

L'IPspace par défaut est utilisé sauf si vous spécifiez une valeur pour ce paramètre.

° *ports\_list* est la liste des ports qui seront ajoutés au broadcast domain.

Les ports sont ajoutés au format *node\_name:port\_number*, par exemple, *node1:e0c*.

3. Vérifiez que le domaine de diffusion a été créé comme vous le souhaitez :

```
network port show -instance -broadcast-domain new_domain
```

## Exemple

La commande suivante crée broadcast domain bcast1 dans l'IPspace par défaut, définit le MTU sur 1500 et ajoute quatre ports :

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

## Une fois que vous avez terminé

Vous pouvez définir le pool d'adresses IP qui seront disponibles dans le broadcast domain en créant un sous-réseau, ou encore attribuer des SVM et des interfaces au IPspace à ce moment. Pour plus d'informations, voir ["Cluster et SVM peering"](#).

Si vous devez modifier le nom d'un domaine de diffusion existant, utilisez le `network port broadcast-domain rename` commande.

## Ajouter ou supprimer des ports d'un domaine de diffusion (ONTAP 9.7 et versions antérieures)

Vous pouvez ajouter des ports réseau lors de la création initiale d'un domaine de diffusion ou ajouter des ports à un domaine de diffusion existant ou en supprimer. Cela vous permet d'utiliser efficacement tous les ports du cluster.

Si les ports que vous souhaitez ajouter au nouveau broadcast domain appartiennent déjà à un autre broadcast domain, vous devez les supprimer de ce broadcast domain avant de les attribuer au nouveau broadcast domain.



Cette tâche est pertinente pour ONTAP 9.0 - 9.7, et non pour ONTAP 9.8.

### Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Les ports que vous prévoyez d'ajouter à un broadcast domain ne doivent pas appartenir à un autre broadcast domain.
- Les ports qui appartiennent déjà à un groupe d'interface ne peuvent pas être ajoutés individuellement à un broadcast domain.

### Description de la tâche

Les règles suivantes s'appliquent lors de l'ajout et de la suppression de ports réseau :

| Lors de l'ajout de ports...                                                                | Lors de la suppression des ports...                                                          |
|--------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Les ports peuvent être des ports réseau, des VLAN ou des groupes d'interfaces (ifgrps).    | S/O                                                                                          |
| Les ports sont ajoutés au groupe de basculement défini par le système du broadcast domain. | Les ports sont supprimés de tous les failover groups dans le broadcast domain.               |
| La MTU des ports est mise à jour vers la valeur MTU définie dans le domaine de diffusion.  | La MTU des ports est inchangée.                                                              |
| L'IPspace des ports est mis à jour vers la valeur IPspace du broadcast domain.             | Les ports sont déplacés vers l'IPspace « par défaut » sans attribut de domaine de diffusion. |



Si vous supprimez le dernier port membre d'un groupe d'interfaces à l'aide du `network port ifgrp remove-port` commande, il provoque la suppression du port group d'interface du broadcast domain, car un port group d'interface vide n'est pas autorisé dans un broadcast domain.

### Étapes

1. Affiche les ports actuellement affectés ou non affectés à un domaine de diffusion à l'aide de l' `network port show` commande.

## 2. Ajouter ou supprimer des ports réseau du broadcast domain :

| Les fonctions que vous recherchez...                 | Utiliser...                                             |
|------------------------------------------------------|---------------------------------------------------------|
| Permet d'ajouter des ports à un domaine de diffusion | <code>network port broadcast-domain add-ports</code>    |
| Supprime des ports d'un broadcast domain             | <code>network port broadcast-domain remove-ports</code> |

## 3. Vérifiez que les ports ont été ajoutés ou supprimés du broadcast domain :

```
network port show
```

Pour plus d'informations sur ces commandes, reportez-vous à la section ["Référence de commande ONTAP"](#).

### Exemples d'ajout et de suppression de ports

La commande suivante ajoute le port e0g sur le nœud cluster-1-01 et le port e0g sur le nœud cluster-1-02 au broadcast domain bcast1 dans l'IPspace par défaut :

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

La commande suivante ajoute deux ports de cluster à broadcast domain Cluster dans le Cluster IPspace :

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipSpace Cluster
```

La commande suivante supprime le port e0e sur le nœud cluster1-01 du broadcast domain bcast1 dans le Default IPspace :

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain bcast1
-ports cluster-1-01:e0e
```

### Domaines de diffusion divisés (ONTAP 9.7 ou version antérieure)

Vous pouvez modifier un domaine de diffusion existant en le divisant en deux domaines de diffusion différents, chaque domaine de diffusion contenant certains des ports d'origine attribués au domaine de diffusion d'origine.

#### Description de la tâche

- Si les ports font partie d'un failover group, tous les ports d'un failover group doivent être répartis.
- Si les LIF sont associées à ces ports, elles ne peuvent pas faire partie des plages d'un sous-réseau.

#### Étape

Diviser un domaine de diffusion en deux domaines de diffusion :

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` Est le nom de l'IPspace où réside le domaine de diffusion.
- `-broadcast-domain` est le nom du domaine de diffusion qui sera partagé.
- `-new-broadcast-domain` est le nom du nouveau domaine de diffusion qui sera créé.
- `-ports` est le nom du nœud et le port à ajouter au nouveau broadcast domain.

### Fusionner les domaines de diffusion (ONTAP 9.7 et versions antérieures)

Vous pouvez déplacer tous les ports d'un domaine de diffusion vers un domaine de diffusion existant à l'aide de la commande Merge.

Cette opération réduit les étapes requises si vous deviez supprimer tous les ports d'un broadcast domain, puis ajouter les ports à un broadcast domain existant.

#### Étape

Fusionner les ports d'un domaine de diffusion dans un domaine de diffusion existant :

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` Est le nom de l'IPspace où les domaines de diffusion résident.
- `-broadcast-domain` est le nom du domaine de diffusion qui sera fusionné.
- `-into-broadcast-domain` est le nom du domaine de diffusion qui recevra des ports supplémentaires.

#### Exemple

L'exemple suivant fusionne le domaine de broadcast `bd-data1` dans le domaine de broadcast `bd-data2` :

```
network port -ipspace Default broadcast-domain bd-data1 into-broadcast-domain bd-
data2
```

### Modifier la valeur MTU pour les ports d'un domaine de diffusion (ONTAP 9.7 et versions antérieures)

Vous pouvez modifier la valeur MTU d'un domaine de diffusion pour modifier la valeur MTU de tous les ports de ce domaine de diffusion. Cela peut être fait pour prendre en charge les modifications de topologie effectuées sur le réseau.

#### Avant de commencer

La valeur MTU doit correspondre à tous les périphériques connectés à ce réseau de couche 2, à l'exception du trafic de gestion du port e0M.

#### Description de la tâche

La modification de la valeur MTU entraîne une brève interruption du trafic sur les ports affectés. Le système affiche une invite vous demandant de répondre par y pour effectuer la modification de la MTU.

### Étape

Modifier la valeur MTU pour tous les ports d'un domaine de diffusion :

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

- `broadcast_domain` est le nom du domaine de diffusion.
- `mtu` Est la taille de MTU des paquets IP ; 1500 et 9000 sont des valeurs types.
- `ipspace` Est le nom de l'IPspace dans lequel réside ce domaine de diffusion. L'IPspace par défaut est utilisé sauf si vous spécifiez une valeur pour cette option. La commande suivante remplace la MTU sur 9000 pour tous les ports du broadcast domain `bcast1` :

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <
9000 >
Warning: Changing broadcast domain settings will cause a momentary data-
serving interruption.
Do you want to continue? {y|n}: <y>
```

### Afficher les domaines de diffusion (ONTAP 9.7 et versions antérieures)

Vous pouvez afficher la liste des domaines de broadcast au sein de chaque IPspace dans un cluster. La sortie affiche également la liste des ports et la valeur MTU pour chaque domaine de diffusion.

### Étape

Afficher les broadcast domain et les ports associés dans le cluster :

```
network port broadcast-domain show
```

La commande suivante affiche tous les broadcast domain et les ports associés du cluster :



```
network port broadcast-domain show
```

| IPspace | Broadcast   |       |                  | Update         |
|---------|-------------|-------|------------------|----------------|
| Name    | Domain Name | MTU   | Port List        | Status Details |
| -----   | -----       | ----- | -----            | -----          |
| Cluster | Cluster     | 9000  |                  |                |
|         |             |       | cluster-1-01:e0a | complete       |
|         |             |       | cluster-1-01:e0b | complete       |
|         |             |       | cluster-1-02:e0a | complete       |
|         |             |       | cluster-1-02:e0b | complete       |
| Default | Default     | 1500  |                  |                |
|         |             |       | cluster-1-01:e0c | complete       |
|         |             |       | cluster-1-01:e0d | complete       |
|         |             |       | cluster-1-02:e0c | complete       |
|         |             |       | cluster-1-02:e0d | complete       |
|         | bcast1      | 1500  |                  |                |
|         |             |       | cluster-1-01:e0e | complete       |
|         |             |       | cluster-1-01:e0f | complete       |
|         |             |       | cluster-1-01:e0g | complete       |
|         |             |       | cluster-1-02:e0e | complete       |
|         |             |       | cluster-1-02:e0f | complete       |
|         |             |       | cluster-1-02:e0g | complete       |

La commande suivante affiche les ports du domaine de diffusion bcast1 dont l'état de mise à jour est erroné, ce qui indique que le port n'a pas pu être mis à jour correctement :

```
network port broadcast-domain show -broadcast-domain bcast1 -port-update
-status error
```

| IPspace | Broadcast   |       |                  | Update         |
|---------|-------------|-------|------------------|----------------|
| Name    | Domain Name | MTU   | Port List        | Status Details |
| -----   | -----       | ----- | -----            | -----          |
| Default | bcast1      | 1500  |                  |                |
|         |             |       | cluster-1-02:e0g | error          |

Pour plus d'informations, voir ["Référence de commande ONTAP"](#).

## Supprimer un domaine de diffusion

Si vous n'avez plus besoin d'un domaine de diffusion, vous pouvez le supprimer. Cela déplace les ports associés à ce broadcast domain vers le « Default » IPspace.

### Avant de commencer

Il ne doit y avoir aucun sous-réseau, aucune interface réseau ou SVM associé au broadcast domain que vous souhaitez supprimer.

## Description de la tâche

- Le domaine de diffusion « Cluster » créé par le système ne peut pas être supprimé.
- Tous les Failover Groups liés au broadcast domain sont supprimés lorsque vous supprimez le broadcast domain.


La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

### System Manager

**À partir de ONTAP 9.12.0, vous pouvez utiliser System Manager pour supprimer un domaine de diffusion**

L'option de suppression n'est pas affichée lorsque le broadcast domain contient des ports ou est associé à un sous-réseau.

#### Étapes

1. Sélectionnez **réseau > Présentation > domaine de diffusion**.
2. Sélectionnez  **> Supprimer** en regard du domaine de diffusion que vous souhaitez supprimer.

### CLI

**Utilisez l'interface de ligne de commande pour supprimer un domaine de diffusion**

#### Étape

Supprimer un broadcast domain :

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name [-ipspace ipspace_name]
```

La commande suivante supprime le domaine de diffusion default-1 dans IPspace ipspace1 :

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace ipspace1
```

## Groupes et règles de basculement

### Présentation du basculement de LIF

Le basculement de LIF désigne la migration automatique d'une LIF vers un autre port réseau en réponse à une défaillance de liaison sur le port actuel de la LIF. Ce composant clé assure la haute disponibilité des connexions aux SVM. La configuration du basculement de LIF implique la création d'un groupe de basculement, la modification de la LIF afin d'utiliser le groupe de basculement et la spécification d'une règle de basculement.

Un failover group contient un ensemble de ports réseau (ports physiques, VLAN et groupes d'interfaces) à partir d'un ou de plusieurs nœuds d'un cluster. Les ports réseau présents dans le failover group définissent les cibles de failover disponibles pour le LIF. Un groupe de basculement peut disposer des LIF de données intercluster, node management, et NAS qui y sont attribuées.



Lorsqu'une LIF est configurée sans une cible de basculement valide, une panne se produit lorsque la LIF tente de basculer. Vous pouvez utiliser la commande « `network interface show -Failover` » pour vérifier la configuration du basculement.

Lorsque vous créez un broadcast domain, un failover group du même nom est créé automatiquement contenant les mêmes ports réseau. Ce failover group est automatiquement géré par le système, ce qui signifie qu'à mesure que des ports sont ajoutés ou supprimés du broadcast domain, ils sont automatiquement ajoutés ou supprimés de ce failover group. Cela est fourni comme une efficacité pour les administrateurs qui ne souhaitent pas gérer leurs propres groupes de basculement.

## Créer un groupe de basculement

Vous créez un failover group de ports réseau de sorte qu'une LIF peut automatiquement migrer vers un autre port en cas de défaillance de liaison sur le port actuel du LIF. Cela permet au système de rediriger le trafic réseau vers d'autres ports disponibles dans le cluster.

### Description de la tâche

Vous utilisez le `network interface failover-groups create` commande pour créer le groupe et ajouter des ports au groupe.

- Les ports ajoutés à un failover group peuvent être des ports réseau, des VLAN ou des groupes d'interfaces (ifgrps).
- Tous les ports ajoutés au failover group doivent appartenir au même broadcast domain.
- Un seul port peut résider dans plusieurs groupes de basculement.
- Si vous avez des LIF dans différents VLAN ou domaines de diffusion, vous devez configurer des groupes de basculement pour chaque VLAN ou domaine de diffusion.
- Les groupes de basculement ne s'appliquent pas aux environnements SAN iSCSI ou FC.

### Étape

Création d'un groupe de basculement :

```
network interface failover-groups create -vserver vs1 -failover-group failover_group_name -targets ports_list
```

- `vs1` Est le nom du SVM pouvant utiliser le failover group.
- `failover_group_name` est le nom du groupe de basculement que vous souhaitez créer.
- `ports_list` est la liste des ports qui seront ajoutés au failover group.  
Les ports sont ajoutés au format `node_name>:port_number`, par exemple, `node1:e0c`.

La commande suivante crée le failover group fg3 pour SVM vs3 et ajoute deux ports :

```
network interface failover-groups create -vserver vs3 -failover-group fg3 -targets cluster1-01:e0e,cluster1-02:e0e
```

### Une fois que vous avez terminé

- Vous devez appliquer le groupe de basculement à une LIF maintenant que le groupe de basculement a été

créé.

- L'application d'un groupe de basculement qui ne fournit pas de cible de basculement valide pour une LIF entraîne un message d'avertissement.

Si une LIF ne disposant pas de tentatives de basculement cible valides, une panne peut se produire.

## Configurer les paramètres de basculement sur une LIF

Vous pouvez configurer une LIF afin de basculer vers un groupe spécifique de ports réseau en appliquant une politique de basculement et un failover group à la LIF. Vous pouvez également désactiver le basculement d'une LIF vers un autre port.

### Description de la tâche

- Lors de la création d'une LIF, le basculement LIF est activé par défaut et la liste des ports cibles disponibles est déterminée par le groupe de basculement par défaut et la règle de basculement basée sur le type et la stratégie de service LIF.

Depuis 9.5, vous pouvez spécifier une policy de services pour le LIF qui définit les services réseau pouvant utiliser le LIF. Certains services réseau imposent des restrictions de basculement sur une LIF.



Si la politique de service d'une LIF est modifiée de façon à limiter davantage le basculement, la politique de basculement de la LIF est automatiquement mise à jour par le système.

- Vous pouvez modifier le comportement de basculement des LIFs en spécifiant des valeurs des paramètres `-failover-group` et `-failover-policy` dans la commande `network interface modify`.
- La modification d'une LIF entraînant l'absence de cible de basculement valide entraîne un message d'avertissement.

Si une LIF ne disposant pas de tentatives de basculement cible valides, une panne peut se produire.

- À partir de ONTAP 9.11.1, sur les plateformes de baie SAN 100 % Flash (ASA), le basculement de LIF iSCSI est automatiquement activé sur les LIF iSCSI nouvellement créées sur les machines virtuelles de stockage nouvellement créées.

En outre, c'est possible "[Activez manuellement le basculement de LIF iSCSI sur des LIF iSCSI préexistantes](#)", C'est-à-dire les LIF créées avant la mise à niveau vers ONTAP 9.11.1 ou version ultérieure.

- La liste suivante décrit la manière dont le paramètre `-failover-policy` affecte les ports cibles sélectionnés dans le failover group :



Pour le basculement LIF iSCSI, seules les règles de basculement `local-only`, `sfo-partner-only` et `disabled` sont pris en charge.

- `broadcast-domain-wide` S'applique à tous les ports de tous les nœuds du failover group.
- `system-defined` S'applique uniquement aux ports du nœud de rattachement de la LIF et à un autre nœud du cluster, généralement un partenaire non- SFO, le cas échéant.
- `local-only` S'applique uniquement aux ports du nœud de rattachement du LIF.
- `sfo-partner-only` S'applique uniquement aux ports du nœud de rattachement du LIF et à son

partenaire SFO.

- disabled Indique que le LIF n'est pas configuré pour le basculement.

Étapes

Configurez les paramètres de basculement pour une interface existante :

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

Exemples de configuration des paramètres de basculement et de désactivation du basculement

La commande suivante définit la règle de basculement sur broadcast-domain-large et utilise les ports du failover group fg3 comme cibles de basculement pour LIF data1 sur SVM vs3 :

```
network interface modify -vserver vs3 -lif data1 -failover-policy
broadcast-domain-wide -failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif failover-policy failover-group

vs3 data1 broadcast-domain-wide fg3
```

La commande suivante désactive le basculement pour LIF data1 sur le SVM vs3 :

```
network interface modify -vserver vs3 -lif data1 -failover-policy disabled
```

Commandes permettant de gérer les groupes et les règles de basculement

Vous pouvez utiliser le network interface failover-groups commandes permettant de gérer les groupes de basculement. Vous utilisez le network interface modify Commande permettant de gérer les groupes de basculement et les règles de basculement appliquées à une LIF.

| Les fonctions que vous recherchez...                 | Utilisez cette commande...                       |
|------------------------------------------------------|--------------------------------------------------|
| Ajout de ports réseau à un groupe de basculement     | network interface failover-groups add-targets    |
| Supprime les ports réseau d'un groupe de basculement | network interface failover-groups remove-targets |

|                                                                             |                                                                             |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Modifier les ports réseau d'un failover group                               | <code>network interface failover-groups modify</code>                       |
| Afficher les groupes de basculement actuels                                 | <code>network interface failover-groups show</code>                         |
| Configurer le basculement sur un LIF                                        | <code>network interface modify -failover -group -failover-policy</code>     |
| Afficher le failover group et la policy de failover utilisés par chaque LIF | <code>network interface show -fields failover-group, failover-policy</code> |
| Renommer un groupe de basculement                                           | <code>network interface failover-groups rename</code>                       |
| Supprime un groupe de basculement                                           | <code>network interface failover-groups delete</code>                       |



La modification d'un groupe de basculement de manière à ce qu'il n'assure pas une cible de basculement valide pour une LIF du cluster peut entraîner une panne lorsqu'une LIF tente de basculer.

Pour plus d'informations, consultez les pages de manuel du `network interface failover-groups` et `network interface modify` commandes.

## Sous-réseaux (administrateurs du cluster uniquement)

### Présentation du sous-réseau

Les sous-réseaux vous permettent d'allouer des blocs spécifiques, ou des pools, d'adresses IP pour votre configuration réseau ONTAP. Cela vous permet de créer plus facilement les LIF en spécifiant un nom de sous-réseau au lieu de spécifier l'adresse IP et les valeurs du masque réseau.

Un sous-réseau est créé au sein d'un domaine de diffusion et contient un pool d'adresses IP appartenant au même sous-réseau de couche 3. Les adresses IP d'un sous-réseau sont allouées aux ports dans le domaine de broadcast lorsque les LIFs sont créées. Lorsque les LIF sont supprimées, les adresses IP sont renvoyées au pool de sous-réseau et sont disponibles pour les futures LIF.

Il est recommandé d'utiliser les sous-réseaux, car ils facilitent considérablement la gestion des adresses IP et facilitent la création des LIF. En outre, si vous spécifiez une passerelle lors de la définition d'un sous-réseau, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau.

### Créez un sous-réseau

Vous pouvez créer un sous-réseau pour allouer des blocs spécifiques d'adresses IPv4 ou IPv6 à utiliser ultérieurement lors de la création de LIF pour la SVM.

Cela vous permet de créer plus facilement les LIF en spécifiant un nom de sous-réseau au lieu de spécifier une adresse IP et des valeurs de masque réseau pour chaque LIF.

### **Avant de commencer**

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Le broadcast domain et IPspace où vous prévoyez d'ajouter le sous-réseau doivent déjà exister.

### **Description de la tâche**

- Tous les noms de sous-réseau doivent être uniques au sein d'un IPspace.
- Lorsque vous ajoutez des plages d'adresses IP à un sous-réseau, vous devez vous assurer qu'il n'y a pas d'adresses IP redondantes dans le réseau de sorte que différents sous-réseaux ou hôtes ne tentent pas d'utiliser la même adresse IP.
- Si vous spécifiez une passerelle lors de la définition d'un sous-réseau, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau. Si vous n'utilisez pas de sous-réseaux ou si vous n'indiquez pas de passerelle lors de la définition d'un sous-réseau, vous devez utiliser le `route create` Commande pour ajouter manuellement une route au SVM.

### **Procédure**

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## System Manager

Depuis ONTAP 9.12.0, vous pouvez utiliser System Manager pour créer un sous-réseau.

### Étapes

1. Sélectionnez **réseau > Présentation > sous-réseaux**.
2. Cliquez sur **+ Add** pour créer un sous-réseau.
3. Nommez le sous-réseau.
4. Spécifiez l'adresse IP du sous-réseau.
5. Définissez le masque de sous-réseau.
6. Définissez la plage d'adresses IP qui comprend le sous-réseau.
7. Si utile, spécifiez une passerelle.
8. Sélectionnez le domaine de diffusion auquel appartient le sous-réseau.
9. Enregistrez les modifications.
  - a. Si l'adresse IP ou la plage saisie est déjà utilisée par une interface, le message suivant s'affiche :  
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
  - b. Lorsque vous cliquez sur **OK**, la LIF existante est associée au sous-réseau.

### CLI

Pour créer un sous-réseau, utilisez l'interface de ligne de commandes.

```
network subnet create -subnet-name subnet_name -broadcast-domain
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet
<subnet_address> [-gateway <gateway_address>] [-ip-ranges
<ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` est le nom du sous-réseau de couche 3 que vous souhaitez créer.

Le nom peut être une chaîne de texte comme "Mgmt" ou une valeur IP de sous-réseau spécifique comme 192.0.2.0/24.

- `broadcast_domain_name` est le nom du domaine de diffusion sur lequel le sous-réseau sera stocké.
- `ipspace_name` Est le nom de l'IPspace auquel le broadcast domain appartient.

L'IPspace par défaut est utilisé sauf si vous spécifiez une valeur pour cette option.

- `subnet_address` Est l'adresse IP et le masque du sous-réseau ; par exemple, 192.0.2.0/24.
- `gateway_address` est la passerelle pour la route par défaut du sous-réseau ; par exemple, 192.0.2.1.
- `ip_address_list` Est la liste, ou plage, des adresses IP qui seront allouées au sous-réseau.

Les adresses IP peuvent être des adresses individuelles, une plage d'adresses IP ou une combinaison dans une liste séparée par des virgules.



- La valeur `true` peut être réglé pour le `-force-update-lif-associations` option.

Cette commande échoue si un processeur de service ou une interface réseau utilisent actuellement les adresses IP de la plage spécifiée. Si cette valeur est définie sur `true`, elle associe toutes les interfaces adressées manuellement avec le sous-réseau actuel et permet à la commande de réussir.

La commande suivante crée le sous-réseau `sub1` dans broadcast domain `Default-1` dans l'IPspace par défaut. Il ajoute une adresse IP et un masque de sous-réseau IPv4, la passerelle et une plage d'adresses IP :

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

La commande suivante crée le sous-réseau `sub2` dans broadcast domain `Default` dans le « IPspace par défaut ». Il ajoute une plage d'adresses IPv6 :

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

### Une fois que vous avez terminé

Vous pouvez attribuer des SVM et des interfaces à un IPspace en utilisant les adresses dans le sous-réseau.

Si vous devez modifier le nom d'un sous-réseau existant, utilisez le `network subnet rename` commande.

## Ajoutez ou supprimez des adresses IP d'un sous-réseau


Vous pouvez ajouter des adresses IP lors de la création initiale d'un sous-réseau ou ajouter des adresses IP à un sous-réseau existant déjà. Vous pouvez également supprimer les adresses IP d'un sous-réseau existant. Cela vous permet d'allouer uniquement les adresses IP requises pour les SVM.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

### System Manager

À partir de ONTAP 9.12.0, vous pouvez utiliser System Manager pour ajouter ou supprimer des adresses IP vers ou depuis un sous-réseau

#### Étapes

1. Sélectionnez **réseau > Présentation > sous-réseaux**.
2. Sélectionnez  > **Modifier** en regard du sous-réseau à modifier.
3. Ajoutez ou supprimez des adresses IP.
4. Enregistrez les modifications.
  - a. Si l'adresse IP ou la plage saisie est déjà utilisée par une interface, le message suivant s'affiche :  
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
  - b. Lorsque vous cliquez sur **OK**, la LIF existante est associée au sous-réseau.

#### CLI

Utilisez l'interface de ligne de commande pour ajouter ou supprimer des adresses IP vers ou depuis un sous-réseau

#### Description de la tâche

Lors de l'ajout d'adresses IP, une erreur se produit si un processeur de service ou une interface réseau utilise les adresses IP de la plage ajoutée. Si vous souhaitez associer des interfaces adressées manuellement au sous-réseau actuel, vous pouvez définir le `-force-update-lif-associations` option à `true`.

Lors de la suppression d'adresses IP, une erreur s'affiche si un processeur de service ou une interface réseau utilise les adresses IP en cours de suppression. Si vous souhaitez que les interfaces continuent à utiliser les adresses IP après leur suppression du sous-réseau, vous pouvez définir le `-force-update-lif-associations` option à `true`.

#### Étape

Ajout ou suppression d'adresses IP d'un sous-réseau :

| Les fonctions que vous recherchez...       | Utilisez cette commande...           |
|--------------------------------------------|--------------------------------------|
| Ajoutez des adresses IP à un sous-réseau   | plages d'extension de sous-réseau    |
| Supprimez les adresses IP d'un sous-réseau | plages de suppression du sous-réseau |

Pour plus d'informations sur ces commandes, consultez les pages de manuels.

La commande suivante ajoute les adresses IP 192.0.2.82 à 192.0.2.85 au sous-réseau 1 :

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-192.0.2.85>
```

La commande suivante supprime l'adresse IP 198.51.100.9 du sous-réseau 3 :

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges <198.51.100.9>
```

Si la plage actuelle comprend 1 à 10 et 20 à 40 et que vous voulez ajouter 11 à 19 et 41 à 50 (en autorisant 1 à 50), vous pouvez chevaucher la plage d'adresses existante à l'aide de la commande suivante. Cette commande ajoute uniquement les nouvelles adresses, sans affecter les adresses existantes :

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-198.51.10.50>
```

## Modifiez les propriétés du sous-réseau

Vous pouvez modifier l'adresse de sous-réseau et la valeur de masque, l'adresse de passerelle ou la plage d'adresses IP dans un sous-réseau existant.

### Description de la tâche

- Lors de la modification des adresses IP, vous devez vous assurer qu'il n'y a pas d'adresses IP qui se chevauchent dans le réseau de sorte que les différents sous-réseaux ou hôtes ne tentent pas d'utiliser la même adresse IP.
- Si vous ajoutez ou modifiez l'adresse IP de la passerelle, la passerelle modifiée s'applique aux nouveaux SVM lorsqu'une LIF est créée en utilisant le sous-réseau. Une route par défaut vers la passerelle est créée pour le SVM si cette route n'existe pas déjà. Vous pouvez avoir à ajouter manuellement une nouvelle route à la SVM lorsque vous modifiez l'adresse IP de la passerelle.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## System Manager

À partir de ONTAP 9.12.0, vous pouvez utiliser System Manager pour modifier les propriétés du sous-réseau

### Étapes

1. Sélectionnez **réseau > Présentation > sous-réseaux**.
2. Sélectionnez **Modifier** en regard du sous-réseau à modifier.
3. Apportez les modifications nécessaires.
4. Enregistrez les modifications.
  - a. Si l'adresse IP ou la plage saisie est déjà utilisée par une interface, le message suivant s'affiche :  
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
  - b. Lorsque vous cliquez sur **OK**, la LIF existante est associée au sous-réseau.

### CLI

Utilisez l'interface de ligne de commande pour modifier les propriétés du sous-réseau

### Étape

Modifier les propriétés du sous-réseau :

```
network subnet modify -subnet-name <subnet_name> [-ipSPACE
<ipSPACE_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` est le nom du sous-réseau à modifier.
- `ipSPACE` Est le nom de l'IPspace où réside le sous-réseau.
- `subnet` est la nouvelle adresse et le nouveau masque du sous-réseau, le cas échéant ; par exemple, 192.0.2.0/24.
- `gateway` est la nouvelle passerelle du sous-réseau, le cas échéant ; par exemple, 192.0.2.1. La saisie "" supprime l'entrée de passerelle.
- `ip_ranges` Nouvelle liste ou plage d'adresses IP qui seront allouées au sous-réseau, le cas échéant. Les adresses IP peuvent être des adresses individuelles, une plage ou des adresses IP, ou une combinaison dans une liste séparée par des virgules. La plage spécifiée ici remplace les adresses IP existantes.
- `force-update-lif-associations` Est requis lorsque vous modifiez la plage d'adresses IP. Vous pouvez définir la valeur **true** pour cette option lors de la modification de la plage d'adresses IP. Cette commande échoue si un processeur de service ou une interface réseau utilisent les adresses IP de la plage spécifiée. La définition de cette valeur sur **true** associe toutes les interfaces adressées manuellement avec le sous-réseau actuel et permet à la commande de réussir.

La commande suivante modifie l'adresse IP de la passerelle du sous-réseau 3 :

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

## Afficher les sous-réseaux

Vous pouvez afficher la liste des adresses IP allouées à chaque sous-réseau au sein d'un IPspace. Le résultat indique également le nombre total d'adresses IP disponibles dans chaque sous-réseau, ainsi que le nombre d'adresses actuellement utilisées.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

### System Manager

À partir de ONTAP 9.12.0, vous pouvez utiliser System Manager pour afficher les sous-réseaux

#### Étapes

- 1. Sélectionnez **réseau > Présentation > sous-réseaux**.
- 2. Afficher la liste des sous-réseaux.

### CLI

Utilisez l'interface de ligne de commande pour afficher les sous-réseaux

#### Étape

Afficher la liste des sous-réseaux et les plages d'adresses IP associées utilisés dans ces sous-réseaux :

```
network subnet show
```

La commande suivante affiche les sous-réseaux et les propriétés du sous-réseau :

```
network subnet show

IPspace: Default
Subnet
Name Subnet Broadcast
----- -
sub1 192.0.2.0/24 bcast1
192.0.2.100
sub3 198.51.100.0/24 bcast3
198.51.100.7,198.51.100.9
Gateway

192.0.2.1
198.51.100.1
Avail/
Total
5/9
3/3
Ranges
192.0.2.92-
```

## Supprimez un sous-réseau

Si vous n'avez plus besoin d'un sous-réseau et que vous souhaitez désaffecter les adresses IP qui ont été attribuées au sous-réseau, vous pouvez le supprimer.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## System Manager

À partir de ONTAP 9.12.0, vous pouvez utiliser System Manager pour supprimer un sous-réseau

### Étapes

1. Sélectionnez **réseau > Présentation > sous-réseaux**.
2. Sélectionnez **⋮ > Supprimer** en regard du sous-réseau à supprimer.
3. Enregistrez les modifications.

### CLI

Utilisez l'interface de ligne de commande pour supprimer un sous-réseau

#### Description de la tâche

Vous recevrez une erreur si un processeur de service ou une interface réseau utilise actuellement des adresses IP dans les plages spécifiées. Si vous souhaitez que les interfaces continuent à utiliser les adresses IP, même après la suppression du sous-réseau, vous pouvez définir l'option `-force-update-lif-associations` à `true` afin de supprimer l'association du sous-réseau avec les LIF.

#### Étape

Supprimer un sous-réseau :

```
network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-force-update-lif-associations true]
```

La commande suivante supprime le sous-réseau sub1 dans IPspace ipspace1 :

```
network subnet delete -subnet-name sub1 -ipspace ipspace1
```

## Créer des SVM

Vous devez créer un SVM afin de fournir des données aux clients.

### Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez savoir quel style de sécurité le volume root du SVM sera mis en place.

Si vous prévoyez d'implémenter une solution Hyper-V ou SQL Server over SMB sur ce SVM, vous devez utiliser le style de sécurité NTFS pour le volume root. Au moment de leur création, les volumes contenant des fichiers Hyper-V ou des fichiers de base de données SQL doivent être définis sur la sécurité NTFS. En définissant le style de sécurité du volume racine sur NTFS, vous assurez que vous ne créez pas de volumes de données UNIX ou de type sécurité mixte par inadvertance.

- À partir de la version ONTAP 9.13.1, vous pouvez définir une capacité maximale pour une machine virtuelle de stockage. Vous pouvez également configurer des alertes lorsque la SVM approche un niveau de capacité seuil. Pour plus d'informations, voir [Gestion de la capacité des SVM](#).

## System Manager

Vous pouvez utiliser System Manager pour créer une machine virtuelle de stockage.

### Étapes

1. Sélectionnez **machines virtuelles de stockage**.
2. Cliquez **+ Add** pour créer une VM de stockage.
3. Nommez la VM de stockage.
4. Sélectionnez le protocole d'accès :
  - SMB/CIFS, NFS
  - iSCSI
  - FC
  - NVMe
  - i. Si vous sélectionnez **Activer SMB/CIFS**, effectuez la configuration suivante :

| Champ ou case à cocher                                                                 | Description                                                                                                                                                                       |
|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nom de l'administrateur                                                                | Préciser le nom d'utilisateur administrateur pour la VM de stockage SMB/CIFS.                                                                                                     |
| Mot de passe                                                                           | Préciser le mot de passe administrateur pour la VM de stockage SMB/CIFS.                                                                                                          |
| Nom du serveur                                                                         | Spécifier le nom du serveur pour la VM de stockage SMB/CIFS                                                                                                                       |
| Domaine Active Directory                                                               | Spécifiez le domaine Active Directory pour fournir l'authentification utilisateur pour la machine virtuelle de stockage SMB/CIFS.                                                 |
| Unité organisationnelle                                                                | Spécifiez l'unité organisationnelle dans le domaine Active Directory associé au serveur SMB/CIFS. « CN=calculateurs » est la valeur par défaut, qui peut être modifiée.           |
| Cryptage des données tout en accédant aux partages de la machine virtuelle de stockage | Cochez cette case pour chiffrer les données à l'aide de SMB 3.0 pour empêcher tout accès non autorisé aux fichiers sur les partages de la machine virtuelle de stockage SMB/CIFS. |
| Domaines                                                                               | Ajoutez, supprimez ou réorganisez les domaines répertoriés pour la machine virtuelle de stockage SMB/CIFS.                                                                        |
| Serveurs de noms                                                                       | Ajoutez, supprimez ou réorganisez les serveurs de noms pour la machine virtuelle de stockage SMB/CIFS.                                                                            |

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Langue par défaut                | Spécifie le paramètre de codage de langue par défaut pour la VM de stockage et ses volumes. Utilisez l'interface de ligne de commandes pour modifier les paramètres des volumes individuels d'une machine virtuelle de stockage.                                                                                                                                                                                                                                                                                                                                                                       |
| Interface réseau                 | <p>Pour chaque interface réseau configurée pour la machine virtuelle de stockage, sélectionnez un sous-réseau existant (s'il existe au moins un sous-réseau) ou spécifiez <b>sans sous-réseau</b> et renseignez les champs <b>adresse IP</b> et <b>masque de sous-réseau</b>.</p> <p>Si utile, cochez la case <b>utiliser le même masque de sous-réseau et la même passerelle pour toutes les interfaces</b> suivantes.</p> <p>Vous pouvez permettre au système de sélectionner automatiquement le port d'accueil ou de sélectionner manuellement celui que vous souhaitez utiliser dans la liste.</p> |
| Gérer le compte d'administrateur | Cochez cette case pour gérer le compte d'administrateur de la machine virtuelle de stockage. Lorsque cette option est sélectionnée, spécifiez le nom d'utilisateur, le mot de passe, confirmez le mot de passe et indiquez si vous souhaitez ajouter une interface réseau pour la gestion des machines virtuelles de stockage.                                                                                                                                                                                                                                                                         |

1. Si vous sélectionnez **Activer NFS**, effectuez la configuration suivante :

| Champ ou case à cocher                      | Description                                                                                                                                                                                                                                                 |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cochez la case Autoriser l'accès client NFS | Cochez cette case si tous les volumes créés sur la VM de stockage NFS doivent utiliser le chemin du volume racine «/ » pour monter et parcourir. Ajoutez des règles à la stratégie d'export « default » pour permettre un parcours de montage ininterrompu. |



|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Règles            | <p>Cliquez <b>+ Add</b> pour créer des règles.</p> <ul style="list-style-type: none"> <li>• Spécification client : spécifiez les noms d'hôte, les adresses IP, les groupes réseau ou les domaines.</li> <li>• Protocoles d'accès : sélectionnez une combinaison des options suivantes : <ul style="list-style-type: none"> <li>◦ SMB/CIFS</li> <li>◦ FlexCache</li> <li>◦ NFS <ul style="list-style-type: none"> <li>▪ NFSv3</li> <li>▪ NFSv4</li> </ul> </li> </ul> </li> <li>• Détails d'accès : pour chaque type d'utilisateur, spécifiez le niveau d'accès, soit en lecture seule, en lecture/écriture ou superutilisateur. Les types d'utilisateur sont les suivants : <ul style="list-style-type: none"> <li>◦ Tout</li> <li>◦ Tous (en tant qu'utilisateur anonyme)</li> <li>◦ UNIX</li> <li>◦ Kerberos 5</li> <li>◦ Kerberos 5i</li> <li>◦ Kerberos 5p</li> <li>◦ NTLM</li> </ul> </li> </ul> <p>Enregistrez la règle.</p> |
| Langue par défaut | <p>Spécifie le paramètre de codage de langue par défaut pour la VM de stockage et ses volumes. Utilisez l'interface de ligne de commandes pour modifier les paramètres des volumes individuels d'une machine virtuelle de stockage.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Interface réseau  | <p>Pour chaque interface réseau configurée pour la machine virtuelle de stockage, sélectionnez un sous-réseau existant (s'il existe au moins un sous-réseau) ou spécifiez <b>sans sous-réseau</b> et renseignez les champs <b>adresse IP</b> et <b>masque de sous-réseau</b>.</p> <p>Si utile, cochez la case <b>utiliser le même masque de sous-réseau et la même passerelle pour toutes les interfaces</b> suivantes.</p> <p>Vous pouvez permettre au système de sélectionner automatiquement le port d'accueil ou de sélectionner manuellement celui que vous souhaitez utiliser dans la liste.</p>                                                                                                                                                                                                                                                                                                                             |

|                                  |                                                                                                                                                                                                                                                                                                                                |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gérer le compte d'administrateur | Cochez cette case pour gérer le compte d'administrateur de la machine virtuelle de stockage. Lorsque cette option est sélectionnée, spécifiez le nom d'utilisateur, le mot de passe, confirmez le mot de passe et indiquez si vous souhaitez ajouter une interface réseau pour la gestion des machines virtuelles de stockage. |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

1. Si vous sélectionnez **Activer iSCSI**, effectuez la configuration suivante :

| Champ ou case à cocher           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface réseau                 | <p>Pour chaque interface réseau configurée pour la machine virtuelle de stockage, sélectionnez un sous-réseau existant (s'il existe au moins un sous-réseau) ou spécifiez <b>sans sous-réseau</b> et renseignez les champs <b>adresse IP</b> et <b>masque de sous-réseau</b>.</p> <p>Si utile, cochez la case <b>utiliser le même masque de sous-réseau et la même passerelle pour toutes les interfaces</b> suivantes.</p> <p>Vous pouvez permettre au système de sélectionner automatiquement le port d'accueil ou de sélectionner manuellement celui que vous souhaitez utiliser dans la liste.</p> |
| Gérer le compte d'administrateur | Cochez cette case pour gérer le compte d'administrateur de la machine virtuelle de stockage. Lorsque cette option est sélectionnée, spécifiez le nom d'utilisateur, le mot de passe, confirmez le mot de passe et indiquez si vous souhaitez ajouter une interface réseau pour la gestion des machines virtuelles de stockage.                                                                                                                                                                                                                                                                         |

1. Si vous sélectionnez **Activer FC**, effectuez la configuration suivante :

| Champ ou case à cocher           | Description                                                                                                                                                                                                                                                                                                                    |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configurez les ports FC          | Sélectionnez les interfaces réseau sur les nœuds que vous souhaitez inclure dans la VM de stockage. Deux interfaces réseau par nœud sont recommandées.                                                                                                                                                                         |
| Gérer le compte d'administrateur | Cochez cette case pour gérer le compte d'administrateur de la machine virtuelle de stockage. Lorsque cette option est sélectionnée, spécifiez le nom d'utilisateur, le mot de passe, confirmez le mot de passe et indiquez si vous souhaitez ajouter une interface réseau pour la gestion des machines virtuelles de stockage. |

1. Si vous sélectionnez **Activer NVMe/FC**, effectuez la configuration suivante :

| Champ ou case à cocher           | Description                                                                                                                                                                                                                                                                                                                    |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configurez les ports FC          | Sélectionnez les interfaces réseau sur les nœuds que vous souhaitez inclure dans la VM de stockage. Deux interfaces réseau par nœud sont recommandées.                                                                                                                                                                         |
| Gérer le compte d'administrateur | Cochez cette case pour gérer le compte d'administrateur de la machine virtuelle de stockage. Lorsque cette option est sélectionnée, spécifiez le nom d'utilisateur, le mot de passe, confirmez le mot de passe et indiquez si vous souhaitez ajouter une interface réseau pour la gestion des machines virtuelles de stockage. |

1. Si vous sélectionnez **Activer NVMe/TCP**, effectuez la configuration suivante :

| Champ ou case à cocher           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface réseau                 | <p>Pour chaque interface réseau configurée pour la machine virtuelle de stockage, sélectionnez un sous-réseau existant (s'il existe au moins un sous-réseau) ou spécifiez <b>sans sous-réseau</b> et renseignez les champs <b>adresse IP</b> et <b>masque de sous-réseau</b>.</p> <p>Si utile, cochez la case <b>utiliser le même masque de sous-réseau et la même passerelle pour toutes les interfaces</b> suivantes.</p> <p>Vous pouvez permettre au système de sélectionner automatiquement le port d'accueil ou de sélectionner manuellement celui que vous souhaitez utiliser dans la liste.</p> |
| Gérer le compte d'administrateur | Cochez cette case pour gérer le compte d'administrateur de la machine virtuelle de stockage. Lorsque cette option est sélectionnée, spécifiez le nom d'utilisateur, le mot de passe, confirmez le mot de passe et indiquez si vous souhaitez ajouter une interface réseau pour la gestion des machines virtuelles de stockage.                                                                                                                                                                                                                                                                         |

1. Enregistrez les modifications.

## CLI

Pour créer un sous-réseau, utilisez l'interface de ligne de commandes de ONTAP.

## Étapes

1. Déterminer les agrégats candidats à l'ajout du volume root du SVM.

```
storage aggregate show -has-mroot false
```

Vous devez choisir un agrégat qui dispose d'au moins 1 Go d'espace libre pour contenir le volume root. Si vous prévoyez de configurer l'audit NAS sur le SVM, vous devez disposer d'au moins 3 Go d'espace libre supplémentaire sur l'agrégat racine, l'espace supplémentaire étant utilisé pour créer le volume d'activation de l'audit lorsque l'audit est activé.



Si l'audit NAS est déjà activé sur un SVM existant, le volume intermédiaire de l'agrégat est créé immédiatement après la fin de la création de l'agrégat.

2. Noter le nom de l'agrégat sur lequel vous souhaitez créer le volume root du SVM.
3. Si vous prévoyez de spécifier une langue lors de la création du SVM et ne connaissez pas la valeur à utiliser, identifier et enregistrer la valeur du langage que vous souhaitez spécifier :

```
vserver create -language ?
```

4. Si vous prévoyez de spécifier une politique Snapshot lors de la création de la SVM et ne connaissez pas le nom de la politique, indiquez les règles disponibles et identifiez et enregistrez le nom de la règle Snapshot que vous souhaitez utiliser :

```
volume snapshot policy show -vserver vserver_name
```

5. Si vous prévoyez de spécifier une politique de quotas lors de la création de la SVM et ne connaissez pas le nom de la politique, lister les politiques disponibles et identifier et enregistrer le nom de la politique de quotas que vous souhaitez utiliser :

```
volume quota policy show -vserver vserver_name
```

6. Création d'un SVM :

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace
IPspace_name] [-language <language>] [-snapshot-policy
snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
```

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
-rootvolume-security-style ntfs -ipspace ipspacel -language
en_US.UTF-8
```

```
[Job 72] Job succeeded: Vserver creation completed
```

7. Vérifier que la configuration des SVM est correcte.

```
vserver show -vserver vs1
```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

Dans cet exemple, la commande crée le SVM nommé « vs1 » dans l'IPspace « ipspace1 ». Le volume racine est nommé « vs1\_root » et est créé sur aggr3 avec le style de sécurité NTFS.



À partir de la ONTAP 9.13.1, vous pouvez définir un modèle de groupe de règles de QoS adaptative, en appliquant une limite plafond et un seuil de débit aux volumes du SVM. Vous ne pouvez appliquer cette politique qu'après avoir créé la SVM. Pour en savoir plus sur ce processus, voir [Définissez un modèle de groupe de règles adaptatives](#).

## Interfaces logiques

### Présentation de la LIF

#### Configurer la présentation des LIFs

Une LIF (Logical interface) représente un point d'accès réseau à un nœud du cluster. Vous pouvez configurer les LIF sur les ports sur lesquels le cluster envoie et reçoit des communications sur le réseau.

Un administrateur de cluster peut créer, afficher, modifier, migrer, restaurer, ou supprimer les LIFs. Un administrateur SVM ne peut afficher que les LIFs associées à la SVM.

Une LIF est une adresse IP ou un WWPN qui présente des caractéristiques associées, telles qu'une politique de service, un port d'accueil, un nœud de rattachement, une liste de ports à basculer et une politique de pare-feu. Vous pouvez configurer les LIF sur les ports sur lesquels le cluster envoie et reçoit des communications sur le réseau.



Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir ["Configuration des politiques de pare-feu pour les LIF"](#).

Les LIFs peuvent être hébergées sur les ports suivants :

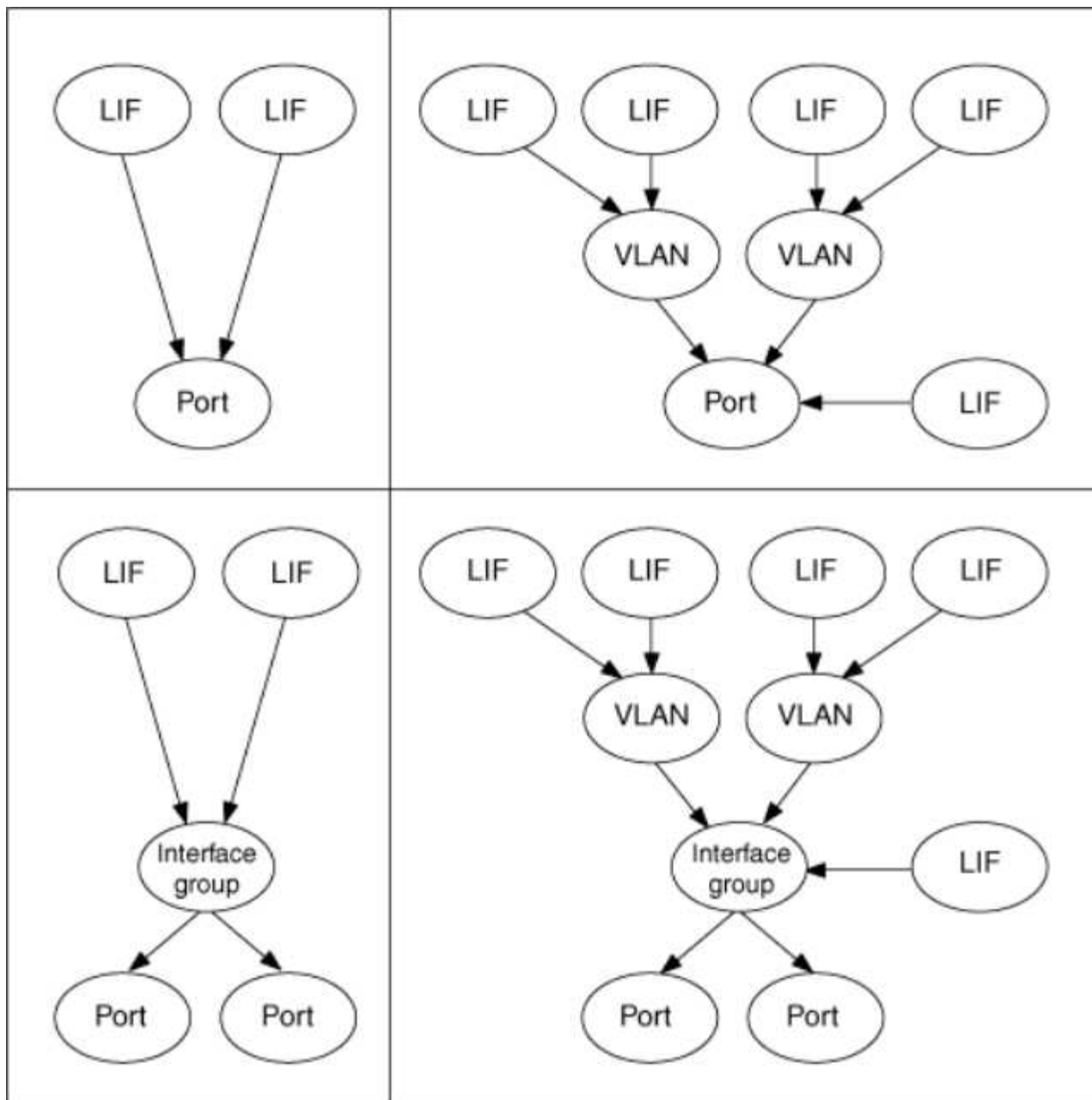
- Ports physiques ne faisant pas partie de groupes d'interfaces
- Groupes d'interface
- VLAN
- Ports physiques ou groupes d'interfaces qui hébergent des VLAN
- Ports VIP (Virtual IP)

Depuis ONTAP 9.5, les LIFs VIP sont prises en charge et hébergées sur des ports VIP.

Lors de la configuration des protocoles SAN tels que FC sur une LIF, ils seront associés à un WWPN.

["Administration SAN"](#)

La figure suivante illustre la hiérarchie de ports dans un système ONTAP :



### Basculement et rétablissement de LIF

Un basculement de LIF se produit lorsqu'une LIF se déplace de son nœud ou port de rattachement vers le nœud ou le port HA Partner. Un basculement de LIF peut être déclenché automatiquement par ONTAP ou manuellement par un administrateur du cluster pour certains événements, tels qu'un lien Ethernet physique en panne ou un nœud qui dévie du quorum de la base de données répliquée (RDB). Lorsqu'un basculement de LIF se produit, ONTAP continue son fonctionnement normal sur le nœud partenaire jusqu'à ce que la raison du basculement soit résolue. Lorsque le nœud ou le port de rattachement retrouve sa santé, la LIF est reconvertie du partenaire HA en nœud ou port de rattachement. Ce retour s'appelle un retour.

Pour le basculement et le rétablissement LIF, les ports de chaque nœud doivent appartenir au même broadcast domain. Pour vérifier que les ports appropriés de chaque nœud appartiennent au même broadcast domain, consultez les documents suivants :

- ONTAP 9.8 et versions ultérieures : ["Réparation de l'accessibilité de l'orifice"](#)
- ONTAP 9.7 et versions antérieures : ["Ajouter ou supprimer des ports d'un broadcast domain"](#)

Pour les LIF avec basculement LIF activé (automatiquement ou manuellement), les points suivants s'appliquent :

- Pour les LIF utilisant une policy de service de données, vous pouvez vérifier les restrictions de failover-policy :
  - ONTAP 9.6 et versions ultérieures : ["LIF et politiques de services dans ONTAP 9.6 et versions ultérieures"](#)
  - ONTAP 9.5 et versions antérieures : ["Rôles LIF dans ONTAP 9.5 et versions antérieures"](#)
- La restauration automatique des LIF se produit lorsque la restauration automatique est définie sur `true` Et lorsque le port de attache de la LIF est sain et peut héberger la LIF.
- En cas de basculement de nœud planifié ou non planifié, la LIF sur le nœud repris bascule vers le partenaire haute disponibilité. Le port sur lequel la LIF tombe en panne est déterminé par vif Manager.
- Une fois le basculement terminé, le LIF fonctionne normalement.
- Lorsqu'un rétablissement est initié, la LIF retourne à son nœud et port de rattachement, si la restauration automatique est définie sur `true`.
- Lorsqu'une liaison ethernet est indisponible sur un port hébergeant une ou plusieurs LIF, vif Manager migre les LIFs du port DOWN vers un autre port du même broadcast domain. Le nouveau port peut se trouver sur le même nœud ou sur son partenaire HA. Une fois la liaison restaurée et si la restauration automatique est définie sur `true`, Le vif Manager restaure les LIF sur leur nœud de rattachement et leur port de rattachement.
- Lorsqu'un nœud quitte le quorum RDB (Replicated database), il migre les LIF du nœud de quorum vers son partenaire haute disponibilité. Une fois que le nœud revient au quorum et que la restauration automatique est définie sur `true`, Le vif Manager restaure les LIF sur leur nœud de rattachement et leur port de rattachement.

**Compatibilité de LIF avec les types de ports**

Les LIF peuvent présenter des caractéristiques différentes pour prendre en charge différents types de ports.



Lorsque les LIF intercluster et de gestion sont configurées dans le même sous-réseau, le trafic de gestion peut être bloqué par un pare-feu externe et les connexions AutoSupport et NTP peuvent tomber en panne. Vous pouvez restaurer le système en exécutant le `network interface modify -vserver vservice name -lif intercluster LIF -status -admin up|down` Commande pour basculer le LIF intercluster. Cependant, vous devez définir la LIF intercluster et la LIF de gestion dans différents sous-réseaux pour éviter ce problème.

| LIF            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LIF de données | <p>LIF associée à un SVM (Storage Virtual machine) et servant à la communication avec les clients.</p> <p>Vous pouvez avoir plusieurs LIFs data sur un port. Ces interfaces peuvent migrer ou basculer sur l'ensemble du cluster. Vous pouvez modifier une LIF de données afin de servir de LIF de gestion SVM en modifiant sa politique de pare-feu en gestion.</p> <p>Les sessions établies aux serveurs NIS, LDAP, Active Directory, WINS, et DNS utilisent les LIFs data.</p> |



|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LIF Cluster              | <p>Une LIF utilisée pour acheminer le trafic intracluster entre les nœuds d'un cluster. Les LIFs cluster doivent toujours être créées sur les ports de type cluster.</p> <p>Les LIFs de cluster peuvent basculer entre les ports de cluster sur le même nœud, mais elles ne peuvent pas être migrées ou basculer vers un nœud distant. Lorsqu'un nouveau nœud rejoint un cluster, les adresses IP sont générées automatiquement. Toutefois, si vous souhaitez attribuer manuellement des adresses IP aux LIF de cluster, vous devez vous assurer que les nouvelles adresses IP se trouvent dans la même plage de sous-réseau que les LIF de cluster existantes.</p> |
| LIF Cluster-management   | <p>LIF qui offre une interface de gestion unique pour l'ensemble du cluster.</p> <p>Une LIF de cluster management peut basculer vers n'importe quel nœud du cluster. Il ne peut pas basculer vers le cluster ou les ports intercluster</p>                                                                                                                                                                                                                                                                                                                                                                                                                          |
| FRV InterCluster         | <p>LIF utilisée pour la communication, la sauvegarde et la réplication entre clusters. Vous devez créer une LIF intercluster sur chaque node du cluster avant qu'une relation de peering de cluster ne puisse être établie.</p> <p>Ces LIFs peuvent uniquement basculer sur les ports du même nœud. Ils ne peuvent pas être migrés ni basculés vers un autre nœud du cluster.</p>                                                                                                                                                                                                                                                                                   |
| FRV de gestion des nœuds | <p>Une LIF qui fournit une adresse IP dédiée pour gérer un nœud particulier dans un cluster. Les LIFs de node-management sont créées au moment de la création ou de l'arrivée du cluster. Ces LIFs sont utilisées pour la maintenance du système, par exemple lorsqu'un nœud devient inaccessible depuis le cluster.</p>                                                                                                                                                                                                                                                                                                                                            |
| LIF VIP                  | <p>Une LIF VIP est toute LIF de données créée sur un port VIP. Pour en savoir plus, voir <a href="#">"Configuration des LIF IP virtuelles (VIP)"</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## LIF et règles de service (ONTAP 9.6 et versions ultérieures)

Vous pouvez attribuer des politiques de service (au lieu de rôles LIF ou de politiques de pare-feu) aux LIF qui déterminent le type de trafic pris en charge pour les LIF. Les stratégies de service définissent une collection de services réseau prise en charge par une LIF. ONTAP fournit un ensemble de règles de service intégrées qui peuvent être associées à une LIF.

Vous pouvez afficher les stratégies de service et leurs détails à l'aide de la commande suivante :

```
network interface service-policy show
```

Les fonctionnalités qui ne sont pas liées à un service spécifique utiliseront un comportement défini par le système pour sélectionner les LIFs pour les connexions sortantes.

Les applications qui se trouvent sur une LIF avec une politique de service vide peuvent se comporter de manière inattendue.

### Règles de service pour les SVM système

Le SVM d'administration et tout SVM système contiennent des politiques de service qui peuvent être utilisées pour les LIF au sein de ce SVM, y compris les LIFs de type management et intercluster. Ces règles sont

automatiquement créées par le système lorsqu'un IPspace est créé.

Le tableau suivant répertorie les règles intégrées pour les LIF dans les SVM système à partir de ONTAP 9.12.1. Pour les autres versions, afficher les politiques de service et leurs détails à l'aide de la commande suivante :

```
network interface service-policy show
```

| Politique                      | Services inclus                                                                                                                                                                                                                                                 | Rôle équivalent                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| valeur-par-défaut intercluster | intercluster-core, management-https                                                                                                                                                                                                                             | intercluster                              | Utilisé par les LIFs transportant le trafic intercluster.<br>Attention : le service intercluster est disponible depuis le ONTAP 9.5 avec le nom net-intercluster service policy.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| annonce-route-par-défaut       | gestion-bgp                                                                                                                                                                                                                                                     | -                                         | Utilisé par les LIFs transportant des connexions homologues BGP<br>Remarque : disponible auprès de ONTAP 9.5 avec le nom net-route-annonce service policy.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| gestion par défaut             | management-core, management-https, management-http, management-ssh, management-autosupport, management-ems, management-dns-client, management-ad-client, management-ldap-client, management-nis-client, management-ntp-client, transfert-journalisation-gestion | nœuds de gestion et de gestion de cluster | Utilisez cette politique de gestion étendue du système pour créer des LIFs de gestion du type node-and-cluster détenues par un SVM système. Ces LIF peuvent être utilisées pour les connexions sortantes vers des serveurs DNS, AD, LDAP ou NIS, ainsi que pour prendre en charge des connexions supplémentaires pour prendre en charge les applications s'exécutant pour le compte de l'ensemble du système. À partir de ONTAP 9.12.1, vous pouvez utiliser le management-log-forwarding Service pour contrôler les LIFs utilisées pour transférer les journaux d'audit à un serveur syslog distant. |

Le tableau suivant répertorie les services que les LIFs peuvent utiliser sur un SVM système à partir de ONTAP 9.11.1 :

| Service           | Limites du basculement | Description                       |
|-------------------|------------------------|-----------------------------------|
| intercluster-core | home-node-uniquement   | Services intercluster de base     |
| cœur de gestion   | -                      | Services de gestion centrale      |
| management-ssh    | -                      | Services d'accès à la gestion SSH |

|                                  |                           |                                                                                    |
|----------------------------------|---------------------------|------------------------------------------------------------------------------------|
| gestion-http                     | -                         | Services de gestion de l'accès HTTP                                                |
| gestion-https                    | -                         | Services pour l'accès à la gestion HTTPS                                           |
| gestion-autosupport              | -                         | Services liés à l'imputation de charges utiles AutoSupport                         |
| gestion-bgp                      | port d'origine uniquement | Services liés aux interactions BGP par les pairs                                   |
| backup-ndmp-control              | -                         | Services pour les commandes de sauvegarde NDMP                                     |
| gestion-ems                      | -                         | Services d'accès à la messagerie de gestion                                        |
| client-ntp-management            | -                         | Introduit dans ONTAP 9.10.1.<br>Services pour l'accès client NTP.                  |
| serveur-ntp-management           | -                         | Introduit dans ONTAP 9.10.1.<br>Services pour l'accès à la gestion de serveurs NTP |
| management-portmap               | -                         | Services de gestion de portmap                                                     |
| serveur-rsh de gestion           | -                         | Services de gestion de serveur rsh                                                 |
| serveur-gestion-snmp             | -                         | Services de gestion de serveur SNMP                                                |
| serveur-telnet-gestion           | -                         | Services de gestion de serveur telnet                                              |
| transfert de journaux de gestion | -                         | Introduit dans ONTAP 9.12.1.<br>Services de transfert de journaux d'audit          |

### Règles de service pour les SVM de données

Tous les SVM de données contiennent des règles de service qui peuvent être utilisées par les LIF de ce SVM.

Le tableau suivant répertorie les règles intégrées pour les LIF dans des SVM de données à partir de ONTAP 9.11.1. Pour les autres versions, afficher les politiques de service et leurs détails à l'aide de la commande suivante :

```
network interface service-policy show
```

| Politique | Services inclus | Protocole de données équivalent | Description |
|-----------|-----------------|---------------------------------|-------------|
|-----------|-----------------|---------------------------------|-------------|

|                             |                                                                                                                                                          |                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| gestion par défaut          | management-https, management-http, management-ssh, management-dns-client, management-ad-client, gestion-ldap-client, gestion-nis-client                  | Aucune            | Utiliser cette politique de gestion « SVM-scoped » pour créer des LIFs de management du SVM détenues par un SVM de données. Ces LIF peuvent fournir un accès SSH ou HTTPS aux administrateurs du SVM. Lorsque nécessaire, ces LIF peuvent être utilisées pour des connexions sortantes vers des serveurs DNS externes, AD, LDAP ou NIS.                                                                                                                         |
| blocs de données par défaut | cœur de données, iscsi                                                                                                                                   | iscsi             | Utilisée par les LIF transportant un trafic de données SAN orienté bloc. Depuis ONTAP 9.10.1, la politique « blocs de données par défaut » est obsolète. Utilisez plutôt la stratégie de service « default-data-iscsi ».                                                                                                                                                                                                                                        |
| fichiers-données-par-défaut | client data-fpolicy, serveur-dns, data-flexcache, données-cifs, data-nfs, gestion-dns-client, gestion-ad-client, gestion-ldap-client, gestion-nis-client | nfs, cifs, fcache | Utilisez la stratégie par défaut-data-Files pour créer des LIF NAS qui prennent en charge des protocoles de données basés sur des fichiers. Parfois, il n'y a qu'une seule LIF présente au SVM, donc cette politique permet à la LIF d'être utilisée pour les connexions sortantes vers un serveur DNS externe, AD, LDAP ou NIS. Vous pouvez supprimer ces services de cette règle si vous préférez que ces connexions utilisent uniquement des LIF de gestion. |
| iscsi-données-par-défaut    | cœur de données, iscsi                                                                                                                                   | iscsi             | Utilisé par les LIF transportant le trafic de données iSCSI.                                                                                                                                                                                                                                                                                                                                                                                                    |
| données-défaut-nvme-tcp     | cœur de données, nvme-tcp                                                                                                                                | nvme-tcp          | Utilisé par les LIF transportant du trafic de données NVMe/TCP.                                                                                                                                                                                                                                                                                                                                                                                                 |

Le tableau suivant répertorie les services qui peuvent être utilisés sur un SVM de données et les restrictions que chaque service impose à la politique de basculement d'une LIF à partir de ONTAP 9.11.1 :

| Service        | Restrictions de basculement | Description                                                        |
|----------------|-----------------------------|--------------------------------------------------------------------|
| management-ssh | -                           | Services d'accès à la gestion SSH                                  |
| gestion-http   | -                           | Introduit dans ONTAP 9.10.1<br>Services de gestion de l'accès HTTP |
| gestion-https  | -                           | Services pour l'accès à la gestion HTTPS                           |

|                        |                                                                                  |                                                                                   |
|------------------------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| management-portmap     | -                                                                                | Services d'accès à la gestion de portmap                                          |
| serveur-gestion-snmp   | -                                                                                | Introduit dans ONTAP 9.10.1<br>Services pour l'accès à la gestion de serveur SNMP |
| cœur des données       | -                                                                                | Services de données centrales                                                     |
| nfs-données            | -                                                                                | Service de données NFS                                                            |
| cifs-données           | -                                                                                | Service de données CIFS                                                           |
| flexcache              | -                                                                                | Service de données FlexCache                                                      |
| iscsi données          | Port d'attache uniquement pour l'AFF/FAS ;<br>partenaire sfo uniquement pour ASA | Service de données iSCSI                                                          |
| backup-ndmp-control    | -                                                                                | Introduit dans ONTAP 9.10.1<br>Backup NDMP contrôle le service de données         |
| serveur-données-dns    | -                                                                                | Introduit dans ONTAP 9.10.1<br>Service de données du serveur DNS                  |
| client-données fpolicy | -                                                                                | Service de données de stratégie de filtrage de fichiers                           |
| tcp-nvme-données       | port d'origine uniquement                                                        | Introduit dans ONTAP 9.10.1<br>Service de données TCP NVMe                        |
| serveur data s3        | -                                                                                | Service de données des serveurs simple Storage Service (S3)                       |

Vous devez savoir comment les règles de service sont attribuées aux LIF dans les SVM de données :

- Lorsqu'un SVM de données est créé avec une liste de services de données, les règles de service « fichiers de données par défaut » et « blocs de données par défaut » intégrées à ce SVM sont créées à l'aide des services spécifiés.
- Si un SVM de données est créé sans spécifier une liste de services de données, les règles de service « fichiers de données par défaut » et « blocs de données par défaut » intégrées à ce SVM sont créées à l'aide d'une liste de services de données par défaut.

La liste des services de données par défaut comprend les services iSCSI, NFS, NVMe, SMB et FlexCache.

- Lorsqu'une LIF est créée avec une liste de protocoles de données, une politique de service équivalente aux protocoles de données spécifiés est assignée à la LIF.
- Si aucune stratégie de service équivalente n'existe, une stratégie de service personnalisée est créée.
- Lorsqu'une LIF est créée sans une policy de service ou une liste de protocoles de données, la politique de

service default-data-Files est assignée à la LIF par défaut.

### Service Data-core

Le service « Data-core » permet à des composants qui utilisaient auparavant les LIF avec le rôle de données de fonctionner comme prévu sur les clusters mis à niveau pour gérer les LIF à l'aide de politiques de service plutôt que de rôles LIF (qui sont obsolètes dans ONTAP 9.6).

La spécification data-core en tant que service n'ouvre aucun port du pare-feu, mais le service doit être inclus dans toute politique de service d'un SVM de données. Par exemple, la règle de service Default-data-Files contient les services suivants par défaut :

- cœur des données
- nfs-données
- cifs-données
- flexcache

Le service « data-core » doit être inclus dans la règle afin de garantir que toutes les applications utilisant la LIF comme prévu, mais que les trois autres services peuvent être supprimés, si nécessaire.

### Service LIF côté client

Depuis ONTAP 9.10.1, ONTAP fournit des services LIF côté client pour de nombreuses applications. Ces services permettent de contrôler les LIFs utilisées pour les connexions sortantes pour le compte de chaque application.

Les nouveaux services suivants permettent aux administrateurs de contrôler la liste des LIF utilisées comme adresses source pour certaines applications.

| Service                | Restrictions des SVM | Description                                                                                                                     |
|------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------|
| client-annonce-gestion | -                    | Depuis ONTAP 9.11.1, ONTAP fournit un service client Active Directory pour les connexions sortantes vers un serveur AD externe. |
| client-dns-gestion     | -                    | À partir de ONTAP 9.11.1, ONTAP fournit un service client DNS pour les connexions sortantes vers un serveur DNS externe.        |
| gestion-ldap-client    | -                    | Depuis ONTAP 9.11.1, ONTAP fournit un service client LDAP pour les connexions sortantes vers un serveur LDAP externe.           |
| gestion-nis-client     | -                    | À partir de ONTAP 9.11.1, ONTAP fournit un service client NIS pour les connexions sortantes à un serveur NIS externe.           |
| client-ntp-management  | système uniquement   | Depuis ONTAP 9.10.1, ONTAP fournit un service client NTP pour les connexions sortantes vers un serveur NTP externe.             |

|                        |                    |                                                                                          |
|------------------------|--------------------|------------------------------------------------------------------------------------------|
| client-données fpolicy | données uniquement | Depuis ONTAP 9.8, ONTAP fournit un service client pour les connexions FPolicy de sortie. |
|------------------------|--------------------|------------------------------------------------------------------------------------------|

Chacun des services est automatiquement inclus dans certaines règles de service intégrées, mais les administrateurs peuvent les supprimer des règles intégrées ou les ajouter à des règles personnalisées afin de contrôler les LIF utilisées pour les connexions sortantes pour le compte de chaque application.

### Rôles LIF (ONTAP 9.5 et versions antérieures)

Les LIF avec des rôles différents ont des caractéristiques différentes. Un rôle LIF détermine le type de trafic pris en charge via l'interface, ainsi que les règles de basculement qui s'appliquent, les restrictions de pare-feu en place, la sécurité, l'équilibrage de la charge et le comportement de routage pour chaque LIF. Une LIF peut avoir l'un des rôles suivants : cluster, gestion du cluster, données, intercluster, node management, et undef (non défini). Le rôle undef est utilisé pour les LIF BGP.

Depuis la version ONTAP 9.6, les rôles LIF sont obsolètes. Vous devez définir des stratégies de service pour les LIF au lieu d'un rôle. Il n'est pas nécessaire de spécifier un rôle LIF lors de la création d'une LIF avec une policy de services.

### Sécurité de LIF

|                                      | LIF de données  | LIF Cluster        | FRV de gestion des nœuds | LIF Cluster-management | FRV InterCluster |
|--------------------------------------|-----------------|--------------------|--------------------------|------------------------|------------------|
| Besoin d'un sous-réseau IP privé ?   | Non             | Oui.               | Non                      | Non                    | Non              |
| Besoin d'un réseau sécurisé ?        | Non             | Oui.               | Non                      | Non                    | Oui.             |
| Politique de pare-feu par défaut     | Très restrictif | Entièrement ouvert | Moyen                    | Moyen                  | Très restrictif  |
| Le pare-feu est-il personnalisable ? | Oui.            | Non                | Oui.                     | Oui.                   | Oui.             |

### Le basculement de LIF

|  | LIF de données | LIF Cluster | FRV de gestion des nœuds | LIF Cluster-management | FRV InterCluster |
|--|----------------|-------------|--------------------------|------------------------|------------------|
|--|----------------|-------------|--------------------------|------------------------|------------------|

|                         |                                                                                                                                   |                                                                            |                                                                            |                                                        |                                                                            |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------|--------------------------------------------------------|----------------------------------------------------------------------------|
| Comportement par défaut | Seuls les ports du même groupe de basculement se trouvent sur le nœud de rattachement de la LIF et sur un nœud partenaire non SFO | Seuls les ports du même failover group qui sont sur le home node de la LIF | Seuls les ports du même failover group qui sont sur le home node de la LIF | N'importe quel port dans le même groupe de basculement | Seuls les ports du même failover group qui sont sur le home node de la LIF |
| Est personnalisable ?   | Oui.                                                                                                                              | Non                                                                        | Oui.                                                                       | Oui.                                                   | Oui.                                                                       |

### Routage de LIF

|                                                                                  | LIF de données                                                                                                                                                                                             | LIF Cluster | FRV de gestion des nœuds                                                                    | LIF Cluster-management                                                  | FRV InterCluster                                                                                         |
|----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Quand une route par défaut est-elle nécessaire ?                                 | Lorsque les clients ou le contrôleur de domaine se trouvent sur un sous-réseau IP différent                                                                                                                | Jamais      | Lorsque l'un des types de trafic principaux nécessite l'accès à un sous-réseau IP différent | Lorsque l'administrateur se connecte à partir d'un autre sous-réseau IP | Lorsque d'autres LIFs intercluster se trouvent sur un sous-réseau IP différent                           |
| Quand une route statique vers un sous-réseau IP spécifique est-elle nécessaire ? | Rares                                                                                                                                                                                                      | Jamais      | Rares                                                                                       | Rares                                                                   | Lorsque les nœuds d'un autre cluster disposent de leurs LIF intercluster dans différents sous-réseaux IP |
| Quand une route hôte statique vers un serveur spécifique est-elle nécessaire ?   | Pour obtenir l'un des types de trafic répertoriés sous LIF de node-management, passez par une LIF de données plutôt qu'une LIF de node-management. Cela nécessite un changement de pare-feu correspondant. | Jamais      | Rares                                                                                       | Rares                                                                   | Rares                                                                                                    |

### Rééquilibrage LIF



|                                    | LIF de données | LIF Cluster | FRV de gestion des nœuds | LIF Cluster-management | FRV InterCluster |
|------------------------------------|----------------|-------------|--------------------------|------------------------|------------------|
| DNS : utiliser comme serveur DNS ? | Oui.           | Non         | Non                      | Non                    | Non              |
| DNS : exporter en tant que zone ?  | Oui.           | Non         | Non                      | Non                    | Non              |

### Types de trafic principaux LIF

|                            | LIF de données                                                                                          | LIF Cluster  | FRV de gestion des nœuds                                                                                              | LIF Cluster-management       | FRV InterCluster               |
|----------------------------|---------------------------------------------------------------------------------------------------------|--------------|-----------------------------------------------------------------------------------------------------------------------|------------------------------|--------------------------------|
| Types de trafic principaux | Serveur NFS, serveur CIFS, client NIS, Active Directory, LDAP, WINS, client et serveur DNS, iSCSI et FC | Intracluster | Serveur SSH, serveur HTTPS, client NTP, SNMP, client AutoSupport, Client DNS, chargement des mises à jour logicielles | Serveur SSH et serveur HTTPS | Réplication entre les clusters |

## Gestion des LIF

### Configurer les règles de service LIF

Vous pouvez configurer les stratégies de service LIF afin d'identifier un seul service ou une liste de services qui utiliseront une LIF.

#### Création d'une policy de service pour les LIFs

Vous pouvez créer une policy de service pour les LIF. Vous pouvez affecter une stratégie de service à une ou plusieurs LIF, permettant ainsi au LIF de transporter du trafic pour un seul service ou une liste de services.

Vous avez besoin de privilèges avancés pour exécuter le `network interface service-policy create` commande.

#### Description de la tâche

Les services et les règles de service intégrés sont disponibles pour la gestion du trafic de données et de gestion sur les SVM de données et de système. La plupart des cas d'utilisation sont satisfaits à l'aide d'une règle de service intégrée plutôt que de créer une règle de service personnalisée.

Vous pouvez modifier ces règles de service intégrées, si nécessaire.

#### Étapes

1. Afficher les services disponibles dans le cluster :

```
network interface service show
```

Les services représentent les applications auxquelles un LIF accède, ainsi que les applications servies par le cluster. Chaque service inclut zéro ou plus de ports TCP et UDP sur lesquels l'application écoute.

Les services de gestion et de données supplémentaires suivants sont disponibles :

```
cluster1::> network interface service show
```

| Service                    | Protocol:Ports  |
|----------------------------|-----------------|
| -----                      | -----           |
| cluster-core               | -               |
| data-cifs                  | -               |
| data-core                  | -               |
| data-flexcache             | -               |
| data-iscsi                 | -               |
| data-nfs                   | -               |
| intercluster-core          | tcp:11104-11105 |
| management-autosupport     | -               |
| management-bgp             | tcp:179         |
| management-core            | -               |
| management-https           | tcp:443         |
| management-ssh             | tcp:22          |
| 12 entries were displayed. |                 |

2. Afficher les politiques de service qui existent dans le cluster :

```
cluster1::> network interface service-policy show
```

| Vserver  | Policy                 | Service: Allowed Addresses                                                                                                  |
|----------|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| -----    |                        |                                                                                                                             |
| -----    |                        |                                                                                                                             |
| cluster1 |                        |                                                                                                                             |
|          | default-intercluster   | intercluster-core: 0.0.0.0/0<br>management-https: 0.0.0.0/0                                                                 |
|          | default-management     | management-core: 0.0.0.0/0<br>management-autosupport: 0.0.0.0/0<br>management-ssh: 0.0.0.0/0<br>management-https: 0.0.0.0/0 |
|          | default-route-announce | management-bgp: 0.0.0.0/0                                                                                                   |
| Cluster  |                        |                                                                                                                             |
|          | default-cluster        | cluster-core: 0.0.0.0/0                                                                                                     |
| vs0      |                        |                                                                                                                             |
|          | default-data-blocks    | data-core: 0.0.0.0/0<br>data-iscsi: 0.0.0.0/0                                                                               |
|          | default-data-files     | data-core: 0.0.0.0/0<br>data-nfs: 0.0.0.0/0<br>data-cifs: 0.0.0.0/0<br>data-flexcache: 0.0.0.0/0                            |
|          | default-management     | data-core: 0.0.0.0/0<br>management-ssh: 0.0.0.0/0<br>management-https: 0.0.0.0/0                                            |

```
7 entries were displayed.
```

### 3. Création d'une règle de services :

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
```

```
Do you wish to continue? (y or n): y
```

```
cluster1::> network interface service-policy create -vserver <svm_name>
-policy <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>
```

- « nom\_service » indique une liste de services à inclure dans la stratégie.
- "IP\_address/mask" spécifie la liste des masques de sous-réseau pour les adresses autorisées à accéder aux services dans la stratégie de service. Par défaut, tous les services spécifiés sont ajoutés avec une liste d'adresses par défaut autorisée de 0.0.0.0/0, ce qui permet le trafic de tous les sous-réseaux. Lorsqu'une liste d'adresses autorisées par défaut est fournie, les LIF utilisant la règle sont configurées pour bloquer toutes les demandes avec une adresse source qui ne correspond à aucun des masques spécifiés.

L'exemple suivant montre comment créer une stratégie de service de données, *svm1\_Data\_policy*, pour une SVM qui inclut *NFS* et *SMB* services :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

L'exemple suivant montre comment créer une politique de service intercluster :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

#### 4. Vérifiez que la stratégie de service est créée.

```
cluster1::> network interface service-policy show
```

Le résultat suivant indique les règles de service disponibles :

```
cluster1::> network interface service-policy show
```

| Vserver  | Policy                 | Service: Allowed Addresses                                                                                                  |
|----------|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| -----    |                        |                                                                                                                             |
| -----    |                        |                                                                                                                             |
| cluster1 |                        |                                                                                                                             |
|          | default-intercluster   | intercluster-core: 0.0.0.0/0<br>management-https: 0.0.0.0/0                                                                 |
|          | intercluster1          | intercluster-core: 0.0.0.0/0                                                                                                |
|          | default-management     | management-core: 0.0.0.0/0<br>management-autosupport: 0.0.0.0/0<br>management-ssh: 0.0.0.0/0<br>management-https: 0.0.0.0/0 |
|          | default-route-announce | management-bgp: 0.0.0.0/0                                                                                                   |
| Cluster  |                        |                                                                                                                             |
|          | default-cluster        | cluster-core: 0.0.0.0/0                                                                                                     |
| vs0      |                        |                                                                                                                             |
|          | default-data-blocks    | data-core: 0.0.0.0/0<br>data-iscsi: 0.0.0.0/0                                                                               |
|          | default-data-files     | data-core: 0.0.0.0/0<br>data-nfs: 0.0.0.0/0<br>data-cifs: 0.0.0.0/0<br>data-flexcache: 0.0.0.0/0                            |
|          | default-management     | data-core: 0.0.0.0/0<br>management-ssh: 0.0.0.0/0<br>management-https: 0.0.0.0/0                                            |
|          | svm1_data_policy       | data-core: 0.0.0.0/0<br>data-nfs: 0.0.0.0/0<br>data-cifs: 0.0.0.0/0                                                         |

```
9 entries were displayed.
```

### Une fois que vous avez terminé

Assigner la policy de service à une LIF soit au moment de la création, soit en modifiant une LIF existante.

Assigner une policy de service à une LIF

Vous pouvez affecter une policy de service à une LIF au moment de la création de cette LIF ou en modifiant la LIF. Une policy de service définit la liste de services qui peuvent être utilisés avec la LIF.

Description de la tâche

Vous pouvez attribuer des règles de service pour les LIF dans les SVM admin et data.

Étape

Selon l'heure à laquelle vous souhaitez affecter la policy de service à une LIF, effectuez l'une des actions suivantes :

| Si vous êtes...        | Affecter la stratégie de service...                                                                                                                                                                                           |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Création d'une LIF     | Interface réseau create -vserver svm_name -lif <lif_name> -home-node <nom_node> -home-port <nom_port> {( -adresse <adresse_IP> -masque de réseau <adresse_IP> ) -subnet-name <nom_sous-réseau>} -service-policy <nom_service> |
| Modification d'une LIF | interface réseau modify -vserver <svm_name> -lif <lif_name> -service-policy <service_name>                                                                                                                                    |

Lorsque vous spécifiez une policy de services pour une LIF, il n'est pas nécessaire de spécifier le protocole de données et le rôle de cette dernière. La création des LIF en spécifiant le rôle et les protocoles de données est également pris en charge.



Une politique de service peut uniquement être utilisée par les LIFs dans le même SVM que vous avez spécifié lors de la création de la policy de service.

Exemples

L'exemple suivant montre comment modifier la policy de service d'une LIF pour utiliser la policy de service de gestion par défaut :

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service
-policy default-management
```

Commandes permettant de gérer les règles de service LIF

Utilisez le `network interface service-policy` Commandes permettant de gérer les règles de service LIF.

Avant de commencer

La modification de la politique de service d'une LIF dans une relation SnapMirror active interrompt la planification de la réplication. Si vous convertissez une LIF de intercluster en non-intercluster (ou inversement), ces modifications ne sont pas répliquées sur le cluster peering. Pour mettre à jour le Peer Cluster après avoir modifié la politique de service LIF, effectuez d'abord la procédure `snapmirror abort` ensuite [resynchroniser la relation de réplication](#).

| Les fonctions que vous recherchez...                                                                          | Utilisez cette commande...                                     |
|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| Création d'une stratégie de service (privilèges avancés requis)                                               | <code>network interface service-policy create</code>           |
| Ajouter une entrée de service supplémentaire à une stratégie de service existante (privilèges avancés requis) | <code>network interface service-policy add-service</code>      |
| Cloner une stratégie de service existante (privilèges avancés requis)                                         | <code>network interface service-policy clone</code>            |
| Modification d'une entrée de service dans une stratégie de service existante (privilèges avancés requis)      | <code>network interface service-policy modify-service</code>   |
| Suppression d'une entrée de service d'une stratégie de service existante (privilèges avancés requis)          | <code>network interface service-policy remove-service</code>   |
| Renommer une stratégie de service existante (privilèges avancés requis)                                       | <code>network interface service-policy rename</code>           |
| Suppression d'une stratégie de service existante (privilèges avancés requis)                                  | <code>network interface service-policy delete</code>           |
| Restaurer une stratégie de service intégrée à son état d'origine (privilèges avancés requis)                  | <code>network interface service-policy restore-defaults</code> |
| Afficher les stratégies de service existantes                                                                 | <code>network interface service-policy show</code>             |

## Créer une LIF (interface réseau)

Un SVM fournit des données aux clients via une ou plusieurs interfaces logiques réseau (LIF). Vous devez créer les LIFs sur les ports que vous souhaitez utiliser pour accéder aux données. Une LIF (interface réseau) est une adresse IP associée à un port physique ou logique. En cas de panne d'un composant, une LIF peut basculer vers un autre port physique ou la migrer vers un autre port, ce qui continue à communiquer avec le réseau.

### Et des meilleures pratiques

Les ports de commutateur connectés à ONTAP doivent être configurés en tant que ports de périphérie « spanning Tree » afin de réduire les retards lors de la migration des LIF.

### Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Le port réseau physique ou logique sous-jacent doit avoir été configuré pour que le statut administratif soit activé.
- Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de

réseau à une LIF, le sous-réseau doit déjà exister.

Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche 3. Ils sont créés à l'aide de System Manager ou de `network subnet create` commande.

- Le mécanisme de spécification du type de trafic traité par une LIF a changé. Pour ONTAP 9.5 et versions antérieures, la LIF utilisait des rôles pour spécifier le type de trafic qu'elle entraînerait. Depuis ONTAP 9.6, les LIF utilisent des politiques de service pour spécifier le type de trafic qu'elles seraient à traiter.

### Description de la tâche

- Vous ne pouvez pas attribuer des protocoles NAS et SAN à la même LIF.

Les protocoles pris en charge sont SMB, NFS, FlexCache, iSCSI et FC ; iSCSI et FC ne peuvent pas être associés à d'autres protocoles. Les protocoles NAS et SAN Ethernet peuvent toutefois être présents sur le même port physique.

- Vous ne devez pas configurer les LIF qui transportent le trafic SMB afin de revenir automatiquement à leurs nœuds de départ. Cette recommandation est obligatoire si le serveur SMB doit héberger une solution pour la continuité de l'activité avec Hyper-V ou SQL Server over SMB.
- Vous pouvez créer des LIF IPv4 et IPv6 sur le même port réseau.
- Tous les services de mappage de noms et de résolution de noms d'hôte utilisés par un SVM, tel que DNS, NIS, LDAP, et Active Directory, Doit être accessible à partir d'au moins une LIF gérant le trafic de données du SVM.
- Une LIF gérant le trafic intracluster entre des nœuds ne doit pas se trouver sur le même sous-réseau que le trafic de gestion d'une LIF ou encore le trafic de données géré par une LIF.
- La création d'une LIF ne disposant pas de cible de basculement valide entraîne un message d'avertissement.
- Si vous disposez d'un grand nombre de LIF dans le cluster, vous pouvez vérifier la capacité LIF prise en charge sur le cluster :
  - System Manager : depuis ONTAP 9.12.0, consultez le débit de la grille de l'interface réseau.
  - Interface de ligne de commandes : utilisez le `network interface capacity show` Et la capacité LIF prise en charge sur chaque nœud à l'aide de `network interface capacity details show` commande (au niveau de privilège avancé).
- Depuis ONTAP 9.7, si d'autres LIF existent déjà pour le SVM dans le même sous-réseau, il n'est pas nécessaire de spécifier le home port de la LIF. ONTAP choisit automatiquement un port aléatoire sur le nœud de rattachement spécifié dans le même domaine de diffusion que les autres LIFs déjà configurées dans le même sous-réseau.

Le protocole FC-NVMe est pris en charge à partir de la version ONTAP 9.4. Si vous créez une LIF FC-NVMe, notez les éléments suivants :

- Le protocole NVMe doit être pris en charge par l'adaptateur FC sur lequel la LIF est créée.
- FC-NVMe est le seul protocole de données sur les LIF de données.
- Un trafic de gestion des LIF doit être configuré pour chaque SVM (Storage Virtual machine) prenant en charge les protocoles SAN.
- Les LIFs et namespaces NVMe doivent être hébergés sur le même nœud.
- Un seul protocole LIF NVMe traitant le trafic de données peut être configuré par SVM.
- Lorsque vous créez une interface réseau avec un sous-réseau, ONTAP sélectionne automatiquement une adresse IP disponible à partir du sous-réseau sélectionné et l'attribue à l'interface réseau. Vous pouvez



modifier le sous-réseau s'il y a plusieurs sous-réseaux, mais vous ne pouvez pas modifier l'adresse IP.

- Lorsque vous créez (ajoutez) un SVM, pour une interface réseau, vous ne pouvez pas spécifier une adresse IP comprise dans la plage d'un sous-réseau existant. Vous recevrez une erreur de conflit de sous-réseau. Ce problème survient sur d'autres flux de production d'une interface réseau, comme la création ou la modification des interfaces réseau inter-cluster dans les paramètres des SVM ou les paramètres du cluster.
- Avec ONTAP 9.10.1, le `network interface` Les commandes de l'interface de ligne de commande incluent un `-rdma-protocols` Paramètre des configurations NFS sur RDMA. System Manager prend en charge la création d'interfaces réseau pour les configurations NFS sur RDMA à partir de la version ONTAP 9.12.1. Pour plus d'informations, voir [Configuration DES LIF pour NFS sur RDMA](#).
- Depuis la version ONTAP 9.11.1, le basculement automatique des LIF iSCSI est disponible sur les plateformes ASA (All-Flash SAN Array).

Le basculement de LIF iSCSI est automatiquement activé (la règle de basculement est définie sur `sfo-partner-only` la valeur de restauration automatique est définie sur `true`) Sur les LIF iSCSI nouvellement créées si aucune LIF iSCSI n'existe dans le SVM spécifié ou si toutes les LIFs iSCSI existantes du SVM spécifié sont déjà activées avec le basculement LIF iSCSI.

Si après une mise à niveau vers ONTAP 9.11.1 ou version ultérieure, vous disposez de LIF iSCSI existantes dans un SVM qui n'ont pas été activées avec la fonctionnalité de basculement LIF iSCSI et que vous créez de nouvelles LIF iSCSI dans le même SVM, les nouvelles LIF iSCSI supposent la même politique de basculement (`disabled`) Des LIFs iSCSI existantes du SVM.

### "Basculement de LIF iSCSI pour les plateformes ASA"

Depuis ONTAP 9.7, ONTAP choisit automatiquement le port de base d'une LIF, tant qu'au moins une LIF existe déjà dans le même sous-réseau dans cet IPspace. ONTAP choisit un port home-port dans le même domaine de diffusion que d'autres LIFs de ce sous-réseau. Vous pouvez toujours spécifier un port home port, mais ce n'est plus nécessaire (sauf si aucune LIF n'existe encore dans ce sous-réseau dans l'IPspace spécifié).

Depuis ONTAP 9.12.0, la procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## System Manager

### Utilisez System Manager pour ajouter une interface réseau

#### Étapes

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez **+ Add**.
3. Sélectionnez l'un des rôles d'interface suivants :
  - a. Les données
  - b. Intercluster
  - c. Gestion SVM
4. Sélectionnez le protocole :
  - a. SMB/CIFS ET NFS
  - b. iSCSI
  - c. FC
  - d. NVMe/FC
  - e. NVMe/TCP
5. Nommez la LIF ou acceptez le nom généré par vos sélections précédentes.
6. Acceptez le nœud de départ ou utilisez le menu déroulant pour en sélectionner un.
7. Si au moins un sous-réseau est configuré dans l'IPspace du SVM sélectionné, la liste déroulante sous-réseau est affichée.
  - a. Si vous sélectionnez un sous-réseau, choisissez-le dans la liste déroulante.
  - b. Si vous continuez sans sous-réseau, la liste déroulante broadcast domain s'affiche :
    - i. Spécifiez l'adresse IP. Si l'adresse IP est utilisée, un message d'avertissement s'affiche.
    - ii. Spécifiez un masque de sous-réseau.
8. Sélectionnez le port d'accueil dans le domaine de diffusion, soit automatiquement (recommandé), soit en sélectionnant un dans le menu déroulant. Le contrôle du port Home s'affiche en fonction du domaine de diffusion ou de la sélection du sous-réseau.
9. Enregistrez l'interface réseau.

#### CLI

### Utilisez l'interface de ligne de commande pour créer une LIF

#### Étapes

1. Déterminez les ports de broadcast domain que vous souhaitez utiliser pour le LIF.

```
network port broadcast-domain show -ipspace ipspace1
```

| IPspace<br>Name | Broadcast<br>Domain name | MTU  | Port List | Update<br>Status Details |
|-----------------|--------------------------|------|-----------|--------------------------|
| ipspace1        | default                  | 1500 |           |                          |
|                 |                          |      | node1:e0d | complete                 |
|                 |                          |      | node1:e0e | complete                 |
|                 |                          |      | node2:e0d | complete                 |
|                 |                          |      | node2:e0e | complete                 |

2. Vérifiez que le sous-réseau que vous souhaitez utiliser pour les LIF contient suffisamment d'adresses IP inutilisées.

```
network subnet show -ipspace ipspace1
```

3. Créez une ou plusieurs LIF sur les ports que vous souhaitez utiliser pour accéder aux données.

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

- **-home-node** Est le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.

Vous pouvez également indiquer si la LIF doit revenir automatiquement au nœud home et au port home-port avec l'option `-auto-revert`.

- **-home-port** Est le port physique ou logique vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.
- Vous pouvez spécifier une adresse IP avec le `-address` et `-netmask` ou vous activez l'allocation à partir d'un sous-réseau avec `-subnet_name` option.
- Lors de l'utilisation d'un sous-réseau pour fournir l'adresse IP et le masque de réseau, si le sous-réseau a été défini avec une passerelle, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau.
- Si vous attribuez des adresses IP manuellement (sans utiliser de sous-réseau), vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un autre sous-réseau IP. Le `network route create` La page man contient des informations sur la création d'une route statique au sein d'un SVM.
- **-auto-revert** Vous permet de spécifier si une LIF de données est automatiquement rétablie sur le nœud de rattachement en cas de démarrage, de modifications du statut de la base de données de gestion ou lors de la connexion réseau. Le paramètre par défaut est `false`, mais vous pouvez le définir sur `true` selon les stratégies de gestion de réseau de votre environnement.
- **-service-policy** Depuis ONTAP 9.5, vous pouvez attribuer une policy de service pour la LIF avec le `-service-policy` option.

Lorsqu'une politique de services est spécifiée pour une LIF, cette règle est utilisée pour construire un rôle par défaut, une politique de basculement et une liste de protocoles de données pour la LIF. Dans ONTAP 9.5, les stratégies de service sont prises en charge uniquement pour les services de pairs intercluster et BGP. Dans ONTAP 9.6, vous pouvez créer des stratégies de service pour plusieurs services de données et de gestion.

- ° `-data-protocol` Permet de créer une LIF qui prend en charge les protocoles FCP ou NVMe/FC. Cette option n'est pas requise lors de la création d'une LIF IP.

4. **Facultatif** : attribuez une adresse IPv6 dans l'option `-address` :

- Utilisez la commande `network npd prefix show` pour afficher la liste des préfixes RA appris sur diverses interfaces.

Le `network npd prefix show` la commande est disponible au niveau de privilège avancé.

- Utiliser le format `prefix::id` Pour construire l'adresse IPv6 manuellement.

`prefix` est le préfixe utilisé sur les différentes interfaces.

Pour calculer le `id`, choisissez un nombre hexadécimal 64 bits aléatoire.

5. Vérifier que la configuration de l'interface LIF est correcte.

```
network interface show -vserver vs1
```

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Is Port |
|---------|-------------------|-------------------|----------------------|--------------|-----------------|
| Home    |                   |                   |                      |              |                 |
| vs1     | lif1              | up/up             | 10.0.0.128/24        | node1        | e0d             |
| true    |                   |                   |                      |              |                 |

6. Vérifiez que la configuration du groupe de basculement est la plus appropriée.

```
network interface show -failover -vserver vs1
```

| Vserver                                                      | Logical interface | Home Node:Port | Failover Policy | Failover Group |
|--------------------------------------------------------------|-------------------|----------------|-----------------|----------------|
| vs1                                                          | lif1              | node1:e0d      | system-defined  | ipspace1       |
| Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e |                   |                |                 |                |

7. Vérifiez que l'adresse IP configurée est accessible :

|                  |             |
|------------------|-------------|
| Pour vérifier... | Utiliser... |
|------------------|-------------|

|              |              |
|--------------|--------------|
| Adresse IPv4 | ping réseau  |
| Adresse IPv6 | réseau ping6 |

### Exemples

La commande suivante crée une LIF et spécifie les valeurs d'adresse IP et de masque réseau à l'aide de `-address` et `-netmask` paramètres :

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port elc
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

La commande suivante crée une LIF et attribue des valeurs d'adresse IP et de masque réseau à partir du sous-réseau spécifié (nommé `client1_sub`) :

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port elc
-subnet-name client1_sub - auto-revert true
```

La commande suivante crée une LIF NVMe/FC et spécifie le `nvme-fc` protocole de données :

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port lc -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

## Modifier une LIF

Vous pouvez modifier une LIF en modifiant les attributs, tels que le nœud de rattachement ou le nœud actuel, l'état administratif, l'adresse IP, le masque de réseau, la règle de basculement, la politique de pare-feu et la politique de service. Vous pouvez également modifier la famille d'adresses d'une LIF d'IPv4 à IPv6.

### Description de la tâche

- Lorsque vous modifiez le statut administratif d'une LIF en cas de panne, tout verrouillage NFSv4 en attente est conservé jusqu'à ce que le statut administratif de la LIF soit renvoyé à une date supérieure.

Pour éviter les conflits de verrouillage pouvant survenir lorsque d'autres LIFs tentent d'accéder aux fichiers verrouillés, vous devez déplacer les clients NFSv4 vers une autre LIF avant de définir le statut administratif sur `down`.

- Vous ne pouvez pas modifier les protocoles de données utilisés par une LIF FC. Toutefois, vous pouvez modifier les services affectés à une politique de service ou modifier la politique de service attribuée à une LIF IP.

Pour modifier les protocoles de données utilisés par une LIF FC, il faut supprimer cette LIF, puis la recréer. Pour modifier la stratégie de service à une LIF IP, une brève interruption se produit lors des mises à jour.

- Vous ne pouvez pas modifier le nœud de rattachement ou le nœud actuel d'un LIF de management scoped node-scoped.
- Lors de l'utilisation d'un sous-réseau pour modifier l'adresse IP et la valeur du masque réseau d'une LIF, une adresse IP est allouée à partir du sous-réseau spécifié ; si l'adresse IP précédente de la LIF provient d'un autre sous-réseau, l'adresse IP est renvoyée à ce sous-réseau.
- Pour modifier la famille d'adresses d'une LIF d'IPv4 vers IPv6, vous devez utiliser la notation des deux-points pour l'adresse IPv6 et ajouter une nouvelle valeur pour le `-netmask-length` paramètre.
- Vous ne pouvez pas modifier les adresses IPv6 lien-local configurées automatiquement.
- La modification d'une LIF entraînant l'absence de cible de basculement valide entraîne un message d'avertissement.

Si une LIF ne disposant pas de tentatives de basculement cible valides, une panne peut se produire.

- Depuis ONTAP 9.5, vous pouvez modifier la politique de service associée à une LIF.

Dans ONTAP 9.5, les stratégies de service sont prises en charge uniquement pour les services de pairs intercluster et BGP. Dans ONTAP 9.6, vous pouvez créer des stratégies de service pour plusieurs services de données et de gestion.

- Depuis la version ONTAP 9.11.1, le basculement automatique des LIF iSCSI est disponible sur les plateformes ASA (All-Flash SAN Array).


Pour les LIF iSCSI préexistantes, c'est-à-dire les LIF créées avant la mise à niveau vers la version 9.11.1 ou ultérieure, vous pouvez modifier la règle de basculement sur incident en "[Activer le basculement automatique de LIF iSCSI](#)".

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## System Manager

À partir de ONTAP 9.12.0, vous pouvez utiliser System Manager pour modifier une interface réseau

### Étapes

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez  > **Modifier** en regard de l'interface réseau que vous souhaitez modifier.
3. Modifiez un ou plusieurs paramètres de l'interface réseau. Pour plus de détails, voir "[Créer une LIF](#)".
4. Enregistrez les modifications.

## CLI

### Utilisez l'interface de ligne de commande pour modifier une LIF

### Étapes

1. Modifier les attributs d'une LIF à l'aide de `network interface modify` commande.

L'exemple suivant montre comment modifier l'adresse IP et le masque de réseau de LIF datalif2 en utilisant une adresse IP et la valeur du masque de réseau de subnet client1\_sub :

```
network interface modify -vserver vs1 -lif datalif2 -subnet-name
client1_sub
```

L'exemple suivant montre comment modifier la politique de service d'une LIF.

```
network interface modify -vserver siteA -lif node1_inter1 -service
-policy example
```

2. Vérifiez que les adresses IP sont accessibles.

| Si vous utilisez... | Puis utilisez...           |
|---------------------|----------------------------|
| Adresses IPv4       | <code>network ping</code>  |
| Adresses IPv6       | <code>network ping6</code> |

## Migrer un LIF

Vous pouvez avoir à migrer une LIF vers un autre port du même nœud ou d'un autre nœud du cluster, si le port est défectueux ou nécessite une maintenance. La migration d'une LIF est similaire au basculement de LIF, mais la migration de LIF est une opération manuelle, tandis que le basculement de LIF est la migration automatique d'une LIF en réponse à une défaillance de liaison sur le port réseau actuel du LIF.

## Avant de commencer

- Un failover group doit avoir été configuré pour les LIFs.
- Le nœud et les ports de destination doivent être opérationnels et doivent pouvoir accéder au même réseau que le port source.

## Description de la tâche

- Les LIF BGP résident sur le port de rattachement et ne peuvent pas être migrées vers un autre nœud ou port.
- Vous devez migrer les LIFs hébergées sur les ports appartenant à une carte réseau vers d'autres ports du cluster, avant de retirer la carte réseau du nœud.
- Vous devez exécuter la commande pour migrer une LIF de cluster à partir du nœud sur lequel la LIF de cluster est hébergée.
- Un LIF node-scoped, tel qu'une LIF node-scoped management, cluster LIF, intercluster LIF, ne peut pas être migré vers un nœud distant.
- Lorsqu'une LIF NFSv4 est migrée entre les nœuds, un délai de 45 secondes peut atteindre les résultats avant que la LIF ne soit disponible sur un nouveau port.

Pour contourner ce problème, utilisez NFSv4.1 en cas de retard.

- Vous pouvez migrer des LIF iSCSI sur des plateformes ASA exécutant ONTAP 9.11.1 ou une version ultérieure.

La migration des LIF iSCSI est limitée aux ports du nœud de rattachement ou du partenaire de haute disponibilité.

- Si votre plateforme n'est pas une baie SAN 100 % Flash (ASA) exécutant ONTAP version 9.11.1 ou ultérieure, vous ne pouvez pas migrer les LIF iSCSI d'un nœud vers un autre.

Pour contourner cette restriction, vous devez créer une LIF iSCSI sur le nœud de destination. En savoir plus sur ["Création des LIFs iSCSI"](#).

- Si vous souhaitez migrer une LIF (interface réseau) pour NFS sur RDMA, vous devez vous assurer que le port de destination est compatible RoCE. Vous devez exécuter ONTAP 9.10.1 ou version ultérieure pour migrer une LIF avec l'interface de ligne de commandes ou ONTAP 9.12.1 pour effectuer la migration à l'aide de System Manager. Dans System Manager, une fois que vous avez sélectionné votre port de destination compatible RoCE, vous devez cocher la case en regard de **utiliser les ports RoCE** pour terminer la migration. En savoir plus sur ["Configuration des LIFs pour NFS sur RDMA"](#).
- Les opérations de déchargement des copies VMware VAAI échouent lors de la migration du LIF source ou de destination. En savoir plus sur la copie hors chargement :
  - ["Les environnements NFS"](#)
  - ["Environnements SAN"](#)

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :



## System Manager

### Utilisez System Manager pour migrer une interface réseau

#### Étapes

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez **⋮ > migrer** en regard de l'interface réseau à modifier.



Pour une LIF iSCSI, dans la boîte de dialogue **Migrate interface**, sélectionnez le nœud de destination et le port du partenaire HA.

Si vous souhaitez migrer définitivement la LIF iSCSI, cochez la case. La LIF iSCSI doit être hors ligne avant d'être définitivement migrée. De plus, une fois la migration permanente d'une LIF iSCSI, celle-ci ne peut pas être annulée. Il n'y a pas d'option de restauration.

3. Cliquez sur **migrer**.
4. Enregistrez les modifications.

#### CLI

### Utilisez l'interface de ligne de commande pour migrer une LIF

#### Étape

Selon que vous souhaitez migrer une LIF ou toutes les LIF, effectuez l'action appropriée :

| Pour migrer...                                                  | Saisissez la commande suivante...                                                |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------|
| Une LIF spécifique                                              | <code>network interface migrate</code>                                           |
| Toutes les LIF de gestion des données et du cluster sur un nœud | <code>network interface migrate-all</code>                                       |
| Toutes les LIFs hors d'un port                                  | <code>network interface migrate-all -node &lt;node&gt; -port &lt;port&gt;</code> |

L'exemple suivant montre comment migrer une LIF nommée `datalif1` Sur le SVM `vs0` vers le port `e0d` marche `node0b`:

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b
-dest-port e0d
```

L'exemple suivant montre comment migrer toutes les LIFs de données et cluster-management depuis le nœud actuel (local) :

```
network interface migrate-all -node local
```

**Ne rétablit pas un LIF à son port de départ**

Vous pouvez restaurer une LIF vers son port de base après qu’elle échoue ou qu’elle est migrée vers un autre port manuellement ou automatiquement. Si le port de home d’une LIF particulière n’est pas disponible, la LIF reste sur son port actuel et n’est pas rétablie.

**Description de la tâche**


- Si vous rétablir d’un point de vue administratif l’état du port de base d’une LIF avant de configurer l’option de restauration automatique, la LIF n’est pas renvoyée au port de base.
- La LIF ne revient pas automatiquement, sauf si la valeur de l’option « auto-revert » est définie sur vrai.
- Vous devez vous assurer que l’option de restauration automatique est activée pour que les LIF puissent revenir à leurs ports de base.

La procédure à suivre dépend de l’interface que vous utilisez—System Manager ou de l’interface de ligne de commandes :

**System Manager**

**Utilisez System Manager pour rétablir une interface réseau à son port d’accueil**

**Étapes**

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez  > **Revert** en regard de l’interface réseau que vous souhaitez modifier.
3. Sélectionnez **Revert** pour rétablir une interface réseau à son port d’origine.

**CLI**

**Utilisez l’interface de ligne de commande pour rétablir une LIF à son port d’accueil**

**Étape**

Restaurez une LIF manuellement ou automatiquement sur son port de base :

|                                                              |                                                                                              |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Si vous souhaitez restaurer une LIF vers son port de base... | Entrez ensuite la commande suivante...                                                       |
| Manuellement                                                 | <code>network interface revert -vserver vservice_name -lif lif_name</code>                   |
| Automatiquement                                              | <code>network interface modify -vserver vservice_name -lif lif_name -auto-revert true</code> |

**ONTAP 9.8 et versions ultérieures : récupération depuis une LIF de cluster mal configurée**

Un cluster ne peut pas être créé lorsque le réseau de cluster est câblé à un commutateur, mais tous les ports configurés dans le Cluster IPspace peuvent atteindre les autres ports configurés dans le Cluster IPspace.

**Description de la tâche**

Dans un cluster commuté, si une interface réseau de cluster (LIF) est configurée sur le port inapproprié ou si

un port de cluster est câblé dans le mauvais réseau, le `cluster create` la commande peut échouer avec l'erreur suivante :

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

Les résultats du `network port show` La commande peut montrer que plusieurs ports sont ajoutés au Cluster IPspace car ils sont connectés à un port configuré avec une LIF de cluster. Toutefois, les résultats du `network port reachability show -detail` commande permet d'identifier les ports qui ne sont pas en connexion.

Pour restaurer une LIF de cluster configurée sur un port qui n'est pas accessible aux autres ports configurés avec des LIFs de cluster, effectuez les opérations suivantes :

### Étapes

1. Réinitialiser le home port de la LIF de cluster sur le port correct :

```
network port modify -home-port
```

2. Retirer les ports qui ne disposent pas de LIFs de cluster configurées sur eux du cluster broadcast domain :

```
network port broadcast-domain remove-ports
```

3. Création du cluster :

```
cluster create
```

### Résultat

Une fois le cluster créé, le système détecte la configuration correcte et place les ports dans les domaines de diffusion appropriés.

### Supprimer une LIF

Vous pouvez supprimer une interface réseau (LIF) qui n'est plus requise.

#### Avant de commencer

Les LIFs à supprimer ne doivent pas être en cours d'utilisation.

### Étapes

1. Marquez les LIFs que vous souhaitez supprimer comme administrativement arrêtées à l'aide de la commande suivante :

```
network interface modify -vserver vservice_name -lif lif_name -status
-admin down
```

2. Utilisez le `network interface delete` Commande de suppression d'une ou de l'ensemble des LIFs :

| Si vous souhaitez supprimer... | Entrez la commande ...                                           |
|--------------------------------|------------------------------------------------------------------|
| Une LIF spécifique             | <code>network interface delete -vserver vs1 -lif lif_name</code> |
| Toutes les LIF                 | <code>network interface delete -vserver vs1 -lif *</code>        |

La commande suivante supprime le LIF `mgmtlif2` :

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. Utilisez le `network interface show` Commande pour confirmer que la LIF est supprimée.

## Équilibrer les charges réseau

### Vue d'ensemble du réseau d'équilibrage

Vous pouvez configurer votre cluster pour qu'il serve les demandes des clients à partir des LIFs chargées correctement. L'utilisation des LIF et des ports est ainsi plus équilibrée, ce qui permet d'améliorer les performances du cluster.

L'équilibrage de la charge DNS permet de sélectionner une LIF de données correctement chargée et d'équilibrer le trafic du réseau utilisateur sur tous les ports disponibles (physique, groupes d'interface et VLAN).

Avec l'équilibrage de la charge DNS, les LIFs sont associées à la zone d'équilibrage de charge d'un SVM. Un serveur DNS à l'échelle du site est configuré pour transférer toutes les requêtes DNS et renvoyer la LIF la moins chargée en fonction du trafic réseau et de la disponibilité des ressources des ports (utilisation du CPU, débit, connexions ouvertes, etc.). L'équilibrage de charge DNS offre les avantages suivants :

- Les nouvelles connexions client sont équilibrées sur les ressources disponibles.
- Aucune intervention manuelle n'est requise pour déterminer quelles LIFs à utiliser lors du montage d'un SVM particulier.
- Équilibrage de la charge DNS prenant en charge NFSv3, NFSv4, NFSv4.1, SMB 2.0, SMB 2.1, SMB 3.0 et S3.

### Fonctionnement de l'équilibrage de charge DNS

Les clients montent un SVM en spécifiant une adresse IP (associée à une LIF) ou un nom d'hôte (associé à plusieurs adresses IP). Par défaut, les LIFs sont sélectionnées par le serveur DNS à l'échelle du site de manière round-Robin, qui équilibre la charge de travail sur tous les LIFs.

L'équilibrage de charge round-Robin peut entraîner la surcharge de certaines LIF. Vous avez donc la possibilité d'utiliser une zone d'équilibrage de charge DNS qui gère la résolution host-name dans un SVM. L'utilisation

d'une zone d'équilibrage de charge DNS permet de mieux équilibrer les nouvelles connexions client sur les ressources disponibles, ce qui améliore les performances du cluster.

Une zone d'équilibrage de charge DNS est un serveur DNS au sein du cluster qui évalue dynamiquement la charge sur toutes les LIFs et renvoie un LIF chargé correctement. Dans une zone d'équilibrage de la charge, DNS attribue un poids (métrique), en fonction de la charge, à chaque LIF.

Un poids est attribué à chaque LIF en fonction de la charge des ports et de l'utilisation du CPU de son nœud de rattachement. Les LIF qui font partie de ports moins chargés ont plus de chances d'être renvoyées dans une requête DNS. Les poids peuvent également être attribués manuellement.

## Créer une zone d'équilibrage de charge DNS

Vous pouvez créer une zone d'équilibrage de charge DNS afin de faciliter la sélection dynamique d'une LIF basée sur la charge, c'est-à-dire le nombre de clients montés sur une LIF. Vous pouvez créer une zone d'équilibrage de la charge lors de la création d'une LIF de données.

### Avant de commencer

Le DNS Forwarder du serveur DNS à l'échelle du site doit être configuré pour transférer toutes les requêtes de la zone d'équilibrage de charge vers les LIFs configurées.

Article de la base de connaissances ["Configuration de l'équilibrage de charge DNS en Cluster-mode"](#) Sur le site de support NetApp, vous trouverez plus d'informations sur la configuration de l'équilibrage de la charge DNS à l'aide de la transmission conditionnelle.

### Description de la tâche

- Toute LIF de données peut répondre aux requêtes DNS pour un nom de zone d'équilibrage de charge DNS.
- Une zone d'équilibrage de charge DNS doit porter un nom unique dans le cluster, et le nom de zone doit répondre aux exigences suivantes :
  - Il ne doit pas dépasser 256 caractères.
  - Il doit inclure au moins une période.
  - Le premier et le dernier caractère ne doivent pas être un point ou tout autre caractère spécial.
  - Il ne peut pas inclure d'espace entre les caractères.
  - Chaque étiquette du nom DNS ne doit pas dépasser 63 caractères.

Un libellé est le texte qui apparaît avant ou après la période. Par exemple, la zone DNS nommée `storage.company.com` comporte trois étiquettes.

### Étape

Utilisez le `network interface create` commande avec `dns-zone` Option pour créer une zone d'équilibrage de charge DNS.

Si la zone d'équilibrage de charge existe déjà, le LIF le est ajouté. Pour plus d'informations sur la commande, reportez-vous à la ["Référence de commande ONTAP"](#).

L'exemple suivant montre comment créer une zone d'équilibrage de charge DNS nommée `storage.company.com` lors de la création de la LIF `lif1`:

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

## Ajout ou suppression d'une LIF d'une zone d'équilibrage de la charge

Vous pouvez ajouter ou supprimer une LIF de la zone DNS load balancing d'une machine virtuelle (SVM). Vous pouvez également supprimer toutes les LIFs simultanément d'une zone d'équilibrage de charge.

### Avant de commencer

- Toutes les LIFs d'une zone d'équilibrage de charge doivent appartenir au même SVM.
- Une LIF ne peut faire partie que d'une seule zone d'équilibrage de charge DNS.
- Si les LIF appartiennent à un sous-réseau différent, les groupes de basculement doivent avoir été configurés pour chaque sous-réseau.

### Description de la tâche

Une LIF qui est à l'état administratif down est temporairement supprimée de la zone d'équilibrage de la charge DNS. Lorsque la LIF revient au statut administratif up, elle est automatiquement ajoutée à la zone DNS d'équilibrage de la charge.

### Étape

Ajouter une LIF à ou supprimer une LIF d'une zone d'équilibrage de la charge :

| Les fonctions que vous recherchez... | Entrer...                                                                                                                                                                                                                                                                                 |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ajouter une LIF                      | <pre>network interface modify -vserver vs1 -lif lif1 -dns-zone storage.company.com</pre> <p>Exemple :</p> <pre>network interface modify -vserver vs1 -lif data1 -dns-zone cifs.company.com</pre>                                                                                          |
| Supprimer une seule LIF              | <pre>network interface modify -vserver vs1 -lif lif1 -dns-zone none</pre> <p>Exemple :</p> <pre>network interface modify -vserver vs1 -lif data1 -dns-zone none</pre>                                                                                                                     |
| Supprime toutes les LIFs             | <pre>network interface modify -vserver vs0 -lif * -dns-zone none</pre> <p>Exemple :</p> <pre>network interface modify -vserver vs0 -lif * -dns-zone none</pre> <p>Vous pouvez supprimer un SVM d'une zone d'équilibrage de charge en supprimant toutes les LIFs du SVM de cette zone.</p> |

## Configuration des services DNS (ONTAP 9.8 et versions ultérieures)

On doit configurer les services DNS pour le SVM avant de créer un serveur NFS ou SMB. En général, les serveurs de noms DNS sont des serveurs DNS intégrés à Active Directory pour le domaine auquel le serveur NFS ou SMB sera joint.

### Description de la tâche

Les serveurs DNS intégrés à Active Directory contiennent les enregistrements SRV (Service Location Records) pour les serveurs LDAP de domaine et de contrôleur de domaine. Si le SVM ne trouve pas les serveurs LDAP et les contrôleurs de domaine Active Directory, l'installation du serveur NFS ou SMB échoue.

Les SVM utilisent la base de données des services de nom d'hôtes ns-switch pour déterminer quels services de noms utiliser et dans quel ordre lors de la recherche d'informations sur les hôtes. Les deux services de noms pris en charge pour la base de données des hôtes sont des fichiers et dns.

Vous devez vous assurer que dns est l'une des sources avant de créer le serveur SMB.



Pour afficher les statistiques des services de noms DNS pour le processus mgwd et SECD, utilisez l'interface utilisateur Statistiques.

### Étapes

1. Déterminez la configuration actuelle de la base de données des services de noms des hôtes. Dans cet exemple, la base de données du service nom des hôtes utilise les paramètres par défaut.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Vserver: vs1 Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Effectuez les actions suivantes, si nécessaire.

- a. Ajoutez le service de noms DNS dans la base de données du service de noms d'hôtes dans l'ordre souhaité ou réorganisez les sources.

Dans cet exemple, la base de données hosts est configurée pour utiliser les fichiers DNS et locaux dans cet ordre.

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

- b. Vérifiez que la configuration des services de noms est correcte.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files
```

### 3. Configurez les services DNS.

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```



La commande `vserver services name-service dns create` effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP n'est pas en mesure de contacter le serveur name.

### 4. Vérifiez que la configuration DNS est correcte et que le service est activé.

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

### 5. Valider l'état des serveurs de noms.

```
vserver services name-service dns check -vserver vs1
```

| Vserver | Name Server | Status | Status Details          |
|---------|-------------|--------|-------------------------|
| vs1     | 10.0.0.50   | up     | Response time (msec): 2 |
| vs1     | 10.0.0.51   | up     | Response time (msec): 2 |

## Configuration de DNS dynamique sur le SVM

Si vous souhaitez que le serveur DNS intégré à Active Directory enregistre de manière dynamique les enregistrements DNS d'un serveur NFS ou SMB dans DNS, vous devez configurer le DNS dynamique (DDNS) sur le SVM.

### Avant de commencer

Les services de nom DNS doivent être configurés sur le SVM. Si vous utilisez DDNS sécurisé, vous devez utiliser des serveurs de noms DNS intégrés à Active Directory et vous devez avoir créé un serveur NFS ou SMB ou un compte Active Directory pour la SVM.

### Description de la tâche

Le nom de domaine complet (FQDN) spécifié doit être unique :

Le nom de domaine complet (FQDN) spécifié doit être unique :

- Pour NFS, valeur spécifiée dans `-vserver-fqdn` dans le cadre du `vserver services name-service dns dynamic-update` La commande devient le FQDN enregistré pour les LIFS.



- Pour SMB, les valeurs spécifiées comme nom NetBIOS du serveur CIFS et nom de domaine complet du serveur CIFS deviennent le FQDN enregistré pour les LIFS. Ceci n'est pas configurable dans ONTAP. Dans le scénario suivant, le FQDN du LIF est « CIFS\_VS1.EXAMPLE.COM »:

```
cluster1::> cifs server show -vserver vs1

Vserver: vs1
CIFS Server NetBIOS Name: CIFS_VS1
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
Workgroup Name: -
Kerberos Realm: -
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -
```



Pour éviter un échec de configuration d'un FQDN du SVM qui n'est pas conforme aux règles RFC pour les mises à jour DDNS, utilisez un nom de FQDN qui est conforme à RFC. Pour plus d'informations, voir ["RFC 1123"](#).

## Étapes

### 1. Configurer DDNS sur le SVM :

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is- enabled true [-use-secure {true|false}] -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Les astérisques ne peuvent pas être utilisés dans le cadre du FQDN personnalisé. Par exemple : \*.netapp.com n'est pas valide.

### 2. Vérifiez que la configuration DDNS est correcte :

```
vserver services name-service dns dynamic-update show
```

| Vserver | Is-Enabled | Use-Secure | Vserver FQDN    | TTL |
|---------|------------|------------|-----------------|-----|
| vs1     | true       | true       | vs1.example.com | 24h |

## Configuration des services DNS (ONTAP 9.7 et versions antérieures)

On doit configurer les services DNS pour le SVM avant de créer un serveur NFS ou SMB. En général, les serveurs de noms DNS sont des serveurs DNS intégrés à Active Directory pour le domaine auquel le serveur NFS ou SMB sera joint.

### Description de la tâche

Les serveurs DNS intégrés à Active Directory contiennent les enregistrements SRV (Service Location Records) pour les serveurs LDAP de domaine et de contrôleur de domaine. Si le SVM ne trouve pas les serveurs LDAP et les contrôleurs de domaine Active Directory, l'installation du serveur NFS ou SMB échoue.

Les SVM utilisent la base de données des services de nom d'hôtes `ns-switch` pour déterminer quels services de noms utiliser et dans quel ordre lors de la recherche d'informations sur les hôtes. Les deux services de noms pris en charge pour la base de données des hôtes sont `files` et `dns`.

Vous devez vous assurer que `dns` est l'une des sources avant de créer le serveur SMB.



Pour afficher les statistiques des services de noms DNS pour le processus `mgwd` et `SECD`, utilisez l'interface utilisateur Statistiques.

### Étapes

1. Déterminez la configuration actuelle du `hosts` base de données des services de noms.

Dans cet exemple, la base de données du service nom des hôtes utilise les paramètres par défaut.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Effectuez les actions suivantes, si nécessaire.

- a. Ajoutez le service de noms DNS dans la base de données du service de noms d'hôtes dans l'ordre souhaité ou réorganisez les sources.

Dans cet exemple, la base de données `hosts` est configurée pour utiliser les fichiers DNS et locaux dans cet ordre.

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

- a. Vérifiez que la configuration des services de noms est correcte.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

3. Configurez les services DNS.

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```



Les services Vserver name-service dns create Commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP n'est pas en mesure de contacter le serveur de noms.

4. Vérifiez que la configuration DNS est correcte et que le service est activé.

```
Vserver: vs1
Domains: example.com, example2.com Name
Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. Valider l'état des serveurs de noms.

```
vserver services name-service dns check -vserver vs1
```

| Vserver | Name Server | Status | Status Details          |
|---------|-------------|--------|-------------------------|
| vs1     | 10.0.0.50   | up     | Response time (msec): 2 |
| vs1     | 10.0.0.51   | up     | Response time (msec): 2 |

## Configuration de DNS dynamique sur le SVM

Si vous souhaitez que le serveur DNS intégré à Active Directory enregistre de manière dynamique les enregistrements DNS d'un serveur NFS ou SMB dans DNS, vous devez configurer le DNS dynamique (DDNS) sur le SVM.

### Avant de commencer

Les services de nom DNS doivent être configurés sur le SVM. Si vous utilisez DDNS sécurisé, vous devez utiliser des serveurs de noms DNS intégrés à Active Directory et vous devez avoir créé un serveur NFS ou SMB ou un compte Active Directory pour la SVM.

### Description de la tâche

Le nom de domaine complet (FQDN) spécifié doit être unique :

- Pour NFS, valeur spécifiée dans `-vserver-fqdn` dans le cadre du `vserver services name-service dns dynamic-update` La commande devient le FQDN enregistré pour les LIFS.
- Pour SMB, les valeurs spécifiées comme nom NetBIOS du serveur CIFS et nom de domaine complet du serveur CIFS deviennent le FQDN enregistré pour les LIFS. Ceci n'est pas configurable dans ONTAP. Dans le scénario suivant, le FQDN du LIF est « CIFS\_VS1.EXAMPLE.COM »:

```
cluster1::> cifs server show -vserver vs1
```

```

 Vserver: vs1
 CIFS Server NetBIOS Name: CIFS_VS1
 NetBIOS Domain/Workgroup Name: EXAMPLE
 Fully Qualified Domain Name: EXAMPLE.COM
 Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
 Workgroup Name: -
 Kerberos Realm: -
 Authentication Style: domain
 CIFS Server Administrative Status: up
 CIFS Server Description:
 List of NetBIOS Aliases: -
```



Pour éviter un échec de configuration d'un FQDN du SVM qui n'est pas conforme aux règles RFC pour les mises à jour DDNS, utilisez un nom de FQDN qui est conforme à RFC. Pour plus d'informations, voir ["RFC 1123"](#).

## Étapes

### 1. Configurer DDNS sur le SVM :

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is- enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Les astérisques ne peuvent pas être utilisés dans le cadre du FQDN personnalisé. Par exemple :  
\*.netapp.com n'est pas valide.

### 2. Vérifiez que la configuration DDNS est correcte :

```
vserver services name-service dns dynamic-update show
```

| Vserver | Is-Enabled | Use-Secure | Vserver FQDN    | TTL |
|---------|------------|------------|-----------------|-----|
| vs1     | true       | true       | vs1.example.com | 24h |

## Configuration des services DNS dynamiques

Si vous souhaitez que le serveur DNS intégré à Active Directory enregistre de manière dynamique les enregistrements DNS d'un serveur NFS ou SMB dans DNS, vous devez configurer le DNS dynamique (DDNS) sur le SVM.

## Avant de commencer

Les services de nom DNS doivent être configurés sur le SVM. Si vous utilisez DDNS sécurisé, vous devez utiliser des serveurs de noms DNS intégrés à Active Directory et vous devez avoir créé un serveur NFS ou SMB ou un compte Active Directory pour la SVM.

## Description de la tâche

Le FQDN spécifié doit être unique.



Pour éviter un échec de configuration d'un FQDN du SVM qui n'est pas conforme aux règles RFC pour les mises à jour DDNS, utilisez un nom de FQDN qui est conforme à RFC.

## Étapes

1. Configurer DDNS sur le SVM :

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is-enabled true [-use-secure {true|false}] -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is-
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Les astérisques ne peuvent pas être utilisés dans le cadre du FQDN personnalisé. Par exemple :  
\*.netapp.com n'est pas valide.

2. Vérifiez que la configuration DDNS est correcte :

```
vserver services name-service dns dynamic-update show
```

| Vserver | Is-Enabled | Use-Secure | Vserver FQDN    | TTL |
|---------|------------|------------|-----------------|-----|
| vs1     | true       | true       | vs1.example.com | 24h |

# Résolution du nom d'hôte

## Présentation de la résolution du nom d'hôte

ONTAP doit être en mesure de traduire des noms d'hôtes en adresses IP numériques afin de fournir un accès aux clients et d'accéder aux services. Pour résoudre les informations relatives aux hôtes, il est nécessaire de configurer des SVM (Storage Virtual machines) afin d'utiliser des services de noms locaux ou externes. ONTAP prend en charge la configuration d'un serveur DNS externe ou la configuration du fichier hosts local pour la résolution du nom d'hôte.

Lorsque vous utilisez un serveur DNS externe, vous pouvez configurer le DNS dynamique (DDNS), qui envoie automatiquement des informations DNS nouvelles ou modifiées de votre système de stockage au serveur DNS. Sans mises à jour DNS dynamiques, vous devez ajouter manuellement des informations DNS (nom DNS et adresse IP) aux serveurs DNS identifiés lorsqu'un nouveau système est mis en ligne ou lorsqu'une information DNS existante change. Ce processus est lent et sujet aux erreurs. Pendant la reprise sur incident,

la configuration manuelle peut avoir de longs temps d'indisponibilité.

## Configurez le DNS pour la résolution du nom d'hôte

Vous utilisez DNS pour accéder aux sources locales ou distantes pour obtenir des informations sur l'hôte. Vous devez configurer DNS pour accéder à l'une de ces sources, ou aux deux.

ONTAP doit être en mesure de rechercher les informations relatives à l'hôte afin de fournir aux clients un accès approprié. Vous devez configurer les services de noms pour permettre à ONTAP d'accéder aux services DNS locaux ou externes afin d'obtenir les informations sur l'hôte.

ONTAP stocke les informations de configuration du service de noms dans un tableau équivalent à `/etc/nsswitch.conf` Fichier sur les systèmes UNIX.

### Configurer un SVM et des LIFs de données pour la résolution de nom d'hôte à l'aide d'un serveur DNS externe

Vous pouvez utiliser le `vserver services name-service dns` Commande permettant d'activer DNS sur un SVM et de le configurer afin d'utiliser DNS pour la résolution de nom d'hôte. Les noms d'hôte sont résolus à l'aide de serveurs DNS externes.

#### Avant de commencer

Un serveur DNS au niveau du site doit être disponible pour les recherches de noms d'hôte.

Vous devez configurer plusieurs serveurs DNS pour éviter un point de défaillance unique. Le `vserver services name-service dns create` Commande émet un avertissement si vous entrez un seul nom de serveur DNS.

#### Description de la tâche

Voir [Configuration des services DNS dynamiques](#) Pour plus d'informations sur la configuration de DNS dynamique sur le SVM.

#### Étapes

1. Activer le DNS sur le SVM :

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

La commande suivante permet d'activer les serveurs DNS externes sur le SVM vs1 :

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



Le `vserver services name-service dns create` Commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP ne parvient pas à contacter le serveur de noms.

2. Validez l'état des serveurs de noms à l'aide de la `vserver services name-service dns check` commande.

```
vserver services name-service dns check -vserver vs1.example.com
```

|                 |             | Name Server |                         |
|-----------------|-------------|-------------|-------------------------|
| Vserver         | Name Server | Status      | Status Details          |
| vs1.example.com | 10.0.0.50   | up          | Response time (msec): 2 |
| vs1.example.com | 10.0.0.51   | up          | Response time (msec): 2 |

Pour plus d'informations sur les stratégies de service liées à DNS, reportez-vous à la section ["LIF et politiques de services dans ONTAP 9.6 et versions ultérieures"](#).

### Configurez la table du commutateur de service de noms pour la résolution du nom d'hôte

Vous devez configurer correctement la table du commutateur de service de noms pour permettre à ONTAP de consulter le service de noms local ou externe afin de récupérer les informations relatives à l'hôte.

#### Avant de commencer

Vous devez avoir déterminé le service de nom à utiliser pour le mappage des hôtes dans votre environnement.

#### Étapes

1. Ajoutez les entrées nécessaires à la table de changement de nom du service :

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. Vérifiez que le tableau des commutateurs de service de noms contient les entrées attendues dans l'ordre souhaité :

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

#### Exemple

L'exemple suivant modifie une entrée dans la table des switches de service de noms pour SVM vs1 afin d'utiliser d'abord le fichier hosts local, puis un serveur DNS externe pour résoudre les noms d'hôtes :

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

### Gestion de la table hosts (administrateurs du cluster uniquement)

Un administrateur de cluster peut ajouter, modifier, supprimer et afficher les entrées de nom d'hôte dans le tableau hosts de la machine virtuelle de stockage (SVM) admin. Un

administrateur SVM peut configurer les entrées de nom d'hôte uniquement pour la SVM attribuée.

### Commandes permettant de gérer les entrées locales de nom d'hôte

Vous pouvez utiliser le `vserver services name-service dns hosts` Commande pour créer, modifier ou supprimer des entrées de table hôte DNS.

Lorsque vous créez ou modifiez les entrées de nom d'hôte DNS, vous pouvez spécifier plusieurs adresses d'alias séparées par des virgules.

| Les fonctions que vous recherchez...   | Utilisez cette commande...                                  |
|----------------------------------------|-------------------------------------------------------------|
| Créez une entrée de nom d'hôte DNS     | <code>vserver services name-service dns hosts create</code> |
| Modifier une entrée de nom d'hôte DNS  | <code>vserver services name-service dns hosts modify</code> |
| Supprimer une entrée de nom d'hôte DNS | <code>vserver services name-service dns hosts delete</code> |

Pour plus d'informations sur les `vserver services name-service dns hosts` commandes, reportez-vous à la section "[Référence de commande ONTAP](#)".

## Sécurisez votre réseau

### Configurer la sécurité des réseaux à l'aide des normes de traitement des informations fédérales (FIPS)

ONTAP est conforme à la norme FIPS 140-2 (Federal Information Processing Standards) pour toutes les connexions SSL. Vous pouvez activer et désactiver le mode SSL FIPS, définir globalement les protocoles SSL et désactiver tout chiffrement faible tel que RC4 au sein de ONTAP.

Par défaut, SSL sur ONTAP est défini avec la conformité FIPS désactivée et le protocole SSL activé avec les éléments suivants :

- TLSv1.3 (à partir de ONTAP 9.11.1)
- TLSv1.2
- TLSv1.1
- TLSv1

Lorsque le mode SSL FIPS est activé, la communication SSL de ONTAP à des clients externes ou des composants de serveur en dehors de ONTAP utilise une fonctionnalité crypto pour SSL conforme à la norme FIPS.

Si vous souhaitez que les comptes d'administrateur accèdent aux SVM avec une clé publique SSH, vous



devez vous assurer que l'algorithme de clé hôte est pris en charge avant d'activer le mode SSL FIPS.

**Remarque :** la prise en charge de l'algorithme de clé hôte a changé dans ONTAP 9.11.1 et versions ultérieures.

| Version de ONTAP               | Types de clés pris en charge       | Types de clés non pris en charge                                  |
|--------------------------------|------------------------------------|-------------------------------------------------------------------|
| 9.11.1 et versions ultérieures | ecdsa-sha2-nistp256                | rsa-sha2-512<br>rsa-sha2-256<br>ssh-ed25519<br>ssh-dss<br>ssh-rsa |
| 9.10.1 et versions antérieures | ecdsa-sha2-nistp256<br>ssh-ed25519 | ssh-dss<br>ssh-rsa                                                |

Les comptes de clés publiques SSH existants sans les algorithmes de clé pris en charge doivent être reconfigurés avec un type de clé pris en charge avant l'activation de FIPS, sinon l'authentification de l'administrateur échoue.

Pour plus d'informations, voir ["Activez les comptes de clé publique SSH"](#).

Pour plus d'informations sur la configuration du mode SSL FIPS, reportez-vous au `security config modify` page de manuel.

## Activez FIPS

Il est recommandé que tous les utilisateurs sécurisés ajustent leur configuration de sécurité immédiatement après l'installation ou la mise à niveau du système. Lorsque le mode SSL FIPS est activé, la communication SSL de ONTAP à des clients externes ou des composants de serveur en dehors de ONTAP utilise une fonctionnalité crypto pour SSL conforme à la norme FIPS.



Lorsque FIPS est activé, vous ne pouvez ni installer ni créer de certificat avec une clé RSA d'une longueur de 4096.

## Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Activer FIPS :

```
security config modify -interface SSL -is-fips-enabled true
```

3. Lorsque vous êtes invité à continuer, entrez `y`

4. Si vous exécutez ONTAP 9.8 ou une version antérieure, redémarrez manuellement chaque nœud du cluster, un à un. Depuis ONTAP 9.9.1, un redémarrage n'est pas nécessaire.

## Exemple

Si vous exécutez ONTAP 9.9.1 ou une version ultérieure, le message d'avertissement ne s'affiche pas.

```
security config modify -interface SSL -is-fips-enabled true
```

Warning: This command will enable FIPS compliance and can potentially cause some non-compliant components to fail. MetroCluster and Vserver DR require FIPS to be enabled on both sites in order to be compatible.

Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster. This is necessary to prevent components from failing due to an inconsistent security configuration state in the cluster. To avoid a service outage, reboot one node at a time and wait for it to completely initialize before rebooting the next node. Run "security config status show" command to monitor the reboot status.

Do you want to continue? {y|n}: y

## Désactivez FIPS

Si vous exécutez toujours une ancienne configuration système et que vous souhaitez configurer ONTAP avec compatibilité descendante, vous pouvez activer SSLv3 uniquement lorsque FIPS est désactivé.

### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Désactiver FIPS en tapant :

```
security config modify -interface SSL -is-fips-enabled false
```

3. Lorsque vous êtes invité à continuer, entrez y.
4. Si vous exécutez ONTAP 9.8 ou une version antérieure, redémarrez manuellement chaque nœud du cluster. Depuis ONTAP 9.9.1, un redémarrage n'est pas nécessaire.

### Exemple

Si vous exécutez ONTAP 9.9.1 ou une version ultérieure, le message d'avertissement ne s'affiche pas.

```
security config modify -interface SSL -supported-protocols SSLv3
```

Warning: Enabling the SSLv3 protocol may reduce the security of the interface, and is not recommended.

Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster. This is necessary to prevent components from failing due to an inconsistent security configuration state in the cluster. To avoid a service outage, reboot one node at a time and wait for it to completely initialize before rebooting the next node. Run "security config status show" command to monitor the reboot status.

Do you want to continue? {y|n}: y

## Affichez l'état de conformité FIPS

Vous pouvez vérifier si le cluster entier exécute les paramètres de configuration de sécurité actuels.

### Étapes

1. Redémarrez chaque nœud un par un dans le cluster.

Ne redémarrez pas tous les nœuds du cluster simultanément. Un redémarrage est requis pour s'assurer que toutes les applications du cluster exécutent la nouvelle configuration de sécurité et que toutes les modifications apportées au mode FIPS on/off, aux protocoles et au chiffrement.

2. Afficher le statut de conformité actuel :

```
security config show
```

```
security config show
```

|           | Cluster   |                         | Cluster                  |
|-----------|-----------|-------------------------|--------------------------|
| Security  |           |                         |                          |
| Interface | FIPS Mode | Supported Protocols     | Supported Ciphers Config |
| Ready     |           |                         |                          |
| -----     | -----     | -----                   | -----                    |
| -----     |           |                         |                          |
| SSL       | false     | TLSv1_2, TLSv1_1, TLSv1 | ALL:!LOW:!aNULL: yes     |
|           |           |                         | !EXP:!eNULL              |

## Configurez la sécurité IP (IPsec) sur le cryptage filaire

ONTAP utilise IPsec en mode de transport pour assurer la sécurité et le chiffrement en continu des données, même en transit. IPsec offre le cryptage des données pour tout le trafic IP, y compris les protocoles NFS, iSCSI et SMB.

À partir de ONTAP 9.12.1, la prise en charge IPsec du protocole hôte frontal est disponible dans les configurations MetroCluster IP et MetroCluster reliées à la structure.

La prise en charge IPsec dans les clusters MetroCluster est limitée au trafic hôte frontal et n'est pas prise en charge sur les LIF intercluster MetroCluster.

À partir de ONTAP 9.10.1, vous pouvez utiliser des clés prépartagées (PSK) ou des certificats pour l'authentification avec IPsec. Auparavant, seuls les PSK étaient pris en charge par IPsec.

À partir de ONTAP 9.9.1, les algorithmes de cryptage utilisés par IPsec sont validés par la norme FIPS 140-2. Les algorithmes sont générés par le module de chiffrement NetApp dans ONTAP qui assure la validation FIPS 140-2-2.

À partir de ONTAP 9.8, ONTAP prend en charge IPsec en mode transport.

Une fois IPsec configuré, le trafic réseau entre le client et ONTAP est protégé par des mesures préventives pour lutter contre les attaques par replay et les attaques de l'homme au milieu.

Pour le cryptage NetApp SnapMirror et du trafic de peering de clusters, le cryptage de peering de clusters (CPE), la sécurité de la couche de transport (TLS) est toujours recommandée sur IPsec afin de garantir la sécurité en transit sur le réseau. Ceci est dû au fait que TLS offre de meilleures performances que IPsec.

Bien que la fonctionnalité IPsec soit activée sur le cluster, le réseau nécessite une entrée SPD (Security Policy Database) pour correspondre au trafic à protéger et pour spécifier les détails de protection (tels que la suite de chiffrement et la méthode d'authentification) avant que le trafic ne puisse circuler. Une entrée SPD correspondante est également nécessaire sur chaque client.

## Activez IPsec sur le cluster

Vous pouvez activer IPsec sur le cluster pour vous assurer que les données sont continuellement sécurisées et cryptées, même en transit.

### Étapes

1. Découvrez si IPsec est déjà activé :

```
security ipsec config show
```

Si le résultat inclut `IPsec Enabled: false`, passez à l'étape suivante.

2. Activer IPsec :

```
security ipsec config modify -is-enabled true
```

3. Exécutez à nouveau la commande de découverte :

```
security ipsec config show
```

Le résultat inclut maintenant `IPsec Enabled: true`.

## Préparez la création de stratégies IPsec avec l'authentification par certificat

Vous pouvez ignorer cette étape si vous utilisez uniquement des clés prépartagées (PSK) pour l'authentification et que vous n'utilisez pas l'authentification par certificat.

Avant de créer une stratégie IPsec qui utilise des certificats pour l'authentification, vous devez vérifier que les

conditions préalables suivantes sont remplies :

- ONTAP et le client doivent avoir installé le certificat CA de l'autre partie afin que les certificats de l'entité finale (ONTAP ou le client) soient vérifiables des deux côtés
- Un certificat est installé pour la LIF de ONTAP qui participe à la politique



Les LIF ONTAP peuvent partager des certificats. Un mappage un-à-un entre les certificats et les LIFs n'est pas nécessaire.

## Étapes

1. Installez tous les certificats de l'autorité de certification utilisés lors de l'authentification mutuelle, y compris les autorités de certification côté ONTAP et côté client, dans la gestion des certificats ONTAP, sauf s'il est déjà installé (comme c'est le cas pour une autorité de certification racine auto-signée ONTAP).

### Commande exemple

```
cluster::> security certificate install -vserver svm_name -type server-ca
-cert-name my_ca_cert
```

2. Pour vous assurer que l'autorité de certification installée se trouve dans le chemin de recherche de l'autorité de certification IPSec lors de l'authentification, ajoutez les autorités de certification de gestion de certificat ONTAP au module IPSec à l'aide du `security ipsec ca-certificate add` commande.

### Commande exemple

```
cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
my_ca_cert
```

3. Créez et installez un certificat pour une utilisation par le LIF ONTAP. L'autorité de certification de l'émetteur de ce certificat doit déjà être installée sur ONTAP et ajoutée à IPSec.

### Commande exemple

```
cluster::> security certificate install -vserver svm_name -type server -cert
-name my_nfs_server_cert
```

Pour plus d'informations sur les certificats dans ONTAP, consultez les commandes de certificat de sécurité dans la documentation de ONTAP 9 .

## Définir la base de données de règles de sécurité (SPD)

IPSec requiert une entrée SPD avant d'autoriser le trafic à circuler sur le réseau. Ceci est vrai si vous utilisez un PSK ou un certificat pour l'authentification.

## Étapes

1. Utilisez le `security ipsec policy create` commande pour :
  - a. Sélectionnez l'adresse IP ONTAP ou le sous-réseau d'adresses IP pour participer au transport IPSec.
  - b. Sélectionnez les adresses IP des clients qui se connectent aux adresses IP ONTAP.



Le client doit prendre en charge Internet Key Exchange version 2 (IKEv2) avec une clé pré-partagée (PSK).

- c. Facultatif. Sélectionnez les paramètres de trafic à granularité fine, tels que les protocoles de couche supérieure (UDP, TCP, ICMP, etc.) , les numéros de port local et les numéros de port distant pour

protéger le trafic. Les paramètres correspondants sont `protocols`, `local-ports` et `remote-ports` respectivement.

Ignorez cette étape pour protéger tout le trafic entre l'adresse IP ONTAP et l'adresse IP du client. La protection de tout le trafic est la valeur par défaut.

- d. Entrez PSK ou PKI (public-Key Infrastructure) pour le `auth-method` paramètre de la méthode d'authentification souhaitée.
  - i. Si vous entrez une clé PSK, incluez les paramètres, puis appuyez sur <enter> pour que l'invite vous demande d'entrer et de vérifier la clé pré-partagée.



`local-identity` et `remote-identity` Les paramètres sont facultatifs si l'hôte et le client utilisent StrongSwan et qu'aucune règle générique n'est sélectionnée pour l'hôte ou le client.

- ii. Si vous entrez une PKI, vous devez également entrer `cert-name`, `local-identity`, `remote-identity` paramètres. Si l'identité du certificat côté distant est inconnue ou si plusieurs identités client sont attendues, entrez l'identité spéciale `ANYTHING`.

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

Le trafic IP ne peut pas circuler entre le client et le serveur tant que ONTAP et le client n'ont pas configuré les stratégies IPsec correspondantes et que les informations d'identification d'authentification (PSK ou certificat) ne sont pas en place des deux côtés. Pour plus de détails, reportez-vous à la configuration IPsec côté client.

## Utiliser les identités IPsec

Pour la méthode d'authentification par clé pré-partagée, les identités locales et distantes sont facultatives si l'hôte et le client utilisent StrongSwan et qu'aucune règle générique n'est sélectionnée pour l'hôte ou le client.

Pour la méthode d'authentification PKI/certificat, les identités locales et distantes sont obligatoires. Les identités spécifient quelle identité est certifiée dans le certificat de chaque côté et sont utilisées dans le processus de vérification. Si l'identité distante est inconnue ou si elle peut être de nombreuses identités différentes, utilisez l'identité spéciale `ANYTHING`.

## Description de la tâche

Au sein de ONTAP, les identités sont spécifiées en modifiant l'entrée du démon du processeur de service ou pendant sa création. Le démon du processeur de service peut être un nom d'identité avec une adresse IP ou un format de chaîne.

## Étape

Pour modifier un paramètre d'identité SPD existant, utilisez la commande suivante :

```
security ipsec policy modify
```

### Commande exemple

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity
192.168.134.34 -remote-identity client.fooboo.com
```

## Configuration client multiple IPsec

Lorsqu'un petit nombre de clients doivent utiliser IPsec, l'utilisation d'une seule entrée SPD pour chaque client est suffisante. Toutefois, lorsque des centaines voire des milliers de clients doivent utiliser IPsec, NetApp recommande l'utilisation d'une configuration client multiple IPsec.

### Description de la tâche

ONTAP prend en charge la connexion de plusieurs clients sur de nombreux réseaux à une seule adresse IP de SVM avec IPsec activé. Vous pouvez effectuer cette opération en utilisant l'une des méthodes suivantes :

- **Configuration du sous-réseau**

Pour permettre à tous les clients d'un sous-réseau particulier (192.168.134.0/24 par exemple) de se connecter à une seule adresse IP de SVM à l'aide d'une seule entrée de la politique SPD, vous devez spécifier le `remote-ip-subnets` sous-réseau. De plus, vous devez spécifier le `remote-identity` champ avec l'identité côté client correcte.



Lors de l'utilisation d'une seule entrée de stratégie dans une configuration de sous-réseau, les clients IPsec de ce sous-réseau partagent l'identité IPsec et la clé pré-partagée (PSK). Cependant, ceci n'est pas vrai avec l'authentification par certificat. Lors de l'utilisation de certificats, chaque client peut utiliser son propre certificat unique ou un certificat partagé pour s'authentifier. ONTAP IPsec vérifie la validité du certificat en fonction des autorités de certification installées dans son magasin de confiance local. ONTAP prend également en charge la vérification de la liste de révocation de certificats (CRL).

- **Autoriser la configuration de tous les clients**

Pour permettre à n'importe quel client, quelle que soit son adresse IP source, de se connecter à l'adresse IP du SVM IPsec, utilisez l' `0.0.0.0/0` caractère générique lors de la spécification du `remote-ip-subnets` légale.

De plus, vous devez spécifier le `remote-identity` champ avec l'identité côté client correcte. Pour l'authentification par certificat, vous pouvez entrer `ANYTHING`.

Aussi, lorsque le `0.0.0.0/0` le caractère générique est utilisé, vous devez configurer un numéro de port local ou distant spécifique à utiliser. Par exemple : `NFS port 2049`.

### Étapes

- Utilisez l'une des commandes suivantes pour configurer IPsec pour plusieurs clients.
  - Si vous utilisez **subnet configuration** pour prendre en charge plusieurs clients IPsec :

```
security ipsec policy create -vserver vs1 -name policy_name
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
```

```
IP_address/subnet -local-identity local_id -remote-identity remote_id
```

### Commande exemple

```
security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
ontap_side_identity -remote-identity client_side_identity
```

- i. Si vous utilisez **Autoriser la configuration de tous les clients** à prendre en charge plusieurs clients IPsec :

```
security ipsec policy create -vserver vserver_name -name policy_name
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
-ports port_number -local-identity local_id -remote-identity remote_id
```

### Commande exemple

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

## Statistiques IPsec

Lors de la négociation, un canal de sécurité appelé Association de sécurité IKE (sa) peut être établi entre l'adresse IP du SVM ONTAP et l'adresse IP du client. IPSec SAS est installé sur les deux noeuds finaux pour effectuer le cryptage et le décryptage des données.

Vous pouvez utiliser les commandes de statistiques pour vérifier l'état des ports SAS IPsec et SAS IKE.

### Exemples de commandes

IKE sa exemple de commande :

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

Exemple de commande et de sortie IPsec sa :

```
security ipsec show-ipseca -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
```

| Vserver | Policy Name | Local Address  | Remote Address | Initiator-SPI    | State       |
|---------|-------------|----------------|----------------|------------------|-------------|
| vs1     | test34      | 192.168.134.34 | 192.168.134.44 | c764f9ee020cec69 | ESTABLISHED |

Exemple de commande et de sortie IPsec sa :



```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
 Policy Local Remote Inbound Outbound
Vserver Name Address Address SPI SPI
State

vs1 test34
 192.168.134.34 192.168.134.44 c4c5b3d6 c2515559
INSTALLED
```

## Configuration des politiques de pare-feu pour les LIF

La configuration d'un pare-feu améliore la sécurité du cluster et permet d'empêcher tout accès non autorisé au système de stockage. Par défaut, le pare-feu intégré est configuré pour autoriser l'accès à distance à un ensemble spécifique de services IP pour les données, la gestion et les LIF intercluster.

À partir d'ONTAP 9.10.1 :

- Les politiques de pare-feu sont obsolètes et sont remplacées par les politiques de service LIF. Auparavant, le pare-feu intégré était géré à l'aide de politiques de pare-feu. Cette fonctionnalité s'effectue désormais à l'aide d'une politique de service LIF.
- Toutes les politiques de pare-feu sont vides et n'ouvrent aucun port dans le pare-feu sous-jacent. En revanche, tous les ports doivent être ouverts via une règle de service LIF.
- Aucune action n'est requise après une mise à niveau vers la version 9.10.1 ou ultérieure afin de passer des politiques de pare-feu aux politiques de service LIF. Le système construit automatiquement des politiques de service LIF conformes aux politiques de pare-feu utilisées dans la version précédente de ONTAP. Si vous utilisez des scripts ou d'autres outils qui créent et gèrent des politiques de pare-feu personnalisées, vous devrez peut-être mettre à niveau ces scripts pour créer des stratégies de service personnalisées.

Pour en savoir plus, voir ["LIF et politiques de services dans ONTAP 9.6 et versions ultérieures"](#).

Les politiques de pare-feu peuvent être utilisées pour contrôler l'accès aux protocoles de service de gestion tels que SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPs, RSH, DNS OU SNMP. Les politiques de pare-feu ne peuvent pas être définies pour des protocoles de données tels que NFS ou SMB.

Vous pouvez gérer le service et les politiques de pare-feu des manières suivantes :

- Activation ou désactivation du service de pare-feu
- Affichage de la configuration actuelle du service de pare-feu
- Création d'une nouvelle politique de pare-feu avec le nom de la politique et les services réseau spécifiés
- Application d'une politique de pare-feu à une interface logique
- Création d'une nouvelle politique de pare-feu qui est une copie exacte d'une politique existante

Vous pouvez l'utiliser pour créer une politique avec des caractéristiques similaires au sein d'une même SVM ou pour copier la politique dans une autre SVM.

- Affichage d'informations sur les politiques de pare-feu
- Modification des adresses IP et des masques de réseau utilisés par une politique de pare-feu
- Suppression d'une politique de pare-feu qui n'est pas utilisée par une LIF

## Politiques de pare-feu et LIF

Les politiques de pare-feu de LIF sont utilisées pour restreindre l'accès au cluster sur chaque LIF. Vous devez comprendre comment la politique de pare-feu par défaut affecte l'accès au système sur chaque type de LIF, et comment personnaliser une politique de pare-feu pour augmenter ou diminuer la sécurité par rapport à une LIF.

Lors de la configuration d'une LIF à l'aide du `network interface create` ou `network interface modify` commande, valeur spécifiée pour le `-firewall-policy` Paramètre détermine les protocoles de service et les adresses IP autorisés à accéder à la LIF.

Dans de nombreux cas, vous pouvez accepter la valeur de la stratégie de pare-feu par défaut. Dans d'autres cas, vous devrez peut-être restreindre l'accès à certaines adresses IP et à certains protocoles de service de gestion. Les protocoles de service de gestion disponibles sont : SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPs, RSH, DNS ET SNMP.

La politique de pare-feu de toutes les LIFs de cluster est par défaut définie sur "" et ne peut pas être modifié.

Le tableau ci-dessous décrit les politiques de pare-feu par défaut qui sont attribuées à chaque LIF, en fonction de leur rôle (ONTAP 9.5 et versions antérieures) ou de la politique de service (ONTAP 9.6 et versions ultérieures) lors de la création de cette LIF :

| Politique de pare-feu | Protocoles de service par défaut                       | Accès par défaut          | LIFs appliquées à                                                             |
|-----------------------|--------------------------------------------------------|---------------------------|-------------------------------------------------------------------------------|
| gstin                 | dns, http, https, ndmp, ndmps, ntp, snmp, ssh          | Toute adresse (0.0.0.0/0) | Gestion du cluster, gestion SVM et LIF de node-management                     |
| gestion-nfs           | dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh | Toute adresse (0.0.0.0/0) | LIF de données qui prennent également en charge l'accès à la gestion des SVMs |
| intercluster          | https, ndmp, ndmps                                     | Toute adresse (0.0.0.0/0) | Toutes les LIFs intercluster                                                  |
| les données           | dns, ndmp, ndmps, portmap                              | Toute adresse (0.0.0.0/0) | Toutes les LIF de données                                                     |

## Configuration du service portmap

Le service portmap mappe les services RPC aux ports sur lesquels ils écoutent.

Le service portmap était toujours accessible à ONTAP 9.3 et versions antérieures, est devenu configurable

dans ONTAP 9.4 à ONTAP 9.6 et est géré automatiquement à partir de ONTAP 9.7.

- Dans ONTAP 9.3 et versions antérieures, le service portmap (rpcbind) était toujours accessible sur le port 111 dans les configurations réseau qui s'appuyaient sur le pare-feu ONTAP intégré plutôt qu'un pare-feu tiers.
- De ONTAP 9.4 à ONTAP 9.6, vous pouvez modifier les politiques de pare-feu pour contrôler si le service portmap est accessible sur des LIF spécifiques.
- Depuis ONTAP 9.7, le service de pare-feu de portmap est supprimé. En revanche, le port portmap est ouvert automatiquement pour toutes les LIF qui prennent en charge le service NFS.

### **Le service portmap est configurable dans le pare-feu de ONTAP 9.4 à ONTAP 9.6.**

Le reste de cette rubrique explique comment configurer le service de pare-feu portmap pour ONTAP 9.4 à ONTAP 9.6.

En fonction de votre configuration, vous pouvez disautoriser l'accès au service sur des types spécifiques de LIF, généralement les LIF intercluster et de gestion. Dans certains cas, vous pourriez même refuser l'accès aux LIF de données.

#### **Quel comportement pouvez-vous attendre**

Les ONTAP 9.4 à ONTAP 9.6 Behavior ont été conçus pour offrir une transition transparente lors de la mise à niveau. Si le service portmap est déjà accessible sur des types spécifiques de LIF, il sera toujours accessible sur ces types de LIF. Comme dans ONTAP 9.3 et versions antérieures, vous pouvez spécifier les services accessibles à l'intérieur du pare-feu dans la politique de pare-feu pour le type de LIF.

Pour que le comportement soit effectif, tous les nœuds du cluster doivent exécuter ONTAP 9.4 à ONTAP 9.6. Seul le trafic entrant est affecté.

Les nouvelles règles sont les suivantes :

- Lors de la mise à niveau vers les versions 9.4 à 9.6, ONTAP ajoute le service portmap à toutes les politiques de pare-feu existantes, par défaut ou personnalisées.
- Lorsque vous créez un cluster ou un nouvel IPspace, ONTAP ajoute le service portmap uniquement à la politique de données par défaut, et non aux politiques de gestion par défaut ou intercluster.
- Vous pouvez ajouter le service portmap aux règles par défaut ou personnalisées selon vos besoins, puis supprimer le service selon vos besoins.

#### **Comment ajouter ou supprimer le service portmap**

Pour ajouter le service de mappage de port à une SVM ou à une politique de pare-feu de cluster (le rendre accessible via le pare-feu), entrez :

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Pour supprimer le service portmap d'une SVM ou d'une politique de pare-feu de cluster (celle-ci doit être inaccessible au sein du pare-feu), entrez :

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Vous pouvez utiliser la commande `network interface modify` pour appliquer la politique de pare-feu à une LIF existante. Pour obtenir la syntaxe complète de la commande, reportez-vous à la ["Référence de commande ONTAP"](#).

## Créer une politique de pare-feu et l'affecter à une LIF

Des politiques de pare-feu par défaut sont attribuées à chaque LIF lorsque vous créez la LIF. Dans de nombreux cas, les paramètres par défaut du pare-feu fonctionnent bien et vous n'avez pas besoin de les modifier. Si vous souhaitez modifier les services réseau ou les adresses IP pouvant accéder à une LIF, vous pouvez créer une politique de pare-feu personnalisée et l'affecter à la LIF.

### Description de la tâche

- Vous ne pouvez pas créer de politique de pare-feu avec `policy` nom `data`, `intercluster`, `cluster`, ou `mgmt`.

Ces valeurs sont réservées aux politiques de pare-feu définies par le système.

- Vous ne pouvez ni définir ni modifier une politique de pare-feu pour les LIFs de `cluster`.

La politique de pare-feu des LIFs de `cluster` est définie sur `0.0.0.0/0` pour tous les types de services.

- Si vous avez besoin de supprimer un service d'une politique, vous devez supprimer la politique de pare-feu existante et en créer une nouvelle.
- Si IPv6 est activé sur le `cluster`, vous pouvez créer des politiques de pare-feu avec des adresses IPv6.

Une fois IPv6 activé, `data`, `intercluster`, et `mgmt` Les politiques de pare-feu incluent `::/0`, le caractère générique IPv6, dans leur liste d'adresses acceptées.

- Lorsque vous utilisez System Manager pour configurer la fonctionnalité de protection des données sur les clusters, vous devez vous assurer que les adresses IP LIF `intercluster` sont incluses dans la liste des autorisés et que le service HTTPS est autorisé sur les LIF `intercluster` et sur les pare-feu de votre entreprise.

Par défaut, le `intercluster` La politique de pare-feu permet l'accès à partir de toutes les adresses IP (`0.0.0.0/0`, ou `::/0` pour IPv6) et active les services HTTPS, NDMP et NDMPs. Si vous modifiez cette politique par défaut ou si vous créez votre propre politique de pare-feu pour les LIF `intercluster`, vous devez ajouter chaque adresse IP LIF `intercluster` à la liste des autorisés et activer le service HTTPS.

- Depuis ONTAP 9.6, les services de pare-feu HTTPS et SSH ne sont pas pris en charge.

Dans ONTAP 9.6, le `management-https` et `management-ssh` Les services LIF sont disponibles pour l'accès à la gestion HTTPS et SSH.

### Étapes

1. Créer une politique de pare-feu qui sera disponible pour les LIF sur un SVM spécifique :

```
system services firewall policy create -vserver vservice_name -policy
policy_name -service network_service -allow-list ip_address/mask
```

Vous pouvez utiliser cette commande plusieurs fois pour ajouter plusieurs services réseau et une liste d'adresses IP autorisées pour chaque service de la politique de pare-feu.

2. Vérifiez que la stratégie a été correctement ajoutée en utilisant le `system services firewall policy show` commande.

3. Appliquer la politique de pare-feu à une LIF :

```
network interface modify -vserver vservice_name -lif lif_name -firewall-policy
```

*policy\_name*

4. Vérifier que la policy a été correctement ajoutée à la LIF à l'aide de l' `network interface show -fields firewall-policy` commande.

#### **Exemple de création d'une politique de pare-feu et de son assignation à une LIF**

La commande suivante crée une politique de pare-feu nommée `Data_http` qui active l'accès au protocole HTTP et HTTPS à partir des adresses IP sur le sous-réseau 10.10, applique cette politique à la LIF nommée `data1` sur le SVM `vs1`, puis affiche toutes les politiques de pare-feu sur le cluster :

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show
```

| Vserver   | Policy       | Service | Allowed      |
|-----------|--------------|---------|--------------|
| -----     | -----        | -----   | -----        |
| cluster-1 |              |         |              |
|           | data         |         |              |
|           |              | dns     | 0.0.0.0/0    |
|           |              | ndmp    | 0.0.0.0/0    |
|           |              | ndmps   | 0.0.0.0/0    |
| cluster-1 |              |         |              |
|           | intercluster |         |              |
|           |              | https   | 0.0.0.0/0    |
|           |              | ndmp    | 0.0.0.0/0    |
|           |              | ndmps   | 0.0.0.0/0    |
| cluster-1 |              |         |              |
|           | mgmt         |         |              |
|           |              | dns     | 0.0.0.0/0    |
|           |              | http    | 0.0.0.0/0    |
|           |              | https   | 0.0.0.0/0    |
|           |              | ndmp    | 0.0.0.0/0    |
|           |              | ndmps   | 0.0.0.0/0    |
|           |              | ntp     | 0.0.0.0/0    |
|           |              | snmp    | 0.0.0.0/0    |
|           |              | ssh     | 0.0.0.0/0    |
| vs1       |              |         |              |
|           | data_http    |         |              |
|           |              | http    | 10.10.0.0/16 |
|           |              | https   | 10.10.0.0/16 |

```
network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http
```

```
network interface show -fields firewall-policy
```

| vserver   | lif          | firewall-policy |
|-----------|--------------|-----------------|
| -----     | -----        | -----           |
| Cluster   | node1_clus_1 |                 |
| Cluster   | node1_clus_2 |                 |
| Cluster   | node2_clus_1 |                 |
| Cluster   | node2_clus_2 |                 |
| cluster-1 | cluster_mgmt | mgmt            |
| cluster-1 | node1_mgmt1  | mgmt            |
| cluster-1 | node2_mgmt1  | mgmt            |
| vs1       | data1        | data_http       |
| vs3       | data2        | data            |

## Commandes permettant de gérer le service et les politiques de pare-feu

Vous pouvez utiliser le `system services firewall` commandes permettant de gérer le service de pare-feu, le `system services firewall policy` commandes pour gérer les politiques de pare-feu et `network interface modify` Commande permettant de gérer les paramètres de pare-feu des LIF.

| Les fonctions que vous recherchez...                                                        | Utilisez cette commande...                                          |
|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| Activez ou désactivez le service de pare-feu                                                | <code>system services firewall modify</code>                        |
| Affiche la configuration actuelle du service de pare-feu                                    | <code>system services firewall show</code>                          |
| Créez une politique de pare-feu ou ajoutez un service à une politique de pare-feu existante | <code>system services firewall policy create</code>                 |
| Appliquer une politique de pare-feu à une LIF                                               | <code>network interface modify -lif lifname -firewall-policy</code> |
| Modifiez les adresses IP et les masques de réseau associés à une politique de pare-feu      | <code>system services firewall policy modify</code>                 |
| Affiche des informations sur les politiques de pare-feu                                     | <code>system services firewall policy show</code>                   |
| Créez une nouvelle politique de pare-feu qui est une copie exacte d'une politique existante | <code>system services firewall policy clone</code>                  |
| Supprimez une politique de pare-feu qui n'est pas utilisée par une LIF                      | <code>system services firewall policy delete</code>                 |

Pour plus d'informations, consultez les pages de manuel du `system services firewall`, `system services firewall policy`, et `network interface modify` commandes dans "[Référence de commande ONTAP 9](#)".

## Marquage QoS (administrateurs du cluster uniquement)

### Présentation de la QoS

Le marquage qualité de service du réseau (QoS) vous permet de hiérarchiser différents types de trafic en fonction des conditions du réseau afin d'utiliser efficacement les ressources du réseau. Vous pouvez définir la valeur DSCP (Différenciée services code point) des paquets IP sortants pour les types de trafic pris en charge par IPspace.

### Marquage DSCP pour la conformité UC

Vous pouvez activer le marquage DSCP sur le trafic de paquets IP sortant (sortie) pour un protocole donné

avec un code DSCP par défaut ou fourni par l'utilisateur. Le marquage DSCP est un mécanisme de classification et de gestion du trafic réseau et est un composant de la conformité UC (Unified Capability).

Le marquage DSCP (également appelé *QoS marking* ou *Quality of service marking*) est activé en fournissant une valeur IPspace, protocole et DSCP. Les protocoles sur lesquels le marquage DSCP peut être appliqué sont les suivants : NFS, SMB, iSCSI, SnapMirror, NDMP, FTP, HTTP/HTTPS, SSH, Telnet et SNMP.

Si vous ne fournissez pas de valeur DSCP lors de l'activation du marquage DSCP pour un protocole donné, une valeur par défaut est utilisée :

- La valeur par défaut pour les protocoles de données/le trafic est 0x0A (10).
- La valeur par défaut pour les protocoles de contrôle/trafic est 0x30 (48).

## Modifier les valeurs de marquage QoS

Il est possible de modifier les valeurs du marquage qualité de service (QoS) pour différents protocoles, pour chaque IPspace.

### Avant de commencer

Tous les nœuds d'un cluster doivent exécuter la même version de ONTAP.

### Étape

Modifiez les valeurs de marquage QoS à l'aide de `network qos-marking modify` commande.

- Le `-ipspace` Paramètre spécifie l'IPspace pour lequel l'entrée de marquage QoS doit être modifiée.
- Le `-protocol` Paramètre spécifie le protocole pour lequel l'entrée de marquage QoS doit être modifiée. Le `network qos-marking modify` la page man décrit les valeurs possibles du protocole.
- Le `-dscp` Paramètre spécifie la valeur DSCP (Differentiated Services Code point). Les valeurs possibles sont comprises entre 0 et 63.
- Le `-is-enabled` Paramètre permet d'activer ou de désactiver le marquage QoS pour le protocole spécifié dans l'IPspace fourni par le `-ipspace` paramètre.

La commande suivante active le marquage QoS pour le protocole NFS dans l'IPspace par défaut :

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

La commande suivante définit la valeur DSCP sur 20 pour le protocole NFS dans l'IPspace par défaut :

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

## Afficher les valeurs de marquage QoS

Vous pouvez afficher les valeurs de marquage QoS pour différents protocoles, pour chaque IPspace.

### Étape

Afficher les valeurs de marquage QoS à l'aide du `network qos-marking show` commande.



La commande suivante affiche le marquage QoS pour tous les protocoles dans l'IPspace par défaut :

```
network qos-marking show -ipspace Default
IPspace Protocol DSCP Enabled?

Default
 CIFS 10 false
 FTP 48 false
 HTTP-admin 48 false
 HTTP-filesrv 10 false
 NDMP 10 false
 NFS 10 true
 SNMP 48 false
 SSH 48 false
 SnapMirror 10 false
 Telnet 48 false
 iSCSI 10 false

11 entries were displayed.
```

## Gestion SNMP (administrateurs du cluster uniquement)

### Présentation SNMP

Vous pouvez configurer le protocole SNMP pour surveiller les SVM au sein de votre cluster afin d'éviter les problèmes avant qu'ils ne se produisent et de répondre aux problèmes en cas de survenue. La gestion de SNMP implique la configuration des utilisateurs SNMP et la configuration des destinations de Traphost SNMP (stations de travail de gestion) pour tous les événements SNMP. SNMP est désactivé par défaut sur les LIFs de données.

Vous pouvez créer et gérer des utilisateurs SNMP en lecture seule dans la SVM de données. Les LIFs data doivent être configurées de sorte à recevoir des requêtes SNMP sur le SVM.

Les postes de travail SNMP de gestion de réseau, ou gestionnaires, peuvent interroger l'agent SNMP du SVM pour obtenir des informations. L'agent SNMP recueille des informations et les transmet aux gestionnaires SNMP. L'agent SNMP génère également des notifications d'interruption lorsque des événements spécifiques se produisent. L'agent SNMP du SVM possède des privilèges en lecture seule ; il ne peut pas être utilisé pour des opérations définies ou pour effectuer une action corrective en réponse à un trap. ONTAP fournit un agent SNMP compatible avec les versions SNMP v1, v2c et v3. SNMPv3 offre une sécurité avancée en utilisant des phrases de passe et le cryptage.

Pour plus d'informations sur la prise en charge SNMP dans les systèmes ONTAP, voir ["Tr-4220 : prise en charge SNMP dans Data ONTAP"](#).

### Présentation MIB

Une base MIB (Management information base) est un fichier texte qui décrit les objets SNMP et les traps.

Les MIB décrivent la structure des données de gestion du système de stockage et utilisent un espace de noms hiérarchique contenant des identifiants d'objets (OID). Chaque OID identifie une variable qui peut être lue à l'aide de SNMP.

Étant donné que les MIB ne sont pas des fichiers de configuration et que ONTAP ne lit pas ces fichiers, la fonctionnalité SNMP n'est pas affectée par les MIB. ONTAP fournit le fichier MIB suivant :

- Une MIB personnalisées NetApp (`netapp.mib`)

ONTAP prend en charge les MIB IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113) et ICMP (RFC 2466), qui affichent à la fois des données IPv4 et IPv6.

ONTAP fournit également une référence croisée courte entre les identificateurs d'objet (OID) et les noms courts d'objet dans le `traps.dat` fichier.



Les dernières versions des fichiers MIB ONTAP et `traps.dat` sont disponibles sur le site de support NetApp. Cependant, les versions de ces fichiers sur le site de support ne correspondent pas nécessairement aux capacités SNMP de votre version ONTAP. Ces fichiers sont fournis pour vous aider à évaluer les fonctions SNMP dans la dernière version de ONTAP.

## Interruptions SNMP

Les interruptions SNMP capturent les informations de surveillance du système envoyées en tant que notification asynchrone de l'agent SNMP au gestionnaire SNMP.

Il existe trois types d'interruptions SNMP : standard, intégré et défini par l'utilisateur. Les interruptions définies par l'utilisateur ne sont pas prises en charge dans ONTAP.

Un trap peut être utilisé pour vérifier périodiquement les seuils opérationnels ou les échecs définis dans la MIB. Si un seuil est atteint ou qu'une panne est détectée, l'agent SNMP envoie un message (interruption) aux Traphosts les alertant de l'événement.



ONTAP prend en charge les dérouterments SNMPv1 et, starting dans ONTAP 9.1, SNMPv3 dérouterments. ONTAP ne prend pas en charge les dérouterments SNMPv2c et n'informe pas.

## Interruptions SNMP standard

Ces interruptions sont définies dans RFC 1215. Il existe cinq interruptions SNMP standard prises en charge par ONTAP : coldstart, warmstart, Linkdown, linkup et authenticationFailure.



Le trap authenticationFailure est désactivé par défaut. Vous devez utiliser `system snmp authtrap` la commande pour activer le trap. Pour plus d'informations, consultez les pages man : ["Référence de commande ONTAP"](#)

## Interruptions SNMP intégrées

Les interruptions intégrées sont prédéfinies dans ONTAP et sont automatiquement envoyées aux stations de gestion du réseau de la liste des Traphost si un événement se produit. Ces interruptions, telles que diskFailedShutdown, cpuTooBusy et volume NearlyFull, sont définies dans la MIB personnalisées.

Chaque trappe intégrée est identifiée par un code d'interruption unique.

## Créer une communauté SNMP et l'attribuer à une LIF

Vous pouvez créer une communauté SNMP qui agit comme un mécanisme d'authentification entre le poste de gestion et le SVM (Storage Virtual machine) en cas d'utilisation des protocoles SNMPv1 et SNMPv2c.

En créant des communautés SNMP dans un SVM de données, vous pouvez exécuter des commandes telles que `snmpwalk` et `snmpget` Sur les LIF de données.

### Description de la tâche

- Dans les nouvelles installations de ONTAP, SNMPv1 et SNMPv2c sont désactivés par défaut.

Les protocoles SNMPv1 et SNMPv2c sont activés après la création d'une communauté SNMP.

- ONTAP prend en charge les communautés en lecture seule.
- Par défaut la politique de pare-feu « données » qui est attribuée aux LIFs de données a le service SNMP défini sur `deny`.

Vous devez créer une nouvelle politique de pare-feu avec le service SNMP défini sur `allow` Lors de la création d'un utilisateur SNMP pour un SVM de données.



Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "[Configuration des politiques de pare-feu pour les LIF](#)".

- Vous pouvez créer des communautés SNMP pour les utilisateurs SNMPv1 et SNMPv2c pour la SVM d'administration et la SVM de données.
- Comme un SVM ne fait pas partie de la norme SNMP, les requêtes relatives aux LIF de données doivent inclure l'OID racine NetApp (1.3.6.1.4.1.789), par exemple `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

### Étapes

1. Créez une communauté SNMP en utilisant le `system snmp community add` commande. La commande suivante montre comment créer une communauté SNMP dans le SVM admin cluster-1 :

```
system snmp community add -type ro -community-name comty1 -vserver
cluster-1
```

La commande suivante montre comment créer une communauté SNMP dans le SVM de données vs1 :

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. Vérifiez que les communautés ont été créées à l'aide de la commande `system snmp community show`.

La commande suivante présente les deux communautés créées pour SNMPv1 et SNMPv2c :

```

system snmp community show
cluster-1
rocomty1
vs1
rocomty2

```

3. Vérifier si SNMP est autorisé en tant que service dans la politique de pare-feu « data » en utilisant le `system services firewall policy show` commande.

La commande suivante indique que le service snmp n'est pas autorisé dans la politique de pare-feu « data » par défaut (le service snmp est autorisé dans la politique de pare-feu « mgmt » uniquement) :

```

system services firewall policy show
Vserver Policy Service Allowed

cluster-1
 data
 dns 0.0.0.0/0
 ndmp 0.0.0.0/0
 ndmps 0.0.0.0/0
cluster-1
 intercluster
 https 0.0.0.0/0
 ndmp 0.0.0.0/0
 ndmps 0.0.0.0/0
cluster-1
 mgmt
 dns 0.0.0.0/0
 http 0.0.0.0/0
 https 0.0.0.0/0
 ndmp 0.0.0.0/0
 ndmps 0.0.0.0/0
 ntp 0.0.0.0/0
 snmp 0.0.0.0/0
 ssh 0.0.0.0/0

```

4. Créez une nouvelle politique de pare-feu qui autorise l'accès à l'aide du système `snmp` service à l'aide du `system services firewall policy create` commande.

Les commandes suivantes créent une nouvelle politique de pare-feu de données nommée « data1 » qui autorise le `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver vs1 -allow-list 0.0.0.0/0
```

```
cluster-1::> system services firewall policy show -service snmp
```

| Vserver   | Policy | Service | Allowed   |
|-----------|--------|---------|-----------|
| -----     |        |         |           |
| cluster-1 |        |         |           |
|           | mgmt   |         |           |
|           |        | snmp    | 0.0.0.0/0 |
| vs1       |        |         |           |
|           | data1  |         |           |
|           |        | snmp    | 0.0.0.0/0 |

5. Appliquer la politique de pare-feu à une LIF de données à l'aide de la commande `network interface modify` avec le paramètre -firewall-policy.

La commande suivante attribue la nouvelle politique de pare-feu « data1 » à LIF « datalif1 » :

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

## Configurez les utilisateurs SNMPv3 dans un cluster

SNMPv3 est un protocole sécurisé lorsqu'il est comparé au protocole SNMPv1 et SNMPv2c. Pour utiliser SNMPv3, vous devez configurer un utilisateur SNMPv3 pour exécuter les utilitaires SNMP à partir du gestionnaire SNMP.

### Étape

Utilisez la commande « Security login create » pour créer un utilisateur SNMPv3.

Vous êtes invité à fournir les informations suivantes :

- ID moteur : la valeur par défaut et la valeur recommandée sont l'ID moteur local
- Protocole d'authentification
- Mot de passe d'authentification
- Protocole de confidentialité
- Mot de passe du protocole de confidentialité

### Résultat

L'utilisateur SNMPv3 peut se connecter à partir du gestionnaire SNMP en utilisant le nom d'utilisateur et le mot de passe et en exécutant les commandes de l'utilitaire SNMP.

### Paramètres de sécurité SNMPv3

SNMPv3 inclut une fonctionnalité d'authentification qui, lorsqu'elle est sélectionnée, demande aux utilisateurs

de saisir leurs noms, un protocole d'authentification, une clé d'authentification et le niveau de sécurité souhaité lors de l'appel d'une commande.

Le tableau suivant répertorie les paramètres de sécurité SNMPv3 :

| Paramètre                                                      | Option de ligne de commandes                                                                                                                                    | Description                                                                      |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| ID d'ingénierie                                                | -E EngineID                                                                                                                                                     | ID moteur de l'agent SNMP. La valeur par défaut est local EngineID (recommandé). |
| Nom de sécurité                                                | -U Nom                                                                                                                                                          | Le nom d'utilisateur ne doit pas dépasser 32 caractères.                         |
| Protocole d'authentification                                   | -A {none                                                                                                                                                        | MD5                                                                              |
| SHA                                                            | SHA-256}                                                                                                                                                        | Le type d'authentification peut être aucun, MD5, SHA ou SHA-256.                 |
| AuthKey                                                        | -UNE PHRASE DE PASSE                                                                                                                                            | Phrase de passe avec un minimum de huit caractères.                              |
| Niveau de sécurité                                             | -L {authNoPriv                                                                                                                                                  | AuthPriv                                                                         |
| noAuthNoPriv}                                                  | Le niveau de sécurité peut être authentification, aucune confidentialité, authentification, confidentialité ou aucune authentification, Aucune confidentialité. | Protocole privé                                                                  |
| -x { none                                                      | des                                                                                                                                                             | aes128}                                                                          |
| Le protocole de confidentialité peut être aucun, des ou aes128 | Mot de passe privé                                                                                                                                              | -X mot de passe                                                                  |

### Exemples de niveaux de sécurité différents

Cet exemple montre comment un utilisateur SNMPv3 créé avec différents niveaux de sécurité peut utiliser les commandes SNMP côté client, telles que `snmpwalk`, pour interroger les objets de cluster.

Pour améliorer les performances, vous devez récupérer tous les objets d'un tableau plutôt qu'un seul objet ou quelques objets du tableau.



Vous devez utiliser `snmpwalk` 5.3.1 ou version ultérieure lorsque le protocole d'authentification est SHA.

## Niveau de sécurité : AuthPriv

Le résultat suivant montre la création d'un utilisateur SNMPv3 avec le niveau de sécurité d'authPriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

## Mode FIPS

```
security login create -username snmpv3user -application snmp -authmethod
usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

## Test snmpwalk

La sortie suivante montre l'utilisateur SNMPv3 exécutant la commande snmpwalk :

Pour améliorer les performances, vous devez récupérer tous les objets d'un tableau plutôt qu'un seul objet ou quelques objets du tableau.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

### Niveau de sécurité : AuthNoPriv

Le résultat suivant montre la création d'un utilisateur SNMPv3 avec le niveau de sécurité authNoPriv.

```
security login create -username snmpv3user1 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

### Mode FIPS

FIPS ne vous permet pas de choisir **none** pour le protocole de confidentialité. En conséquence, il n'est pas possible de configurer un utilisateur authNoPriv SNMPv3 en mode FIPS.

### Test snmpwalk

La sortie suivante montre l'utilisateur SNMPv3 exécutant la commande snmpwalk :

Pour améliorer les performances, vous devez récupérer tous les objets d'un tableau plutôt qu'un seul objet ou quelques objets du tableau.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1! -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

### Niveau de sécurité : NoAuthNoPriv

La sortie suivante montre la création d'un utilisateur SNMPv3 avec le niveau de sécurité noAuthNoPriv.

```
security login create -username snmpv3user2 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

### Mode FIPS

FIPS ne vous permet pas de choisir **none** pour le protocole de confidentialité.



## Test snmpwalk

La sortie suivante montre l'utilisateur SNMPv3 exécutant la commande snmpwalk :

Pour améliorer les performances, vous devez récupérer tous les objets d'un tableau plutôt qu'un seul objet ou quelques objets du tableau.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

## Configurez les Traphosts pour recevoir des notifications SNMP

Vous pouvez configurer le Traphost (gestionnaire SNMP) pour recevoir des notifications (PDU d'interruption SNMP) lorsque des interruptions SNMP sont générées dans le cluster. Vous pouvez spécifier le nom d'hôte ou l'adresse IP (IPv4 ou IPv6) du Traphost SNMP.

### Avant de commencer

- Les traps SNMP doivent être activés sur le cluster.



Les interruptions SNMP et SNMP sont activées par défaut.

- Le DNS doit être configuré sur le cluster pour la résolution des noms de Traphost.
- IPv6 doit être activé sur le cluster pour configurer les Traphosts SNMP à l'aide des adresses IPv6.
- Pour ONTAP 9.1 et versions ultérieures, vous devez avoir spécifié l'authentification d'un modèle de sécurité utilisateur prédéfini (USM) et des informations d'identification de confidentialité lors de la création de Traphosts.

### Étape

Ajouter un Traphost SNMP :

```
system snmp traphost add
```



Les interruptions ne peuvent être envoyées que lorsqu'au moins une station de gestion SNMP est spécifiée comme un traphost.

La commande suivante ajoute un nouvel hôte SNMPv3 nommé yyy.example.com avec un utilisateur USM connu :

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

La commande suivante ajoute un Traphost à l'aide de l'adresse IPv6 de l'hôte :

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

## Tester l'interrogation SNMP

Une fois le protocole SNMP configuré, vous devez vérifier que vous pouvez interroger le cluster.

### Description de la tâche

Pour interroger un cluster, vous devez utiliser une commande tierce par exemple `snmpwalk`.

### Étapes

1. Envoyer une commande SNMP pour interroger le cluster depuis un autre cluster.

Pour les systèmes exécutant SNMPv1, utilisez la commande CLI `snmpwalk -v version -c community_string ip_address_or_host_name system` Pour découvrir le contenu de la base MIB (Management information base).

Dans cet exemple, l'adresse IP de la LIF de gestion du cluster dont vous disposez est 10.11.12.123. La commande affiche les informations demandées à partir de la MIB :

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
 Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

Pour les systèmes exécutant SNMPv2c, utilisez la commande CLI `snmpwalk -v version -c community_string ip_address_or_host_name system` Pour découvrir le contenu de la base MIB (Management information base).

Dans cet exemple, l'adresse IP de la LIF de gestion du cluster dont vous disposez est 10.11.12.123. La commande affiche les informations demandées à partir de la MIB :

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

Pour les systèmes exécutant SNMPv3, utilisez la commande CLI `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` Pour découvrir le contenu de la base MIB (Management information base).

Dans cet exemple, l'adresse IP de la LIF de gestion du cluster dont vous disposez est 10.11.12.123. La commande affiche les informations demandées à partir de la MIB :

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
-A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

## Commandes pour la gestion de SNMP

Vous pouvez utiliser le `system snmp` Commandes permettant de gérer SNMP, les traps et les Traphosts. Vous pouvez utiliser le `security` Commandes permettant de gérer les utilisateurs SNMP par SVM. Vous pouvez utiliser le `event` Commandes pour gérer les événements liés aux traps SNMP.

### Commandes permettant de configurer SNMP

| Les fonctions que vous recherchez... | Utilisez cette commande... |
|--------------------------------------|----------------------------|
|--------------------------------------|----------------------------|

|                                             |                                                                                                                                                                                                                                                                                      |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Activez SNMP sur le cluster                 | <pre>options -option-name snmp.enable -option-value on</pre> <p>Le service SNMP doit être autorisé conformément à la politique de pare-feu de gestion. Vous pouvez vérifier si le protocole SNMP est autorisé via la commande <code>system services firewall policy show</code>.</p> |
| Désactiver le protocole SNMP sur le cluster | <pre>options -option-name snmp.enable -option-value off</pre>                                                                                                                                                                                                                        |

### Commandes pour la gestion des utilisateurs SNMP v1, v2c et v3

| Les fonctions que vous recherchez...                                                              | Utilisez cette commande...                                                |
|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Configurez les utilisateurs SNMP                                                                  | <code>security login create</code>                                        |
| Afficher les utilisateurs SNMP                                                                    | <code>security snmpusers and security login show -application snmp</code> |
| Supprimer les utilisateurs SNMP                                                                   | <code>security login delete</code>                                        |
| Modifier le nom du rôle de contrôle d'accès d'une méthode de connexion pour les utilisateurs SNMP | <code>security login modify</code>                                        |

### Commandes permettant de fournir des informations de contact et d'emplacement

| Les fonctions que vous recherchez...                      | Utilisez cette commande...        |
|-----------------------------------------------------------|-----------------------------------|
| Afficher ou modifier les détails du contact du cluster    | <code>system snmp contact</code>  |
| Afficher ou modifier les détails d'emplacement du cluster | <code>system snmp location</code> |

### Commandes pour la gestion des communautés SNMP

| Les fonctions que vous recherchez...                                                     | Utilisez cette commande...                |
|------------------------------------------------------------------------------------------|-------------------------------------------|
| Ajoutez une communauté en lecture seule (ro) pour un SVM ou pour tous les SVM du cluster | <code>system snmp community add</code>    |
| Supprimer une communauté ou toutes les communautés                                       | <code>system snmp community delete</code> |
| Afficher la liste de toutes les communautés                                              | <code>system snmp community show</code>   |

Les SVM ne faisant pas partie de la norme SNMP, les requêtes relatives aux LIF de données doivent inclure l'OID racine NetApp (1.3.6.1.4.1.789), par exemple. `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

### Commande pour l'affichage des valeurs d'option SNMP

| Les fonctions que vous recherchez...                                                                                                                                                                                                                      | Utilisez cette commande...    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| Afficher les valeurs actuelles de toutes les options SNMP, y compris le contact de cluster, l'emplacement de contact, si le cluster est configuré pour envoyer des traps, la liste des Traphosts, la liste des communautés et le type de contrôle d'accès | <code>system snmp show</code> |

### Commandes pour la gestion des interruptions SNMP et des Traphosts

| Les fonctions que vous recherchez...                                                                  | Utilisez cette commande...               |
|-------------------------------------------------------------------------------------------------------|------------------------------------------|
| Activer les traps SNMP envoyés depuis le cluster                                                      | <code>system snmp init -init 1</code>    |
| Désactiver les traps SNMP envoyés depuis le cluster                                                   | <code>system snmp init -init 0</code>    |
| Ajoutez un Traphost qui reçoit des notifications SNMP pour des événements spécifiques dans le cluster | <code>system snmp traphost add</code>    |
| Supprimer un Traphost                                                                                 | <code>system snmp traphost delete</code> |
| Affiche la liste des Traphosts                                                                        | <code>system snmp traphost show</code>   |

### Commandes pour la gestion des événements liés aux traps SNMP

| Les fonctions que vous recherchez...                                                   | Utilisez cette commande...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Afficher les événements pour lesquels des interruptions SNMP (intégrées) sont générées | <code>event route show</code><br><br>Utilisez le <code>-snmp-support true</code> Paramètre pour afficher uniquement les événements SNMP.<br><br>Utilisez le instance <code>-messagename &lt;message&gt;</code> paramètre permettant d'afficher une description détaillée de la raison d'un événement et de toute action corrective.<br><br>Le routage des événements de déROUTement SNMP individuels vers des destinations de traphost spécifiques n'est pas pris en charge. Tous les événements de déROUTement SNMP sont envoyés à toutes les destinations de Traphost. |

|                                                                                                                                                        |                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| Affiche la liste des enregistrements de l'historique des interruptions SNMP, qui sont des notifications d'événements envoyées à des interruptions SNMP | <code>event snmphistory show</code>   |
| Supprimer un enregistrement de l'historique des interruptions SNMP                                                                                     | <code>event snmphistory delete</code> |

Pour plus d'informations sur `system snmp` les commandes `, , `security` et `event`, reportez-vous à la section ["Référence de commande ONTAP"](#).

## Gestion du routage dans un SVM

### Présentation du routage des SVM

La table de routage d'un SVM détermine le chemin réseau utilisé par la SVM pour communiquer avec une destination. Il est important de comprendre le fonctionnement des tables de routage afin d'éviter les problèmes de réseau avant qu'ils ne surviennent.

Les règles de routage sont les suivantes :

- ONTAP achemine le trafic sur l'itinéraire le plus spécifique disponible.
- ONTAP achemine le trafic sur une route de passerelle par défaut (ayant 0 bits de masque de réseau) comme dernier recours, lorsque des routes plus spécifiques ne sont pas disponibles.

Dans le cas de routes avec la même destination, le même masque de réseau et la même mesure, il n'est pas garanti que le système utilisera la même route après un redémarrage ou après une mise à niveau. Ceci est particulièrement un problème si vous avez configuré plusieurs routes par défaut.

Il est recommandé de configurer une route par défaut uniquement pour un SVM. Pour éviter toute interruption, assurez-vous que la route par défaut peut atteindre toute adresse réseau inaccessible par une route plus spécifique. Pour plus d'informations, consultez l'article de la base de connaissances ["SU134 : l'accès au réseau peut être interrompu par une configuration de routage incorrecte dans clustered ONTAP"](#)

### Créer une route statique

Vous pouvez créer des routes statiques au sein d'une machine virtuelle de stockage (SVM) pour contrôler la manière dont les LIF utilisent le réseau pour le trafic sortant.

Lorsque vous créez une entrée de route associée à un SVM, la route sera utilisée par toutes les LIFs qui sont détenues par le SVM spécifié et qui se trouvent sur le même sous-réseau que la passerelle.

#### Étape

Utilisez le `network route create` commande pour créer une route.

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

## Activez le routage multivoie

Si plusieurs routes ont la même mesure pour une destination, seule une des routes est sélectionnée pour le trafic sortant. Cela entraîne l'utilisation d'autres itinéraires pour l'envoi du trafic sortant. Vous pouvez activer le routage multivoie pour équilibrer la charge sur toutes les routes disponibles proportionnellement à leurs mesures, par opposition au routage ECMP, qui équilibre la charge sur les routes disponibles de la même mesure.

### Étapes

1. Connectez-vous au niveau de privilège avancé :

```
set -privilege advanced
```

2. Activer le routage multivoie :

```
network options multipath-routing modify -is-enabled true
```

Le routage multivoie est activé pour tous les nœuds du cluster.

```
network options multipath-routing modify -is-enabled true
```

## Supprimer une route statique

Vous pouvez supprimer une route statique inutile d'une machine virtuelle de stockage (SVM).

### Étape

Utilisez le `network route delete` commande pour supprimer une route statique.

Pour plus d'informations sur cette commande, reportez-vous au .

L'exemple suivant supprime une route statique associée à SVM vs0 avec une passerelle de 10.63.0.1 et une adresse IP de destination de 0.0.0.0/0 :

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

## Afficher les informations de routage

Vous pouvez afficher des informations sur la configuration de routage pour chaque SVM sur le cluster. Cela peut vous aider à diagnostiquer les problèmes de routage impliquant des problèmes de connectivité entre les applications ou les services client et un LIF sur un nœud du cluster.

### Étapes

1. Utilisez le `network route show` Commande permettant d'afficher les routes au sein d'un ou plusieurs

SVM. L'exemple suivant montre une route configurée sur le SVM vs0 :

```
network route show
(network route show)
Vserver Destination Gateway Metric

vs0
 0.0.0.0/0 172.17.178.1 20
```

2. Utilisez le `network route show-lifs` Commande pour afficher l'association des routes et LIFs au sein d'un ou plusieurs SVM.

L'exemple suivant montre les LIFs avec des routes détenues par le SVM vs0 :

```
network route show-lifs
(network route show-lifs)

Vserver: vs0
Destination Gateway Logical Interfaces

0.0.0.0/0 172.17.178.1 cluster_mgmt,
 LIF-b-01_mgmt1,
 LIF-b-02_mgmt1
```

3. Utilisez le `network route active-entry show` Commande permettant d'afficher les routes installées sur un ou plusieurs nœuds, SVM, sous-réseaux ou routes avec des destinations spécifiées.

L'exemple suivant montre toutes les routes installées sur un SVM spécifique :

```
network route active-entry show -vserver Data0

Vserver: Data0
Node: node-1
Subnet Group: 0.0.0.0/0
Destination Gateway Interface Metric Flags

127.0.0.1 127.0.0.1 lo 10 UHS
127.0.10.1 127.0.20.1 losk 10 UHS
127.0.20.1 127.0.20.1 losk 10 UHS

Vserver: Data0
Node: node-1
Subnet Group: fd20:8b1e:b255:814e::/64
Destination Gateway Interface Metric Flags

```



```

default fd20:8b1e:b255:814e::1
 e0d 20 UGS

fd20:8b1e:b255:814e::/64
 link#4 e0d 0 UC

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination Gateway Interface Metric Flags

127.0.0.1 127.0.0.1 lo 10 UHS

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination Gateway Interface Metric Flags

127.0.10.1 127.0.20.1 losk 10 UHS
127.0.20.1 127.0.20.1 losk 10 UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination Gateway Interface Metric Flags

default fd20:8b1e:b255:814e::1
 e0d 20 UGS

fd20:8b1e:b255:814e::/64
 link#4 e0d 0 UC
fd20:8b1e:b255:814e::1 link#4 e0d 0 UHL
11 entries were displayed.

```

## Supprimer des routes dynamiques des tables de routage

Lorsque des redirections ICMP sont reçues pour IPv4 et IPv6, des routes dynamiques sont ajoutées à la table de routage. Par défaut, les routes dynamiques sont supprimées au bout de 300 secondes. Si vous souhaitez maintenir des itinéraires dynamiques pendant une durée différente, vous pouvez modifier la valeur de délai d'exécution.

### Description de la tâche

Vous pouvez définir la valeur de temporisation de 0 à 65,535 secondes. Si vous définissez la valeur sur 0, les routes n'expirent jamais. La suppression de routes dynamiques empêche la perte de connectivité causée par la persistance de routes non valides.

### Étapes

1. Afficher la valeur de temporisation actuelle.

- Pour IPv4 :

```
network tuning icmp show
```

- Pour IPv6 :

```
network tuning icmp6 show
```

## 2. Modifiez la valeur de temporisation.

- Pour IPv4 :

```
network tuning icmp modify -node node_name -redirect-timeout
timeout_value
```

- Pour IPv6 :

```
network tuning icmp6 modify -node node_name -redirect-v6-timeout
timeout_value
```

## 3. Vérifiez que la valeur de temporisation a été modifiée correctement.

- Pour IPv4 :

```
network tuning icmp show
```

- Pour IPv6 :

```
network tuning icmp6 show
```

# Afficher les informations sur le réseau

## Afficher la présentation des informations sur le réseau

Via l'interface de ligne de commandes, vous pouvez afficher des informations relatives aux ports, aux LIF, aux routes, aux règles de basculement, aux groupes de basculement, règles de pare-feu, DNS, NIS et connexions. Depuis ONTAP 9.8, vous pouvez également télécharger les données affichées dans System Manager relatives à votre réseau.

Ces informations peuvent être utiles dans des situations comme la reconfiguration des paramètres réseau ou le dépannage du cluster.

Si vous êtes administrateur de cluster, vous pouvez afficher toutes les informations de mise en réseau disponibles. Si vous êtes administrateur des SVM, vous pouvez afficher uniquement les informations relatives aux SVM qui vous sont attribuées.

Dans System Manager, lorsque vous affichez des informations dans une *vue liste*, vous pouvez cliquer sur **Télécharger** et la liste des objets affichés est téléchargée.

- La liste est téléchargée au format CSV (valeurs séparées par des virgules).
- Seules les données des colonnes visibles sont téléchargées.
- Le nom de fichier CSV est formaté avec le nom de l'objet et un horodatage.

## Affiche les informations relatives aux ports réseau

Vous pouvez afficher des informations sur un port spécifique ou sur tous les ports de tous les nœuds du cluster.

### Description de la tâche

Les informations suivantes s'affichent :

- Nom du nœud
- Nom du port
- Nom IPspace
- Nom du domaine de diffusion
- État de la liaison (haut ou bas)
- Paramètre MTU
- Réglage de la vitesse du port et état de fonctionnement (1 Gigabit ou 10 gigabits par seconde)
- Paramètre de négociation automatique (vrai ou faux)
- Mode duplex et état de fonctionnement (moitié ou plein)
- Le groupe d'interface du port, le cas échéant
- Les informations de balise VLAN du port, le cas échéant
- État de santé du port (état de santé ou dégradé)
- Raisons pour lesquelles un port est marqué comme dégradé

Si les données d'un champ ne sont pas disponibles (par exemple, le duplex opérationnel et la vitesse d'un port inactif ne sont pas disponibles), la valeur du champ est indiquée comme –.

### Étape

Affiche les informations relatives aux ports réseau à l'aide du `network port show` commande.

Vous pouvez afficher des informations détaillées pour chaque port en spécifiant le `-instance` paramètre ou obtenir des informations spécifiques en spécifiant les noms de champs à l'aide du `-fields` paramètre.

```
network port show
```

```
Node: node1
```

```
Ignore
```

|        |         |           |        |      |      | Speed(Mbps) | Health   |
|--------|---------|-----------|--------|------|------|-------------|----------|
| Health |         |           |        |      |      |             |          |
| Port   | IPspace | Broadcast | Domain | Link | MTU  | Admin/Oper  | Status   |
| Status |         |           |        |      |      |             |          |
| -----  | -----   | -----     | -----  | ---- | ---- | -----       | -----    |
| -----  |         |           |        |      |      |             |          |
| e0a    | Cluster | Cluster   |        | up   | 9000 | auto/1000   | healthy  |
| false  |         |           |        |      |      |             |          |
| e0b    | Cluster | Cluster   |        | up   | 9000 | auto/1000   | healthy  |
| false  |         |           |        |      |      |             |          |
| e0c    | Default | Default   |        | up   | 1500 | auto/1000   | degraded |
| false  |         |           |        |      |      |             |          |
| e0d    | Default | Default   |        | up   | 1500 | auto/1000   | degraded |
| true   |         |           |        |      |      |             |          |

```
Node: node2
```

```
Ignore
```

|        |         |           |        |      |      | Speed(Mbps) | Health  |
|--------|---------|-----------|--------|------|------|-------------|---------|
| Health |         |           |        |      |      |             |         |
| Port   | IPspace | Broadcast | Domain | Link | MTU  | Admin/Oper  | Status  |
| Status |         |           |        |      |      |             |         |
| -----  | -----   | -----     | -----  | ---- | ---- | -----       | -----   |
| -----  |         |           |        |      |      |             |         |
| e0a    | Cluster | Cluster   |        | up   | 9000 | auto/1000   | healthy |
| false  |         |           |        |      |      |             |         |
| e0b    | Cluster | Cluster   |        | up   | 9000 | auto/1000   | healthy |
| false  |         |           |        |      |      |             |         |
| e0c    | Default | Default   |        | up   | 1500 | auto/1000   | healthy |
| false  |         |           |        |      |      |             |         |
| e0d    | Default | Default   |        | up   | 1500 | auto/1000   | healthy |
| false  |         |           |        |      |      |             |         |

```
8 entries were displayed.
```

## Afficher les informations relatives à un VLAN (administrateurs de cluster uniquement)

Vous pouvez afficher des informations sur un VLAN spécifique ou sur tous les VLAN du cluster.

### Description de la tâche

Vous pouvez afficher des informations détaillées pour chaque VLAN en spécifiant le `-instance` paramètre.

Vous pouvez afficher des informations spécifiques en spécifiant des noms de champ à l'aide de l' `-fields` paramètre.

### Étape

Affiche des informations sur les VLAN à l'aide de `network port vlan show` commande. La commande suivante affiche des informations sur tous les VLAN du cluster :

```
network port vlan show
```

| Node         | VLAN Name | Port | VLAN ID | MAC Address       |
|--------------|-----------|------|---------|-------------------|
| cluster-1-01 |           |      |         |                   |
|              | a0a-10    | a0a  | 10      | 02:a0:98:06:10:b2 |
|              | a0a-20    | a0a  | 20      | 02:a0:98:06:10:b2 |
|              | a0a-30    | a0a  | 30      | 02:a0:98:06:10:b2 |
|              | a0a-40    | a0a  | 40      | 02:a0:98:06:10:b2 |
|              | a0a-50    | a0a  | 50      | 02:a0:98:06:10:b2 |
| cluster-1-02 |           |      |         |                   |
|              | a0a-10    | a0a  | 10      | 02:a0:98:06:10:ca |
|              | a0a-20    | a0a  | 20      | 02:a0:98:06:10:ca |
|              | a0a-30    | a0a  | 30      | 02:a0:98:06:10:ca |
|              | a0a-40    | a0a  | 40      | 02:a0:98:06:10:ca |
|              | a0a-50    | a0a  | 50      | 02:a0:98:06:10:ca |

## Afficher les informations sur les groupes d'interfaces (administrateurs du cluster uniquement)

Vous pouvez afficher des informations relatives à un groupe d'interfaces afin de déterminer sa configuration.

### Description de la tâche

Les informations suivantes s'affichent :

- Nœud sur lequel est situé le groupe d'interface
- Liste des ports réseau inclus dans le groupe d'interface
- Nom du groupe d'interface
- Fonction de distribution (MAC, IP, port ou séquentiel)
- Adresse MAC (Media Access Control) du groupe d'interfaces
- Statut de l'activité du port ; c'est-à-dire si tous les ports agrégés sont actifs (participation complète), si certains sont actifs (participation partielle) ou si aucun n'est actif

### Étape

Affiche des informations sur les groupes d'interfaces en utilisant le `network port ifgrp show` commande.

Vous pouvez afficher des informations détaillées pour chaque nœud en spécifiant le `-instance` paramètre. Vous pouvez afficher des informations spécifiques en spécifiant des noms de champ à l'aide de l' `-fields`

paramètre.

La commande suivante affiche des informations sur tous les groupes d'interfaces du cluster :

```
network port ifgrp show
```

| Node         | Port  | Distribution | MAC Address       | Active | Ports    |
|--------------|-------|--------------|-------------------|--------|----------|
| Node         | IfGrp | Function     | MAC Address       | Ports  | Ports    |
| cluster-1-01 | a0a   | ip           | 02:a0:98:06:10:b2 | full   | e7a, e7b |
| cluster-1-02 | a0a   | sequential   | 02:a0:98:06:10:ca | full   | e7a, e7b |
| cluster-1-03 | a0a   | port         | 02:a0:98:08:5b:66 | full   | e7a, e7b |
| cluster-1-04 | a0a   | mac          | 02:a0:98:08:61:4e | full   | e7a, e7b |

La commande suivante affiche des informations détaillées sur les groupes d'interfaces pour un nœud unique :

```
network port ifgrp show -instance -node cluster-1-01
```

```
Node: cluster-1-01
Interface Group Name: a0a
Distribution Function: ip
Create Policy: multimode
MAC Address: 02:a0:98:06:10:b2
Port Participation: full
Network Ports: e7a, e7b
Up Ports: e7a, e7b
Down Ports: -
```

## Affiche les informations relatives aux LIF

Vous pouvez afficher des informations détaillées sur une LIF afin de déterminer sa configuration.

Vous pouvez également vouloir afficher ces informations pour diagnostiquer les problèmes de base d'une LIF, comme vérifier la présence d'adresses IP en double ou vérifier si le port réseau appartient au sous-réseau correct. Les administrateurs des SVM (Storage Virtual machine) ne peuvent afficher que les informations concernant les LIFs associées à la SVM.

### Description de la tâche

Les informations suivantes s'affichent :

- Adresse IP associée à la LIF
- Statut administratif de la LIF

- Statut opérationnel de la LIF

L'état opérationnel des LIFs de données est déterminé par le statut du SVM auquel les LIFs de données sont associées. Lorsque le SVM est arrêté, le statut opérationnel de la LIF est modifié en down. Lorsque le SVM est de nouveau démarré, le statut opérationnel devient "active"

- Et le port sur lequel réside la LIF

Si les données d'un champ ne sont pas disponibles (par exemple, s'il n'y a pas d'informations d'état étendu), la valeur du champ est répertoriée comme –.

### **Étape**

Affiche les informations relatives aux LIF via la commande `network interface show`.

Vous pouvez afficher des informations détaillées pour chaque LIF en spécifiant le paramètre `-instance`, ou obtenir des informations spécifiques en spécifiant les noms de champs à l'aide du paramètre `-fields`.

La commande suivante affiche des informations générales sur toutes les LIFs d'un cluster :

# network interface show

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Is Port |
|---------|-------------------|-------------------|----------------------|--------------|-----------------|
| Home    |                   |                   |                      |              |                 |
| -----   | -----             | -----             | -----                | -----        | -----           |
| example |                   |                   |                      |              |                 |
|         | lif1              | up/up             | 192.0.2.129/22       | node-01      | e0d             |
| false   |                   |                   |                      |              |                 |
| node    | cluster_mgmt      | up/up             | 192.0.2.3/20         | node-02      | e0c             |
| false   |                   |                   |                      |              |                 |
| node-01 | clus1             | up/up             | 192.0.2.65/18        | node-01      | e0a             |
| true    |                   |                   |                      |              |                 |
|         | clus2             | up/up             | 192.0.2.66/18        | node-01      | e0b             |
| true    |                   |                   |                      |              |                 |
|         | mgmt1             | up/up             | 192.0.2.1/20         | node-01      | e0c             |
| true    |                   |                   |                      |              |                 |
| node-02 | clus1             | up/up             | 192.0.2.67/18        | node-02      | e0a             |
| true    |                   |                   |                      |              |                 |
|         | clus2             | up/up             | 192.0.2.68/18        | node-02      | e0b             |
| true    |                   |                   |                      |              |                 |
|         | mgmt2             | up/up             | 192.0.2.2/20         | node-02      | e0d             |
| true    |                   |                   |                      |              |                 |
| vs1     | d1                | up/up             | 192.0.2.130/21       | node-01      | e0d             |
| false   |                   |                   |                      |              |                 |
|         | d2                | up/up             | 192.0.2.131/21       | node-01      | e0d             |
| true    |                   |                   |                      |              |                 |
|         | data3             | up/up             | 192.0.2.132/20       | node-02      | e0c             |
| true    |                   |                   |                      |              |                 |



La commande suivante affiche des informations détaillées sur une seule LIF :

```
network interface show -lif data1 -instance

Vserver Name: vs1
Logical Interface Name: data1
Role: data
Data Protocol: nfs,cifs
Home Node: node-01
Home Port: e0c
Current Node: node-03
Current Port: e0c
Operational Status: up
Extended Status: -
Is Home: false
Network Address: 192.0.2.128
Netmask: 255.255.192.0
Bits in the Netmask: 18
IPv4 Link Local: -
Subnet Name: -
Administrative Status: up
Failover Policy: local-only
Firewall Policy: data
Auto Revert: false
Fully Qualified DNS Zone Name: xxx.example.com
DNS Query Listen Enable: false
Failover Group Name: Default
FCP WWPN: -
Address family: ipv4
Comment: -
IPspace of LIF: Default
```

**Afficher les informations de routage**

Vous pouvez afficher les informations relatives aux routes au sein d'une SVM.

**Étape**

Selon le type d'informations de routage que vous souhaitez afficher, entrez la commande applicable :

|                                       |                         |
|---------------------------------------|-------------------------|
| Pour afficher des informations sur... | Entrer...               |
| Routes statiques, par SVM             | network route show      |
| LIF sur chaque route, par SVM         | network route show-lifs |

Vous pouvez afficher des informations détaillées pour chaque itinéraire en spécifiant le `-instance` paramètre. La commande suivante affiche les routes statiques au sein des SVM en cluster- 1 :

```
network route show
Vserver Destination Gateway Metric

Cluster
0.0.0.0/0 10.63.0.1 10
cluster-1
0.0.0.0/0 198.51.9.1 10
vs1
0.0.0.0/0 192.0.2.1 20
vs3
0.0.0.0/0 192.0.2.1 20
```

La commande suivante affiche l'association de routes statiques et d'interfaces logiques (LIF) au sein de tous les SVM au sein du cluster-1 :

```
network route show-lifs
Vserver: Cluster
Destination Gateway Logical Interfaces

0.0.0.0/0 10.63.0.1 -

Vserver: cluster-1
Destination Gateway Logical Interfaces

0.0.0.0/0 198.51.9.1 cluster_mgmt,
cluster-1_mgmt1,

Vserver: vs1
Destination Gateway Logical Interfaces

0.0.0.0/0 192.0.2.1 data1_1, data1_2

Vserver: vs3
Destination Gateway Logical Interfaces

0.0.0.0/0 192.0.2.1 data2_1, data2_2
```

## Afficher les entrées de la table des hôtes DNS (administrateurs du cluster uniquement)

Les entrées de la table hôte DNS mappent les noms d'hôte aux adresses IP. Vous pouvez afficher les noms d'hôte et d'alias ainsi que l'adresse IP qu'ils mappent à pour

tous les SVM d'un cluster.

Étape

Afficher les entrées du nom d'hôte pour tous les SVM via la commande `vserver services name-service dns hosts show`.

L'exemple suivant affiche les entrées de la table hôte :

```
vserver services name-service dns hosts show
```

| Vserver   | Address      | Hostname  | Aliases               |
|-----------|--------------|-----------|-----------------------|
| cluster-1 | 10.72.219.36 | lnx219-36 | -                     |
| vs1       | 10.72.219.37 | lnx219-37 | lnx219-37.example.com |

Vous pouvez utiliser le `vserver services name-service dns` Commande permettant d'activer DNS sur un SVM et de le configurer afin d'utiliser DNS pour la résolution de nom d'hôte. Les noms d'hôte sont résolus à l'aide de serveurs DNS externes.

Afficher les configurations de domaine DNS

Vous pouvez afficher la configuration du domaine DNS d'un ou plusieurs SVM (Storage Virtual machine) dans votre cluster pour vérifier qu'ils sont correctement configurés.

Étape

Affichage des configurations de domaine DNS à l'aide de `vserver services name-service dns show` commande.

La commande suivante affiche les configurations DNS pour tous les SVM du cluster :

```
vserver services name-service dns show
```

| Vserver   | State   | Domains         | Name Servers                  |
|-----------|---------|-----------------|-------------------------------|
| cluster-1 | enabled | xyz.company.com | 192.56.0.129,<br>192.56.0.130 |
| vs1       | enabled | xyz.company.com | 192.56.0.129,<br>192.56.0.130 |
| vs2       | enabled | xyz.company.com | 192.56.0.129,<br>192.56.0.130 |
| vs3       | enabled | xyz.company.com | 192.56.0.129,<br>192.56.0.130 |

La commande suivante affiche des informations détaillées de configuration DNS pour le SVM vs1 :

```
vserver services name-service dns show -vserver vs1
 Vserver: vs1
 Domains: xyz.company.com
 Name Servers: 192.56.0.129, 192.56.0.130
 Enable/Disable DNS: enabled
 Timeout (secs): 2
 Maximum Attempts: 1
```

## Affiche des informations relatives aux groupes de basculement

Vous pouvez afficher des informations sur les groupes de basculement, notamment la liste des nœuds et des ports de chaque failover group, si le failover est activé ou désactivé, et le type de failover policy qui est appliquée à chaque LIF.

### Étapes

1. Afficher les ports cibles de chaque failover group en utilisant le `network interface failover-groups show` commande.

La commande suivante affiche des informations sur tous les groupes de basculement sur un cluster à deux nœuds :

```
network interface failover-groups show
 Failover
Vserver Group Targets

Cluster
 Cluster
 cluster1-01:e0a, cluster1-01:e0b,
 cluster1-02:e0a, cluster1-02:e0b
vs1
 Default
 cluster1-01:e0c, cluster1-01:e0d,
 cluster1-01:e0e, cluster1-02:e0c,
 cluster1-02:e0d, cluster1-02:e0e
```

2. Afficher les ports cibles et le broadcast domain d'un failover group spécifique en utilisant le `network interface failover-groups show` commande.

La commande suivante affiche des informations détaillées sur le failover group data12 pour SVM vs4 :

```
network interface failover-groups show -vserver vs4 -failover-group data12
```

```
Vserver Name: vs4
Failover Group Name: data12
Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
 cluster1-02:e0g
Broadcast Domain: Default
```

3. Afficher les paramètres de basculement utilisés par toutes les LIFs à l'aide du `network interface show` commande.

La commande suivante affiche la règle de basculement et le groupe de basculement utilisés par chaque LIF :

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
```

| vserver  | lif                | failover-policy       | failover-group |
|----------|--------------------|-----------------------|----------------|
| -----    | -----              | -----                 | -----          |
| Cluster  | cluster1-01_clus_1 | local-only            | Cluster        |
| Cluster  | cluster1-01_clus_2 | local-only            | Cluster        |
| Cluster  | cluster1-02_clus_1 | local-only            | Cluster        |
| Cluster  | cluster1-02_clus_2 | local-only            | Cluster        |
| cluster1 | cluster_mgmt       | broadcast-domain-wide | Default        |
| cluster1 | cluster1-01_mgmt1  | local-only            | Default        |
| cluster1 | cluster1-02_mgmt1  | local-only            | Default        |
| vs1      | data1              | disabled              | Default        |
| vs3      | data2              | system-defined        | group2         |

## Affiche les cibles de basculement LIF

Vous devrez peut-être vérifier si les stratégies de basculement et les groupes de basculement d'une LIF sont correctement configurés. Pour éviter les erreurs de configuration des règles de basculement, vous pouvez afficher les cibles de basculement d'une seule LIF ou de toutes les LIF.

### Description de la tâche

L'affichage des cibles de basculement LIF vous permet de vérifier les points suivants :

- Indique si les LIF sont configurées avec le bon groupe de basculement et la règle de basculement
- Si la liste des ports cibles de basculement obtenue est appropriée pour chaque LIF
- Si la cible de basculement d'une LIF de données n'est pas un port de gestion (e0M)

### Étape

Afficher les cibles de basculement d'une LIF à l'aide du failover de la network interface show commande.

La commande suivante affiche des informations sur les cibles de basculement pour toutes les LIFs d'un cluster à deux nœuds. Le Failover Targets Ligne affiche la liste (hiérarchisée) de combinaisons nœud-port pour une LIF donnée.

```

network interface show -failover
 Logical Home Failover Failover
Vserver Interface Node:Port Policy Group
----- -
Cluster
 node1_clus1 node1:e0a local-only Cluster
 Failover Targets: node1:e0a,
 node1:e0b
 node1_clus2 node1:e0b local-only Cluster
 Failover Targets: node1:e0b,
 node1:e0a
 node2_clus1 node2:e0a local-only Cluster
 Failover Targets: node2:e0a,
 node2:e0b
 node2_clus2 node2:e0b local-only Cluster
 Failover Targets: node2:e0b,
 node2:e0a
cluster1
 cluster_mgmt node1:e0c broadcast-domain-wide
 Default
 Failover Targets: node1:e0c,
 node1:e0d,
 node2:e0c,
 node2:e0d
 node1_mgmt1 node1:e0c local-only Default
 Failover Targets: node1:e0c,
 node1:e0d
 node2_mgmt1 node2:e0c local-only Default
 Failover Targets: node2:e0c,
 node2:e0d
vs1
 data1 node1:e0e system-defined bcast1
 Failover Targets: node1:e0e,
 node1:e0f,
 node2:e0e,
 node2:e0f

```

## Afficher les LIFs dans une zone d'équilibrage de charge

Vous pouvez vérifier si une zone d'équilibrage de charge est correctement configurée en affichant toutes les LIFs qui l'appartiennent. Vous pouvez également afficher la zone d'équilibrage de la charge d'une LIF particulière ou les zones d'équilibrage de la charge pour toutes les LIFs.

### Étape

Afficher les LIFs et les détails d'équilibrage de charge que vous recherchez à l'aide de l'une des commandes suivantes

| Pour afficher...                                       | Entrer...                                                                                                                    |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| LIF dans une zone d'équilibrage de charge spécifique   | <code>network interface show -dns-zone zone_name</code><br><br>zone_name spécifie le nom de la zone d'équilibrage de charge. |
| La zone d'équilibrage de charge d'une LIF particulière | <code>network interface show -lif lif_name -fields dns-zone</code>                                                           |
| Les zones d'équilibrage de la charge de tous les LIFs  | <code>network interface show -fields dns-zone</code>                                                                         |

### Exemples d'affichage des zones d'équilibrage de charge pour les LIF

La commande suivante affiche le détail de toutes les LIFs de la zone d'équilibrage de la charge storage.company.com pour SVM vs0 :

```
net int show -vserver vs0 -dns-zone storage.company.com
```

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is Home |
|---------|-------------------|-------------------|----------------------|--------------|--------------|---------|
| vs0     | lif3              | up/up             | 10.98.226.225/20     | ndeux-11     | e0c          | true    |
|         | lif4              | up/up             | 10.98.224.23/20      | ndeux-21     | e0c          | true    |
|         | lif5              | up/up             | 10.98.239.65/20      | ndeux-11     | e0c          | true    |
|         | lif6              | up/up             | 10.98.239.66/20      | ndeux-11     | e0c          | true    |
|         | lif7              | up/up             | 10.98.239.63/20      | ndeux-21     | e0c          | true    |
|         | lif8              | up/up             | 10.98.239.64/20      | ndeux-21     | e0c          | true    |

La commande suivante affiche les détails de la zone DNS du datas3 :

```
network interface show -lif data3 -fields dns-zone
Vserver lif dns-zone

vs0 data3 storage.company.com
```

La commande suivante affiche la liste de toutes les LIFs du cluster et leurs zones DNS correspondantes :

```
network interface show -fields dns-zone
Vserver lif dns-zone

cluster cluster_mgmt none
ndeux-21 clus1 none
ndeux-21 clus2 none
ndeux-21 mgmt1 none
vs0 data1 storage.company.com
vs0 data2 storage.company.com
```

## Afficher les connexions du cluster

Vous pouvez afficher toutes les connexions actives du cluster ou un nombre de connexions actives sur le nœud par client, interface logique, protocole ou service. Vous pouvez également afficher toutes les connexions d'écoute dans le cluster.

### Affichage des connexions actives par le client (administrateurs du cluster uniquement)

Vous pouvez afficher les connexions actives par client pour vérifier le nœud qu'un client spécifique utilise et pour afficher les écarts possibles entre le nombre de clients par nœud.

#### Description de la tâche

Le nombre de connexions actives par client est utile dans les scénarios suivants :

- Recherche d'un nœud occupé ou surchargé.
- Déterminer pourquoi l'accès d'un client à un volume est lent.

Vous pouvez afficher des informations sur le nœud auquel le client accède, puis les comparer avec le nœud sur lequel réside le volume. Si l'accès au volume nécessite la gestion du réseau en cluster, les performances des clients peuvent être réduites en raison de l'accès à distance au volume sur un nœud distant sursouscrit.

- Vérification de l'utilisation de tous les nœuds identique pour l'accès aux données.
- Détection des clients disposant d'un nombre de connexions élevé de manière inattendue.
- Vérifier si certains clients ont des connexions à un nœud.

#### Étape

Affiche le nombre de connexions actives par client sur un nœud à l'aide du `network connections active show-clients` commande.



Pour plus d'informations sur cette commande, reportez-vous au ["Référence de commande ONTAP"](#).

```
network connections active show-clients
Node Vserver Name Client IP Address Count

node0 vs0 192.0.2.253 1
 vs0 192.0.2.252 2
 Cluster 192.10.2.124 5
node1 vs0 192.0.2.250 1
 vs0 192.0.2.252 3
 Cluster 192.10.2.123 4
node2 vs1 customer.example.com 1
 vs1 192.0.2.245 3
 Cluster 192.10.2.122 4
node3 vs1 customer.example.org 1
 vs1 customer.example.net 3
 Cluster 192.10.2.121 4
```

### Affichage des connexions actives par protocole (administrateurs du cluster uniquement)

Vous pouvez afficher un nombre de connexions actives par protocole (TCP ou UDP) sur un nœud afin de comparer l'utilisation des protocoles au sein du cluster.

#### Description de la tâche

Le nombre de connexions actives par protocole est utile dans les scénarios suivants :

- Recherche des clients UDP qui perdent leur connexion.

Si un nœud se trouve à proximité de sa limite de connexion, les clients UDP sont les premiers à être abandonnés.

- Vérification qu'aucun autre protocole n'est utilisé

#### Étape

Affiche le nombre de connexions actives par protocole sur un nœud à l'aide de `network connections active show-protocols` commande.

Pour plus d'informations sur cette commande, consultez la page `man`.

```

network connections active show-protocols
Node Vserver Name Protocol Count

node0
 vs0 UDP 19
 Cluster TCP 11
node1
 vs0 UDP 17
 Cluster TCP 8
node2
 vs1 UDP 14
 Cluster TCP 10
node3
 vs1 UDP 18
 Cluster TCP 4

```

### Affichage des connexions actives par service (administrateurs du cluster uniquement)

Vous pouvez afficher un nombre de connexions actives par type de service (par exemple, par NFS, SMB, montage, etc.) pour chaque nœud d'un cluster. Cette fonction est utile pour comparer l'utilisation des services au sein du cluster, ce qui permet de déterminer la charge de travail principale d'un nœud.

#### Description de la tâche

Le nombre de connexions actives par service est utile dans les scénarios suivants :

- Vérifier que tous les nœuds sont utilisés pour les services appropriés et que l'équilibrage de la charge pour ce service fonctionne.
- Vérifier qu'aucun autre service n'est utilisé. Affiche le nombre de connexions actives par service sur un nœud à l'aide du `network connections active show-services` commande.

Pour plus d'informations sur cette commande, reportez-vous à la page man : ["Référence de commande ONTAP"](#)

```

network connections active show-services
Node Vserver Name Service Count

node0
 vs0 mount 3
 vs0 nfs 14
 vs0 nlm_v4 4
 vs0 cifs_srv 3
 vs0 port_map 18
 vs0 rclopcp 27
 Cluster ctlopcp 60
node1
 vs0 cifs_srv 3
 vs0 rclopcp 16
 Cluster ctlopcp 60
node2
 vs1 rclopcp 13
 Cluster ctlopcp 60
node3
 vs1 cifs_srv 1
 vs1 rclopcp 17
 Cluster ctlopcp 60

```

## Afficher les connexions actives par LIF sur un nœud et un SVM

Vous pouvez afficher un nombre de connexions actives pour chaque LIF, par nœud et SVM (Storage Virtual machine), afin d'afficher les déséquilibres de connexion entre les LIF au sein du cluster.

### Description de la tâche

Le nombre de connexions actives par LIF est utile dans les scénarios suivants :

- Trouver une LIF surchargée en comparant le nombre de connexions sur chaque LIF.
- Vérification du fonctionnement de l'équilibrage de la charge DNS pour toutes les LIFs de données.
- Comparaison du nombre de connexions aux différents SVM pour trouver les SVM les plus utilisés.

### Étape

Afficher le nombre de connexions actives pour chaque LIF par SVM et nœud en utilisant le `network connections active show-lifs` commande.

Pour plus d'informations sur cette commande, reportez-vous à la page man : ["Référence de commande ONTAP"](#)

```

network connections active show-lifs
Node Vserver Name Interface Name Count

node0
 vs0 datalif1 3
 Cluster node0_clus_1 6
 Cluster node0_clus_2 5
node1
 vs0 datalif2 3
 Cluster node1_clus_1 3
 Cluster node1_clus_2 5
node2
 vs1 datalif2 1
 Cluster node2_clus_1 5
 Cluster node2_clus_2 3
node3
 vs1 datalif1 1
 Cluster node3_clus_1 2
 Cluster node3_clus_2 2

```

## Affiche les connexions actives dans un cluster

Vous pouvez afficher des informations sur les connexions actives dans un cluster pour afficher les LIF, le port, l'hôte distant, le service, les SVM (Storage Virtual machines) et le protocole utilisé par des connexions individuelles.

### Description de la tâche

L'affichage des connexions actives dans un cluster est utile dans les scénarios suivants :

- Vérifier que chaque client utilise le protocole et le service appropriés sur le nœud.
- Si un client rencontre des difficultés pour accéder aux données à l'aide d'une certaine combinaison de nœud, de protocole et de service, vous pouvez utiliser cette commande pour trouver un client similaire pour la comparaison de la configuration ou de la trace des paquets.

### Étape

Afficher les connexions actives dans un cluster à l'aide du `network connections active show` commande.

Pour plus d'informations sur cette commande, reportez-vous à la page man : "[Référence de commande ONTAP](#)".

La commande suivante affiche les connexions actives sur le nœud node1 :

```
network connections active show -node node1
```

| Vserver     | Interface          | Remote             |                  |
|-------------|--------------------|--------------------|------------------|
| Name        | Name:Local Port    | Host:Port          | Protocol/Service |
| -----       | -----              | -----              | -----            |
| Node: node1 |                    |                    |                  |
| Cluster     | node1_clus_1:50297 | 192.0.2.253:7700   | TCP/ctlopcp      |
| Cluster     | node1_clus_1:13387 | 192.0.2.253:7700   | TCP/ctlopcp      |
| Cluster     | node1_clus_1:8340  | 192.0.2.252:7700   | TCP/ctlopcp      |
| Cluster     | node1_clus_1:42766 | 192.0.2.252:7700   | TCP/ctlopcp      |
| Cluster     | node1_clus_1:36119 | 192.0.2.250:7700   | TCP/ctlopcp      |
| vs1         | data1:111          | host1.aa.com:10741 | UDP/port-map     |
| vs3         | data2:111          | host1.aa.com:10741 | UDP/port-map     |
| vs1         | data1:111          | host1.aa.com:12017 | UDP/port-map     |
| vs3         | data2:111          | host1.aa.com:12017 | UDP/port-map     |

La commande suivante montre les connexions actives sur le SVM vs1 :

```
network connections active show -vserver vs1
```

| Vserver     | Interface       | Remote             |                  |
|-------------|-----------------|--------------------|------------------|
| Name        | Name:Local Port | Host:Port          | Protocol/Service |
| -----       | -----           | -----              | -----            |
| Node: node1 |                 |                    |                  |
| vs1         | data1:111       | host1.aa.com:10741 | UDP/port-map     |
| vs1         | data1:111       | host1.aa.com:12017 | UDP/port-map     |

## Affiche les connexions d'écoute dans un cluster

Vous pouvez afficher les informations relatives aux connexions d'écoute dans un cluster pour afficher les LIFs et les ports qui acceptent les connexions pour un protocole et un service donnés.

### Description de la tâche

L'affichage des connexions d'écoute dans un cluster est utile dans les scénarios suivants :

- Vérifier que le protocole ou le service désiré est à l'écoute d'une LIF si les connexions client à cette LIF échouent de manière cohérente.
- Vérification de l'ouverture d'un écouteur UDP/rclopcp au niveau de chaque LIF du cluster si l'accès des données à distance à un volume sur un nœud via une LIF sur un autre nœud échoue.
- Vérifier qu'un écouteur UDP/rclopcp est ouvert au niveau de chaque LIF du cluster si le transfert SnapMirror entre deux nœuds du même cluster échoue.
- Vérifier qu'un écouteur TCP/ctlopcp est ouvert sur chaque LIF intercluster si les transferts SnapMirror entre deux nœuds de différents clusters échouent.

### Étape

Affichez les connexions d'écoute par nœud à l'aide du `network connections listening show` commande.

```

network connections listening show
Vserver Name Interface Name:Local Port Protocol/Service

Node: node0
Cluster node0_clus_1:7700 TCP/ctlopcp
vs1 data1:4049 UDP/unknown
vs1 data1:111 TCP/port-map
vs1 data1:111 UDP/port-map
vs1 data1:4046 TCP/sm
vs1 data1:4046 UDP/sm
vs1 data1:4045 TCP/nlm-v4
vs1 data1:4045 UDP/nlm-v4
vs1 data1:2049 TCP/nfs
vs1 data1:2049 UDP/nfs
vs1 data1:635 TCP/mount
vs1 data1:635 UDP/mount
Cluster node0_clus_2:7700 TCP/ctlopcp

```

## Commandes permettant de diagnostiquer les problèmes réseau

Vous pouvez diagnostiquer des problèmes sur votre réseau à l'aide de commandes telles que `ping`, `tracert`, `ndp`, et `tcpdump`. Vous pouvez également utiliser des commandes comme `ping6` et `tracert6` Pour diagnostiquer les problèmes IPv6.

| Les fonctions que vous recherchez...                                                                                                                                                     | Entrez cette commande...                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Vérifiez si le nœud peut atteindre d'autres hôtes sur votre réseau                                                                                                                       | <code>network ping</code>                                                                                        |
| Vérifiez si le nœud peut atteindre d'autres hôtes sur votre réseau IPv6                                                                                                                  | <code>network ping6</code>                                                                                       |
| Suivez la route que les paquets IPv4 prennent à un nœud réseau                                                                                                                           | <code>network tracert</code>                                                                                     |
| Suivez la route que les paquets IPv6 prennent sur un nœud réseau                                                                                                                         | <code>network tracert6</code>                                                                                    |
| Gérer le Protocole de découverte des voisins (NDP)                                                                                                                                       | <code>network ndp</code>                                                                                         |
| Affiche des statistiques sur les paquets reçus et envoyés sur une interface réseau spécifiée ou sur toutes les interfaces réseau                                                         | <code>run -node node_name ifstat</code><br><br><b>Note:</b> Cette commande est disponible à partir du nodeshell. |
| Affiche des informations sur les périphériques voisins découverts à partir de chaque nœud et port du cluster, y compris le type de périphérique distant et la plateforme de périphérique | <code>network device-discovery show</code>                                                                       |

|                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Afficher les voisins CDP du nœud (ONTAP prend uniquement en charge les publicités CDPv1) | <pre>run -node <i>node_name</i> cdpd show-neighbors</pre> <p><b>Note:</b> Cette commande est disponible à partir du nodeshell.</p>                                                                                                                                                                                                                                                            |
| Suivez les paquets envoyés et reçus sur le réseau                                        | <pre>network tcpdump start -node <i>node-name</i> -port <i>port_name</i></pre> <p><b>Note:</b> Cette commande est disponible à partir du nodeshell.</p>                                                                                                                                                                                                                                       |
| Mesure de la latence et du débit entre les nœuds intercluster ou intracluster            | <pre>network test -path -source-node <i>source_nodename</i> local -destination -cluster <i>destination_clustername</i> -destination-node <i>destination_nodename</i> -session-type <i>Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer</i></pre> <p>Pour plus d'informations, reportez-vous à la section <a href="#">"Gestion des performances"</a>.</p> |

Pour plus d'informations sur ces commandes, reportez-vous à la section ["Référence de commande ONTAP"](#).

## Affiche la connectivité réseau avec les protocoles de détection de voisins

### Affiche la connectivité réseau avec les protocoles de détection de voisins

Dans un data Center, vous pouvez utiliser des protocoles de découverte voisins pour afficher la connectivité réseau entre une paire de systèmes physiques ou virtuels et leurs interfaces réseau. ONTAP prend en charge deux protocoles de découverte de voisins : le Cisco Discovery Protocol (CDP) et le Link Layer Discovery Protocol (LLDP).

Les protocoles de détection de voisins vous permettent de détecter et d'afficher automatiquement des informations sur les périphériques compatibles avec des protocoles directement connectés sur un réseau. Chaque appareil transmet des informations d'identification, de fonctionnalités et de connectivité. Ces informations sont transmises en trames Ethernet à une adresse MAC multicast et sont reçues par tous les périphériques compatibles avec les protocoles voisins.

Pour que deux périphériques deviennent voisins, un protocole doit être activé et correctement configuré. La fonctionnalité du protocole de découverte est limitée aux réseaux directement connectés. Les voisins peuvent inclure des périphériques compatibles avec les protocoles, tels que des commutateurs, des routeurs, des ponts, etc. ONTAP prend en charge deux protocoles de détection de voisins, qui peuvent être utilisés individuellement ou conjointement.

### Cisco Discovery Protocol (CDP)

CDP est un protocole propriétaire de couche de liaison développé par Cisco Systems. Il est activé par défaut dans ONTAP pour les ports de cluster, mais il doit être activé explicitement pour les ports de données.

### Protocole LLDP (Link Layer Discovery Protocol)

LLDP est un protocole indépendant du fournisseur spécifié dans le document de normes IEEE 802.1AB. Elle

doit être activée explicitement pour tous les ports.

### Utilisez CDP pour détecter la connectivité réseau

L'utilisation de CDP pour détecter la connectivité réseau consiste à examiner les considérations relatives au déploiement, à l'activer sur les ports de données, à afficher les périphériques voisins et à ajuster les valeurs de configuration CDP selon les besoins. Le protocole CDP est activé par défaut sur les ports du cluster.

Le protocole CDP doit également être activé sur tous les commutateurs et routeurs avant que les informations relatives aux périphériques voisins puissent être affichées.

| Version de ONTAP               | Description                                                                                                                                                                           |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9.10.1 et versions antérieures | Le protocole CDP est également utilisé par le contrôle de l'état du switch du cluster pour détecter automatiquement les commutateurs du cluster et du réseau de gestion.              |
| 9.11.1 et versions ultérieures | Le protocole CDP est également utilisé par le contrôle de l'état du switch du cluster pour détecter automatiquement les commutateurs du cluster, du stockage et du réseau de gestion. |

### Informations associées

["Administration du système"](#)

### Considérations relatives à l'utilisation de CDP

Par défaut, les périphériques compatibles CDP envoient des publicités CDPv2. Les appareils compatibles CDP envoient des publicités CDPv1 uniquement lorsqu'ils reçoivent des publicités CDPv1. ONTAP ne prend en charge que CDPv1. Par conséquent, lorsqu'un nœud ONTAP envoie des publicités CDPv1, les périphériques voisins compatibles CDP envoient des publicités CDPv1.

Avant d'activer le CDP sur un nœud, tenez compte des informations suivantes :

- Tous les ports CDP sont pris en charge.
- Les publicités CDP sont envoyées et reçues par les ports qui sont à l'état up.
- Le CDP doit être activé sur les appareils d'émission et de réception pour l'envoi et la réception de publicités CDP.
- Les annonces CDP sont envoyées à intervalles réguliers et vous pouvez configurer l'intervalle de temps.
- Lorsque les adresses IP sont modifiées pour une LIF, le nœud envoie les informations mises à jour dans la prochaine publicité CDP.
- ONTAP 9.10.1 et versions antérieures :
  - Le protocole CDP est toujours activé sur les ports du cluster.
  - Le protocole CDP est désactivé par défaut sur tous les ports qui ne sont pas du cluster.
- ONTAP 9.11.1 et versions ultérieures :
  - Le protocole CDP est toujours activé sur les ports du cluster et de stockage.
  - Par défaut, le protocole CDP est désactivé sur tous les ports non-cluster et non-stockage.





Parfois, lorsque les LIFs sont modifiées sur le nœud, les informations du CDP ne sont pas mises à jour côté du périphérique de réception (par exemple, un switch). Si vous rencontrez un tel problème, vous devez configurer l'interface réseau du nœud sur l'état down, puis sur l'état up.

- Seules les adresses IPv4 sont annoncées dans les publicités CDP.
- Pour les ports réseau physique avec des VLAN, toutes les LIF configurées sur ce port sont annoncées.
- Pour les ports physiques faisant partie d'un groupe d'interfaces, toutes les adresses IP configurées sur ce groupe d'interfaces sont annoncées sur chaque port physique.
- Pour un groupe d'interface qui héberge les VLAN, toutes les LIF configurées sur le groupe d'interface et les VLAN sont annoncés sur chacun des ports réseau.
- En raison de la restriction des paquets CDP à 1500 octets maximum, sur les ports Configuré avec un grand nombre de LIF, seul un sous-ensemble de ces adresses IP peut être signalé sur le commutateur adjacent.

### Activer ou désactiver CDP

Pour détecter et envoyer des publicités aux périphériques voisins conformes à la norme CDP, le protocole CDP doit être activé sur chaque nœud du cluster.

Par défaut dans ONTAP 9.10.1 et versions antérieures, CDP est activée sur tous les ports de cluster d'un nœud et désactivée sur tous les ports qui ne sont pas du cluster d'un nœud.

Par défaut dans ONTAP 9.11.1 et versions ultérieures, CDP est activée sur l'ensemble du cluster et des ports de stockage d'un nœud et désactivée sur tous les ports non-cluster et non-stockage d'un nœud.

### Description de la tâche

Le `cdpd.enable` Option contrôle si CDP est activée ou désactivée sur les ports d'un nœud :

- Pour les versions ONTAP 9.10.1 et antérieures, on active le CDP sur les ports hors cluster.
- Pour les versions ONTAP 9.11.1 et ultérieures, on active le CDP sur les ports non-cluster et non-stockage.
- Pour les versions ONTAP 9.10.1 et antérieures, off désactive le protocole CDP sur les ports hors cluster ; vous ne pouvez pas désactiver le protocole CDP sur les ports de cluster.
- Pour ONTAP 9.11.1 et versions ultérieures, off désactive le protocole CDP sur les ports non-cluster et non-stockage ; vous ne pouvez pas désactiver le protocole CDP sur les ports du cluster.

Lorsque le protocole CDP est désactivé sur un port connecté à un périphérique compatible CDP, le trafic réseau peut ne pas être optimisé.

### Étapes

1. Afficher le paramètre CDP actuel d'un nœud ou de tous les nœuds d'un cluster :

|                                      |                                                               |
|--------------------------------------|---------------------------------------------------------------|
| Pour afficher le paramètre CDP de... | Entrer...                                                     |
| Un nœud                              | <code>run - node &lt;node_name&gt; options cdpd.enable</code> |
| Tous les nœuds d'un cluster          | <code>options cdpd.enable</code>                              |

2. Activer ou désactiver CDP sur tous les ports d'un nœud, ou sur tous les ports de tous les nœuds d'un cluster :

|                                       |                                                                  |
|---------------------------------------|------------------------------------------------------------------|
| Pour activer ou désactiver CDP sur... | Entrer...                                                        |
| Un nœud                               | <code>run -node node_name options cdpd.enable {on or off}</code> |
| Tous les nœuds d'un cluster           | <code>options cdpd.enable {on or off}</code>                     |

### Afficher les informations sur les voisins CDP

Vous pouvez afficher des informations sur les périphériques voisins qui sont connectés à chaque port des nœuds de votre cluster, à condition que le port soit connecté à un périphérique compatible CDP. Vous pouvez utiliser le `network device-discovery show -protocol cdp` commande pour afficher les informations relatives au voisin.

### Description de la tâche

Dans les versions ONTAP 9.10.1 et antérieures, étant donné que le protocole CDP est toujours activé pour les ports de cluster, les informations des voisins CDP sont toujours affichées pour ces ports. Le protocole CDP doit être activé sur des ports autres que le cluster pour que les informations relatives aux voisins s'affichent sur ces ports.

Dans la version ONTAP 9.11.1 et ultérieure, étant donné que le protocole CDP est toujours activé pour les ports de cluster et de stockage, les informations des voisins CDP sont toujours affichées pour ces ports. Le protocole CDP doit être activé sur les ports non-cluster et non-stockage afin que les informations relatives aux voisins s'affichent pour ces ports.

### Étape

Affiche des informations sur tous les appareils compatibles CDP connectés aux ports d'un nœud du cluster :

```
network device-discovery show -node node -protocol cdp
```

La commande suivante indique les voisins connectés aux ports du nœud sti2650-212 :

```

network device-discovery show -node sti2650-212 -protocol cdp
Node/ Local Discovered
Protocol Port Device (LLDP: ChassisID) Interface Platform

sti2650-212/cdp
 e0M RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
 Ethernet1/14 N9K-
C93120TX
 e0a CS:RTP-CS01-510K35 0/8 CN1610
 e0b CS:RTP-CS01-510K36 0/8 CN1610
 e0c RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
 Ethernet1/21 N9K-
C93180YC-FX
 e0d RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
 Ethernet1/22 N9K-
C93180YC-FX
 e0e RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
 Ethernet1/23 N9K-
C93180YC-FX
 e0f RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
 Ethernet1/24 N9K-
C93180YC-FX

```

La sortie répertorie les périphériques Cisco connectés à chaque port du nœud spécifié.

#### Configurez la durée de mise en attente des messages CDP

La durée de conservation correspond à la période pendant laquelle les publicités CDP sont stockées en cache sur les périphériques compatibles CDP voisins. Le temps de mise en attente est annoncé dans chaque paquet CDPv1 et mis à jour chaque fois qu'un paquet CDPv1 est reçu par un nœud.

- La valeur du `cdpd.holdtime` L'option doit être définie sur la même valeur sur les deux nœuds d'une paire HA.
- La valeur par défaut du temps de maintien est de 180 secondes, mais vous pouvez entrer des valeurs comprises entre 10 secondes et 255 secondes.
- Si une adresse IP est supprimée avant l'expiration du délai de mise en attente, les informations CDP sont mises en cache jusqu'à ce que le délai de mise en attente expire.

#### Étapes

1. Afficher l'heure de maintien CDP actuelle d'un nœud ou de tous les nœuds d'un cluster :

|                                          |                                                        |
|------------------------------------------|--------------------------------------------------------|
| Pour afficher le temps de maintien de... | Entrer...                                              |
| Un nœud                                  | <code>run -node node_name options cdpd.holdtime</code> |

|                             |                                    |
|-----------------------------|------------------------------------|
| Tous les nœuds d'un cluster | <code>options cdpd.holdtime</code> |
|-----------------------------|------------------------------------|

2. Configurer le délai de mise en attente du CDP sur tous les ports d'un nœud ou sur tous les ports de tous les nœuds d'un cluster :

|                                      |                                                                 |
|--------------------------------------|-----------------------------------------------------------------|
| Pour activer le temps de maintien... | Entrer...                                                       |
| Un nœud                              | <code>run -node node_name options cdpd.holdtime holdtime</code> |
| Tous les nœuds d'un cluster          | <code>options cdpd.holdtime holdtime</code>                     |

### Définissez l'intervalle d'envoi de publicités CDP

Les publicités CDP sont envoyées régulièrement aux voisins CDP. Vous pouvez augmenter ou réduire l'intervalle d'envoi de publicités CDP en fonction du trafic réseau et des modifications de la topologie réseau.

- La valeur du `cdpd.interval` L'option doit être définie sur la même valeur sur les deux nœuds d'une paire HA.
- L'intervalle par défaut est de 60 secondes, mais vous pouvez entrer une valeur de 5 à 900 secondes.

### Étapes

1. Afficher l'intervalle de temps publicitaire du CDP actuel pour un nœud ou pour tous les nœuds d'un cluster :

|                                  |                                                        |
|----------------------------------|--------------------------------------------------------|
| Pour afficher l'intervalle de... | Entrer...                                              |
| Un nœud                          | <code>run -node node_name options cdpd.interval</code> |
| Tous les nœuds d'un cluster      | <code>options cdpd.interval</code>                     |

2. Configurer l'intervalle d'envoi de publicités CDP pour tous les ports d'un nœud ou pour tous les ports de tous les nœuds d'un cluster :

|                                 |                                                                 |
|---------------------------------|-----------------------------------------------------------------|
| Pour définir l'intervalle de... | Entrer...                                                       |
| Un nœud                         | <code>run -node node_name options cdpd.interval interval</code> |
| Tous les nœuds d'un cluster     | <code>options cdpd.interval interval</code>                     |

### Afficher ou effacer les statistiques CDP

Vous pouvez afficher les statistiques CDP des ports du cluster et non du cluster sur chaque nœud afin de détecter d'éventuels problèmes de connectivité réseau. Les statistiques CDP sont cumulatives à partir de leur dernière suppression.

### Description de la tâche

Dans les versions ONTAP 9.10.1 et antérieures, étant donné que le protocole CDP est toujours activé pour les ports, les statistiques CDP sont toujours affichées pour le trafic sur ces ports. Le protocole CDP doit être activé sur les ports pour que les statistiques apparaissent sur ces ports.

Dans les versions ONTAP 9.11.1 et ultérieures, puisque le CDP est toujours activé pour les ports du cluster et de stockage, les statistiques CDP sont toujours affichées pour le trafic sur ces ports. Le protocole CDP doit être activé sur des ports non-cluster ou non-Storage pour que les statistiques de ces ports s’affichent.

Étape

Afficher ou effacer les statistiques CDP actuelles de tous les ports d’un nœud :

|                                      |                                     |
|--------------------------------------|-------------------------------------|
| Les fonctions que vous recherchez... | Entrer...                           |
| Afficher les statistiques CDP        | run -node node_name cdpd show-stats |
| Effacer les statistiques CDP         | run -node node_name cdpd zero-stats |

Exemple d’affichage et d’effacement des statistiques

La commande suivante affiche les statistiques CDP avant leur effacement. La sortie affiche le nombre total de paquets envoyés et reçus depuis la dernière suppression des statistiques.

```
run -node nodel cdpd show-stats

RECEIVE
Packets: 9116 | Csum Errors: 0 | Unsupported Vers: 4561
Invalid length: 0 | Malformed: 0 | Mem alloc fails: 0
Missing TLVs: 0 | Cache overflow: 0 | Other errors: 0

TRANSMIT
Packets: 4557 | Xmit fails: 0 | No hostname: 0
Packet truncated: 0 | Mem alloc fails: 0 | Other errors: 0

OTHER
Init failures: 0
```

La commande suivante efface les statistiques CDP :

```
run -node nodel cdpd zero-stats
```

```
run -node nodel cdpd show-stats
```

#### RECEIVE

|                 |   |  |                 |   |  |                   |   |
|-----------------|---|--|-----------------|---|--|-------------------|---|
| Packets:        | 0 |  | Csum Errors:    | 0 |  | Unsupported Vers: | 0 |
| Invalid length: | 0 |  | Malformed:      | 0 |  | Mem alloc fails:  | 0 |
| Missing TLVs:   | 0 |  | Cache overflow: | 0 |  | Other errors:     | 0 |

#### TRANSMIT

|                   |   |  |                  |   |  |               |   |
|-------------------|---|--|------------------|---|--|---------------|---|
| Packets:          | 0 |  | Xmit fails:      | 0 |  | No hostname:  | 0 |
| Packet truncated: | 0 |  | Mem alloc fails: | 0 |  | Other errors: | 0 |

#### OTHER

|                |   |
|----------------|---|
| Init failures: | 0 |
|----------------|---|

Une fois les statistiques effacées, elles commencent à s'accumuler après l'envoi ou la réception de la prochaine annonce CDP.

### Connexion à des commutateurs Ethernet qui ne prennent pas en charge CDP

Les commutateurs de plusieurs fournisseurs ne prennent pas en charge le protocole CDP. Consultez l'article de la base de connaissances ["La découverte de périphériques ONTAP affiche les nœuds au lieu du commutateur"](#) pour plus d'informations.

Il existe deux options pour résoudre ce problème :

- Désactivez CDP et activez LLDP, si pris en charge. Voir ["Utilisez LLDP pour détecter la connectivité réseau"](#) pour plus d'informations.
- Configurez un filtre de paquets d'adresses MAC sur les commutateurs pour abandonner les annonces CDP.

### Utilisez LLDP pour détecter la connectivité réseau

L'utilisation du protocole LLDP pour détecter la connectivité réseau consiste à examiner les considérations de déploiement, à l'activer sur tous les ports, à visualiser les périphériques voisins et à ajuster les valeurs de configuration LLDP si nécessaire.

Le protocole LLDP doit également être activé sur tous les commutateurs et routeurs avant que des informations sur les périphériques voisins puissent être affichées.

ONTAP indique actuellement les structures de valeur de type-longueur (TLV) suivantes :

- ID de châssis
- ID de port
- Durée de vie (TTL)
- Nom du système

Le nom système TLV n'est pas envoyé sur les périphériques CNA.

Certains adaptateurs réseau convergés (CNA), tels que l'adaptateur X1143 et les ports intégrés UTA2, contiennent la prise en charge de l'allègement de la charge pour le protocole LLDP :

- Le déchargement LLDP est utilisé pour le pontage du Data Center (DCB).
- Les informations affichées peuvent différer entre le cluster et le commutateur.

Les données d'ID de châssis et de port affichées par le commutateur peuvent être différentes pour les ports CNA et non CNA.

Par exemple :

- Pour les ports non CNA :
  - L'ID de châssis est une adresse MAC fixe de l'un des ports du nœud
  - ID de port correspond au nom du port respectif sur le nœud
- Pour les ports CNA :
  - L'ID de châssis et l'ID de port sont les adresses MAC des ports respectifs du nœud.

Cependant, les données affichées par le cluster sont cohérentes pour ces types de port.



La spécification LLDP définit l'accès aux informations collectées via une MIB SNMP. Cependant, ONTAP ne supporte pas actuellement la MIB LLDP.

#### Activer ou désactiver le protocole LLDP

Pour détecter et envoyer des publicités aux périphériques voisins conformes au protocole LLDP, LLDP doit être activé sur chaque nœud du cluster. Depuis ONTAP 9.7, LLDP est activé par défaut sur tous les ports d'un nœud.

#### Description de la tâche

Pour ONTAP 9.10.1 et versions antérieures, le `lldp.enable` Option contrôle si LLDP est activé ou désactivé sur les ports d'un nœud :

- `on` Active LLDP sur tous les ports.
- `off` Désactive LLDP sur tous les ports.

Pour ONTAP 9.11.1 et versions ultérieures, le `lldp.enable` Option contrôle si LLDP est activé ou désactivé sur les ports non-cluster et non-stockage d'un nœud :

- `on` Active LLDP sur tous les ports non-cluster et non-stockage.
- `off` Désactive LLDP sur tous les ports non-cluster et non-stockage.

#### Étapes

1. Afficher le paramètre LLDP actuel pour un nœud ou pour tous les nœuds d'un cluster :
  - Un seul nœud : `run -node node_name options lldp.enable`
  - Tous les nœuds : `options lldp.enable`
2. Activer ou désactiver le protocole LLDP sur tous les ports d'un nœud ou sur tous les ports de tous les nœuds d'un cluster :

|                                           |                                              |
|-------------------------------------------|----------------------------------------------|
| Pour activer ou désactiver LLDP activé... | Entrer...                                    |
| Un nœud                                   | `run -node node_name options lldp.enable {on |
| off}`                                     | Tous les nœuds d'un cluster                  |
| `options lldp.enable {on                  | off}`                                        |

- Un seul nœud :

```
run -node node_name options lldp.enable {on|off}
```

- Tous les nœuds :

```
options lldp.enable {on|off}
```

### Afficher les informations de voisinage LLDP

Vous pouvez afficher des informations sur les périphériques voisins qui sont connectés à chaque port des nœuds de votre cluster, à condition que le port soit connecté à un périphérique compatible LLDP. Vous utilisez la commande `network device-discovery show` pour afficher les informations relatives aux voisins.

#### Étape

1. Affiche des informations sur tous les périphériques conformes au protocole LLDP connectés aux ports d'un nœud du cluster :

```
network device-discovery show -node node -protocol lldp
```

La commande suivante affiche les voisins connectés aux ports du nœud `cluster-1_01`. La sortie répertorie les périphériques compatibles LLDP qui sont connectés à chaque port du nœud spécifié. Si le `-protocol` Option omise, la sortie répertorie également les périphériques compatibles CDP.

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/ Local Discovered
Protocol Port Device

cluster-1_01/lldp
 e2a 0013.c31e.5c60 GigabitEthernet1/36
 e2b 0013.c31e.5c60 GigabitEthernet1/35
 e2c 0013.c31e.5c60 GigabitEthernet1/34
 e2d 0013.c31e.5c60 GigabitEthernet1/33
```



## Réglez l'intervalle de transmission des annonces LLDP

Les annonces du LLDP sont envoyées à intervalles réguliers aux voisins du LLDP. Vous pouvez augmenter ou diminuer l'intervalle d'envoi des annonces LLDP en fonction du trafic réseau et des modifications de la topologie du réseau.

### Description de la tâche

L'intervalle par défaut recommandé par IEEE est de 30 secondes, mais vous pouvez entrer une valeur de 5 secondes à 300 secondes.

### Étapes

1. Afficher l'intervalle de temps de publicité LLDP actuel pour un nœud ou pour tous les nœuds d'un cluster :

- Un seul nœud :

```
run -node <node_name> options lldp.xmit.interval
```

- Tous les nœuds :

```
options lldp.xmit.interval
```

2. Réglez l'intervalle d'envoi des annonces LLDP pour tous les ports d'un nœud ou pour tous les ports de tous les nœuds d'un cluster :

- Un seul nœud :

```
run -node <node_name> options lldp.xmit.interval <interval>
```

- Tous les nœuds :

```
options lldp.xmit.interval <interval>
```

## Réglez la valeur de temps de mise en ligne pour les annonces LLDP

Le temps de mise en service (TTL) est la période pendant laquelle les publicités LLDP sont stockées dans le cache dans les périphériques conformes LLDP voisins. TTL est annoncé dans chaque paquet LLDP et mis à jour chaque fois qu'un paquet LLDP est reçu par un nœud. TTL peut être modifié dans les trames LLDP sortantes.

### Description de la tâche

- TTL est une valeur calculée, produit de l'intervalle de transmission (`lldp.xmit.interval`) et le multiplicateur hold (`lldp.xmit.hold`) plus un.
- La valeur par défaut du multiplicateur de maintien est 4, mais vous pouvez entrer des valeurs comprises entre 1 et 100.
- Le TTL par défaut est donc de 121 secondes, comme recommandé par l'IEEE, mais en ajustant l'intervalle de transmission et les valeurs multiplicatrices de maintien, vous pouvez spécifier une valeur pour les trames sortantes de 6 à 30001 secondes.

- Si une adresse IP est supprimée avant l'expiration du TTL, les informations LLDP sont mises en cache jusqu'à expiration du TTL.

## Étapes

1. Afficher la valeur du multiplicateur de maintien actuel pour un nœud ou pour tous les nœuds d'un cluster :

- Un seul nœud :

```
run -node <node_name> options lldp.xmit.hold
```

- Tous les nœuds :

```
options lldp.xmit.hold
```

2. Ajustez la valeur du multiplicateur de maintien sur tous les ports d'un nœud ou sur tous les ports de tous les nœuds d'un cluster :

- Un seul nœud :

```
run -node <node_name> options lldp.xmit.hold <hold_value>
```

- Tous les nœuds :

```
options lldp.xmit.hold <hold_value>
```

## Afficher ou effacer les statistiques LLDP

Vous pouvez afficher les statistiques LLDP pour les ports cluster et non-cluster sur chaque nœud afin de détecter d'éventuels problèmes de connectivité réseau. Les statistiques LLDP sont cumulatives à partir de la dernière fois qu'elles ont été effacées.

### Description de la tâche

Pour les versions ONTAP 9.10.1 et antérieures, étant donné que LLDP est toujours activé pour les ports de cluster, les statistiques LLDP sont toujours affichées pour le trafic sur ces ports. Le protocole LLDP doit être activé sur des ports non-cluster pour que les statistiques s'affichent pour ces ports.

Pour ONTAP 9.11.1 et versions ultérieures, étant donné que LLDP est toujours activé pour le cluster et les ports de stockage, les statistiques LLDP sont toujours affichées pour le trafic sur ces ports. Le protocole LLDP doit être activé sur les ports non-cluster et non-stockage pour que les statistiques s'affichent sur ces ports.

## Étape

Afficher ou effacer les statistiques actuelles du LLDP pour tous les ports d'un nœud :

|                                      |                                             |
|--------------------------------------|---------------------------------------------|
| Les fonctions que vous recherchez... | Entrer...                                   |
| Afficher les statistiques LLDP       | <code>run -node node_name lldp stats</code> |

Effacer les statistiques LLDP

```
run -node node_name lldp stats -z
```

### Affiche et efface un exemple de statistiques

La commande suivante affiche les statistiques LLDP avant leur effacement. La sortie affiche le nombre total de paquets envoyés et reçus depuis la dernière suppression des statistiques.

```
cluster-1::> run -node vsim1 lldp stats
```

RECEIVE

```
Total frames: 190k | Accepted frames: 190k | Total drops:
0
```

TRANSMIT

```
Total frames: 5195 | Total failures: 0
```

OTHER

```
Stored entries: 64
```

La commande suivante efface les statistiques LLDP.

```
cluster-1::> The following command clears the LLDP statistics:
```

```
run -node vsim1 lldp stats -z
```

```
run -node node1 lldp stats
```

RECEIVE

```
Total frames: 0 | Accepted frames: 0 | Total drops:
0
```

TRANSMIT

```
Total frames: 0 | Total failures: 0
```

OTHER

```
Stored entries: 64
```

Une fois les statistiques effacées, elles commencent à s'accumuler après l'envoi ou la réception de la prochaine annonce du PLLDP.

# Gestion du stockage NAS

## Gérez les protocoles NAS avec System Manager

### Présentation de la gestion NAS avec System Manager

Les rubriques de cette section vous expliquent comment configurer et gérer les environnements NAS avec System Manager dans ONTAP 9.7 et versions ultérieures.

Si vous utilisez System Manager classique (disponible uniquement dans ONTAP 9.7 et versions antérieures), reportez-vous aux rubriques suivantes :

- ["Présentation de la configuration NFS"](#)
- ["Présentation de la configuration SMB"](#)

System Manager prend en charge les flux de production pour :

- Configuration initiale des clusters que vous prévoyez d'utiliser pour les services de fichiers NAS.
- Provisionnement de volumes supplémentaire pour répondre à l'évolution des besoins de stockage.
- Configuration et maintenance pour les installations de sécurité et d'authentification standard.

System Manager vous permet de gérer les services NAS au niveau des composants :

- Protocoles : NFS, SMB ou les deux (NAS multiprotocole)
- Services de noms : DNS, LDAP et NIS
- Nommer le commutateur de service
- Sécurité Kerberos et TLS
- Exportations et partages
- Qtrees
- Mappage des noms des utilisateurs et des groupes

### Provisionnez le stockage NFS pour les datastores VMware

Avant d'utiliser Virtual Storage Console pour VMware vSphere (VSC) pour provisionner des volumes NFS sur un système de stockage ONTAP pour les hôtes ESXi, activez NFS à l'aide de System Manager pour ONTAP 9.7 ou version ultérieure.

Après avoir créé un ["Machine virtuelle de stockage compatible NFS"](#) Dans System Manager, vous pouvez ensuite provisionner des volumes NFS et gérer des datastores à l'aide de VSC.

VSC fait partie du produit depuis la version 7.0 de VSC ["Appliance virtuelle ONTAP Tools pour VMware vSphere"](#), Qui inclut VSC, le fournisseur vStorage APIs for Storage Awareness (VASA) et l'outil Storage Replication adapter (SRA) pour les fonctionnalités VMware vSphere.

Assurez-vous de vérifier le ["Matrice d'interopérabilité NetApp"](#) Pour vérifier la compatibilité entre vos versions actuelles de ONTAP et VSC.

Pour configurer l'accès NFS pour les hôtes ESXi aux datastores à l'aide de System Manager Classic (pour

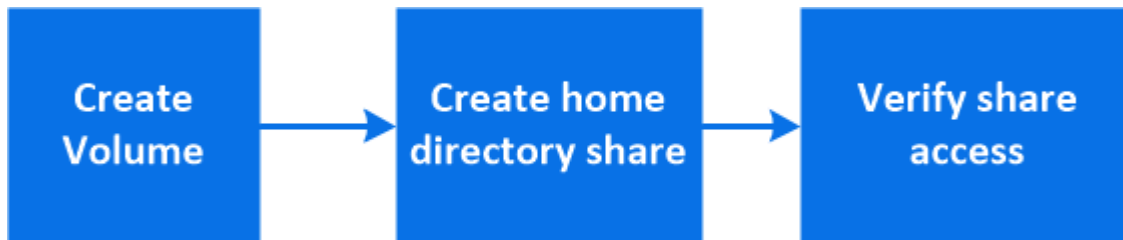
ONTAP 9.7 et les versions antérieures), voir ["Présentation de la configuration NFS pour ESXi à l'aide de VSC"](#)

Pour plus d'informations, voir ["Tr-4597 : VMware vSphere pour ONTAP"](#) Et de la documentation relative à la version de VSC.

## Provisionnement du stockage NAS pour les répertoires locaux

Créez des volumes pour fournir un stockage pour les répertoires locaux à l'aide du protocole SMB.

Cette procédure crée de nouveaux volumes pour des répertoires locaux sur un ["VM de stockage compatible SMB"](#). Vous pouvez accepter les valeurs par défaut des systèmes lors de la configuration de volumes ou de la spécification de configurations personnalisées.



Vous pouvez créer des volumes FlexVol, ou pour des systèmes de fichiers volumineux répondant à des besoins de performances élevées, des volumes FlexGroup. Voir aussi ["Provisionnez le stockage NAS pour les systèmes de fichiers volumineux à l'aide de FlexGroup volumes"](#).

Vous pouvez également enregistrer les spécifications de ce volume dans un PlayBook Ansible. Pour plus d'informations, consultez la page ["Utilisez les manuels de vente Ansible pour ajouter ou modifier des volumes ou des LUN"](#).

### Étapes

1. Ajout d'un nouveau volume dans une machine virtuelle de stockage compatible SMB
  - a. Sélectionnez **stockage > volumes**, puis cliquez sur **Ajouter**.
  - b. Entrez un nom, sélectionnez la machine virtuelle de stockage, puis entrez une taille.

Seules les machines virtuelles de stockage configurées avec le protocole SMB sont répertoriées. Si une seule machine virtuelle de stockage configurée avec le protocole SMB est disponible, le champ **Storage VM** n'est pas affiché.

- Si vous cliquez sur **Enregistrer** à ce stade, System Manager utilise les valeurs par défaut du système pour créer et ajouter un volume FlexVol.
- Vous pouvez cliquer sur **plus d'options** pour personnaliser la configuration du volume afin d'activer des services tels que l'autorisation, la qualité de service et la protection des données. Reportez-vous à la section [Personnaliser la configuration de volume](#), puis revenez ici pour effectuer les étapes suivantes.

2. cliquez sur **stockage > partages**, cliquez sur **Ajouter** et sélectionnez **répertoire d'accueil**.
3. Sur un client Windows, procédez comme suit pour vérifier que le partage est accessible.
  - a. Dans l'Explorateur Windows, mappez un lecteur sur le partage au format suivant :  
`\\<SMB_Server_Name>\<Share_Name>`

Si le nom du partage a été créé avec des variables (%w, %d ou %u), vérifiez l'accès avec un nom

résolu.

- b. Sur le lecteur nouvellement créé, créez un fichier test, puis supprimez le fichier.

## Personnaliser la configuration de volume

Vous pouvez personnaliser la configuration du volume lorsque vous ajoutez des volumes au lieu d'accepter les valeurs par défaut du système.

### Procédure

Après avoir cliqué sur **plus d'options**, sélectionnez la fonctionnalité dont vous avez besoin et saisissez les valeurs requises.

- Cache pour le volume distant.
- Niveau de service de performance (qualité de service, QoS)

Depuis la version ONTAP 9.8, vous pouvez spécifier une règle de QoS personnalisée ou désactiver la QoS, en plus de la sélection de valeur par défaut.

- Pour désactiver QoS, sélectionnez **personnalisé**, **existant**, puis **aucun**.
- Si vous sélectionnez **personnalisé** et spécifiez un niveau de service existant, un niveau local est automatiquement choisi.
- À partir de ONTAP 9.9.1, si vous choisissez de créer un niveau de service de performances personnalisé, vous pouvez utiliser System Manager pour sélectionner manuellement le niveau local (**placement manuel**) sur lequel vous souhaitez placer le volume que vous créez.

Cette option n'est pas disponible si vous sélectionnez les options de cache distant ou de volume FlexGroup.

- Volumes FlexGroup (sélectionnez **distribuer les données de volume sur le cluster**).

Cette option n'est pas disponible si vous avez précédemment sélectionné **placement manuel** sous **niveau de service de performance**. Sinon, le volume que vous ajoutez devient par défaut un volume FlexVol.

- Autorisations d'accès pour les protocoles pour lesquels le volume est configuré.
- Protection des données avec SnapMirror (local ou distant), spécifiez ensuite la règle de protection et les paramètres du cluster de destination dans les listes déroulantes.
- Sélectionnez **Save** pour créer le volume et l'ajouter au cluster et à la machine virtuelle de stockage.



Une fois le volume enregistré, revenez à [étape 2 dans le flux de travail](#) pour effectuer le provisionnement complet des répertoires locaux.

## Provisionnement du stockage NAS pour les serveurs Linux via NFS

Créez des volumes pour fournir un stockage pour les serveurs Linux en utilisant le protocole NFS avec ONTAP System Manager (9.7 et versions ultérieures).

Cette procédure crée de nouveaux volumes sur un ["VM de stockage existante compatible NFS"](#). Vous pouvez accepter les valeurs par défaut du système lors de la configuration de volumes ou spécifier des configurations personnalisées.

Vous pouvez créer des volumes FlexVol, ou pour des systèmes de fichiers volumineux répondant à des besoins de performances élevées, des volumes FlexGroup. Voir aussi ["Provisionnez le stockage NAS pour les systèmes de fichiers volumineux à l'aide de FlexGroup volumes"](#).

Vous pouvez également enregistrer les spécifications de ce volume dans un PlayBook Ansible. Pour plus d'informations, consultez la page ["Utilisez les manuels de vente Ansible pour ajouter ou modifier des volumes ou des LUN"](#).

Pour plus d'informations sur la plage de fonctionnalités du protocole NFS ONTAP, consultez le ["Présentation de référence NFS"](#).

## Étapes

1. Ajoutez un nouveau volume dans une VM de stockage compatible NFS.
  - a. Cliquez sur **Storage > volumes**, puis sur **Add**.
  - b. Entrez un nom, sélectionnez la machine virtuelle de stockage, puis entrez une taille.

Seules les machines virtuelles de stockage configurées avec le protocole NFS sont répertoriées. Si une seule machine virtuelle de stockage configurée avec le protocole SMB est disponible, le champ **Storage VM** n'est pas affiché.

- Si vous cliquez sur **Enregistrer** à ce stade, System Manager utilise les valeurs par défaut du système pour créer et ajouter un volume FlexVol.



La stratégie d'exportation par défaut accorde un accès complet à tous les utilisateurs.

- Vous pouvez cliquer sur **plus d'options** pour personnaliser la configuration du volume afin d'activer des services tels que l'autorisation, la qualité de service et la protection des données. Reportez-vous à la section [Personnaliser la configuration de volume](#), puis revenez ici pour effectuer les étapes suivantes.
2. sur un client Linux, procédez comme suit pour vérifier l'accès.
    - a. Créez et montez le volume à l'aide de l'interface réseau du VM de stockage.
    - b. Sur le volume récemment monté, créez un fichier test, écrivez du texte et supprimez le fichier.

Après avoir vérifié l'accès, vous pouvez ["limitez l'accès client grâce à l'export policy du volume"](#) Et définissez les droits de propriété et les autorisations UNIX souhaités sur le volume monté.

## Personnaliser la configuration de volume

Vous pouvez personnaliser la configuration du volume lorsque vous ajoutez des volumes au lieu d'accepter les valeurs par défaut du système.

### Procédure

Après avoir cliqué sur **plus d'options**, sélectionnez la fonctionnalité dont vous avez besoin et saisissez les valeurs requises.

- Cache pour le volume distant.
- Niveau de service de performance (qualité de service, QoS)

Depuis la version ONTAP 9.8, vous pouvez spécifier une règle de QoS personnalisée ou désactiver la QoS, en plus de la sélection de valeur par défaut.

- Pour désactiver QoS, sélectionnez **personnalisé, existant**, puis **aucun**.
- Si vous sélectionnez **personnalisé** et spécifiez un niveau de service existant, un niveau local est automatiquement choisi.
- À partir de ONTAP 9.9.1, si vous choisissez de créer un niveau de service de performances personnalisé, vous pouvez utiliser System Manager pour sélectionner manuellement le niveau local (**placement manuel**) sur lequel vous souhaitez placer le volume que vous créez.

Cette option n'est pas disponible si vous sélectionnez les options de cache distant ou de volume FlexGroup.

- Volumes FlexGroup (sélectionnez **distribuer les données de volume sur le cluster**).

Cette option n'est pas disponible si vous avez précédemment sélectionné **placement manuel** sous **niveau de service de performance**. Sinon, le volume que vous ajoutez devient par défaut un volume FlexVol.

- Autorisations d'accès pour les protocoles pour lesquels le volume est configuré.
- Protection des données avec SnapMirror (local ou distant), spécifiez ensuite la règle de protection et les paramètres du cluster de destination dans les listes déroulantes.
- Sélectionnez **Save** pour créer le volume et l'ajouter au cluster et à la machine virtuelle de stockage.



Une fois le volume enregistré, revenez à [\[step2-complete-prov\]](#) Pour terminer le provisionnement des serveurs Linux à l'aide de NFS.

## D'autres façons de le faire dans ONTAP

| Pour effectuer cette tâche avec...                         | Reportez-vous à...                                                                           |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| System Manager Classic (ONTAP 9.7 et versions antérieures) | <a href="#">"Présentation de la configuration NFS"</a>                                       |
| Interface de ligne de commande ONTAP                       | <a href="#">"Présentation de la configuration NFS avec l'interface de ligne de commande"</a> |

## Gérez l'accès à l'aide de règles d'exportation

Activez l'accès client Linux aux serveurs NFS à l'aide de règles d'exportation.

Cette procédure crée ou modifie des export-polices pour un ["VM de stockage existante compatible NFS"](#).

### Étapes

1. Dans System Manager, cliquez sur **Storage > volumes**.
2. Cliquez sur un volume compatible NFS et cliquez sur **plus**.
3. Cliquez sur **Modifier la stratégie d'exportation**, puis sur **Sélectionner une stratégie existante** ou **Ajouter une nouvelle stratégie**.

## Provisionnement du stockage NAS pour les serveurs Windows avec SMB

Créer des volumes pour fournir un stockage aux serveurs Windows à l'aide du protocole SMB utilisant System Manager, disponible avec ONTAP 9.7 et versions ultérieures.



Cette procédure crée de nouveaux volumes sur un ["VM de stockage compatible SMB"](#) et crée un partage pour le répertoire racine du volume (/). Vous pouvez accepter les valeurs par défaut des systèmes lors de la configuration de volumes ou de la spécification de configurations personnalisées. Une fois la configuration SMB initiale effectuée, vous pouvez également créer des partages supplémentaires et modifier leurs propriétés.

Vous pouvez créer des volumes FlexVol, ou pour des systèmes de fichiers volumineux répondant à des besoins de performances élevées, des volumes FlexGroup. Voir aussi ["Provisionnez le stockage NAS pour les systèmes de fichiers volumineux à l'aide de FlexGroup volumes"](#).

Vous pouvez également enregistrer les spécifications de ce volume dans un PlayBook Ansible. Pour plus d'informations, consultez la page ["Utilisez les manuels de vente Ansible pour ajouter ou modifier des volumes ou des LUN"](#).

Pour plus d'informations sur la plage de fonctionnalités du protocole SMB de ONTAP, consultez le ["Présentation des références SMB"](#).

### Avant de commencer

- À partir de ONTAP 9.13.1, vous pouvez activer l'analyse de la capacité et le suivi des activités par défaut sur les nouveaux volumes. Dans System Manager, vous pouvez gérer les paramètres par défaut au niveau du cluster ou de la VM de stockage. Pour plus d'informations, voir ["Activez l'analyse du système de fichiers"](#).

### Étapes

#### 1. Ajout d'un nouveau volume dans une machine virtuelle de stockage compatible SMB

- a. Cliquez sur **Storage > volumes**, puis sur **Add**.
- b. Entrez un nom, sélectionnez la machine virtuelle de stockage, puis entrez une taille.

Seules les machines virtuelles de stockage configurées avec le protocole SMB sont répertoriées. Si une seule machine virtuelle de stockage configurée avec le protocole SMB est disponible, le champ **Storage VM** n'est pas affiché.

- Si vous sélectionnez **Enregistrer** à ce stade, System Manager utilise les paramètres par défaut du système pour créer et ajouter un volume FlexVol.
- Vous pouvez sélectionner **plus d'options** pour personnaliser la configuration du volume afin d'activer des services tels que l'autorisation, la qualité de service et la protection des données. Reportez-vous à la section [Personnaliser la configuration de volume](#), puis revenez ici pour effectuer les étapes suivantes.

#### 2. [[step2-complète-Prov-win,étape 2 du flux de travail] passer à un client Windows pour vérifier que le partage est accessible.

- a. Dans l'Explorateur Windows, mappez un lecteur sur le partage au format suivant :  
`\\_SMB_Server_Name__Share_Name_`
- b. Sur le lecteur nouvellement créé, créez un fichier test, écrivez du texte et supprimez le fichier.

Après vérification de l'accès, vous pouvez restreindre l'accès du client à l'aide de la liste de contrôle d'accès du partage et définir toutes les propriétés de sécurité souhaitées sur le lecteur mappé. Voir ["Créez un partage SMB"](#) pour en savoir plus.

### Ajouter ou modifier des partages

Vous pouvez ajouter des partages supplémentaires après la configuration SMB initiale. Les partages sont créés avec les valeurs et les propriétés par défaut que vous sélectionnez. Ils peuvent être modifiés

ultérieurement.

Vous pouvez définir les propriétés de partage suivantes lors de la configuration d'un partage :

- Autorisations d'accès
- Propriétés du partage
  - Disponibilité sans interruption pour les partages qui contiennent des données Hyper-V et SQL Server sur SMB (à partir de ONTAP 9.10.1). Voir aussi :
    - ["Exigences de partage disponibles en continu pour Hyper-V sur SMB"](#)
    - ["Exigences de partage constamment disponibles pour SQL Server sur SMB"](#)
  - Chiffrez les données avec SMB 3.0 lors de l'accès à ce partage.

Après la configuration initiale, vous pouvez également modifier les propriétés suivantes :

- Liens symboliques
  - Activez ou désactivez les liens symlinks et les boutons de fonction
- Propriétés du partage
  - Autoriser les clients à accéder au répertoire de copies Snapshot.
  - Activez oplocks, ce qui permet aux clients de verrouiller les fichiers et le contenu en cache localement (par défaut).
  - Activez l'énumération basée sur l'accès (ABE) pour afficher les ressources partagées en fonction des autorisations d'accès de l'utilisateur.

## Procédures

Pour ajouter un nouveau partage dans un volume compatible SMB, cliquez sur **stockage > partages**, cliquez sur **Ajouter** et sélectionnez **partage**.

Pour modifier un partage existant, cliquez sur **stockage > partages**, puis cliquez sur  et sélectionnez **Modifier**.

## Personnaliser la configuration de volume

Vous pouvez personnaliser la configuration du volume lorsque vous ajoutez des volumes au lieu d'accepter les valeurs par défaut du système.

## Procédure

Après avoir cliqué sur **plus d'options**, sélectionnez la fonctionnalité dont vous avez besoin et saisissez les valeurs requises.

- Cache pour le volume distant.
- Niveau de service de performance (qualité de service, QoS)

Depuis ONTAP 9.8, vous pouvez spécifier une règle QoS personnalisée ou désactiver QoS en plus de la sélection de valeur par défaut.

- Pour désactiver QoS, sélectionnez **personnalisé**, **existant**, puis **aucun**.
- Si vous sélectionnez **personnalisé** et spécifiez un niveau de service existant, un niveau local est automatiquement choisi.

- À partir de ONTAP 9.9.1, si vous choisissez de créer un niveau de service de performances personnalisé, vous pouvez utiliser System Manager pour sélectionner manuellement le niveau local (**placement manuel**) sur lequel vous souhaitez placer le volume que vous créez.

Cette option n'est pas disponible si vous sélectionnez les options de cache distant ou de volume FlexGroup.

- Volumes FlexGroup (sélectionnez **distribuer les données de volume sur le cluster**).

Cette option n'est pas disponible si vous avez précédemment sélectionné **placement manuel** sous **niveau de service de performance**. Sinon, le volume que vous ajoutez devient par défaut un volume FlexVol.

**Cette option n'est pas disponible si vous avez précédemment sélectionné \*placement manuel sous niveau de service de performance.** Sinon, le volume que vous ajoutez devient par défaut un volume FlexVol.

**Autorisation d'accès pour les protocoles pour lesquels le volume est configuré.**

**\*Protection des données avec SnapMirror (local ou distant), spécifiez ensuite la stratégie de protection et les paramètres du cluster de destination dans les listes déroulantes.**

**\*Cliquez sur \*Enregistrer** pour créer le volume et l'ajouter au cluster et à la machine virtuelle de stockage.

Vous pouvez personnaliser la configuration du volume lorsque vous ajoutez des volumes au lieu d'accepter les valeurs par défaut du système.

## Procédure

Après avoir cliqué sur **plus d'options**, sélectionnez la fonctionnalité dont vous avez besoin et saisissez les valeurs requises.

- Cache pour le volume distant.
- Niveau de service de performance (qualité de service, QoS)

Depuis la version ONTAP 9.8, vous pouvez spécifier une règle de QoS personnalisée ou désactiver la QoS, en plus de la sélection de valeur par défaut.

- Pour désactiver QoS, sélectionnez **personnalisé, existant**, puis **aucun**.
- Si vous sélectionnez **personnalisé** et spécifiez un niveau de service existant, un niveau local est automatiquement choisi.
- À partir de ONTAP 9.9.1, si vous choisissez de créer un niveau de service de performances personnalisé, vous pouvez utiliser System Manager pour sélectionner manuellement le niveau local (**placement manuel**) sur lequel vous souhaitez placer le volume que vous créez.

Cette option n'est pas disponible si vous sélectionnez les options de cache distant ou de volume FlexGroup.

- Volumes FlexGroup (sélectionnez **distribuer les données de volume sur le cluster**).

Cette option n'est pas disponible si vous avez précédemment sélectionné **placement manuel** sous **niveau de service de performance**. Sinon, le volume que vous ajoutez devient par défaut un volume FlexVol.

- Autorisations d'accès pour les protocoles pour lesquels le volume est configuré.
- Protection des données avec SnapMirror (local ou distant), spécifiez ensuite la règle de protection et les paramètres du cluster de destination dans les listes déroulantes.
- Sélectionnez **Save** pour créer le volume et l'ajouter au cluster et à la machine virtuelle de stockage.



Une fois le volume enregistré, revenez à [\[step2-compl-prov-win\]](#) Pour effectuer le provisionnement complet des serveurs Windows avec SMB.

## D'autres façons de le faire dans ONTAP

| Pour effectuer cette tâche avec...                         | Reportez-vous à...                                                                           |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| System Manager Classic (ONTAP 9.7 et versions antérieures) | <a href="#">"Présentation de la configuration SMB"</a>                                       |
| Interface de ligne de commande ONTAP                       | <a href="#">"Présentation de la configuration SMB avec l'interface de ligne de commande"</a> |

## Provisionnement de stockage NAS pour Windows et Linux à l'aide des protocoles NFS et SMB

Créer des volumes afin de fournir un stockage aux clients qui utilisent le protocole NFS ou SMB.

Cette procédure crée de nouveaux volumes sur un ["VM de stockage existante activée pour les protocoles NFS et SMB"](#).



Le protocole NFS est généralement utilisé dans les environnements Linux. Le protocole SMB est généralement utilisé dans les environnements Windows. Cependant, NFS et SMB peuvent être utilisés avec Linux ou Windows.

Vous pouvez créer des volumes FlexVol, ou pour des systèmes de fichiers volumineux répondant à des besoins de performances élevées, des volumes FlexGroup. Voir ["Provisionnez le stockage NAS pour les systèmes de fichiers volumineux à l'aide de FlexGroup volumes"](#).

Vous pouvez également enregistrer les spécifications de ce volume dans un PlayBook Ansible. Pour plus d'informations, consultez la page ["Utilisez les manuels de vente Ansible pour ajouter ou modifier des volumes ou des LUN"](#).

### Étapes

1. Ajoutez un nouveau volume dans une machine virtuelle de stockage activée pour les protocoles NFS et SMB.
  - a. Cliquez sur **Storage > volumes**, puis sur **Add**.
  - b. Entrez un nom, sélectionnez la machine virtuelle de stockage, puis entrez une taille.

Seules les machines virtuelles de stockage configurées avec les protocoles NFS et SMB sont répertoriées. Si une seule machine virtuelle de stockage configurée avec les protocoles NFS et SMB est disponible, le champ **Storage VM** n'est pas affiché.

- c. Cliquez sur **plus d'options** et sélectionnez **Exporter via NFS**.

Le paramètre par défaut permet un accès complet à tous les utilisateurs. Vous pouvez ajouter ultérieurement des règles plus restrictives à l'export policy.

d. Sélectionnez **partager via SMB/CIFS**.

Le partage est créé avec une liste de contrôle d'accès par défaut (ACL) définie sur « contrôle total » pour le groupe **Everyone**. Vous pouvez ajouter des restrictions à la liste de contrôle d'accès ultérieurement.

e. Si vous cliquez sur **Enregistrer** à ce stade, System Manager utilise les valeurs par défaut du système pour créer et ajouter un volume FlexVol.

Vous pouvez également continuer à activer tous les services supplémentaires requis, tels que l'autorisation, la qualité de services et la protection des données. Reportez-vous à la section [Personnaliser la configuration de volume](#), puis revenez ici pour effectuer les étapes suivantes.

2. sur un client Linux, vérifiez que l'exportation est accessible.
  - a. Créez et montez le volume à l'aide de l'interface réseau du VM de stockage.
  - b. Sur le volume récemment monté, créez un fichier test, écrivez du texte et supprimez le fichier.
3. Sur un client Windows, procédez comme suit pour vérifier que le partage est accessible.
  - a. Dans l'Explorateur Windows, mappez un lecteur sur le partage au format suivant :  
`\\_SMB_Server_Name__Share_Name_`
  - b. Sur le lecteur nouvellement créé, créez un fichier test, écrivez du texte et supprimez le fichier.

Après avoir vérifié l'accès, vous pouvez "[Limitez l'accès client aux export policy du volume et restreignez l'accès client à l'aide de la liste ACL du partage](#)", et définissez les droits de propriété et autorisations souhaités sur le volume exporté et partagé.

## Personnaliser la configuration de volume

Vous pouvez personnaliser la configuration du volume lorsque vous ajoutez des volumes au lieu d'accepter les valeurs par défaut du système.

### Procédure

Après avoir cliqué sur **plus d'options**, sélectionnez la fonctionnalité dont vous avez besoin et saisissez les valeurs requises.

- Cache pour le volume distant.
- Niveau de service de performance (qualité de service, QoS)

Depuis la version ONTAP 9.8, vous pouvez spécifier une règle de QoS personnalisée ou désactiver la QoS, en plus de la sélection de valeur par défaut.

- Pour désactiver QoS, sélectionnez **personnalisé**, **existant**, puis **aucun**.
- Si vous sélectionnez **personnalisé** et spécifiez un niveau de service existant, un niveau local est automatiquement choisi.
- À partir de ONTAP 9.9.1, si vous choisissez de créer un niveau de service de performances personnalisé, vous pouvez utiliser System Manager pour sélectionner manuellement le niveau local (**placement manuel**) sur lequel vous souhaitez placer le volume que vous créez.

Cette option n'est pas disponible si vous sélectionnez les options de cache distant ou de volume

FlexGroup.

- Volumes FlexGroup (sélectionnez **distribuer les données de volume sur le cluster**).

Cette option n'est pas disponible si vous avez précédemment sélectionné **placement manuel** sous **niveau de service de performance**. Sinon, le volume que vous ajoutez devient par défaut un volume FlexVol.

- Autorisations d'accès pour les protocoles pour lesquels le volume est configuré.
- Protection des données avec SnapMirror (local ou distant), spécifiez ensuite la règle de protection et les paramètres du cluster de destination dans les listes déroulantes.
- Sélectionnez **Save** pour créer le volume et l'ajouter au cluster et à la machine virtuelle de stockage.

Une fois le volume enregistré, revenez à [\[step2-compl-prov-nfs-smb\]](#) Pour assurer un provisionnement multiprotocole complet pour les serveurs Windows et Linux.

### D'autres façons de le faire dans ONTAP

| Pour effectuer ces tâches avec...                          | Voir ce contenu...                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System Manager Classic (ONTAP 9.7 et versions antérieures) | <a href="#">"Présentation de la configuration multiprotocole SMB et NFS"</a>                                                                                                                                                                                                                                                                                                                                                                                       |
| Interface de ligne de commande ONTAP                       | <ul style="list-style-type: none"><li>• <a href="#">"Présentation de la configuration SMB avec l'interface de ligne de commande"</a></li><li>• <a href="#">"Présentation de la configuration NFS avec l'interface de ligne de commande"</a></li><li>• <a href="#">"Quels sont les styles de sécurité et leurs effets"</a></li><li>• <a href="#">"Sensibilité à la casse des noms de fichiers et de répertoires dans un environnement multiprotocole"</a></li></ul> |

## Accès client sécurisé avec Kerberos

Activez Kerberos pour sécuriser l'accès au stockage des clients NAS.

Cette procédure configure Kerberos sur une machine virtuelle de stockage existante activée pour **"NFS"** ou **"PME"**.

Avant de commencer, vous devez avoir configuré les DNS, NTP et **"LDAP"** sur le système de stockage.



### Étapes

1. Sur la ligne de commande ONTAP, définissez les autorisations UNIX pour le volume racine de la machine virtuelle de stockage.
  - a. Afficher les autorisations appropriées sur le volume racine de la VM de stockage :

```
volume show -volume root_vol_name-fields user,group,unix-permissions
```

Le volume root du VM de stockage doit avoir la configuration suivante :

| Nom...             | Paramètre...   |
|--------------------|----------------|
| UID                | Racine ou ID 0 |
| GIDS               | Racine ou ID 0 |
| Autorisations UNIX | 755            |

a. Si ces valeurs ne sont pas affichées, utiliser le `volume modify` pour les mettre à jour.

2. Définissez les autorisations utilisateur pour le volume racine de l'ordinateur virtuel de stockage.

a. Afficher les utilisateurs UNIX locaux : `vserver services name-service unix-user show -vserver vserver_name`

La machine virtuelle de stockage doit avoir les utilisateurs UNIX suivants configurés :

| Nom d'utilisateur | ID d'utilisateur | ID de groupe principal |
|-------------------|------------------|------------------------|
| nfs               | 500              | 0                      |
| racine            | 0                | 0                      |

+

**Remarque** : l'utilisateur NFS n'est pas requis si un mappage de nom Kerberos-UNIX existe pour le SPN de l'utilisateur client NFS ; voir l'étape 5.

a. Si ces valeurs ne sont pas affichées, utiliser le `vserver services name-service unix-user modify` pour les mettre à jour.

3. Définissez les autorisations de groupe pour le volume racine de VM de stockage.

a. Afficher les groupes UNIX locaux : `vserver services name-service unix-group show -vserver vserver_name`

La machine virtuelle de stockage doit avoir les groupes UNIX suivants configurés :

| Nom du groupe | ID de groupe |
|---------------|--------------|
| démon         | 1            |
| racine        | 0            |

a. Si ces valeurs ne sont pas affichées, utiliser le `vserver services name-service unix-group modify` pour les mettre à jour.

4. Basculez dans System Manager pour configurer Kerberos

5. Dans System Manager, cliquez sur **stockage > machines virtuelles de stockage** et sélectionnez la machine virtuelle de stockage.

6. Cliquez sur **Paramètres**.

7. Cliquez  sous Kerberos.

8. Cliquez sur **Ajouter** sous domaine Kerberos, puis complétez les sections suivantes :

- Ajouter un Royaume Kerberos

Entrez les détails de configuration selon le fournisseur de KDC.

- Ajouter l'interface réseau au Royaume

Cliquez sur **Ajouter** et sélectionnez une interface réseau.

9. Si vous le souhaitez, ajoutez des mappages à partir des noms de principal Kerberos aux noms d'utilisateur locaux.
  - a. Cliquez sur **Storage > Storage VM** et sélectionnez la VM de stockage.
  - b. Cliquez sur **Paramètres**, puis cliquez → sous **mappage de noms**.
  - c. Sous **Kerberos à UNIX**, ajoutez des modèles et des remplacements à l'aide d'expressions régulières.

## Activez ou désactivez l'accès client NFS sécurisé avec TLS

Vous pouvez améliorer la sécurité des connexions NFS en configurant NFS sur TLS de manière à chiffrer toutes les données envoyées sur le réseau entre le client NFS et ONTAP. Cela augmente la sécurité des connexions NFS. Vous pouvez le configurer sur une VM de stockage existante activée pour "NFS".



NFS over TLS est disponible dans ONTAP 9.15.1 en tant que préversion publique. À titre de préversion, NFS over TLS n'est pas pris en charge pour les workloads de production dans ONTAP 9.15.1.

### Activez TLS

Vous pouvez activer le chiffrement TLS pour les clients NFS afin d'augmenter la sécurité des données en transit.

#### Avant de commencer

Reportez-vous à la ["de formation"](#) Pour NFS sur TLS.


1. Cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.
2. Dans la mosaïque **NFS**, cliquez sur **NFS over TLS settings**.
3. Dans la zone **NFS over TLS settings**, sélectionnez une interface réseau NFS pour laquelle vous souhaitez activer TLS.
4. Cliquez sur **:** pour cette interface.
5. Cliquez sur **Activer**.
6. Dans la boîte de dialogue **Network interface TLS configuration**, incluez un certificat à utiliser avec TLS en sélectionnant l'une des options suivantes :
  - **Certificat installé** : choisissez un certificat installé précédemment dans la liste déroulante.
  - **Nouveau certificat** : choisissez un nom commun pour le certificat.
  - **Certificat externe signé par une autorité de certification** : suivez les instructions pour coller le contenu de votre certificat et de votre clé privée dans les boîtes.
7. Cliquez sur **Enregistrer**.



## Désactiver TLS

Vous pouvez désactiver TLS pour les clients NFS si vous n'avez plus besoin de la sécurité améliorée pour les données en transit.

### Étapes

1. Cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.
2. Dans la mosaïque **NFS**, cliquez sur **NFS over TLS settings**.
3. Dans la zone **NFS sur TLS settings**, sélectionnez une interface réseau NFS pour laquelle vous souhaitez désactiver TLS.
4. Cliquez sur  pour cette interface.
5. Cliquez sur **Désactiver**.
6. Dans la boîte de dialogue de confirmation qui s'affiche, sélectionnez **Désactiver**.



## Fournir un accès client avec des services de noms

Activez ONTAP pour rechercher des informations sur l'hôte, l'utilisateur, le groupe ou le groupe réseau à l'aide de LDAP ou NIS pour authentifier les clients NAS.

Cette procédure crée ou modifie des configurations LDAP ou NIS sur une VM de stockage existante activée pour "NFS" ou "PME".

Pour les configurations LDAP, vous devez disposer des détails de configuration LDAP requis dans votre environnement et vous devez utiliser un schéma LDAP ONTAP par défaut.

### Étapes

1. Configurez le service requis : cliquez sur **stockage > machines virtuelles de stockage**.
2. Sélectionnez la machine virtuelle de stockage, cliquez sur **Paramètres**, puis cliquez sur  pour LDAP ou NIS.
3. Inclure toute modification dans le commutateur de services de noms : cliquez  sous commutateur de services de noms.

## Gérer des répertoires et des fichiers

Développez l'affichage des volumes de System Manager pour afficher et supprimer des répertoires et des fichiers.

Depuis ONTAP 9.9.1, les répertoires sont supprimés avec une fonctionnalité de suppression rapide des répertoires à faible latence.

Pour plus d'informations sur l'affichage des systèmes de fichiers dans ONTAP 9.9.1 et versions ultérieures, voir "[Présentation de l'analytique du système de fichiers](#)".

### Étape

1. Sélectionnez **stockage > volumes**. Développez un volume pour afficher son contenu.

# Gérez des utilisateurs et des groupes spécifiques à un hôte grâce à System Manager

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour gérer les utilisateurs et les groupes spécifiques à un hôte UNIX ou Windows.

Vous pouvez effectuer les opérations suivantes :

| Répertoires de base                                                                                                                                                                                                     | UNIX                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• <a href="#">Afficher les utilisateurs et les groupes Windows</a></li><li>• <a href="#">[add-edit-delete-Windows]</a></li><li>• <a href="#">[manage-windows-users]</a></li></ul> | <ul style="list-style-type: none"><li>• <a href="#">Afficher les utilisateurs et les groupes UNIX</a></li><li>• <a href="#">[add-edit-delete-UNIX]</a></li><li>• <a href="#">[manage-unix-users]</a></li></ul> |



## Afficher les utilisateurs et les groupes Windows

Dans System Manager, vous pouvez afficher la liste des utilisateurs et groupes Windows.

### Étapes

1. Dans System Manager, cliquez sur **stockage > machines virtuelles de stockage**.
2. Sélectionnez la VM de stockage, puis sélectionnez l'onglet **Paramètres**.
3. Faites défiler jusqu'à la zone **utilisateurs et groupes hôtes**.

La section **Windows** affiche un récapitulatif du nombre d'utilisateurs dans chaque groupe associé à la machine virtuelle de stockage sélectionnée.

4. Cliquez  dans la section **Windows**.
5. Cliquez sur l'onglet **groupes**, puis cliquez sur  en regard d'un nom de groupe pour afficher les détails sur ce groupe.
6. Pour afficher les utilisateurs d'un groupe, sélectionnez-le, puis cliquez sur l'onglet **utilisateurs**.

## Ajouter, modifier ou supprimer un groupe Windows

Dans System Manager, vous pouvez gérer les groupes Windows en les ajoutant, en les modifiant ou en les supprimant.

### Étapes

1. Dans System Manager, affichez la liste des groupes Windows. Reportez-vous à la section [Afficher les utilisateurs et les groupes Windows](#).
2. Dans l'onglet **groupes**, vous pouvez gérer les groupes avec les tâches suivantes :

|                                |                        |
|--------------------------------|------------------------|
| Pour effectuer cette action... | Procédez comme suit... |
|--------------------------------|------------------------|

|                     |                                                                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ajouter un groupe   | <ol style="list-style-type: none"> <li>1. Cliquez sur <b>+</b> <b>Add</b> .</li> <li>2. Entrez les informations du groupe.</li> <li>3. Spécifiez les privilèges.</li> <li>4. Spécifiez les membres du groupe (ajoutez des utilisateurs locaux, des utilisateurs de domaine ou des groupes de domaines).</li> </ol>                   |
| Modifier un groupe  | <ol style="list-style-type: none"> <li>1. En regard du nom du groupe, cliquez sur <b>:</b>, puis sur <b>Modifier</b>.</li> <li>2. Modifier les informations du groupe.</li> </ol>                                                                                                                                                    |
| Supprimer un groupe | <ol style="list-style-type: none"> <li>1. Cochez la case en regard du ou des groupes que vous souhaitez supprimer.</li> <li>2. Cliquez sur <b>🗑 Delete</b> .</li> </ol> <p><b>Remarque :</b> vous pouvez également supprimer un seul groupe en cliquant <b>:</b> à côté du nom du groupe, puis en cliquant sur <b>Supprimer</b>.</p> |






## Gérer les utilisateurs Windows

Dans System Manager, vous pouvez gérer les utilisateurs Windows en les ajoutant, en les modifiant, en les supprimant, en les activant ou en les désactivant. Vous pouvez également modifier le mot de passe d'un utilisateur Windows.

### Étapes

1. Dans System Manager, affichez la liste des utilisateurs du groupe. Reportez-vous à la section [Afficher les utilisateurs et les groupes Windows](#).
2. Dans l'onglet **Users**, vous pouvez gérer les utilisateurs avec les tâches suivantes :

| Pour effectuer cette action... | Procédez comme suit...                                                                                                                                                                  |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ajouter un utilisateur         | <ol style="list-style-type: none"> <li>1. Cliquez sur <b>+</b> <b>Add</b> .</li> <li>2. Entrez les informations utilisateur.</li> </ol>                                                 |
| Modifier un utilisateur        | <ol style="list-style-type: none"> <li>1. En regard du nom d'utilisateur, cliquez sur <b>:</b>, puis sur <b>Modifier</b>.</li> <li>2. Modifier les informations utilisateur.</li> </ol> |

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supprimer un utilisateur             | <ol style="list-style-type: none"> <li>1. Cochez la case en regard du ou des utilisateurs que vous souhaitez supprimer.</li> <li>2. Cliquez sur  <b>Delete</b> .</li> </ol> <p><b>Remarque</b> : vous pouvez également supprimer un seul utilisateur en cliquant  à côté du nom d'utilisateur, puis en cliquant sur <b>Supprimer</b>.</p> |
| Modifier le mot de passe utilisateur | <ol style="list-style-type: none"> <li>1. En regard du nom d'utilisateur, cliquez sur  , puis sur <b>Modifier le mot de passe</b>.</li> <li>2. Entrez le nouveau mot de passe et confirmez-le.</li> </ol>                                                                                                                                                                                                                    |
| Activez un utilisateur               | <ol style="list-style-type: none"> <li>1. Cochez la case en regard de chaque utilisateur désactivé que vous souhaitez activer.</li> <li>2. Cliquez sur  <b>Enable</b> .</li> </ol>                                                                                                                                                                                                                                           |
| Désactiver un utilisateur            | <ol style="list-style-type: none"> <li>1. Cochez la case en regard de chaque utilisateur activé que vous souhaitez désactiver.</li> <li>2. Cliquez sur  <b>Disable</b> .</li> </ol>                                                                                                                                                                                                                                          |


## Afficher les utilisateurs et les groupes UNIX

Dans System Manager, vous pouvez afficher la liste des utilisateurs et groupes UNIX.

### Étapes

1. Dans System Manager, cliquez sur **stockage > machines virtuelles de stockage**.
2. Sélectionnez la VM de stockage, puis sélectionnez l'onglet **Paramètres**.
3. Faites défiler jusqu'à la zone **utilisateurs et groupes hôtes**.

La section **UNIX** affiche un récapitulatif du nombre d'utilisateurs dans chaque groupe associé à la machine virtuelle de stockage sélectionnée.

4. Cliquez  dans la section **UNIX**.
5. Cliquez sur l'onglet **groupes** pour afficher les détails de ce groupe.
6. Pour afficher les utilisateurs d'un groupe, sélectionnez-le, puis cliquez sur l'onglet **utilisateurs**.

## Ajouter, modifier ou supprimer un groupe UNIX

Dans System Manager, vous pouvez gérer les groupes UNIX en les ajoutant, en les modifiant ou en les supprimant.

### Étapes

1. Dans System Manager, afficher la liste des groupes UNIX. Reportez-vous à la section [Afficher les utilisateurs et les groupes UNIX](#).
2. Dans l'onglet **groupes**, vous pouvez gérer les groupes avec les tâches suivantes :



| Pour effectuer cette action... | Procédez comme suit...                                                                                                                                                                                                                                                                                                  |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ajouter un groupe              | <ol style="list-style-type: none"> <li>1. Cliquez sur  <b>Add</b> .</li> <li>2. Entrez les informations du groupe.</li> <li>3. (Facultatif) spécifiez les utilisateurs associés.</li> </ol>                                          |
| Modifier un groupe             | <ol style="list-style-type: none"> <li>1. Sélectionnez le groupe.</li> <li>2. Cliquez sur  <b>Edit</b> .</li> <li>3. Modifier les informations du groupe.</li> <li>4. (Facultatif) Ajouter ou supprimer des utilisateurs.</li> </ol> |
| Supprimer un groupe            | <ol style="list-style-type: none"> <li>1. Sélectionnez le ou les groupes que vous souhaitez supprimer.</li> <li>2. Cliquez sur  <b>Delete</b> .</li> </ol>                                                                           |

## Gérer les utilisateurs UNIX

Dans System Manager, vous pouvez gérer les utilisateurs Windows en les ajoutant, en les modifiant ou en les supprimant.

### Étapes

1. Dans System Manager, affichez la liste des utilisateurs du groupe. Reportez-vous à la section [Afficher les utilisateurs et les groupes UNIX](#).
2. Dans l'onglet **Users**, vous pouvez gérer les utilisateurs avec les tâches suivantes :

| Pour effectuer cette action... | Procédez comme suit...                                                                                                                                                                                                                                                                      |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ajouter un utilisateur         | <ol style="list-style-type: none"> <li>1. Cliquez sur  <b>Add</b> .</li> <li>2. Entrez les informations utilisateur.</li> </ol>                                                                        |
| Modifier un utilisateur        | <ol style="list-style-type: none"> <li>1. Sélectionnez l'utilisateur que vous souhaitez modifier.</li> <li>2. Cliquez sur  <b>Edit</b> .</li> <li>3. Modifier les informations utilisateur.</li> </ol> |
| Supprimer un utilisateur       | <ol style="list-style-type: none"> <li>1. Sélectionnez le ou les utilisateurs que vous souhaitez supprimer.</li> <li>2. Cliquez sur  <b>Delete</b> .</li> </ol>                                        |

## Surveillance des clients NFS actifs

Depuis ONTAP 9.8, System Manager affiche les connexions client NFS actives lorsque NFS est sous licence sur un cluster.

Vous pouvez ainsi vérifier rapidement quels clients NFS sont activement connectés à une machine virtuelle de

stockage, qui est connectée mais inactive et qui sont déconnectés.

Pour chaque adresse IP de client NFS, l'affichage **NFS clients** indique :

- \* Heure du dernier accès
- \* Adresse IP de l'interface réseau
- \* Version de connexion NFS
- \* Nom de la VM de stockage

En outre, une liste de clients NFS actifs au cours des 48 dernières heures est également affichée dans l'affichage **Storage > volumes** et un nombre de clients NFS est inclus dans l'affichage **Dashboard**.

### Étape

1. Afficher l'activité client NFS : cliquez sur **hôtes > clients NFS**.

## Activez le stockage NAS

### Activez le stockage NAS pour les serveurs Linux à l'aide de NFS

Créez ou modifiez des VM de stockage afin de permettre aux serveurs NFS de transmettre des données aux clients Linux.


Utilisez cette procédure pour activer une machine virtuelle de stockage nouvelle ou existante pour le protocole NFS.






### Avant de commencer

Vérifiez que vous avez bien noté les détails de configuration des services de réseau, d'authentification ou de sécurité requis dans votre environnement.

### Étapes

1. Activez NFS sur une VM de stockage.
  - Pour les nouvelles machines virtuelles de stockage : cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur **Ajouter**, entrez un nom de machine virtuelle de stockage et, dans l'onglet **SMB/CIFS, NFS, S3**, sélectionnez **Activer NFS**.
    - i. Confirmez la langue par défaut.
    - ii. Ajouter des interfaces réseau.
    - iii. Mise à jour des informations de compte administrateur de VM de stockage (facultatif)
  - Pour les machines virtuelles de stockage existantes : cliquez sur **Storage > Storage VMs**, sélectionnez une machine virtuelle de stockage, cliquez sur **Settings**, puis cliquez  sous **NFS**.
2. Ouvrir la export policy du volume root de la VM de stockage :
  - a. Cliquez sur **Storage > volumes**, sélectionnez le volume racine de la machine virtuelle de stockage (qui est par défaut *nom-volume \_root*), puis cliquez sur la stratégie affichée sous **règles d'exportation**.
  - b. Cliquez sur **Ajouter** pour ajouter une règle.


- Spécification client = 0.0.0.0/0
  - Protocoles d'accès = NFS
  - Détails d'accès = UNIX en lecture seule
3. Configurer DNS pour la résolution des noms d'hôte : cliquez sur **stockage > Storage VM**, sélectionnez la VM de stockage, cliquez sur **Paramètres**, puis cliquez sous **DNS** .
  4. Configurez les services de noms si nécessaire.
    - a. Cliquez sur **stockage > Storage VMs**, sélectionnez la VM de stockage, cliquez sur **Paramètres**, puis cliquez sur pour  LDAP ou NIS.
    - b. Cliquez sur  la mosaïque changement de services de noms pour inclure les modifications.
  5. Configurez le chiffrement si nécessaire :

### Configurer TLS pour les clients NFS




NFS over TLS est disponible dans ONTAP 9.15.1 en tant que préversion publique. À titre de préversion, NFS over TLS n'est pas pris en charge pour les workloads de production dans ONTAP 9.15.1.

#### Étapes

1. Reportez-vous à la "[de formation](#)" Pour NFS sur TLS avant de commencer.
2. Cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.
3. Dans la mosaïque **NFS**, cliquez sur **NFS over TLS settings**.
4. Dans la zone **NFS over TLS settings**, sélectionnez une interface réseau NFS pour laquelle vous souhaitez activer TLS.
5. Cliquez sur  pour cette interface.
6. Cliquez sur **Activer**.
7. Dans la boîte de dialogue **Network interface TLS configuration**, incluez un certificat à utiliser avec TLS en sélectionnant l'une des options suivantes :
  - **Certificat installé** : choisissez un certificat installé précédemment dans la liste déroulante.
  - **Nouveau certificat** : choisissez un nom commun pour le certificat.
  - **Certificat externe signé par une autorité de certification** : suivez les instructions pour coller le contenu de votre certificat et de votre clé privée dans les boîtes.
8. Cliquez sur **Enregistrer**.

### Configurer Kerberos

#### Étapes

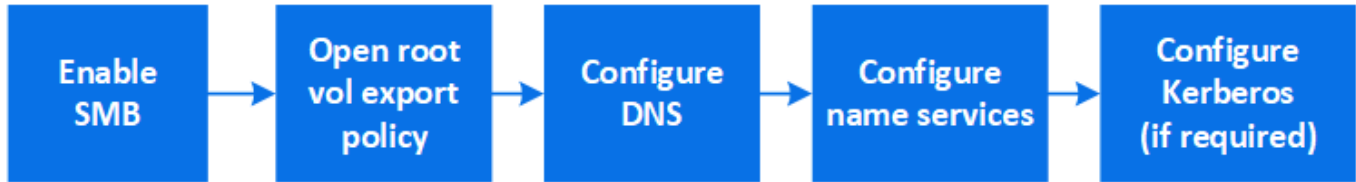
1. Cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.
2. Cliquez  dans la mosaïque Kerberos, puis cliquez sur **Ajouter**.

### Activation du stockage NAS pour serveurs Windows à l'aide de SMB

Créez ou modifiez des VM de stockage afin de permettre aux serveurs SMB de

transmettre des données aux clients Windows.

Cette procédure active une machine virtuelle de stockage nouvelle ou existante pour le protocole SMB. Nous partons du principe que des informations de configuration sont disponibles pour tous les services de réseau, d'authentification ou de sécurité requis dans votre environnement.




## Étapes

### 1. Activation de SMB sur une VM de stockage

- a. Pour les nouvelles machines virtuelles de stockage : cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur **Ajouter**, entrez un nom de machine virtuelle de stockage et, dans l'onglet **SMB/CIFS, NFS, S3**, sélectionnez **Activer SMB/CIFS**.

- Saisissez les informations suivantes :
  - Nom et mot de passe de l'administrateur
  - Nom du serveur
  - Domaine Active Directory
- Confirmez l'unité organisationnelle.
- Confirmez les valeurs DNS.
- Confirmez la langue par défaut.
- Ajouter des interfaces réseau.
- Mise à jour des informations de compte administrateur de VM de stockage (facultatif)

- b. Pour les machines virtuelles de stockage existantes : cliquez sur **Storage > Storage VMS**, sélectionnez une machine virtuelle de stockage, cliquez sur **Settings**, puis cliquez sous **SMB** .


### 2. Ouvrir la export policy du volume root de la VM de stockage :

- a. Cliquez sur **Storage > volumes**, sélectionnez le volume racine de la machine virtuelle de stockage (qui est par défaut *nom-volume\_root*), puis cliquez sur la stratégie affichée sous **règles d'exportation**.

- b. Cliquez sur **Ajouter** pour ajouter une règle.

- Spécification client = 0.0.0.0/0
- Protocoles d'accès = SMB
- Informations d'accès = NTFS lecture seule

### 3. Configurer le DNS pour la résolution de nom d'hôte :

- a. Cliquez sur **Storage > Storage VMS**, sélectionnez la VM de stockage, cliquez sur **Settings**, puis cliquez  sous **DNS**.



- b. Basculez sur le serveur DNS et mappez le serveur SMB.

- Créer des entrées de recherche de transfert (A - enregistrement d'adresse) et de retour (PTR - enregistrement du pointeur) pour mapper le nom du serveur SMB à l'adresse IP de l'interface du réseau de données.
- Si vous utilisez des alias NetBIOS, créez une entrée de recherche nom canonique d'alias



(enregistrement de ressource CNAME) pour mapper chaque alias à l'adresse IP de l'interface de réseau de données du serveur SMB.

4. Configurez les services de noms si nécessaire

- Cliquez sur **stockage > Storage VMS**, sélectionnez la machine virtuelle de stockage, cliquez sur **Paramètres**, puis cliquez  sous **LDAP** ou **NIS**.
- Incluez les modifications dans le fichier de commutateur de services de noms : cliquez  sous **commutateur de services de noms**.

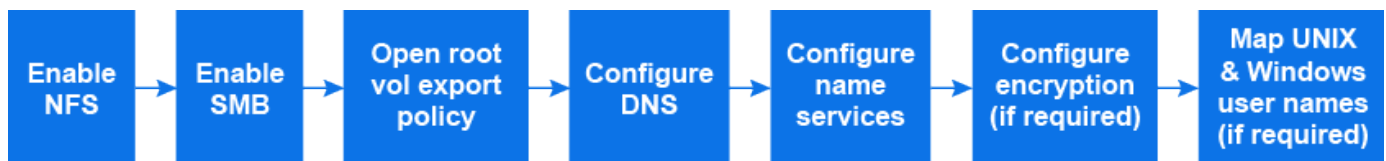
5. Configurez Kerberos si nécessaire :

- Cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.
- Cliquez  sous **Kerberos**, puis cliquez sur **Add**.

## Activez le stockage NAS pour Windows et Linux à l'aide des protocoles NFS et SMB

Créez ou modifiez des VM de stockage afin que les serveurs NFS et SMB puissent transmettre des données aux clients Linux et Windows.

Utilisez cette procédure pour activer une machine virtuelle de stockage, nouvelle ou existante, et desservir à la fois les protocoles NFS et SMB.





### Avant de commencer

Vérifiez que vous avez bien noté les détails de configuration des services de réseau, d'authentification ou de sécurité requis dans votre environnement.

### Étapes

- Activez les protocoles NFS et SMB sur une VM de stockage.
  - Pour les nouvelles machines virtuelles de stockage : cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur **Ajouter**, entrez un nom de machine virtuelle de stockage et, dans l'onglet **SMB/CIFS, NFS, S3**, sélectionnez **Activer SMB/CIFS** et **Activer NFS**.
  - Saisissez les informations suivantes :
    - Nom et mot de passe de l'administrateur
    - Nom du serveur
    - Domaine Active Directory
  - Confirmez l'unité organisationnelle.
  - Confirmez les valeurs DNS.
  - Confirmez la langue par défaut.
  - Ajouter des interfaces réseau.
  - Mise à jour des informations de compte administrateur de VM de stockage (facultatif)
  - Pour les machines virtuelles de stockage existantes : cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez une machine virtuelle de stockage, puis cliquez sur **Paramètres**. Suivez les


sous-étapes suivantes si NFS ou SMB n'est pas déjà activé.

- Cliquez  sous **NFS**.
- Cliquez  sous **SMB**.



2. Ouvrir la export policy du volume root de la VM de stockage :

- a. Cliquez sur **Storage > volumes**, sélectionnez le volume racine de la machine virtuelle de stockage (qui est par défaut *nom-volume\_root*), puis cliquez sur la stratégie affichée sous **règles d'exportation**.
- b. Cliquez sur **Ajouter** pour ajouter une règle.
  - Spécification client = 0.0.0.0/0
  - Protocoles d'accès = NFS
  - Détails d'accès = NFS en lecture seule

3. Configurer le DNS pour la résolution de nom d'hôte :

- a. Cliquez sur **Storage > Storage VMs**, sélectionnez la VM de stockage, cliquez sur **Settings**, puis cliquez  sous **DNS**.
- b. Une fois la configuration DNS terminée, basculer sur le serveur DNS et mapper le serveur SMB.
  - Créer des entrées de recherche de transfert (A - enregistrement d'adresse) et de retour (PTR - enregistrement du pointeur) pour mapper le nom du serveur SMB à l'adresse IP de l'interface du réseau de données.
  - Si vous utilisez des alias NetBIOS, créez une entrée de recherche nom canonique d'alias (enregistrement de ressource CNAME) pour mapper chaque alias à l'adresse IP de l'interface de réseau de données du serveur SMB.

4. Configurer les services de noms selon les besoins :

- a. Cliquez sur **stockage > Storage VMs**, sélectionnez la VM de stockage, cliquez sur **Paramètres**, puis cliquez sur  pour LDAP ou NIS.
- b. Incluez les modifications dans le fichier de commutateur de services de noms : cliquez  sous **commutateur de services de noms**.


5. Configurez l'authentification et le chiffrement si nécessaire :

## Configurer TLS pour les clients NFS




NFS over TLS est disponible dans ONTAP 9.15.1 en tant que préversion publique. À titre de préversion, NFS over TLS n'est pas pris en charge pour les workloads de production dans ONTAP 9.15.1.


### Étapes

- a. Reportez-vous à la ["de formation"](#) Pour NFS sur TLS avant de commencer.
- b. Cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.
- c. Dans la mosaïque **NFS**, cliquez sur **NFS over TLS settings**.
- d. Dans la zone **NFS over TLS settings**, sélectionnez une interface réseau NFS pour laquelle vous souhaitez activer TLS.
- e. Cliquez sur  pour cette interface.
- f. Cliquez sur **Activer**.
- g. Dans la boîte de dialogue **Network interface TLS configuration**, incluez un certificat à utiliser avec TLS en sélectionnant l'une des options suivantes :
  - **Certificat installé** : choisissez un certificat installé précédemment dans la liste déroulante.
  - **Nouveau certificat** : choisissez un nom commun pour le certificat.
  - **Certificat externe signé par une autorité de certification** : suivez les instructions pour coller le contenu de votre certificat et de votre clé privée dans les boîtes.
- h. Cliquez sur **Enregistrer**.

## Configurer Kerberos

### Étapes

- a. Cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.
- b. Cliquez  dans la mosaïque Kerberos, puis cliquez sur **Ajouter**.

6. Mappez les noms d'utilisateur UNIX et Windows si nécessaire : cliquez  sous **mappage de noms**, puis cliquez sur **Ajouter**.

Vous ne devez le faire que si votre site possède des comptes d'utilisateur Windows et UNIX qui ne correspondent pas implicitement, c'est-à-dire lorsque la version minuscule de chaque nom d'utilisateur Windows correspond au nom d'utilisateur UNIX. Vous pouvez mapper des noms d'utilisateur à l'aide de LDAP, NIS ou utilisateurs locaux. Si vous avez deux ensembles d'utilisateurs qui ne correspondent pas, vous devez configurer le mappage de noms.

## Configurez NFS avec l'interface de ligne de commande

### Présentation de la configuration NFS avec l'interface de ligne de commande

Vous pouvez utiliser les commandes de l'interface de ligne de commande de ONTAP 9 pour configurer l'accès des clients NFS aux fichiers contenus dans un nouveau volume ou qtree dans une nouvelle machine virtuelle de stockage (SVM) ou existante.

Suivez les procédures ci-dessous pour configurer l'accès à un volume ou à un qtrees de la manière suivante :

- Vous souhaitez utiliser toute version de NFS actuellement prise en charge par ONTAP : NFS v3, NFS V4, NFS v4.1, NFSv4.2 ou NFSv4.1 avec pNFS.
- Vous souhaitez utiliser l'interface de ligne de commande et non System Manager, ni un outil de création de scripts automatisé.

Pour utiliser System Manager pour configurer l'accès multiprotocole NAS, reportez-vous à la section ["Provisionnement de stockage NAS pour Windows et Linux à l'aide des protocoles NFS et SMB"](#).

- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.

Vous trouverez des détails sur la syntaxe des commandes dans l'aide de l'interface de ligne de commande et dans les pages de manuel ONTAP.

- Les autorisations liées au fichier UNIX seront utilisées pour sécuriser le nouveau volume.
- Vous disposez des privilèges d'administrateur de cluster et non des privilèges d'administrateur de SVM.

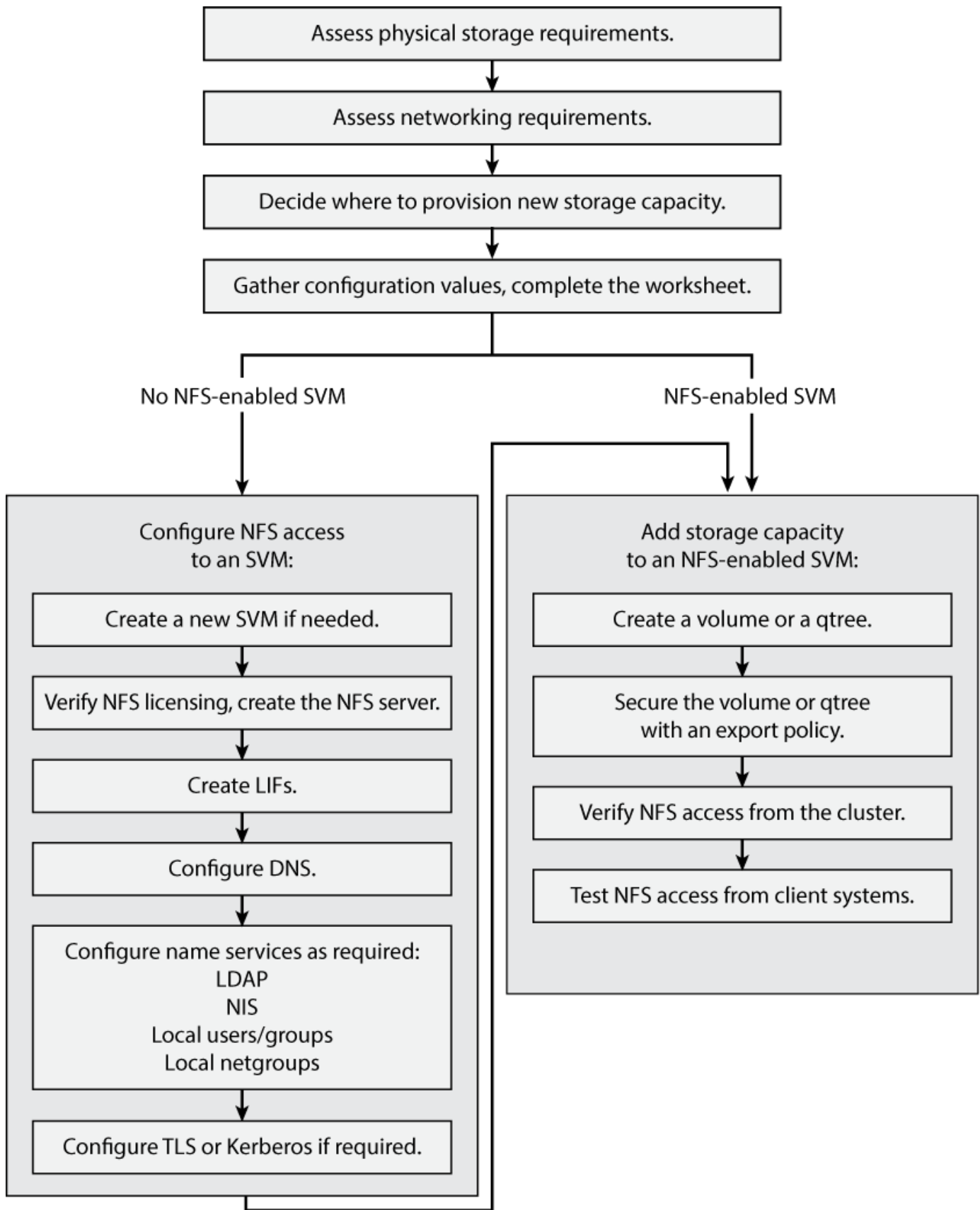
Pour plus d'informations sur la plage de fonctionnalités du protocole NFS ONTAP, consultez le ["Présentation de référence NFS"](#).

**D'autres façons de le faire dans ONTAP**

| Pour effectuer ces tâches avec...                                            | Reportez-vous à...                                                                |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| System Manager redessiné (disponible avec ONTAP 9.7 et versions ultérieures) | <a href="#">"Provisionnement du stockage NAS pour les serveurs Linux via NFS"</a> |
| System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures)   | <a href="#">"Présentation de la configuration NFS"</a>                            |

**Workflow de configuration NFS**

La configuration de NFS implique l'évaluation des besoins en stockage physique et en réseau, puis le choix d'un workflow spécifique à votre objectif : configurer l'accès NFS à un SVM nouveau ou existant, ou ajouter un volume ou un qtrees à un SVM existant déjà entièrement configuré pour l'accès NFS.



## Préparation

## Évaluer les besoins en matière de stockage physique

Avant de provisionner le stockage NFS pour les clients, vous devez vérifier que l'espace disponible sur un agrégat est suffisant pour le nouveau volume. Si ce n'est pas le cas, vous pouvez ajouter des disques à un agrégat existant ou créer un nouvel agrégat du type souhaité.

### Étapes

1. Afficher l'espace disponible dans les agrégats existants :

```
storage aggregate show
```

Si un agrégat dispose d'un espace suffisant, notez son nom dans la fiche de travail.

```
cluster::> storage aggregate show
Aggregate Size Available Used% State #Vols Nodes RAID Status

aggr_0 239.0GB 11.13GB 95% online 1 node1 raid_dp, normal
aggr_1 239.0GB 11.13GB 95% online 1 node1 raid_dp, normal
aggr_2 239.0GB 11.13GB 95% online 1 node2 raid_dp, normal
aggr_3 239.0GB 11.13GB 95% online 1 node2 raid_dp, normal
aggr_4 239.0GB 238.9GB 95% online 5 node3 raid_dp, normal
aggr_5 239.0GB 239.0GB 95% online 4 node4 raid_dp, normal
6 entries were displayed.
```

2. Si aucun agrégat n'a suffisamment d'espace, ajoutez des disques à un agrégat existant en utilisant le `storage aggregate add-disks` ou créez un nouvel agrégat à l'aide de `storage aggregate create` commande.

## Évaluer les exigences de mise en réseau

Avant de fournir un stockage NFS aux clients, vous devez vérifier que la mise en réseau est correctement configurée pour répondre aux exigences de provisionnement NFS.

### Ce dont vous avez besoin

Les objets de réseau de cluster suivants doivent être configurés :

- Ports physiques et logiques
- Les domaines de diffusion
- Sous-réseaux (le cas échéant)
- IPspaces (selon les besoins, en plus de l'IPspace par défaut)

- Failover Groups (si nécessaire, en plus du groupe de basculement par défaut pour chaque broadcast domain)
- Pare-feu externes

## Étapes

1. Afficher les ports physiques et virtuels disponibles :

```
network port show
```

- Dans la mesure du possible, vous devez utiliser le port avec la vitesse la plus élevée pour le réseau de données.
  - Tous les composants du réseau de données doivent avoir le même paramètre MTU pour optimiser les performances.
2. Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer l'adresse IP et la valeur du masque de réseau à une LIF, vérifiez que le sous-réseau existe et dispose des adresses disponibles suffisantes : +

```
network subnet show
```

Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche

3. Les sous-réseaux sont créés à l'aide du `network subnet create` commande.

3. Affichez les IPspaces disponibles :

```
network ipspace show
```

Vous pouvez utiliser l'IPspace par défaut ou un IPspace personnalisé.

4. Si vous souhaitez utiliser des adresses IPv6, vérifiez que l'IPv6 est activé sur le cluster :

```
network options ipv6 show
```

Si nécessaire, vous pouvez activer IPv6 en utilisant le `network options ipv6 modify` commande.

## Choisissez où provisionner la capacité de stockage NFS

Avant de créer un nouveau volume NFS ou qtree, vous devez décider de le placer dans une SVM nouvelle ou existante, et du volume de configuration requis par la SVM. Cette décision détermine votre flux de travail.

### Choix

- Si vous souhaitez provisionner un volume ou qtree sur un nouveau SVM, ou sur un SVM existant sur lequel NFS est activé mais non configuré, suivez les étapes de « Configuration de l'accès NFS à un SVM » et de « Ajout de stockage NFS à un SVM compatible NFS ».

[Configurer l'accès NFS à un SVM](#)

[Ajout d'un stockage NFS à un SVM compatible NFS](#)

Vous pouvez choisir de créer un nouveau SVM si l'un des cas suivants est vrai :

- Vous activez NFS pour la première fois sur un cluster.

- Un cluster contient des SVM existants, dans lequel vous ne souhaitez pas activer la prise en charge de NFS.
- Un cluster possède un ou plusieurs SVM compatibles NFS, et vous souhaitez un autre serveur NFS dans un espace de noms isolé (scénario de colocation).  
Vous devez également choisir cette option pour provisionner le stockage sur un SVM existant sur lequel NFS est activé, mais non configuré. Ce peut être le cas si vous avez créé le SVM pour l'accès SAN ou si aucun protocole n'a été activé au moment de la création de la SVM.

Après avoir activé NFS sur le SVM, procéder au provisionnement d'un volume ou qtree.

- Si vous souhaitez provisionner un volume ou qtree sur un SVM existant entièrement configuré pour l'accès NFS, suivez les étapes de la section « Ajout de stockage NFS à un SVM compatible NFS ».

### [Ajout de stockage NFS à un SVM compatible NFS](#)

## Fiche pour la collecte des informations de configuration NFS

La fiche de configuration NFS vous permet de collecter les informations requises pour configurer l'accès NFS pour les clients.

Vous devez remplir une ou les deux sections de la feuille de travail en fonction de la décision que vous avez prise concernant l'emplacement de provisionnement du stockage :

Si vous configurez l'accès NFS à un SVM, vous devez remplir les deux sections.

- Configuration de l'accès NFS à un SVM
- Ajout de capacité de stockage à un SVM compatible NFS

Si vous ajoutez de la capacité de stockage à un SVM compatible NFS, vous devez remplir uniquement les conditions suivantes :

- Ajout de capacité de stockage à un SVM compatible NFS

Pour plus d'informations sur les paramètres, reportez-vous aux pages de manuels des commandes.

## Configurer l'accès NFS à un SVM

### Paramètres de création d'un SVM

Ces valeurs sont fournies avec le `vserver create` Commande si vous créez un nouveau SVM.

| Champ                 | Description                                                                                                                                                                     | Votre valeur |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <code>-vserver</code> | Un nom que vous fournissez pour le nouveau SVM qui est un nom de domaine complet (FQDN) ou suit une autre convention qui applique des noms de SVM uniques au sein d'un cluster. |              |




|                                         |                                                                                                                           |                      |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------|----------------------|
| <code>-aggregate</code>                 | Nom d'un agrégat du cluster disposant d'un espace suffisant pour accueillir une nouvelle capacité de stockage NFS.        |                      |
| <code>-rootvolume</code>                | Un nom unique que vous fournissez pour le volume root du SVM.                                                             |                      |
| <code>-rootvolume-security-style</code> | Utiliser le style de sécurité UNIX pour la SVM.                                                                           | <code>unix</code>    |
| <code>-language</code>                  | Utilisez le paramètre de langue par défaut de ce flux de travail.                                                         | <code>C.UTF-8</code> |
| <code>ipspace</code>                    | Les IPspaces sont des espaces d'adresse IP distincts dans lesquels (SVM) résident les serveurs (Storage Virtual machine). |                      |

### Paramètres de création d'un serveur NFS

Ces valeurs sont fournies avec le `vserver nfs create` Commande lorsque vous créez un nouveau serveur NFS et spécifiez les versions NFS prises en charge.

Si vous activez NFSv4 ou une version ultérieure, vous devez utiliser LDAP pour renforcer la sécurité.

| Champ                                      | Description                                                                                                                                                                                                                                          | Votre valeur |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <code>-v3, -v4.0, -v4.1, -v4.1-pnfs</code> | <p>Activez les versions NFS si nécessaire.</p> <div>  <p>V4.2 est également pris en charge dans ONTAP 9.8 et versions ultérieures<br/>v4.1 est activé.</p> </div> |              |
| <code>-v4-id-domain</code>                 | ID nom de domaine de mappage.                                                                                                                                                                                                                        |              |
| <code>-v4-numeric-ids</code>               | Prise en charge des ID propriétaires numériques (activés ou désactivés).                                                                                                                                                                             |              |

### Paramètres d'activation du chiffrement TLS pour les connexions NFS

Ces valeurs sont fournies avec le `vserver nfs tls interface enable` commande.



NFS over TLS est disponible dans ONTAP 9.15.1 en tant que préversion publique. À titre de préversion, NFS over TLS n'est pas pris en charge pour les workloads de production dans ONTAP 9.15.1.

| Champ                          | Description                                                                                                       | Votre valeur |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------|
| <code>-vserver</code>          | Vserver dans lequel existe l'interface logique.                                                                   |              |
| <code>-lif</code>              | Nom de l'interface logique sur laquelle vous souhaitez activer le chiffrement en transit à l'aide de NFS sur TLS. |              |
| <code>-certificate-name</code> | Nom du certificat X.509 configuré dans la machine virtuelle de stockage.                                          |              |

### Paramètres de création d'une LIF

Ces valeurs sont fournies avec le `network interface create` Commande lorsque vous créez des LIFs.

Si vous utilisez Kerberos, vous devez activer Kerberos sur plusieurs LIFs.

| Champ                       | Description                                                                                                                                        | Votre valeur      |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| <code>-lif</code>           | Nom que vous fournissez pour la nouvelle LIF.                                                                                                      |                   |
| <code>-role</code>          | Utiliser le rôle LIF de données dans ce workflow                                                                                                   | <code>data</code> |
| <code>-data-protocol</code> | Utilisez uniquement le protocole NFS dans ce workflow.                                                                                             | <code>nfs</code>  |
| <code>-home-node</code>     | Le nœud vers lequel la LIF renvoie lorsque <code>network interface revert</code> La commande est exécutée sur le LIF.                              |                   |
| <code>-home-port</code>     | Le port ou le groupe d'interface sur lequel la LIF renvoie au moment du <code>network interface revert</code> La commande est exécutée sur le LIF. |                   |
| <code>-address</code>       | L'adresse IPv4 ou IPv6 sur le cluster qui seront utilisées pour l'accès aux données par la nouvelle LIF.                                           |                   |

|                  |                                                                                                                                   |      |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------|------|
| -netmask         | Le masque de réseau et la passerelle pour le LIF.                                                                                 |      |
| -subnet          | Un pool d'adresses IP. Utilisé au lieu de -address et -netmask pour attribuer automatiquement des adresses et des masques réseau. |      |
| -firewall-policy | Utilisez la politique de pare-feu de données par défaut dans ce workflow.                                                         | data |

### Paramètres de résolution de nom d'hôte DNS

Ces valeurs sont fournies avec le `vserver services name-service dns create` Commande lorsque vous configurez un DNS.

| Champ         | Description                                                | Votre valeur |
|---------------|------------------------------------------------------------|--------------|
| -domains      | Jusqu'à cinq noms de domaine DNS.                          |              |
| -name-servers | Jusqu'à trois adresses IP pour chaque serveur de noms DNS. |              |

### Nom des informations sur le service

### Paramètres pour la création d'utilisateurs locaux

Vous fournissez ces valeurs si vous créez des utilisateurs locaux à l'aide de l'`vserver services name-service unix-user create` commande. Si vous configurez des utilisateurs locaux en chargeant un fichier contenant des utilisateurs UNIX à partir d'un URI (Uniform Resource identifier), vous n'avez pas besoin de spécifier ces valeurs manuellement.

|         | Nom d'utilisateur (-user) | ID d'utilisateur (-id) | ID de groupe (-primary-gid) | Nom complet (-full-name) |
|---------|---------------------------|------------------------|-----------------------------|--------------------------|
| Exemple | je johnm                  | 123                    | 100                         | John Miller              |
| 1       |                           |                        |                             |                          |
| 2       |                           |                        |                             |                          |
| 3       |                           |                        |                             |                          |
| ...     |                           |                        |                             |                          |

|   |  |  |  |  |
|---|--|--|--|--|
| n |  |  |  |  |
|---|--|--|--|--|

## Paramètres de création de groupes locaux

Vous fournissez ces valeurs si vous créez des groupes locaux à l'aide de l' `vserver services name-service unix-group create` commande. Si vous configurez des groupes locaux en chargeant un fichier contenant des groupes UNIX à partir d'un URI, vous n'avez pas besoin de spécifier ces valeurs manuellement.

|         | Nom du groupe ( <code>-name</code> ) | ID de groupe ( <code>-id</code> ) |
|---------|--------------------------------------|-----------------------------------|
| Exemple | Ingénierie                           | 100                               |
| 1       |                                      |                                   |
| 2       |                                      |                                   |
| 3       |                                      |                                   |
| ...     |                                      |                                   |
| n       |                                      |                                   |

## Paramètres pour NIS

Ces valeurs sont fournies avec le `vserver services name-service nis-domain create` commande.



À partir de ONTAP 9.2, le champ `-nis-servers` remplace le champ `-servers`. Ce nouveau champ peut prendre un nom d'hôte ou une adresse IP pour le serveur NIS.

| Champ                     | Description                                                                                                                                | Votre valeur  |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <code>-domain</code>      | Domaine NIS que la SVM utilisera pour les recherches de noms.                                                                              |               |
| <code>-active</code>      | Serveur de domaine NIS actif.                                                                                                              | true ou false |
| <code>-servers</code>     | ONTAP 9.0, 9.1 : une ou plusieurs adresses IP des serveurs NIS utilisés par la configuration de domaine NIS.                               |               |
| <code>-nis-servers</code> | ONTAP 9.2 : liste séparée par des virgules d'adresses IP et de noms d'hôte pour les serveurs NIS utilisés par la configuration de domaine. |               |

## Paramètres pour LDAP

Ces valeurs sont fournies avec le `vserver services name-service ldap client create` commande.

Vous aurez également besoin d'un certificat d'autorité de certification racine auto-signé .pem fichier.



À partir de ONTAP 9.2, le champ `-ldap-servers` remplace le champ `-servers`. Ce nouveau champ peut prendre un nom d'hôte ou une adresse IP pour le serveur LDAP.

| Champ                              | Description                                                                                                                                                                              | Votre valeur |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <code>-vserver</code>              | Le nom du SVM pour lequel vous souhaitez créer une configuration client LDAP.                                                                                                            |              |
| <code>-client-config</code>        | Nom que vous attribuez pour la nouvelle configuration du client LDAP.                                                                                                                    |              |
| <code>-servers</code>              | ONTAP 9.0, 9.1 : un ou plusieurs serveurs LDAP par adresse IP dans une liste séparée par des virgules.                                                                                   |              |
| <code>-ldap-servers</code>         | ONTAP 9.2 : liste séparée par des virgules d'adresses IP et de noms d'hôte pour les serveurs LDAP.                                                                                       |              |
| <code>-query-timeout</code>        | Utilisez la valeur par défaut 3 secondes pour ce flux de travail.                                                                                                                        | 3            |
| <code>-min-bind-level</code>       | Niveau d'authentification de liaison minimum. La valeur par défaut est <code>anonymous</code> . Doit être réglé sur <code>sasl</code> si la signature et le chiffrement sont configurés. |              |
| <code>-preferred-ad-servers</code> | Un ou plusieurs serveurs Active Directory préférés par adresse IP dans une liste délimitée par des virgules.                                                                             |              |
| <code>-ad-domain</code>            | Domaine Active Directory.                                                                                                                                                                |              |
| <code>-schema</code>               | Le modèle de schéma à utiliser. Vous pouvez utiliser un schéma par défaut ou personnalisé.                                                                                               |              |

| Champ             | Description                                                                                | Votre valeur |
|-------------------|--------------------------------------------------------------------------------------------|--------------|
| -port             | Utilisez le port de serveur LDAP par défaut 389 pour ce flux de travail.                   | 389          |
| -bind-dn          | Nom distinctif de l'utilisateur Bind.                                                      |              |
| -base-dn          | Nom distinctif de base. La valeur par défaut est "" (racine).                              |              |
| -base-scope       | Utilisez l'étendue de recherche de base par défaut subnet pour ce flux de travail.         | subnet       |
| -session-security | Active la signature ou la signature et le chiffrement LDAP. La valeur par défaut est none. |              |
| -use-start-tls    | Active LDAP sur TLS. La valeur par défaut est false.                                       |              |

### Paramètres d'authentification Kerberos

Ces valeurs sont fournies avec le `vserver nfs kerberos realm create` commande. Certaines valeurs diffèrent selon que vous utilisez Microsoft Active Directory en tant que serveur KDC (Key distribution Center), MIT ou autre serveur KDC UNIX.

| Champ          | Description                                                           | Votre valeur |
|----------------|-----------------------------------------------------------------------|--------------|
| -vserver       | La SVM qui communiquera avec le KDC.                                  |              |
| -realm         | Le domaine Kerberos.                                                  |              |
| -clock-skew    | Inclinaison de l'horloge autorisée entre les clients et les serveurs. |              |
| -kdc-ip        | Adresse IP KDC.                                                       |              |
| -kdc-port      | Numéro de port KDC.                                                   |              |
| -adserver-name | Microsoft KDC uniquement : nom du serveur AD.                         |              |
| -adserver-ip   | Microsoft KDC uniquement : adresse IP du serveur AD.                  |              |

|                      |                                                                   |                            |
|----------------------|-------------------------------------------------------------------|----------------------------|
| -adminserver-ip      | UNIX KDC uniquement : adresse IP du serveur d'administration.     |                            |
| -adminserver-port    | UNIX KDC uniquement : numéro de port du serveur d'administration. |                            |
| -passwordserver-ip   | UNIX KDC uniquement : adresse IP du serveur de mots de passe.     |                            |
| -passwordserver-port | UNIX KDC uniquement : port du serveur de mots de passe.           |                            |
| -kdc-vendor          | Fournisseur KDC.                                                  | { Microsoft                |
| Other }              | -comment                                                          | Tout commentaire souhaité. |

Ces valeurs sont fournies avec le `vserver nfs kerberos interface enable` commande.

| Champ                | Description                                                                                                                                         | Votre valeur |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| -vserver             | Le nom du SVM pour lequel vous souhaitez créer une configuration Kerberos.                                                                          |              |
| -lif                 | La LIF de données sur laquelle vous activez Kerberos. Vous pouvez activer Kerberos sur plusieurs LIFs.                                              |              |
| -spn                 | Le nom du principe de service (SPN)                                                                                                                 |              |
| -permitted-enc-types | Les types de chiffrement autorisés pour Kerberos sur NFS ; aes-256 est recommandé en fonction des capacités du client.                              |              |
| -admin-username      | Les informations d'identification de l'administrateur KDC pour récupérer la clé secrète SPN directement à partir du KDC. Un mot de passe est requis |              |
| -keytab-uri          | Le fichier keytab du KDC contenant la clé SPN si vous ne disposez pas d'informations d'identification administrateur KDC.                           |              |

|     |                                                                                                                                                                           |  |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| -ou | L'unité organisationnelle sous laquelle le compte du serveur Microsoft Active Directory sera créé lorsque vous activez Kerberos à l'aide d'un Royaume pour Microsoft KDC. |  |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|

## Ajout de capacité de stockage à un SVM compatible NFS

### Paramètres de création de règles et de politiques d'exportation

Ces valeurs sont fournies avec le `vserver export-policy create` commande.

| Champ       | Description                                              | Votre valeur |
|-------------|----------------------------------------------------------|--------------|
| -vserver    | Nom du SVM qui hébergera le nouveau volume.              |              |
| -policyname | Nom que vous fournissez pour une nouvelle export-policy. |              |

Vous fournissez ces valeurs pour chaque règle avec le `vserver export-policy rule create` commande.

| Champ        | Description                                                  | Votre valeur |
|--------------|--------------------------------------------------------------|--------------|
| -clientmatch | Spécification de correspondance du client.                   |              |
| -ruleindex   | Position de la règle d'exportation dans la liste des règles. |              |
| -protocol    | Utiliser NFS dans ce flux de production.                     | nfs          |
| -rorule      | Méthode d'authentification pour l'accès en lecture seule.    |              |
| -rwrule      | Méthode d'authentification pour l'accès en lecture-écriture. |              |
| -superuser   | Méthode d'authentification pour l'accès superutilisateur.    |              |
| -anon        | ID utilisateur auquel les utilisateurs anonymes sont mappés. |              |

Vous devez créer une ou plusieurs règles pour chaque export-policy.



| <b>-ruleindex</b> | <b>-clientmatch</b>            | <b>-rorule</b> | <b>-rwrule</b> | <b>-superuser</b> | <b>-anon</b> |
|-------------------|--------------------------------|----------------|----------------|-------------------|--------------|
| Exemples          | 0.0.0.0/0,@rootaccess_netgroup | toutes         | krb5           | system            | 65534        |
| 1                 |                                |                |                |                   |              |
| 2                 |                                |                |                |                   |              |
| 3                 |                                |                |                |                   |              |
| ...               |                                |                |                |                   |              |
| n                 |                                |                |                |                   |              |

### Paramètres de création d'un volume

Ces valeurs sont fournies avec le `volume create` commande si vous créez un volume à la place d'un qtrees.

| Champ                         | Description                                                                             | Votre valeur |
|-------------------------------|-----------------------------------------------------------------------------------------|--------------|
| <code>-vserver</code>         | Nom d'un SVM nouveau ou existant qui hébergera le nouveau volume.                       |              |
| <code>-volume</code>          | Un nom descriptif unique que vous fournissez pour le nouveau volume.                    |              |
| <code>-aggregate</code>       | Nom d'un agrégat du cluster disposant d'un espace suffisant pour le nouveau volume NFS. |              |
| <code>-size</code>            | Un entier que vous fournissez pour la taille du nouveau volume.                         |              |
| <code>-user</code>            | Nom ou ID de l'utilisateur défini en tant que propriétaire de la racine du volume.      |              |
| <code>-group</code>           | Nom ou ID du groupe défini comme propriétaire de la racine du volume.                   |              |
| <code>--security-style</code> | Utilisez le style de sécurité UNIX pour ce flux de travail.                             | unix         |
| <code>-junction-path</code>   | Emplacement sous la racine (/) où le nouveau volume doit être monté.                    |              |

|                             |                                                                                                                    |  |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------|--|
| <code>-export-policy</code> | Si vous prévoyez d'utiliser une export-policy existante, vous pouvez entrer son nom lors de la création du volume. |  |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------|--|

## Paramètres pour la création d'un qtree

Ces valeurs sont fournies avec le `volume qtree create` commande si vous créez un qtree à la place d'un volume.

| Champ                          | Description                                                                                                                                                               | Votre valeur |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <code>-vserver</code>          | Nom de la SVM sur lequel réside le volume contenant le qtree.                                                                                                             |              |
| <code>-volume</code>           | Nom du volume qui contiendra le nouveau qtree.                                                                                                                            |              |
| <code>-qtree</code>            | Un nom descriptif unique que vous fournissez pour le nouveau qtree, 64 caractères maximum.                                                                                |              |
| <code>-qtree-path</code>       | L'argument de chemin qtree dans le format<br><i>/vol/volume_name/qtree_name</i> > peut être spécifié au lieu de spécifier volume et qtree en tant qu'arguments distincts. |              |
| <code>-unix-permissions</code> | Facultatif : les autorisations UNIX pour le qtree.                                                                                                                        |              |
| <code>-export-policy</code>    | Si vous prévoyez d'utiliser une export policy existante, vous pouvez saisir son nom lors de la création du qtree.                                                         |              |

## Configurer l'accès NFS à un SVM

### Créer un SVM

Si vous ne disposez pas encore d'au moins un SVM dans un cluster afin de fournir l'accès aux données aux clients NFS, vous devez en créer un.

### Avant de commencer

- À partir de la version ONTAP 9.13.1, vous pouvez définir une capacité maximale pour une machine virtuelle de stockage. Vous pouvez également configurer des alertes lorsque la SVM approche un niveau de capacité seuil. Pour plus d'informations, voir [Gestion de la capacité des SVM](#).

## Étapes

### 1. Création d'un SVM :

```
vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate
aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace
ipspace_name
```

- Utilisez le paramètre `UNIX` pour le `-rootvolume-security-style` option.
- Utilisez le paramètre par défaut `C.UTF-8` `-language` option.
- Le `ipspace` le paramètre est facultatif.

### 2. Vérifier la configuration et le statut du nouveau SVM :

```
vserver show -vserver vserver_name
```

Le `Allowed Protocols NFS` doit être inclus dans le champ. Vous pouvez modifier cette liste ultérieurement.

Le `Vserver Operational State` le champ doit afficher `running` état. S'il affiche le `initializing` État, cela signifie qu'une opération intermédiaire telle que la création du volume root a échoué, et vous devez supprimer la SVM et la recréer.

## Exemples

La commande suivante crée un SVM pour l'accès aux données dans l'IPspace `ipspaceA` :

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA
```

```
[Job 2059] Job succeeded:
Vserver creation completed
```

La commande suivante montre qu'un SVM a été créé avec un volume root de 1 Go, il a été démarré automatiquement et qu'il est en `running` état. Le volume root dispose d'une export policy par défaut qui n'inclut aucune règle et qui ne précise donc pas l'exportation du volume root au moment de sa création.

```
cluster1::> vserver show -vserver vs1.example.com
Vserver: vs1.example.com
Vserver Type: data
Vserver Subtype: default
Vserver UUID: b8375669-19b0-11e5-b9d1-00a0983d9736
Root Volume: root_vs1
Aggregate: aggr1
NIS Domain: -
Root Volume Security Style: unix
LDAP Client: -
Default Volume Language Code: C.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
Disallowed Protocols: -
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspaceA
```



À partir de la ONTAP 9.13.1, vous pouvez définir un modèle de groupe de règles de QoS adaptative, en appliquant une limite plafond et un seuil de débit aux volumes du SVM. Vous ne pouvez appliquer cette politique qu'après avoir créé la SVM. Pour en savoir plus sur ce processus, voir [Définissez un modèle de groupe de règles adaptatives](#).

## Vérifier que le protocole NFS est activé sur le SVM

Avant de pouvoir configurer et utiliser NFS sur les SVM, vous devez vérifier que le protocole est activé.

### Description de la tâche

Cela s'effectue généralement lors de la configuration d'un SVM, mais si vous n'avez pas activé le protocole lors de l'installation, vous pouvez l'activer plus tard à l'aide du `vserver add-protocols` commande.



Vous ne pouvez pas ajouter ou supprimer un protocole d'une LIF une fois qu'il est créé.

Vous pouvez également désactiver les protocoles sur les SVM à l'aide de `vserver remove-protocols` commande.

### Étapes

1. Vérifier les protocoles actuellement activés et désactivés pour le SVM :

```
vserver show -vserver vserver_name -protocols
```

Vous pouvez également utiliser le `vserver show-protocols` Commande permettant d'afficher les protocoles actuellement activés sur tous les SVM du cluster.

2. Si nécessaire, activer ou désactiver un protocole :

- ° Pour activer le protocole NFS :

```
vserver add-protocols -vserver vserver_name -protocols nfs
```

- ° Pour désactiver un protocole :

```
vserver remove-protocols -vserver vserver_name -protocols protocol_name
[,protocol_name,...]
```

3. Vérifiez que les protocoles activés et désactivés ont été correctement mis à jour :

```
vserver show -vserver vserver_name -protocols
```

### Exemple

La commande suivante affiche les protocoles actuellement activés et désactivés (autorisés et interdits) sur le SVM nommé vs1 :

```
vs1::> vserver show -vserver vs1.example.com -protocols
```

| Vserver         | Allowed Protocols | Disallowed Protocols   |
|-----------------|-------------------|------------------------|
| vs1.example.com | nfs               | cifs, fcp, iscsi, ndmp |

La commande suivante permet l'accès via NFS en ajoutant `nfs` Pour la liste des protocoles activés sur le SVM nommé vs1 :

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

### Ouvrir la export policy du volume root du SVM

La export policy par défaut du volume root du SVM doit inclure une règle permettant à tous les clients d'y accéder via NFS. Sans une telle règle, tous les clients NFS se voient refuser l'accès au SVM et à ses volumes.

#### Description de la tâche

Lorsqu'un nouveau SVM est créé, une export policy par défaut (appelée default) est créée automatiquement pour le volume root du SVM. On doit créer une ou plusieurs règles pour l'export policy par défaut avant que les clients puissent accéder aux données sur la SVM.

Vous devez vérifier que l'accès est ouvert à tous les clients NFS dans la stratégie d'exportation par défaut, puis limiter l'accès aux volumes individuels en créant des règles d'exportation personnalisées pour les volumes individuels ou les qtrees.

## Étapes

1. Si vous utilisez un SVM existant, vérifier la root volume export policy par défaut :

```
vserver export-policy rule show
```

Le résultat de la commande doit être similaire à ce qui suit :

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

Vserver: vs1.example.com
Policy Name: default
Rule Index: 1
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
RO Access Rule: any
RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: any
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

Si une telle règle existe et autorise l'accès ouvert, cette tâche est terminée. Si ce n'est pas le cas, passez à l'étape suivante.

2. Créer une règle d'export pour le volume root du SVM:

```
vserver export-policy rule create -vserver vserver_name -policyname default
-ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
-superuser any
```

Si la SVM ne contiendra que des volumes sécurisés par Kerberos, vous pouvez définir les options des règles d'exportation `-rorule`, `-rwrule`, et `-superuser` pour le volume racine à `krb5` ou `krb5i`. Par exemple :

```
-rorule krb5i -rwrule krb5i -superuser krb5i
```

3. Vérifiez la création de règles à l'aide du `vserver export-policy rule show` commande.

## Résultat

Tout client NFS peut désormais accéder à tout volume ou qtrees créé sur le SVM.

## Créez un serveur NFS

Après avoir vérifié que NFS est sous licence sur le cluster, vous pouvez utiliser le `vserver nfs create` Commande permettant de créer un serveur NFS sur le SVM et de spécifier les versions NFS prises en charge.

## Description de la tâche

Le SVM peut être configuré pour prendre en charge une ou plusieurs versions de NFS. Si vous supporte NFSv4 ou version ultérieure :

- Le nom de domaine de mappage de l'ID utilisateur NFSv4 doit être identique sur le serveur NFSv4 et les clients cibles.

Il n'est pas nécessairement nécessaire d'être identique à un nom de domaine LDAP ou NIS tant que le serveur NFSv4 et les clients utilisent le même nom.

- Les clients cibles doivent prendre en charge le paramètre d'ID numérique NFSv4.
- Pour des raisons de sécurité, vous devez utiliser LDAP pour les services de noms dans les déploiements NFSv4.

### Avant de commencer

Le SVM doit avoir été configuré pour permettre le protocole NFS.

### Étapes

1. Vérifiez que NFS est sous licence sur le cluster :

```
system license show -package nfs
```

Si ce n'est pas le cas, contactez votre représentant commercial.

2. Créer un serveur NFS :

```
vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
{enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
{enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
```

Vous pouvez choisir d'activer n'importe quelle combinaison de versions NFS. Si vous souhaitez prendre en charge la norme pNFS, vous devez les activer `-v4.1` et `-v4.1-pnfs` options.

Si vous activez v4 ou version ultérieure, vous devez également vous assurer que les options suivantes sont correctement définies :

- `-v4-id-domain`

Ce paramètre facultatif spécifie la partie domaine de la forme de chaîne de noms d'utilisateurs et de groupes, comme défini par le protocole NFSv4. Par défaut, ONTAP utilise le domaine NIS si l'un est défini ; si ce n'est pas le cas, le domaine DNS est utilisé. Vous devez fournir une valeur correspondant au nom de domaine utilisé par les clients cibles.

- `-v4-numeric-ids`

Ce paramètre facultatif indique si la prise en charge des identificateurs de chaîne numériques dans les attributs propriétaire NFSv4 est activée. Le paramètre par défaut est activé mais vous devez vérifier que les clients cibles le prennent en charge.

Vous pouvez activer d'autres fonctionnalités NFS ultérieurement en utilisant le `vserver nfs modify` commande.

3. Vérifiez que NFS est en cours d'exécution :

```
vserver nfs status -vserver vserver_name
```

#### 4. Vérifiez que NFS est configuré comme vous le souhaitez :

```
vserver nfs show -vserver vserver_name
```

#### Exemples

La commande suivante crée un serveur NFS sur le SVM nommé vs1 avec NFSv3 et NFSv4.0 activés :

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

Les commandes suivantes vérifient les valeurs d'état et de configuration du nouveau serveur NFS nommé vs1 :

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

Vserver: vs1
General NFS Access: true
NFS v3: enabled
NFS v4.0: enabled
UDP Protocol: enabled
TCP Protocol: enabled
Default Windows User: -
NFSv4.0 ACL Support: disabled
NFSv4.0 Read Delegation Support: disabled
NFSv4.0 Write Delegation Support: disabled
NFSv4 ID Mapping Domain: my_domain.com
...
```

#### Créer une LIF

Une LIF est une adresse IP associée à un port physique ou logique. En cas de panne d'un composant, une LIF peut basculer vers un autre port physique ou la migrer vers un autre port, ce qui continue à communiquer avec le réseau.

#### Ce dont vous avez besoin

- Le port réseau physique ou logique sous-jacent doit avoir été configuré sur l'administrateur up état.
- Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, le sous-réseau doit déjà exister.

Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche 3. Ils sont créés à l'aide du `network subnet create` commande.



- Le mécanisme de spécification du type de trafic traité par une LIF a changé. Pour ONTAP 9.5 et versions antérieures, la LIF utilisait des rôles pour spécifier le type de trafic qu'elle entraînerait. Depuis ONTAP 9.6, les LIF utilisent des politiques de service pour spécifier le type de trafic qu'elles seraient à traiter.

### Description de la tâche

- Vous pouvez créer des LIF IPv4 et IPv6 sur le même port réseau.
- Si vous utilisez l'authentification Kerberos, activez Kerberos sur plusieurs LIFs.
- Si vous disposez d'un grand nombre de LIF dans le cluster, vous pouvez vérifier la capacité LIF prise en charge sur le cluster à l'aide de `network interface capacity show` Et la capacité LIF prise en charge sur chaque nœud à l'aide de `network interface capacity details show` commande (au niveau de privilège avancé).
- Depuis ONTAP 9.7, si d'autres LIF existent déjà pour le SVM dans le même sous-réseau, il n'est pas nécessaire de spécifier le home port de la LIF. ONTAP choisit automatiquement un port aléatoire sur le nœud de rattachement spécifié dans le même domaine de diffusion que les autres LIFs déjà configurées dans le même sous-réseau.

Le protocole FC-NVMe est pris en charge à partir de la version ONTAP 9.4. Si vous créez une LIF FC-NVMe, notez les éléments suivants :

- Le protocole NVMe doit être pris en charge par l'adaptateur FC sur lequel la LIF est créée.
- FC-NVMe est le seul protocole de données sur les LIF de données.
- Un trafic de gestion des LIF doit être configuré pour chaque SVM (Storage Virtual machine) prenant en charge les protocoles SAN.
- Les LIFs et namespaces NVMe doivent être hébergés sur le même nœud.
- Un seul protocole LIF NVMe traitant le trafic de données peut être configuré par SVM

### Étapes

#### 1. Créer une LIF :

```
network interface create -vserver vservice_name -lif lif_name -role data -data
-protocol nfs -home-node node_name -home-port port_name {-address IP_address
-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
-revert {true|false}
```

| Option                                                                          | Description                                                                                                                                                                                  |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ONTAP 9.5 et versions antérieures</b>                                        | <code>`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol nfs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address</code> |
| <code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code> | <code>false}`</code>                                                                                                                                                                         |
| <b>ONTAP 9.6 et ultérieur</b>                                                   | <code>`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol nfs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address</code> |

|                                                                    |                     |
|--------------------------------------------------------------------|---------------------|
| <code>-subnet-name <i>subnet_name</i> -firewall-policy data</code> | <code>false}</code> |
| <code>-auto-revert {true</code>                                    |                     |

- ° Le `-role` Paramètre n'est pas requis lors de la création d'une LIF à l'aide d'une politique de service (à partir de avecONTAP 9.6).
- ° Le `-data-protocol` Le paramètre doit être spécifié lors de la création de la LIF et ne peut pas être modifié par la suite sans destruction et recréez la LIF de données.

Le `-data-protocol` Paramètre n'est pas requis lors de la création d'une LIF à l'aide d'une politique de service (à partir de ONTAP 9.6).

- ° `-home-node` Est le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.

Vous pouvez également indiquer si la LIF doit revenir automatiquement au nœud home et au port home-port avec le `-auto-revert` option.

- ° `-home-port` Est le port physique ou logique vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.
- ° Vous pouvez spécifier une adresse IP avec le `-address` et `-netmask` ou vous activez l'allocation à partir d'un sous-réseau avec le `-subnet_name` option.
- ° Lors de l'utilisation d'un sous-réseau pour fournir l'adresse IP et le masque de réseau, si le sous-réseau a été défini avec une passerelle, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau.
- ° Si vous attribuez des adresses IP manuellement (sans utiliser de sous-réseau), vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un autre sous-réseau IP. Le `network route create` La page man contient des informations sur la création d'une route statique au sein d'un SVM.
- ° Pour le `-firewall-policy` utilisez la même option par défaut `data` Comme le rôle LIF.

Vous pouvez créer et ajouter une stratégie de pare-feu personnalisée ultérieurement si vous le souhaitez.



Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "[Configuration des politiques de pare-feu pour les LIF](#)".

- ° `-auto-revert` Vous permet de spécifier si une LIF de données est automatiquement rétablie sur le nœud de rattachement en cas de démarrage, de modifications du statut de la base de données de gestion ou lors de la connexion réseau. Le paramètre par défaut est `false`, mais vous pouvez le définir sur `false` selon les stratégies de gestion de réseau de votre environnement.

2. Vérifier que le LIF a été créé avec succès en utilisant le `network interface show` commande.

3. Vérifiez que l'adresse IP configurée est accessible :

|                  |                           |
|------------------|---------------------------|
| Pour vérifier... | Utiliser...               |
| Adresse IPv4     | <code>network ping</code> |

|              |               |
|--------------|---------------|
| Adresse IPv6 | network ping6 |
|--------------|---------------|

4. Si vous utilisez Kerberos, répétez les étapes 1 à 3 pour en créer d'autres.

Kerberos doit être activé séparément sur chacune de ces LIFs.

### Exemples

La commande suivante crée une LIF et spécifie les valeurs d'adresse IP et de masque réseau à l'aide de `-address` et `-netmask` paramètres :

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port elc -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

La commande suivante crée une LIF et attribue des valeurs d'adresse IP et de masque réseau à partir du sous-réseau spécifié (nommé `client1_sub`) :

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port elc -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

La commande suivante affiche toutes les LIFs du cluster-1. Les LIF de données `datalif1` et `datalif3` sont configurées avec des adresses IPv4 et le `datalif4` est configuré avec une adresse IPv6 :

```
network interface show
```

| Vserver         | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Is Port |
|-----------------|-------------------|-------------------|----------------------|--------------|-----------------|
| Home            |                   |                   |                      |              |                 |
| -----           | -----             | -----             | -----                | -----        | -----           |
| ----            |                   |                   |                      |              |                 |
| cluster-1       |                   |                   |                      |              |                 |
|                 | cluster_mgmt      | up/up             | 192.0.2.3/24         | node-1       | e1a             |
| true            |                   |                   |                      |              |                 |
| node-1          |                   |                   |                      |              |                 |
|                 | clus1             | up/up             | 192.0.2.12/24        | node-1       | e0a             |
| true            |                   |                   |                      |              |                 |
|                 | clus2             | up/up             | 192.0.2.13/24        | node-1       | e0b             |
| true            |                   |                   |                      |              |                 |
|                 | mgmt1             | up/up             | 192.0.2.68/24        | node-1       | e1a             |
| true            |                   |                   |                      |              |                 |
| node-2          |                   |                   |                      |              |                 |
|                 | clus1             | up/up             | 192.0.2.14/24        | node-2       | e0a             |
| true            |                   |                   |                      |              |                 |
|                 | clus2             | up/up             | 192.0.2.15/24        | node-2       | e0b             |
| true            |                   |                   |                      |              |                 |
|                 | mgmt1             | up/up             | 192.0.2.69/24        | node-2       | e1a             |
| true            |                   |                   |                      |              |                 |
| vs1.example.com |                   |                   |                      |              |                 |
|                 | datalif1          | up/down           | 192.0.2.145/30       | node-1       | e1c             |
| true            |                   |                   |                      |              |                 |
| vs3.example.com |                   |                   |                      |              |                 |
|                 | datalif3          | up/up             | 192.0.2.146/30       | node-2       | e0c             |
| true            |                   |                   |                      |              |                 |
|                 | datalif4          | up/up             | 2001::2/64           | node-2       | e0c             |
| true            |                   |                   |                      |              |                 |

5 entries were displayed.

La commande suivante montre comment créer une LIF de données NAS attribuée avec le default-data-files règle de service :

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport e0d -service-policy default-data-files -subnet-name ipspace1
```

### Activez le DNS pour la résolution du nom d'hôte

Vous pouvez utiliser le `vserver services name-service dns` Commande permettant d'activer DNS sur un SVM et de le configurer afin d'utiliser DNS pour la

résolution de nom d'hôte. Les noms d'hôte sont résolus à l'aide de serveurs DNS externes.

**Ce dont vous avez besoin**

Un serveur DNS au niveau du site doit être disponible pour les recherches de noms d'hôte.

Vous devez configurer plusieurs serveurs DNS pour éviter un point de défaillance unique. Le `vserver services name-service dns create` Commande émet un avertissement si vous entrez un seul nom de serveur DNS.

**Description de la tâche**

Le *Network Management Guide* contient des informations sur la configuration de DNS dynamique sur le SVM.


**Étapes**

- 1. Activer le DNS sur le SVM :

```
vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled
```

La commande suivante permet d'activer les serveurs DNS externes sur le SVM vs1 :

```
vserver services name-service dns create -vserver vs1.example.com -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state enabled
```



À partir de ONTAP 9.2, le `vserver services name-service dns create` Commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP ne parvient pas à contacter le serveur de noms.

- 2. Afficher les configurations de domaine DNS à l'aide de `vserver services name-service dns show` commande.

La commande suivante affiche les configurations DNS pour tous les SVM du cluster :

```
vserver services name-service dns show
```

| Vserver         | State   | Domains     | Name Servers                |
|-----------------|---------|-------------|-----------------------------|
| cluster1        | enabled | example.com | 192.0.2.201,<br>192.0.2.202 |
| vs1.example.com | enabled | example.com | 192.0.2.201,<br>192.0.2.202 |

La commande suivante affiche des informations détaillées de configuration DNS pour le SVM vs1 :

```
vserver services name-service dns show -vserver vs1.example.com
Vserver: vs1.example.com
Domains: example.com
Name Servers: 192.0.2.201, 192.0.2.202
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

3. Validez l'état des serveurs de noms à l'aide de la `vserver services name-service dns check` commande.

Le `vserver services name-service dns check` Est disponible à partir de ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com
```

| Vserver         | Name Server | Status | Status Details          |
|-----------------|-------------|--------|-------------------------|
| -----           | -----       | -----  |                         |
| vs1.example.com | 10.0.0.50   | up     | Response time (msec): 2 |
| vs1.example.com | 10.0.0.51   | up     | Response time (msec): 2 |

## Configurer NAME-services

### Configurer les services de noms pour la présentation

En fonction de la configuration de votre système de stockage, ONTAP doit pouvoir rechercher des informations sur l'hôte, l'utilisateur, le groupe ou le groupe réseau afin de fournir un accès approprié aux clients. Vous devez configurer les services de noms pour permettre à ONTAP d'accéder aux services de noms locaux ou externes afin d'obtenir ces informations.

Vous devez utiliser un service de noms tel que NIS ou LDAP pour faciliter les recherches de noms lors de l'authentification client. Il est préférable d'utiliser LDAP dans la mesure du possible pour renforcer la sécurité, notamment lors du déploiement de NFSv4 ou de versions ultérieures. Vous devez également configurer des utilisateurs et des groupes locaux si des serveurs de noms externes ne sont pas disponibles.

Les informations de service de nom doivent être conservées synchronisées sur toutes les sources.

### Configurer la table du commutateur de service de noms

Vous devez configurer correctement la table de commutateur de service de nom pour permettre à ONTAP de consulter les services de noms locaux ou externes pour récupérer les informations relatives à l'hôte, à l'utilisateur, au groupe, au groupe réseau ou au mappage de noms.

### Ce dont vous avez besoin

Vous devez avoir déterminé les services de noms que vous souhaitez utiliser pour le mappage de l'hôte, de l'utilisateur, du groupe, du groupe réseau ou du nom, selon votre environnement.

Si vous prévoyez d'utiliser des netgroups, toutes les adresses IPv6 spécifiées dans netgroups doivent être raccourcies et compressées comme spécifié dans RFC 5952.

### Description de la tâche

N'incluez pas de sources d'information qui ne sont pas utilisées. Par exemple, si NIS n'est pas utilisé dans votre environnement, ne spécifiez pas `-sources nis` option.

### Étapes

1. Ajoutez les entrées nécessaires à la table de changement de nom du service :

```
vserver services name-service ns-switch create -vserver vserver_name -database database_name -sources source_names
```

2. Vérifiez que le tableau des commutateurs de service de noms contient les entrées attendues dans l'ordre souhaité :

```
vserver services name-service ns-switch show -vserver vserver_name
```

Si vous souhaitez apporter des corrections, vous devez utiliser le `vserver services name-service ns-switch modify` ou `vserver services name-service ns-switch delete` commandes.

### Exemple

L'exemple suivant crée une nouvelle entrée dans la table name service switch pour que le SVM vs1 puisse utiliser le fichier netgroup local et un serveur NIS externe pour rechercher les informations netgroup dans cet ordre :

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

### Une fois que vous avez terminé

- Vous devez configurer les services de noms que vous avez spécifiés pour la SVM afin de fournir un accès aux données.
- Si vous supprimez un service de noms pour la SVM, vous devez le supprimer de la table name service switch également.

L'accès client au système de stockage risque de ne pas fonctionner comme prévu si vous ne supprimez pas le service de noms de la table du commutateur de service de noms.

### Configuration des utilisateurs et des groupes UNIX locaux

#### Configurer les utilisateurs et groupes UNIX locaux

Vous pouvez utiliser les utilisateurs et groupes UNIX locaux sur le SVM pour l'authentification et les mappages de noms. Vous pouvez créer des utilisateurs et des groupes UNIX manuellement ou charger un fichier contenant des utilisateurs ou des groupes UNIX à partir d'un URI (Uniform Resource identifier).

Il existe une limite maximale par défaut de 32,768 groupes d'utilisateurs UNIX locaux et membres de groupes regroupés dans le cluster. L'administrateur du cluster peut modifier cette limite.

## Créez un utilisateur UNIX local

Vous pouvez utiliser le `vserver services name-service unix-user create` Commande permettant de créer des utilisateurs UNIX locaux. Un utilisateur UNIX local est un utilisateur UNIX que vous créez sur le SVM en tant qu'option de services de noms UNIX à utiliser lors du traitement des mappages de noms.

### Étape

1. Créer un utilisateur UNIX local :

```
vserver services name-service unix-user create -vserver vserver_name -user
user_name -id integer -primary-gid integer -full-name full_name
```

`-user user_name` spécifie le nom d'utilisateur. La longueur du nom d'utilisateur doit être inférieure ou égale à 64 caractères.

`-id integer` Spécifie l'ID utilisateur que vous attribuez.

`-primary-gid integer` Spécifie l'ID du groupe principal. L'utilisateur est ainsi ajouté au groupe principal. Après avoir créé l'utilisateur, vous pouvez l'ajouter manuellement à tout groupe supplémentaire souhaité.

### Exemple

La commande suivante crée un utilisateur UNIX local nommé johnm (nom complet « John Miller ») sur la SVM nommée vs1. L'utilisateur possède l'ID 123 et le groupe principal ID 100.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

## Chargement des utilisateurs UNIX locaux à partir d'un URI

Comme alternative à la création manuelle d'utilisateurs UNIX locaux dans des SVM, vous pouvez simplifier la tâche en chargeant une liste d'utilisateurs UNIX locaux dans des SVM depuis un identificateur de ressource uniforme (URI) (`vserver services name-service unix-user load-from-uri`).

### Étapes

1. Créez un fichier contenant la liste des utilisateurs UNIX locaux que vous souhaitez charger.

Le fichier doit contenir des informations utilisateur sous UNIX `/etc/passwd` format :

```
user_name: password: user_ID: group_ID: full_name
```

La commande supprime la valeur de l' `password` et les valeurs des champs après le `full_name` légale



(*home\_directory* et *shell*).

La taille maximale de fichier prise en charge est de 2.5 Mo.

2. Vérifiez que la liste ne contient aucune information dupliquée.

Si la liste contient des entrées dupliquées, le chargement de la liste échoue et un message d'erreur s'affiche.

3. Copiez le fichier sur un serveur.

Le serveur doit être accessible par le système de stockage via HTTP, HTTPS, FTP ou FTPS.

4. Déterminez l'URI du fichier.

L'URI est l'adresse que vous fournissez au système de stockage pour indiquer l'emplacement du fichier.

5. Charger le fichier contenant la liste des utilisateurs UNIX locaux dans les SVM à partir de l'URI :

```
vserver services name-service unix-user load-from-uri -vserver vserver_name
-uri {ftp|http|https|https}://uri -overwrite {true|false}
```

`-overwrite {true false}` spécifie s'il faut remplacer les entrées. La valeur par défaut est `false`.

### Exemple

La commande suivante charge la liste des utilisateurs UNIX locaux à partir de l'URI

`ftp://ftp.example.com/passwd` Au SVM nommé `vs1`. Les utilisateurs existants du SVM ne sont pas remplacés par des informations de l'URI.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

### Créer un groupe UNIX local

Vous pouvez utiliser le `vserver services name-service unix-group create` Commande pour créer des groupes UNIX locaux à la SVM. Les groupes UNIX locaux sont utilisés avec des utilisateurs UNIX locaux.

#### Étape

1. Créer un groupe UNIX local :

```
vserver services name-service unix-group create -vserver vserver_name -name
group_name -id integer
```

`-name group_name` spécifie le nom du groupe. Le nom du groupe doit comporter 64 caractères ou moins.

`-id integer` Spécifie l'ID de groupe que vous attribuez.

### Exemple

La commande suivante crée un groupe local nommé eng sur le SVM nommé vs1. Le groupe a l'ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name eng -id 101
```

### Ajouter un utilisateur à un groupe UNIX local

Vous pouvez utiliser le `vserver services name-service unix-group adduser` Commande pour ajouter un utilisateur à un groupe UNIX complémentaire qui est local au SVM.

#### Étape

1. Ajouter un utilisateur à un groupe UNIX local :

```
vserver services name-service unix-group adduser -vserver vserver_name -name group_name -username user_name
```

`-name group_name` Spécifie le nom du groupe UNIX auquel ajouter l'utilisateur en plus du groupe principal de l'utilisateur.

#### Exemple

La commande suivante ajoute un utilisateur nommé max à un groupe UNIX local nommé eng sur le SVM nommé vs1 :

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name eng -username max
```

### Chargement des groupes UNIX locaux à partir d'un URI

Comme alternative à la création manuelle de groupes UNIX locaux, vous pouvez charger une liste de groupes UNIX locaux dans des SVM à partir d'un URI (Uniform Resource identifier) en utilisant le `vserver services name-service unix-group load-from-uri` commande.

#### Étapes

1. Créez un fichier contenant la liste des groupes UNIX locaux que vous souhaitez charger.

Le fichier doit contenir des informations de groupe dans UNIX `/etc/group` format :

```
group_name: password: group_ID: comma_separated_list_of_users
```

La commande supprime la valeur de l' `password` légale.

La taille de fichier maximale prise en charge est de 1 Mo.

La longueur maximale de chaque ligne du fichier de groupe est de 32,768 caractères.

2. Vérifiez que la liste ne contient aucune information dupliquée.

La liste ne doit pas contenir d'entrées dupliquées, sinon le chargement de la liste échoue. Si des entrées sont déjà présentes dans le SVM, il faut soit définir le `-overwrite` paramètre à `true` pour remplacer toutes les entrées existantes par le nouveau fichier ou s'assurer que le nouveau fichier ne contient pas d'entrées qui dupliquent des entrées existantes.

3. Copiez le fichier sur un serveur.

Le serveur doit être accessible par le système de stockage via HTTP, HTTPS, FTP ou FTPS.

4. Déterminez l'URI du fichier.

L'URI est l'adresse que vous fournissez au système de stockage pour indiquer l'emplacement du fichier.

5. Charger le fichier contenant la liste des groupes UNIX locaux dans le SVM depuis l'URI :

```
vserver services name-service unix-group load-from-uri -vserver vserver_name
-uri {ftp|http|https|https}://uri -overwrite {true|false}
```

`-overwrite true false` spécifie s'il faut remplacer les entrées. La valeur par défaut est `false`. Si vous spécifiez ce paramètre comme `true`, ONTAP remplace la totalité de la base de données du groupe UNIX local existant du SVM spécifié par les entrées du fichier que vous chargez.

### Exemple

La commande suivante charge la liste des groupes UNIX locaux à partir de l'URI

`ftp://ftp.example.com/group` Au SVM nommé `vs1`. Les groupes existants sur le SVM ne sont pas remplacés par les informations de l'URI.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

## Travailler avec des groupes réseau

### Utilisation de la vue d'ensemble des groupes réseau

Vous pouvez utiliser `netgroups` pour l'authentification des utilisateurs et pour correspondre des clients dans les règles d'export policy. Vous pouvez fournir l'accès aux `netgroups` à partir de serveurs de noms externes (LDAP ou NIS), ou vous pouvez charger des `netgroups` à partir d'un identifiant de ressource uniforme (URI) dans des SVM à l'aide de `vserver services name-service netgroup load` commande.

### Ce dont vous avez besoin

Avant de travailler avec des groupes réseau, vous devez vous assurer que les conditions suivantes sont remplies :

- Tous les hôtes dans des groupes réseau, indépendamment de la source (fichiers NIS, LDAP ou locaux), doivent avoir des enregistrements DNS avant (A) et arrière (PTR) pour fournir des recherches DNS avant et arrière cohérentes.

En outre, si une adresse IP d'un client possède plusieurs enregistrements PTR, tous ces noms d'hôte

doivent être membres du groupe réseau et avoir les enregistrements correspondants.

- Les noms de tous les hôtes dans des groupes réseau, indépendamment de leur source (fichiers NIS, LDAP ou locaux), doivent être correctement orthographiés et utiliser le cas correct. Les incohérences de cas dans les noms d'hôte utilisés dans les netgroups peuvent entraîner un comportement inattendu, tel que l'échec des vérifications d'exportation.
- Toutes les adresses IPv6 spécifiées dans netgroups doivent être raccourcies et compressées comme indiqué dans RFC 5952.

Par exemple, 2011:hu9:0:0:0:0:0:3:1 doit être réduit à 2011:hu9::3:1.

## Description de la tâche

Lorsque vous travaillez avec des groupes réseau, vous pouvez effectuer les opérations suivantes :

- Vous pouvez utiliser le `vserver export-policy netgroup check-membership` Commande permettant de déterminer si une adresse IP client est membre d'un certain groupe réseau.
- Vous pouvez utiliser le `vserver services name-service getxxbyyy netgrp` commande pour vérifier si un client fait partie d'un groupe réseau.

Le service sous-jacent pour effectuer la recherche est sélectionné en fonction de l'ordre de commutation de service de nom configuré.

## Chargement des netgroups en SVM

L'une des méthodes que vous pouvez utiliser pour faire correspondre les clients dans les règles d'export policy consiste à utiliser les hôtes répertoriés dans netgroups. Vous pouvez charger des netgroups à partir d'un URI (Uniform Resource identifier) dans des SVM, au lieu d'utiliser des netgroups stockés dans des serveurs de noms externes (`vserver services name-service netgroup load`).

## Ce dont vous avez besoin

Les fichiers netgroup doivent respecter les conditions suivantes avant d'être chargés dans un SVM :

- Le fichier doit utiliser le même format de fichier texte de groupe réseau que celui utilisé pour remplir NIS.

ONTAP vérifie le format du fichier texte du groupe réseau avant de le charger. Si le fichier contient des erreurs, il ne sera pas chargé et un message s'affiche indiquant les corrections que vous devez effectuer dans le fichier. Après avoir corrigé les erreurs, vous pouvez recharger le fichier netgroup dans la SVM spécifiée.

- Les caractères alphabétiques des noms d'hôte dans le fichier de groupe réseau doivent être en minuscules.
- La taille de fichier maximale prise en charge est de 5 Mo.
- Le niveau maximal pris en charge pour l'imbrication de groupes réseau est 1000.
- Seuls les noms d'hôte DNS principaux peuvent être utilisés lors de la définition de noms d'hôte dans le fichier netgroup.

Pour éviter les problèmes d'accès à l'exportation, les noms d'hôte ne doivent pas être définis à l'aide d'enregistrements DNS CNAME ou Round Robin.

- Les parties utilisateur et domaine des triples du fichier netgroup doivent être conservées vides car ONTAP ne les prend pas en charge.

Seule la partie hôte/IP est prise en charge.

### Description de la tâche

ONTAP prend en charge les recherches netgroup-by-host pour le fichier netgroup local. Une fois le fichier netgroup chargé, ONTAP crée automatiquement un mappage netgroup.byhost pour activer les recherches netgroup-par-hôte. Cela peut accélérer considérablement les recherches des groupes réseau locaux lors du traitement des règles d'export pour évaluer l'accès client.

### Étape

1. Chargement des netgroups dans des SVM depuis un URI :

```
vserver services name-service netgroup load -vserver vserver_name -source {ftp|http|https|https}://uri
```

Le chargement du fichier netgroup et la création du mappage netgroup.byhost peuvent prendre plusieurs minutes.

Si vous souhaitez mettre à jour les netgroups, vous pouvez modifier le fichier et charger le fichier netgroup mis à jour dans la SVM.

### Exemple

La commande suivante charge les définitions netgroup dans le SVM nommé vs1 à partir de l'URL HTTP `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

### Vérifiez l'état des définitions de groupe réseau

Après avoir chargé des netgroups dans la SVM, vous pouvez utiliser `vserver services name-service netgroup status` commande pour vérifier le statut des définitions de groupe réseau. Vous pouvez ainsi déterminer si les définitions de groupe réseau sont cohérentes sur tous les nœuds qui suivent la SVM.

### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Vérifiez l'état des définitions de groupe réseau :

```
vserver services name-service netgroup status
```

Vous pouvez afficher des informations supplémentaires dans une vue plus détaillée.

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

### Exemple

Une fois le niveau de privilège défini, la commande suivante affiche le statut netgroup pour tous les SVM :

```
vs1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them only
when
```

```
directed to do so by technical support.
```

```
Do you wish to continue? (y or n): y
```

```
vs1::*> vserver services name-service netgroup status
```

```
Virtual
```

```
Server Node Load Time Hash Value
```

```


```

```
vs1
```

```
node1 9/20/2006 16:04:53
```

```
e6cb38ec1396a280c0d2b77e3a84eda2
```

```
node2 9/20/2006 16:06:26
```

```
e6cb38ec1396a280c0d2b77e3a84eda2
```

```
node3 9/20/2006 16:08:08
```

```
e6cb38ec1396a280c0d2b77e3a84eda2
```

```
node4 9/20/2006 16:11:33
```

```
e6cb38ec1396a280c0d2b77e3a84eda2
```

### Créez une configuration de domaine NIS

Si un NIS (Network Information Service) est utilisé dans votre environnement pour les services de noms, vous devez créer une configuration de domaine NIS pour la SVM en utilisant la commande `vserver services name-service nis-domain create`.

### Ce dont vous avez besoin

Tous les serveurs NIS configurés doivent être disponibles et accessibles avant de configurer le domaine NIS sur le SVM.

Si vous prévoyez d'utiliser NIS pour les recherches de répertoires, les cartes de vos serveurs NIS ne peuvent pas comporter plus de 1,024 caractères pour chaque entrée. Ne spécifiez pas le serveur NIS qui ne respecte pas cette limite. Sinon, l'accès client dépendant des entrées NIS risque d'échouer.

### Description de la tâche

Vous pouvez créer plusieurs domaines NIS. Cependant, vous ne pouvez utiliser qu'un seul qui est défini sur `active`.

Si votre base de données NIS contient un `netgroup.byhost` Map, ONTAP peut l'utiliser pour des recherches plus rapides. Le `netgroup.byhost` et `netgroup` les cartes du répertoire doivent être synchronisées en

permanence pour éviter tout problème d'accès client. ONTAP 9.7, NIS `netgroup.byhost` les entrées peuvent être mises en cache à l'aide du `vserver services name-service nis-domain netgroup-database` commandes.

L'utilisation de NIS pour la résolution de nom d'hôte n'est pas prise en charge.

### Étapes

1. Créez une configuration de domaine NIS :

```
vserver services name-service nis-domain create -vserver vs1 -domain
domain_name -active true -servers IP_addresses
```

Vous pouvez spécifier jusqu'à 10 serveurs NIS.



À partir de ONTAP 9.2, le champ `-nis-servers` remplace le champ `-servers`. Ce nouveau champ peut prendre un nom d'hôte ou une adresse IP pour le serveur NIS.

2. Vérifiez que le domaine est créé :

```
vserver services name-service nis-domain show
```

### Exemple

La commande suivante crée et active une configuration de domaine NIS pour un domaine NIS appelé `nisdomain` sur le SVM nommé `vs1` avec un serveur NIS à l'adresse IP `192.0.2.180` :

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -active true -nis-servers 192.0.2.180
```

## Utiliser LDAP

### Présentation de l'utilisation de LDAP

Si LDAP est utilisé dans votre environnement pour des services de noms, vous devez travailler avec votre administrateur LDAP pour déterminer les exigences et les configurations de système de stockage appropriées, puis activer la SVM en tant que client LDAP.

Depuis ONTAP 9.10.1, la liaison de canal LDAP est prise en charge par défaut pour les connexions LDAP Active Directory et services de noms. ONTAP essaiera la liaison des canaux avec les connexions LDAP uniquement si Start-TLS ou LDAPS est activé avec la sécurité de session définie sur Sign ou SEAL. Pour désactiver ou réactiver la liaison de canal LDAP avec les serveurs de noms, utilisez le `-try-channel-binding` paramètre avec le `ldap client modify` commande.

Pour plus d'informations, voir

["2020 exigences de liaison des canaux LDAP et de signature LDAP pour Windows"](#).

- Avant de configurer LDAP pour ONTAP, vérifiez que votre déploiement de site respecte les bonnes pratiques en matière de configuration de serveur LDAP et de client. En particulier, les conditions suivantes doivent être remplies :

- Le nom de domaine du serveur LDAP doit correspondre à l'entrée du client LDAP.
- Les types de hachage de mot de passe utilisateur LDAP pris en charge par le serveur LDAP doivent inclure ceux pris en charge par ONTAP :
  - CRYPT (tous types) et SHA-1 (SHA, SSHA).
  - Depuis ONTAP 9.8, des hachages SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 et SSHA-512) sont également pris en charge.
- Si le serveur LDAP nécessite des mesures de sécurité de session, vous devez les configurer dans le client LDAP.

Les options de sécurité de session suivantes sont disponibles :

- La signature LDAP (fournit un contrôle de l'intégrité des données), la signature et le chiffrement LDAP (assure le contrôle de l'intégrité des données et le chiffrement)
- DÉMARRER TLS
- LDAPS (LDAP sur TLS ou SSL)
- Pour activer les requêtes LDAP signées et scellées, les services suivants doivent être configurés :
  - Les serveurs LDAP doivent prendre en charge le mécanisme GSSAPI (Kerberos) SASL.
  - Les serveurs LDAP doivent avoir des enregistrements DNS A/AAAA ainsi que des enregistrements PTR configurés sur le serveur DNS.
  - Les serveurs Kerberos doivent contenir des enregistrements SRV sur le serveur DNS.
- Pour activer START TLS ou LDAPS, les points suivants doivent être pris en compte.
  - Il s'agit d'une meilleure pratique NetApp d'utiliser Start TLS plutôt que LDAPS.
  - Si LDAPS est utilisé, le serveur LDAP doit être activé pour TLS ou pour SSL dans ONTAP 9.5 et versions ultérieures. SSL n'est pas pris en charge dans ONTAP 9.0-9.4.
  - Un serveur de certificats doit déjà être configuré dans le domaine.
- Pour activer la recherche de recommandation LDAP (dans ONTAP 9.5 et versions ultérieures), les conditions suivantes doivent être remplies :
  - Les deux domaines doivent être configurés avec l'une des relations d'approbation suivantes :
    - Bidirectionnel
    - Aller simple, où le principal fait confiance au domaine de référence
    - Parent-enfant
  - Le DNS doit être configuré pour résoudre tous les noms de serveur mentionnés.
  - Les mots de passe du domaine doivent être identiques pour s'authentifier lorsque --bind-as-cifs -Server est défini sur true.



Les configurations suivantes ne sont pas prises en charge avec la recherche de références LDAP.



- Pour toutes les versions de ONTAP :
  - Clients LDAP sur un SVM d'admin
- Pour ONTAP 9.8 et versions antérieures (ils sont pris en charge dans la version 9.9.1 et ultérieures) :
  - Signature et chiffrement LDAP (le `-session-security` en option)
  - Connexions TLS cryptées ( `-use-start-tls` en option)
  - Communications via le port LDAPS 636 (le `-use-ldaps-for-ad-ldap` en option)

- Vous devez entrer un schéma LDAP lors de la configuration du client LDAP sur le SVM.

Dans la plupart des cas, l'un des schémas ONTAP par défaut sera approprié. Toutefois, si le schéma LDAP de votre environnement diffère de celui-ci, vous devez créer un nouveau schéma client LDAP pour ONTAP avant de créer le client LDAP. Consultez votre administrateur LDAP pour connaître les conditions requises pour votre environnement.

- L'utilisation de LDAP pour la résolution du nom d'hôte n'est pas prise en charge.

### Pour en savoir plus

- ["Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP"](#)
- ["Installer le certificat d'autorité de certification racine auto-signé sur le SVM"](#)

### Créez un nouveau schéma client LDAP

Si le schéma LDAP de votre environnement diffère des valeurs par défaut de ONTAP, vous devez créer un nouveau schéma client LDAP pour ONTAP avant de créer la configuration du client LDAP.

#### Description de la tâche

La plupart des serveurs LDAP peuvent utiliser les schémas par défaut fournis par ONTAP :

- MS-AD-BIS (schéma préféré pour la plupart des serveurs AD Windows 2012 et versions ultérieures)
- AD-IDMU (serveurs AD Windows 2008, Windows 2012 et versions ultérieures)
- AD-SFU (serveurs AD Windows 2003 et versions antérieures)
- RFC-2307 (SERVEURS LDAP UNIX)

Si vous devez utiliser un schéma LDAP autre que celui par défaut, vous devez le créer avant de créer la configuration du client LDAP. Consultez votre administrateur LDAP avant de créer un nouveau schéma.

Les schémas LDAP par défaut fournis par ONTAP ne peuvent pas être modifiés. Pour créer un nouveau schéma, vous créez une copie, puis modifiez la copie en conséquence.

### Étapes

1. Affichez les modèles de schéma client LDAP existants pour identifier celui que vous souhaitez copier :

```
vserver services name-service ldap client schema show
```

2. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

3. Faites une copie d'un schéma client LDAP existant :

```
vserver services name-service ldap client schema copy -vserver vserver_name
-schema existing_schema_name -new-schema-name new_schema_name
```

4. Modifiez le nouveau schéma et personnalisez-le pour votre environnement :

```
vserver services name-service ldap client schema modify
```

5. Retour au niveau de privilège admin :

```
set -privilege admin
```

## Créez une configuration client LDAP

Si vous souhaitez que ONTAP accède aux services LDAP ou Active Directory externes de votre environnement, vous devez d'abord configurer un client LDAP sur le système de stockage.

### Ce dont vous avez besoin

L'un des trois premiers serveurs de la liste des domaines résolus d'Active Directory doit être actif et transmettre des données. Dans le cas contraire, cette tâche échoue.



Il existe plusieurs serveurs, dont plus de deux serveurs sont en panne à tout moment.

### Étapes

1. Consultez votre administrateur LDAP pour déterminer les valeurs de configuration appropriées pour le `vserver services name-service ldap client create` commande :

- a. Spécifiez une connexion basée sur un domaine ou une adresse aux serveurs LDAP.

Le `-ad-domain` et `-servers` les options s'excluent mutuellement.

- Utilisez le `-ad-domain` Option permettant d'activer la découverte de serveur LDAP dans le domaine Active Directory.
  - Vous pouvez utiliser le `-restrict-discovery-to-site` Option permettant de restreindre la découverte du serveur LDAP au site CIFS par défaut du domaine spécifié. Si vous utilisez cette option, vous devez également spécifier le site CIFS par défaut avec `-default-site`.
- Vous pouvez utiliser le `-preferred-ad-servers` Option permettant de spécifier un ou plusieurs serveurs Active Directory préférés par adresse IP dans une liste délimitée par des virgules. Une fois le client créé, vous pouvez modifier cette liste en utilisant le `vserver services name-service ldap client modify` commande.
- Utilisez le `-servers` Option permettant de spécifier un ou plusieurs serveurs LDAP (Active Directory ou UNIX) par adresse IP dans une liste délimitée par des virgules.



Le `-servers` Cette option est obsolète dans ONTAP 9.2. À partir de ONTAP 9.2, le `-ldap-servers` remplace le `-servers` légale. Ce champ peut prendre un nom d'hôte ou une adresse IP pour le serveur LDAP.

b. Spécifiez un schéma LDAP par défaut ou personnalisé.

La plupart des serveurs LDAP peuvent utiliser les schémas en lecture seule par défaut fournis par ONTAP. Il est préférable d'utiliser ces schémas par défaut à moins qu'il n'y ait une obligation de le faire autrement. Si c'est le cas, vous pouvez créer votre propre schéma en copiant un schéma par défaut (en lecture seule), puis en modifiant la copie.

Schémas par défaut :

- MS-AD-BIS

Basé sur RFC-2307bis, il s'agit du schéma LDAP préféré pour la plupart des déploiements LDAP standard de Windows 2012 et versions ultérieures.

- AD-IDMU

Basé sur Active Directory Identity Management pour UNIX, ce schéma est adapté à la plupart des serveurs AD Windows 2008, Windows 2012 et versions ultérieures.

- AD-SFU

Basé sur Active Directory Services pour UNIX, ce schéma est approprié pour la plupart des serveurs AD Windows 2003 et versions antérieures.

- RFC-2307

Basé sur RFC-2307 (*une approche pour l'utilisation de LDAP en tant que service d'informations réseau*), ce schéma est approprié pour la plupart des serveurs AD UNIX.

c. Sélectionnez les valeurs de liaison.

- `-min-bind-level {anonymous|simple|sasl}` spécifie le niveau d'authentification de liaison minimum.

La valeur par défaut est **anonymous**.

- `-bind-dn LDAP_DN` spécifie l'utilisateur de liaison.

Pour les serveurs Active Directory, vous devez spécifier l'utilisateur dans le formulaire compte (DOMAINE\utilisateur) ou principal ([user@domain.com](#)). Sinon, vous devez spécifier l'utilisateur sous le format nom distinctif (CN=user,DC=domain,DC=com).

- `-bind-password password` spécifie le mot de passe de liaison.

d. Sélectionnez les options de sécurité de session, si nécessaire.

Vous pouvez activer soit la signature et le chiffrement LDAP, soit LDAP sur TLS si le serveur LDAP en a besoin.

- `--session-security {none|sign|seal}`

Vous pouvez activer la signature (`sign`, intégrité des données), signature et scellage (`seal`, intégrité et chiffrement des données), ou ni l'un ni l'autre `none`, pas de signature ou d'étanchéité). La valeur par défaut est `none`.

Vous devez également définir `-min-bind-level {sasl}` à moins que vous ne souhaitiez que l'authentification de la liaison revienne à **anonymous** ou **simple** en cas d'échec de la signature et de la liaison d'étanchéité.

- `-use-start-tls {true|false}`

S'il est réglé sur **true** Et le serveur LDAP le prend en charge, le client LDAP utilise une connexion TLS chiffrée vers le serveur. La valeur par défaut est **false**. Vous devez installer un certificat d'autorité de certification racine auto-signé du serveur LDAP pour utiliser cette option.



Si un serveur SMB est ajouté à un domaine de la machine virtuelle de stockage et que le serveur LDAP fait partie des contrôleurs de domaine du domaine principal du serveur SMB, vous pouvez modifier la `-session-security-for-ad-ldap` à l'aide de `vserver cifs security modify` commande.

e. Sélectionnez les valeurs de port, de requête et de base.

Les valeurs par défaut sont recommandées, mais vous devez vérifier auprès de votre administrateur LDAP qu'elles sont adaptées à votre environnement.

- `-port port` Spécifie le port du serveur LDAP.

La valeur par défaut est 389.

Si vous prévoyez d'utiliser Démarrer TLS pour sécuriser la connexion LDAP, vous devez utiliser le port par défaut 389. Start TLS commence comme une connexion en texte clair sur le port par défaut LDAP 389, et cette connexion est ensuite mise à niveau vers TLS. Si vous modifiez le port, le démarrage TLS échoue.

- `-query-timeout integer` spécifie le délai d'expiration de la requête en secondes.

La plage autorisée est de 1 à 10 secondes. La valeur par défaut est 3 secondes.

- `-base-dn LDAP_DN` Spécifie le DN de base.

Plusieurs valeurs peuvent être saisies si nécessaire (par exemple, si la recherche de références LDAP est activée). La valeur par défaut est "" (racine).

- `-base-scope {base|onelevel|subtree}` spécifie l'étendue de la recherche de base.

La valeur par défaut est `subtree`.

- `-referral-enabled {true|false}` Indique si la recherche de recommandation LDAP est activée.

Depuis ONTAP 9.5, ceci permet au client LDAP de ONTAP de renvoyer des demandes de recherche à d'autres serveurs LDAP si une réponse de recommandation LDAP est renvoyée par le serveur LDAP principal indiquant que les enregistrements souhaités sont présents sur les serveurs LDAP mentionnés. La valeur par défaut est **false**.

Pour rechercher des enregistrements présents dans les serveurs LDAP désignés, la base-dn des enregistrements recommandés doit être ajoutée à la base-dn dans le cadre de la configuration du client LDAP.

## 2. Créer une configuration client LDAP sur la VM de stockage :

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```



Vous devez fournir le nom de la VM de stockage lors de la création d'une configuration client LDAP.

## 3. Vérifiez que la configuration du client LDAP a bien été créée :

```
vserver services name-service ldap client show -client-config
client_config_name
```

### Exemples

La commande suivante crée une nouvelle configuration de client LDAP nommée ldap1 pour que la VM de stockage vs1 fonctionne avec un serveur Active Directory pour LDAP :

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

La commande suivante crée une nouvelle configuration de client LDAP nommée ldap1 pour que la machine virtuelle de stockage vs1 fonctionne avec un serveur Active Directory pour LDAP sur lequel la signature et le chiffrement sont nécessaires, et la découverte du serveur LDAP est limitée à un site particulier pour le domaine spécifié :

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

La commande suivante crée une nouvelle configuration de client LDAP nommée ldap1 pour que la VM de stockage vs1 fonctionne avec un serveur Active Directory pour LDAP où la recherche de référence LDAP est requise :

```
cluster1::> vservers services name-service ldap client create -vservers vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

La commande suivante modifie la configuration du client LDAP nommée `ldap1` pour la VM de stockage `vs1` en spécifiant le DN de base :

```
cluster1::> vservers services name-service ldap client modify -vservers vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

La commande suivante modifie la configuration du client LDAP appelée `ldap1` pour la VM de stockage `vs1` en activant la recherche de référence :

```
cluster1::> vservers services name-service ldap client modify -vservers vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com" -referral-enabled true
```

## Associer la configuration client LDAP aux SVM

Pour activer LDAP sur un SVM, vous devez utiliser `vservers services name-service ldap create` Commande permettant d'associer une configuration client LDAP à la SVM.

### Ce dont vous avez besoin

- Un domaine LDAP doit déjà exister au sein du réseau et doit être accessible au cluster sur lequel le SVM est situé.
- Une configuration client LDAP doit exister sur le SVM.

### Étapes

1. Activer LDAP sur le SVM :

```
vservers services name-service ldap create -vservers vservers_name -client-config
client_config_name
```



À partir de ONTAP 9.2, le `vservers services name-service ldap create` Commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP n'est pas en mesure de contacter le serveur de noms.

La commande suivante permet à LDAP sur le SVM « `vs1` » et le configure pour utiliser la configuration du client LDAP « `ldap1` » :

```
cluster1::> vserver services name-service ldap create -vserver vs1
-client-config ldap1 -client-enabled true
```

2. Valider le statut des serveurs name en utilisant la commande `vserver services name-service ldap check`.

La commande suivante valide les serveurs LDAP sur le SVM vs1.

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
| "10.11.12.13". |
```

La commande `name service check` est disponible à partir de ONTAP 9.2.

### Vérifiez les sources LDAP dans la table du commutateur de service de noms

On doit vérifier que les sources LDAP pour les services de noms sont correctement répertoriées dans la table de commutation de services de noms pour la SVM.

#### Étapes

1. Afficher le contenu de la table du commutateur de service du nom actuel :

```
vserver services name-service ns-switch show -vserver svm_name
```

La commande suivante affiche les résultats du SVM My\_SVM :

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
```

| Vserver | Database | Source        |
|---------|----------|---------------|
| -----   | -----    | -----         |
| My_SVM  | hosts    | files,<br>dns |
| My_SVM  | group    | files,ldap    |
| My_SVM  | passwd   | files,ldap    |
| My_SVM  | netgroup | files         |
| My_SVM  | namemap  | files         |

5 entries were displayed.

`namemap` spécifie les sources pour rechercher des informations de mappage de noms et dans quel ordre. Dans un environnement UNIX uniquement, cette entrée n'est pas nécessaire. Le mappage de noms n'est requis que dans un environnement mixte utilisant à la fois UNIX et Windows.

2. Mettez à jour le `ns-switch` saisie au besoin :

| Si vous souhaitez mettre à jour l'entrée du commutateur ns pour... | Entrez la commande...                                                                                                    |
|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Informations utilisateur                                           | <code>vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files</code>   |
| Informations de groupe                                             | <code>vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files</code>    |
| Informations sur le groupe réseau                                  | <code>vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files</code> |

## Utilisez Kerberos avec NFS pour une sécurité renforcée

### Présentation de l'utilisation de Kerberos avec NFS pour une sécurité renforcée

Si Kerberos est utilisé dans votre environnement pour une authentification renforcée, vous devez travailler avec votre administrateur Kerberos pour déterminer les exigences et les configurations de système de stockage appropriées, puis activer la SVM en tant que client Kerberos.

Votre environnement doit respecter les consignes suivantes :

- Votre déploiement de site doit respecter les bonnes pratiques en matière de configuration du serveur Kerberos et du client avant de configurer Kerberos pour ONTAP.
- Si possible, utilisez NFSv4 ou une version ultérieure si l'authentification Kerberos est requise.

NFSv3 peut être utilisé avec Kerberos. Toutefois, les avantages de la sécurité totale de Kerberos ne sont réalisés que dans les déploiements ONTAP de NFSv4 ou versions ultérieures.

- Pour promouvoir un accès serveur redondant, Kerberos doit être activé sur plusieurs LIFs de données sur plusieurs nœuds du cluster à l'aide du même SPN.
- Lorsque Kerberos est activé sur le SVM, l'une des méthodes de sécurité suivantes doit être spécifiée dans des règles d'exportation pour les volumes ou les qtrees, en fonction de votre configuration client NFS.
  - `krb5` (Protocole Kerberos v5)
  - `krb5i` (Protocole Kerberos v5 avec contrôle d'intégrité à l'aide de checksums)
  - `krb5p` (Protocole Kerberos v5 avec service de confidentialité)

En plus du serveur Kerberos et des clients, les services externes suivants doivent être configurés pour ONTAP afin de prendre en charge Kerberos :

- Service d'annuaire



Vous devez utiliser un service d'annuaire sécurisé dans votre environnement, tel qu'Active Directory ou OpenLDAP, configuré pour utiliser LDAP sur SSL/TLS. N'utilisez pas NIS, dont les demandes sont envoyées en clair et ne sont donc pas sécurisées.

- NTP

Vous devez disposer d'un serveur de temps de travail exécutant NTP. Cette opération est nécessaire pour éviter l'échec de l'authentification Kerberos en raison de l'inclinaison du temps.

- Résolution des noms de domaine (DNS)

Chaque client UNIX et chaque LIF de SVM doivent avoir un enregistrement de service (SRV) correct enregistré auprès du KDC dans des zones de recherche avant et arrière. Tous les participants doivent être résolus correctement via DNS.

### Vérifiez les autorisations pour la configuration Kerberos

Kerberos requiert que certaines autorisations UNIX soient définies pour le volume root du SVM et pour les utilisateurs et groupes locaux.

#### Étapes

1. Afficher les autorisations appropriées sur le volume root du SVM :

```
volume show -volume root_vol_name-fields user,group,unix-permissions
```

Le volume root du SVM doit avoir la configuration suivante :

| Nom...             | Paramètre...   |
|--------------------|----------------|
| UID                | Racine ou ID 0 |
| GIDS               | Racine ou ID 0 |
| Autorisations UNIX | 755            |

Si ces valeurs ne sont pas affichées, utiliser le `volume modify` pour les mettre à jour.

2. Afficher les utilisateurs UNIX locaux :

```
vserver services name-service unix-user show -vserver vserver_name
```

Le SVM doit avoir les utilisateurs UNIX suivants configurés :

| Nom d'utilisateur | ID d'utilisateur | ID de groupe principal | Commentaire                                                                                                                                                                                                                                            |
|-------------------|------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| nfs               | 500              | 0                      | Requis pour la phase INIT GSS.<br><br>Le premier composant de l'utilisateur client NFS SPN est utilisé comme utilisateur.<br><br>L'utilisateur nfs n'est pas requis si un mappage de nom Kerberos-UNIX existe pour le SPN de l'utilisateur client NFS. |
| racine            | 0                | 0                      | Nécessaire pour le montage.                                                                                                                                                                                                                            |

Si ces valeurs ne sont pas affichées, vous pouvez utiliser le `vserver services name-service unix-user modify` pour les mettre à jour.

### 3. Afficher les groupes UNIX locaux :

```
vserver services name-service unix-group show -vserver vserver _name
```

La SVM doit avoir les groupes UNIX suivants configurés :

| Nom du groupe | ID de groupe |
|---------------|--------------|
| démon         | 1            |
| racine        | 0            |

Si ces valeurs ne sont pas affichées, vous pouvez utiliser le `vserver services name-service unix-group modify` pour les mettre à jour.

### Créez une configuration de domaine NFS Kerberos

Si vous souhaitez que le ONTAP accède à des serveurs Kerberos externes dans votre environnement, vous devez d'abord configurer le SVM de manière à utiliser un Royaume Kerberos existant. Pour ce faire, vous devez rassembler les valeurs de configuration du serveur KDC Kerberos, puis utiliser l'`vserver nfs kerberos realm create` Commande pour créer la configuration du domaine Kerberos sur un SVM.

### Ce dont vous avez besoin

L'administrateur du cluster doit avoir configuré le protocole NTP sur le système de stockage, le client et le serveur KDC afin d'éviter les problèmes d'authentification. Les différences de temps entre un client et un serveur (inclinaison de l'horloge) sont une cause courante d'échecs d'authentification.

## Étapes

1. Consultez votre administrateur Kerberos pour déterminer les valeurs de configuration appropriées à fournir avec le `vserver nfs kerberos realm create` commande.
2. Créer une configuration de domaine Kerberos sur le SVM :

```
vserver nfs kerberos realm create -vserver vserver_name -realm realm_name
{AD_KDC_server_values |AD_KDC_server_values} -comment "text"
```

3. Vérifiez que la configuration du domaine Kerberos a bien été créée :

```
vserver nfs kerberos realm show
```

## Exemples

La commande suivante crée une configuration de domaine NFS Kerberos pour le SVM vs1 qui utilise un serveur Microsoft Active Directory comme serveur KDC. Le domaine Kerberos est AUTH.EXAMPLE.COM. Le serveur Active Directory est nommé ad-1 et son adresse IP est 10.10.8.14. L'inclinaison de l'horloge autorisée est de 300 secondes (par défaut). L'adresse IP du serveur KDC est 10.10.8.14 et son numéro de port est 88 (par défaut). « Microsoft Kerberos config » est le commentaire.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

La commande suivante crée une configuration de Royaume NFS Kerberos pour le SVM vs1 qui utilise un MIT KDC. Le domaine Kerberos est SECURITY.EXAMPLE.COM. L'inclinaison de l'horloge autorisée est de 300 secondes. L'adresse IP du serveur KDC est 10.10.9.1 et son numéro de port est 88. Le fournisseur de KDC est autre que d'indiquer un fournisseur UNIX. L'adresse IP du serveur d'administration est 10.10.9.1 et son numéro de port est 749 (par défaut). L'adresse IP du serveur de mots de passe est 10.10.9.1 et son numéro de port est 464 (par défaut). « UNIX Kerberos config » est le commentaire.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

## Configurez les types de chiffrement Kerberos NFS autorisés

Par défaut, ONTAP prend en charge les types de cryptage suivants pour Kerberos NFS : DES, 3DES, AES-128 et AES-256. Vous pouvez configurer les types de cryptage autorisés pour chaque SVM en fonction des exigences de sécurité de votre environnement en utilisant le `vserver nfs modify` commande avec `-permitted` `-enc-types` paramètre.

## Description de la tâche

Pour une compatibilité client optimale, ONTAP prend en charge à la fois le chiffrement DES faible et le chiffrement AES fort par défaut. Cela signifie, par exemple, que si vous voulez augmenter la sécurité et que votre environnement le prend en charge, vous pouvez utiliser cette procédure pour désactiver DES et 3DES et demander aux clients d'utiliser uniquement le cryptage AES.

Vous devez utiliser le chiffrement le plus fort disponible. Pour ONTAP, c'est AES-256. Vous devez confirmer auprès de votre administrateur KDC que ce niveau de cryptage est pris en charge dans votre environnement.

- L'activation ou la désactivation totale d'AES (AES-128 et AES-256) sur les SVM provoque des perturbations, car elle détruit le fichier principal/keytab d'origine, ce qui requiert la désactivation de la configuration Kerberos sur toutes les LIFs du SVM.

Avant d'effectuer ces modifications, vérifiez que les clients NFS ne reposent pas sur le chiffrement AES du SVM.

- L'activation ou la désactivation DES ou 3DES ne nécessite aucune modification de la configuration Kerberos sur les LIF.

## Étape

1. Activez ou désactivez le type de cryptage autorisé que vous souhaitez :

| Pour activer ou désactiver... | Suivez ces étapes...                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DES ou 3DES                   | <p>a. Configurer les types de cryptage NFS Kerberos autorisés du SVM :</p> <pre>vserver nfs modify -vserver<br/>vserver_name -permitted-enc-types<br/>encryption_types</pre> <p>Séparez les différents types de cryptage par une virgule.</p> <p>b. Vérifiez que la modification a réussi :</p> <pre>vserver nfs show -vserver<br/>vserver_name -fields permitted-enc-<br/>types</pre> |

| Pour activer ou désactiver... | Suivez ces étapes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AES-128 ou AES-256            | <p>a. Identifier sur quel SVM et LIF Kerberos sont activés :</p> <pre>vserver nfs kerberos interface show</pre> <p>b. Désactiver Kerberos sur toutes les LIFs sur le SVM dont NFS Kerberos autorisé type de cryptage que vous souhaitez modifier :</p> <pre>vserver nfs kerberos interface<br/>disable -lif <i>lif_name</i></pre> <p>c. Configurer les types de cryptage NFS Kerberos autorisés du SVM :</p> <pre>vserver nfs modify -vserver<br/>vserver_name -permitted-enc-types<br/>encryption_types</pre> <p>Séparez les différents types de cryptage par une virgule.</p> <p>d. Vérifiez que la modification a réussi :</p> <pre>vserver nfs show -vserver<br/>vserver_name -fields permitted-enc-<br/>types</pre> <p>e. Réactiver Kerberos sur toutes les LIFs sur le SVM :</p> <pre>vserver nfs kerberos interface<br/>enable -lif <i>lif_name</i> -spn<br/>service_principal_name</pre> <p>f. Vérifier que Kerberos est activé sur toutes les LIFs :</p> <pre>vserver nfs kerberos interface show</pre> |

#### Activez Kerberos sur une LIF donnée

Vous pouvez utiliser le `vserver nfs kerberos interface enable` Commande pour activer Kerberos sur une LIF de données. Cela permet au SVM d'utiliser les services de sécurité Kerberos pour NFS.

#### Description de la tâche

Si vous utilisez un KDC Active Directory, les 15 premiers caractères de tous les noms de domaine utilisés doivent être uniques sur les SVM au sein d'un domaine ou d'un domaine.

#### Étapes

1. Créez la configuration NFS Kerberos :

```
vserver nfs kerberos interface enable -vserver vserver_name -lif
logical_interface -spn service_principal_name
```

ONTAP nécessite la clé secrète pour le SPN à partir du KDC pour activer l'interface Kerberos.

Pour les VDC Microsoft, le KDC est contacté et un nom d'utilisateur et un mot de passe sont émis sur l'CLI pour obtenir la clé secrète. Si vous devez créer le SPN dans une autre UO du domaine Kerberos, vous pouvez spécifier l'option -ou paramètre.

Pour les KDC non Microsoft, la clé secrète peut être obtenue en utilisant l'une des deux méthodes suivantes :

| Si...                                                                                                                      | Vous devez également inclure le paramètre suivant avec la commande... |
|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| Demandez à l'administrateur KDC de récupérer la clé directement à partir du KDC                                            | -admin-username <i>kdc_admin_username</i>                             |
| Ne disposez pas des informations d'identification de l'administrateur KDC mais d'un fichier keytab du KDC contenant la clé | -keytab-uri {ftp                                                      |

2. Vérifier que Kerberos a été activé sur la LIF :

```
vserver nfs kerberos-config show
```

3. Répétez les étapes 1 et 2 pour activer Kerberos sur plusieurs LIFs.

Exemple

La commande suivante crée et vérifie une configuration Kerberos NFS pour le SVM nommé vs1 sur l'interface logique ves03-d1, avec le SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM dans l'UO lab2ou :

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spnn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
 Logical
Vserver Interface Address Kerberos SPN

vs0 ves01-a1
 10.10.10.30 disabled -
vs2 ves01-d1
 10.10.10.40 enabled nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

## Utilisation de TLS avec NFS pour une sécurité renforcée

### Présentation de l'utilisation de TLS avec NFS pour une sécurité renforcée

TLS permet des communications réseau chiffrées avec une sécurité équivalente et moins complexe que Kerberos et IPsec. En tant qu'administrateur, vous pouvez activer, configurer et désactiver TLS pour une sécurité renforcée avec les connexions NFSv3 et NFSv4.x via System Manager, l'interface de ligne de commande ONTAP ou l'API REST ONTAP.



NFS over TLS est disponible dans ONTAP 9.15.1 en tant que préversion publique. À titre de préversion, NFS over TLS n'est pas pris en charge pour les workloads de production dans ONTAP 9.15.1.

ONTAP utilise TLS 1.3 pour les connexions NFS sur TLS.

### De formation

NFS sur TLS nécessite des certificats X.509. Vous pouvez soit créer un certificat de serveur d'installation signé par une autorité de certification sur le cluster ONTAP, soit installer un certificat que le service NFS utilise directement. Vos certificats doivent être conformes aux directives suivantes :

- Chaque certificat doit être configuré avec le nom de domaine complet (FQDN) du serveur NFS (la LIF de données sur laquelle TLS sera activé/configuré) en tant que nom commun (CN).
- Chaque certificat doit être configuré avec l'adresse IP ou le nom de domaine complet du serveur NFS (ou les deux) en tant que nom secondaire de l'objet (SAN). Si l'adresse IP et le nom de domaine complet sont configurés, les clients NFS peuvent se connecter à l'aide de l'adresse IP ou du nom de domaine complet.
- Vous pouvez installer plusieurs certificats de service NFS pour la même LIF, mais un seul d'entre eux peut être utilisé à la fois dans le cadre de la configuration NFS TLS.

### Activez ou désactivez TLS pour les clients NFS

Vous pouvez activer ou désactiver TLS sur une LIF de données pour les clients NFS. Lorsque vous activez NFS sur TLS, le SVM utilise TLS pour chiffrer toutes les données envoyées sur le réseau entre le client NFS et ONTAP. Cela augmente la sécurité des connexions NFS.



NFS over TLS est disponible dans ONTAP 9.15.1 en tant que préversion publique. À titre de préversion, NFS over TLS n'est pas pris en charge pour les workloads de production dans ONTAP 9.15.1.

### Activez TLS

Vous pouvez activer le chiffrement TLS pour les clients NFS afin d'augmenter la sécurité des données en transit.

### Avant de commencer

- Reportez-vous à la ["de formation"](#) Pour NFS sur TLS avant de commencer.
- Reportez-vous à la ["page de manuel"](#) pour plus d'informations sur le `vserver nfs tls interface enable` commande.

Étapes

- 1. Il convient de choisir une machine virtuelle de stockage et une interface logique (LIF) sur laquelle activer TLS.
- 2. Activez TLS pour les connexions NFS sur cette machine virtuelle et cette interface de stockage. Remplacez les valeurs entre parenthèses <> par les informations de votre environnement :

```
vserver nfs tls interface enable -vserver <STORAGE_VM> -lif <LIF_NAME>
-certificate-name <CERTIFICATE_NAME>
```

- 3. Utilisez le `vserver nfs tls interface show` pour afficher les résultats :

```
vserver nfs tls interface show
```

Exemple

La commande suivante active NFS sur TLS sur le `data1` LIF du `vs1` VM de stockage :

```
vserver nfs tls interface enable -vserver vs1 -lif data1 -certificate-name
cert_vs1
```

```
vserver nfs tls interface show
```

| Vserver Name              | Logical Interface | Address  | TLS Status | TLS Certificate |
|---------------------------|-------------------|----------|------------|-----------------|
| vs1                       | data1             | 10.0.1.1 | enabled    | cert_vs1        |
| vs2                       | data2             | 10.0.1.2 | disabled   | -               |
| 2 entries were displayed. |                   |          |            |                 |

Désactiver TLS

Vous pouvez désactiver TLS pour les clients NFS si vous n'avez plus besoin de la sécurité améliorée pour les données en transit.



Lorsque vous désactivez NFS sur TLS, le certificat TLS utilisé pour la connexion NFS est supprimé. Si vous devez activer NFS over TLS à l'avenir, vous devrez à nouveau spécifier un nom de certificat lors de l'activation.

Avant de commencer

Reportez-vous à la ["page de manuel"](#) pour plus d'informations sur le `vserver nfs tls interface`



disable commande.

Étapes

- 1. Choisissez une VM de stockage et une interface logique (LIF) sur laquelle désactiver TLS.
- 2. Désactivez TLS pour les connexions NFS sur cette VM et cette interface de stockage. Remplacez les valeurs entre parenthèses <> par les informations de votre environnement :

```
vserver nfs tls interface disable -vserver <STORAGE_VM> -lif <LIF_NAME>
```

- 3. Utilisez le `vserver nfs tls interface show` pour afficher les résultats :

```
vserver nfs tls interface show
```

Exemple

La commande suivante désactive NFS sur TLS sur le `data1` LIF du `vs1` VM de stockage :

```
vserver nfs tls interface disable -vserver vs1 -lif data1
```

```
vserver nfs tls interface show
```

| Vserver Name              | Logical Interface | Address  | TLS Status | TLS Certificate |
|---------------------------|-------------------|----------|------------|-----------------|
| vs1                       | data1             | 10.0.1.1 | disabled   | -               |
| vs2                       | data2             | 10.0.1.2 | disabled   | -               |
| 2 entries were displayed. |                   |          |            |                 |

Modifier une configuration TLS

Vous pouvez modifier les paramètres d'une configuration NFS sur TLS existante. Par exemple, vous pouvez utiliser cette procédure pour mettre à jour le certificat TLS.

Avant de commencer

Reportez-vous à la ["page de manuel"](#) pour plus d'informations sur le `vserver nfs tls interface modify` commande.

Étapes

- 1. Choisir une VM de stockage et une interface logique (LIF) sur laquelle modifier la configuration TLS pour les clients NFS.

2. Modifier la configuration. Si vous spécifiez un `status` de `enable`, vous devez également spécifier le `certificate-name` paramètre. Remplacez les valeurs entre parenthèses `<>` par les informations de votre environnement :

```
vserver nfs tls interface modify -vserver <STORAGE_VM> -lif <LIF_NAME>
-status <STATUS> -certificate-name <CERTIFICATE_NAME>
```

3. Utilisez le `vserver nfs tls interface show` pour afficher les résultats :

```
vserver nfs tls interface show
```

### Exemple

La commande suivante modifie la configuration NFS sur TLS sur le `data2` LIF du `vs2` VM de stockage :

```
vserver nfs tls interface modify -vserver vs2 -lif data2 -status enable
-certificate-name new_cert
```

```
vserver nfs tls interface show
```

| Vserver<br>Name | Logical<br>Interface | Address  | TLS Status | TLS Certificate |
|-----------------|----------------------|----------|------------|-----------------|
| vs1             | data1                | 10.0.1.1 | disabled   | -               |
| vs2             | data2                | 10.0.1.2 | enabled    | new_cert        |

2 entries were displayed.

## Ajout de capacité de stockage à un SVM compatible NFS

### Ajoutez de la capacité de stockage à une présentation de SVM compatible NFS

Pour ajouter de la capacité de stockage à un SVM compatible NFS, vous devez créer un volume ou `qtree` pour fournir un conteneur de stockage, et créer ou modifier une export policy pour ce conteneur. Vous pouvez ensuite vérifier l'accès client NFS depuis le cluster et tester l'accès depuis les systèmes client.

#### Ce dont vous avez besoin

- NFS doit être entièrement configuré sur le SVM.
- La export policy default du volume root du SVM doit contenir une règle qui permet d'accéder à tous les clients.

- Toute mise à jour de la configuration des services de noms doit être terminée.
- Tout ajout ou modification d'une configuration Kerberos doit être effectué.

### Créer une export-policy

Avant de créer des règles d'exportation, vous devez créer une export-policy pour les tenir. Vous pouvez utiliser le `vserver export-policy create` commande pour créer une export policy.

#### Étapes

1. Créer une export-policy :

```
vserver export-policy create -vserver vserver_name -policyname policy_name
```

Le nom de la stratégie peut comporter jusqu'à 256 caractères.

2. Vérifier que l'export policy a été créée :

```
vserver export-policy show -policyname policy_name
```

#### Exemple

Les commandes suivantes créent et vérifient la création d'une export policy nommée `exp1` sur le SVM nommé `vs1`:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver Policy Name

vs1 exp1
```

### Ajouter une règle à une export-policy

Sans règles, l'export policy ne peut pas fournir aux clients l'accès aux données. Pour créer une nouvelle règle d'exportation, vous devez identifier les clients et sélectionner un format de correspondance client, sélectionner les types d'accès et de sécurité, spécifier un mappage d'ID utilisateur anonyme, sélectionner un numéro d'index de règle et sélectionner le protocole d'accès. Vous pouvez ensuite utiliser le `vserver export-policy rule create` commande pour ajouter la nouvelle règle à une export-policy.

#### Ce dont vous avez besoin

- L'export policy à laquelle vous souhaitez ajouter les règles d'exportation doit déjà exister.
- Le DNS doit être correctement configuré sur le SVM de données et les serveurs DNS doivent avoir des entrées correctes pour les clients NFS.

En effet, ONTAP effectue des recherches DNS en utilisant la configuration DNS du SVM de données pour certains formats de correspondance client, et les échecs de mise en correspondance de règles d'export

peuvent empêcher l'accès aux données client.

- Si vous authentifiez avec Kerberos, vous devez avoir déterminé les méthodes de sécurité suivantes utilisées sur vos clients NFS :
  - `krb5` (Protocole Kerberos V5)
  - `krb5i` (Protocole Kerberos V5 avec contrôle d'intégrité à l'aide de checksums)
  - `krb5p` (Protocole Kerberos V5 avec service de confidentialité)

### Description de la tâche

Il n'est pas nécessaire de créer une nouvelle règle si une règle existante d'une stratégie d'exportation couvre la correspondance de vos clients et les exigences d'accès.

Si vous authentifiez avec Kerberos et si tous les volumes du SVM sont accessibles via Kerberos, vous pouvez définir les options des règles d'exportation `-rorule`, `-rwrule`, et `-superuser` pour le volume racine à `krb5`, `krb5i`, ou `krb5p`.

### Étapes

1. Identifiez les clients et le format de correspondance client pour la nouvelle règle.

Le `-clientmatch` spécifie les clients auxquels la règle s'applique. Des valeurs de correspondance client uniques ou multiples peuvent être spécifiées ; les spécifications de valeurs multiples doivent être séparées par des virgules. Vous pouvez spécifier la correspondance dans l'un des formats suivants :

| Format de correspondance client                                                 | Exemple                                                                                                    |
|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Nom de domaine précédé du caractère "."                                         | <code>.example.com</code> ou <code>.example.com, .example.net, ...</code>                                  |
| Nom d'hôte                                                                      | <code>host1</code> ou <code>host1, host2, ...</code>                                                       |
| Adresse IPv4                                                                    | <code>10.1.12.24</code> ou <code>10.1.12.24, 10.1.12.25, ...</code>                                        |
| Adresse IPv4 avec un masque de sous-réseau exprimé en nombre de bits            | <code>10.1.12.10/4</code> ou <code>10.1.12.10/4, 10.1.12.11/4, ...</code>                                  |
| Adresse IPv4 avec un masque de réseau                                           | <code>10.1.16.0/255.255.255.0</code> ou <code>10.1.16.0/255.255.255.0, 10.1.17.0/255.255.255.0, ...</code> |
| Adresse IPv6 en format pointillé                                                | <code>::1.2.3.4</code> ou <code>::1.2.3.4, ::1.2.3.5, ...</code>                                           |
| Adresse IPv6 avec un masque de sous-réseau exprimé en nombre de bits            | <code>ff::00/32</code> ou <code>ff::00/32, ff::01/32, ...</code>                                           |
| Un seul groupe de réseau avec le nom de groupe de réseau précédé du caractère @ | <code>@netgroup1</code> ou <code>@netgroup1, @netgroup2, ...</code>                                        |

Vous pouvez également combiner des types de définitions de client, par exemple, `.example.com,@netgroup1`.

Lors de la définition des adresses IP, notez les éléments suivants :

- La saisie d'une plage d'adresses IP, par exemple `10.1.12.10-10.1.12.70`, n'est pas autorisée.

Les entrées de ce format sont interprétées comme une chaîne de texte et sont traitées comme un nom d'hôte.

- Lors de la spécification d'adresses IP individuelles dans des règles d'exportation pour la gestion granulaire de l'accès client, ne spécifiez pas d'adresses IP dynamiquement (par exemple, DHCP) ou temporairement (par exemple, IPv6) attribuées.

Sinon, le client perd l'accès lorsque son adresse IP change.

- La saisie d'une adresse IPv6 avec un masque de réseau, par exemple `ff::12/ff::00`, n'est pas autorisée.

## 2. Sélectionnez les types d'accès et de sécurité pour les correspondances client.

Vous pouvez spécifier un ou plusieurs des modes d'accès suivants aux clients qui s'authentifient avec les types de sécurité spécifiés :

- `-rorule` (accès en lecture seule)
- `-rwrule` (accès en lecture/écriture)
- `-superuser` (accès racine)



Un client peut uniquement obtenir un accès en lecture/écriture pour un type de sécurité spécifique si la règle d'exportation autorise également un accès en lecture seule pour ce type de sécurité. Si le paramètre lecture seule est plus restrictif pour un type de sécurité que le paramètre lecture-écriture, il se peut que le client n'ait pas accès en lecture-écriture. Il en va de même pour l'accès superutilisateur.

Vous pouvez spécifier une liste de plusieurs types de sécurité séparés par des virgules pour une règle. Si vous spécifiez le type de sécurité comme `any` ou `never`, ne spécifiez aucun autre type de sécurité. Choisissez parmi les types de sécurité valides suivants :

| Lorsque le type de sécurité est défini sur... | Un client correspondant peut accéder aux données exportées...                                                                                                                                                                                                                                                                           |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>any</code>                              | Toujours, quel que soit le type de sécurité entrant.                                                                                                                                                                                                                                                                                    |
| <code>none</code>                             | S'ils sont répertoriés seuls, l'accès des clients possédant n'importe quel type de sécurité est accordé en tant qu'anonyme. Si elle est répertoriée avec d'autres types de sécurité, les clients avec un type de sécurité spécifié bénéficient d'un accès et les clients avec un autre type de sécurité bénéficient d'un accès anonyme. |
| <code>never</code>                            | Jamais, quel que soit le type de sécurité entrant.                                                                                                                                                                                                                                                                                      |

| Lorsque le type de sécurité est défini sur... | Un client correspondant peut accéder aux données exportées...                                                                                                                                           |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| krb5                                          | S'il est authentifié par Kerberos 5. Authentification uniquement : l'en-tête de chaque requête et réponse est signé.                                                                                    |
| krb5i                                         | S'il est authentifié par Kerberos 5i. Authentification et intégrité : l'en-tête et le corps de chaque requête et réponse sont signés.                                                                   |
| krb5p                                         | S'il est authentifié par Kerberos 5p. Authentification, intégrité et confidentialité : l'en-tête et le corps de chaque requête et réponse sont signés, et la charge utile des données NFS est chiffrée. |
| ntlm                                          | S'il est authentifié par CIFS NTLM.                                                                                                                                                                     |
| sys                                           | S'il est authentifié par NFS AUTH_SYS.                                                                                                                                                                  |

Le type de sécurité recommandé est `sys`, Ou si Kerberos est utilisé, `krb5`, `krb5i`, ou `krb5p`.

Si vous utilisez Kerberos avec NFSv3, la règle de export policy doit autoriser `-rorule` et `-rwrule` accès à `sys` en plus de `krb5`. Ceci est dû au besoin d'autoriser l'accès à Network Lock Manager (NLM) pour l'exportation.

### 3. Spécifiez un mappage d'ID utilisateur anonyme.

Le `-anon` Option spécifie un ID utilisateur ou un nom d'utilisateur UNIX qui est mappé aux demandes client qui arrivent avec un ID utilisateur de 0 (zéro), généralement associé à la racine du nom d'utilisateur. La valeur par défaut est `65534`. Les clients NFS associent généralement l'ID utilisateur `65534` au nom d'utilisateur personne (également appelé *root scaling*). Dans ONTAP, cet ID utilisateur est associé à l'utilisateur `pcuser`. Pour désactiver l'accès par tout client ayant un ID utilisateur de 0, spécifiez une valeur de `65535`.

### 4. Sélectionnez l'ordre d'index des règles.

Le `-ruleindex` option spécifie le numéro d'index de la règle. Les règles sont évaluées en fonction de leur ordre dans la liste des numéros d'index ; les règles avec des numéros d'index inférieurs sont évaluées en premier. Par exemple, la règle avec l'index numéro 1 est évaluée avant la règle avec l'index numéro 2.

| Si vous ajoutez...                       | Alors...  |
|------------------------------------------|-----------|
| La première règle vers une export-policy | Entrez 1. |

| Si vous ajoutez...                         | Alors...                                                                                                                                                                                                                                                                    |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Règles supplémentaires à une export-policy | <p>a. Afficher les règles existantes dans la stratégie :</p> <pre>vserver export-policy rule show -instance -policyname <i>your_policy</i></pre> <p>b. Sélectionnez un numéro d'index pour la nouvelle règle en fonction de l'ordre dans lequel elle doit être évaluée.</p> |

5. Sélectionnez la valeur d'accès NFS applicable : {nfs|nfs3|nfs4}.

*nfs* correspond à n'importe quelle version, *nfs3* et *nfs4* correspondent uniquement à ces versions spécifiques.

6. Créer la règle d'exportation et l'ajouter à une export policy existante :

```
vserver export-policy rule create -vserver vserver_name -policyname
policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text |
" text,text,... " } -rorule security_type -rwrule security_type -superuser
security_type -anon user_ID
```

7. Afficher les règles pour l'export policy pour vérifier que la nouvelle règle est présente :

```
vserver export-policy rule show -policyname policy_name
```

La commande affiche un récapitulatif de cette export policy, y compris une liste des règles appliquées à cette policy. ONTAP attribue à chaque règle un numéro d'index de règle. Après avoir connu le numéro d'index de la règle, vous pouvez l'utiliser pour afficher des informations détaillées sur la règle d'exportation spécifiée.

8. Vérifiez que les règles appliquées à l'export policy sont configurées correctement :

```
vserver export-policy rule show -policyname policy_name -vserver vserver_name
-ruleindex integer
```

## Exemples

Les commandes suivantes créent et vérifient la création d'une règle d'exportation sur le SVM nommé *vs1* dans une export policy nommée *rs1*. La règle a l'index numéro 1. La règle correspond à n'importe quel client du domaine *eng.company.com* et au groupe réseau *@netgroup1*. La règle active tous les accès NFS. Il active l'accès en lecture seule et en lecture-écriture aux utilisateurs authentifiés avec *AUTH\_SYS*. Les clients possédant l'ID utilisateur UNIX 0 (zéro) sont anonymisés sauf s'ils sont authentifiés avec Kerberos.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname expl
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgroup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5
```

```
vs1::> vserver export-policy rule show -policyname nfs_policy
```

| Virtual<br>Server | Policy<br>Name | Rule<br>Index | Access<br>Protocol | Client<br>Match                | RO<br>Rule |
|-------------------|----------------|---------------|--------------------|--------------------------------|------------|
| vs1               | expl           | 1             | nfs                | eng.company.com,<br>@netgroup1 | sys        |

```
vs1::> vserver export-policy rule show -policyname expl -vserver vs1
-ruleindex 1
```

```

Vserver: vs1
Policy Name: expl
Rule Index: 1
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
RO Access Rule: sys
RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: krb5
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

Les commandes suivantes créent et vérifient la création d'une règle d'export sur le SVM nommé vs2 dans une export policy nommée expol2. La règle a le numéro d'index 21. La règle correspond aux clients aux membres du groupe réseau dev\_netgroup\_main. La règle active tous les accès NFS. Il active un accès en lecture seule pour les utilisateurs authentifiés avec AUTH\_SYS et nécessite une authentification Kerberos pour l'accès en lecture-écriture et racine. Les clients possédant l'ID utilisateur UNIX 0 (zéro) se voient refuser l'accès racine sauf s'ils sont authentifiés avec Kerberos.



```
vs2::> vsserver export-policy rule create -vsserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5
```

```
vs2::> vsserver export-policy rule show -policyname nfs_policy
Virtual Policy Rule Access Client RO
Server Name Index Protocol Match Rule

vs2 expol2 21 nfs @dev_netgroup_main sys

vs2::> vsserver export-policy rule show -policyname expol2 -vsserver vs1
-ruleindex 21
```

```

Vserver: vs2
Policy Name: expol2
Rule Index: 21
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
 @dev_netgroup_main
RO Access Rule: sys
RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
Superuser Security Types: krb5
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

## Créer un volume ou un conteneur de stockage qtrees

### Créer un volume

Vous pouvez créer un volume et spécifier son point de jonction et d'autres propriétés en utilisant le `volume create` commande.

### Description de la tâche

Un volume doit inclure une *Junction path* pour que ses données soient mises à disposition des clients. Vous pouvez spécifier le chemin de jonction lorsque vous créez un nouveau volume. Si vous créez un volume sans spécifier un chemin de jonction, vous devez *mount* le volume du namespace du SVM à l'aide de `volume mount` commande.

### Avant de commencer

- NFS doit être configuré et exécuté.
- La sécurité du SVM doit être de style UNIX.
- À partir de ONTAP 9.13.1, vous pouvez créer des volumes dont l'analyse de la capacité et le suivi des activités sont activés. Pour activer le suivi de la capacité ou des activités, exécutez le `volume create` commande avec `-analytics-state` ou `-activity-tracking-state` réglés sur `on`.

Pour en savoir plus sur l'analyse de la capacité et le suivi des activités, reportez-vous à la section "[Activez l'analyse du système de fichiers](#)".

## Étapes

### 1. Créer le volume avec un point de jonction :

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path [-policy
export_policy_name]
```

Les choix pour `-junction-path` sont les suivants :

- Directement sous la racine, par exemple, `/new_vol`

Vous pouvez créer un nouveau volume et préciser qu'il peut être monté directement sur le volume root du SVM.

- Sous un répertoire existant, par exemple, `/existing_dir/new_vol`

Vous pouvez créer un nouveau volume et spécifier qu'il doit être monté sur un volume existant (dans une hiérarchie existante), exprimé en tant que répertoire.

Si vous souhaitez créer un volume dans un nouveau répertoire (dans une nouvelle hiérarchie sous un nouveau volume), par exemple, `/new_dir/new_vol`, Ensuite, vous devez d'abord créer un nouveau volume parent qui est relié par une jonction au volume racine de la SVM. Vous devez ensuite créer le nouveau volume enfant dans la Junction path du nouveau volume parent (nouveau répertoire).

Si vous prévoyez d'utiliser une export policy existante, vous pouvez la spécifier lors de la création du volume. Vous pouvez également ajouter une export-policy plus tard avec le `volume modify` commande.

### 2. Vérifier que le volume a été créé avec le point de jonction souhaité :

```
volume show -vserver svm_name -volume volume_name -junction
```

## Exemples

La commande suivante crée un nouveau volume nommé `users1` sur le SVM `vs1.example.com` et l'agrégat `aggr1`. Le nouveau volume est disponible sur le site `/users`. Le volume a une taille de 750 Go et sa garantie de volume est de type `volume` (par défaut).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
```

| Vserver         | Volume | Active | Junction Path | Junction Path Source |
|-----------------|--------|--------|---------------|----------------------|
| vs1.example.com | users1 | true   | /users        | RW_volume            |

La commande suivante crée un nouveau volume nommé « home4 » sur le SVM « vs1.example.com » et l'agrégat « aggr1 ». Le répertoire /eng/ Existe déjà dans l'espace de nommage de la SVM vs1, et le nouveau volume est mis à disposition à /eng/home, qui devient le répertoire de base de l' /eng/ espace de noms. Le volume a une taille de 750 Go et sa garantie de volume est de type volume (par défaut).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction

```

|                 |        | Junction |               | Junction    |
|-----------------|--------|----------|---------------|-------------|
| Vserver         | Volume | Active   | Junction Path | Path Source |
| vs1.example.com | home4  | true     | /eng/home     | RW_volume   |

### Créer un qtree

Vous pouvez créer un qtree pour contenir vos données et spécifier ses propriétés en utilisant le `volume qtree create` commande.

#### Ce dont vous avez besoin

- La SVM et le volume qui contiendra le nouveau qtree doivent déjà exister.
- La méthode de sécurité SVM doit être UNIX et NFS doit être configuré et en cours d'exécution.

#### Étapes

##### 1. Créer le qtree :

```
volume qtree create -vserver vserver_name { -volume volume_name -qtree
qtree_name | -qtree-path qtree path } -security-style unix [-policy
export_policy_name]
```

Vous pouvez spécifier le volume et qtree en tant qu'arguments distincts ou spécifier l'argument du chemin qtree au format `/vol/volume_name/_qtree_name`.

Par défaut, les qtrees héritent des règles d'exportation du volume parent, mais ils peuvent être configurés pour leur propre volume. Si vous prévoyez d'utiliser une export policy existante, vous pouvez l'indiquer lors de la création du qtree. Vous pouvez également ajouter une export-policy plus tard avec le `volume qtree modify` commande.

##### 2. Vérifier que le qtree a été créé avec le chemin de jonction souhaité :

```
volume qtree show -vserver vserver_name { -volume volume_name -qtree
qtree_name | -qtree-path qtree path }
```

### Exemple

L'exemple suivant crée un qtree nommé qt01 situé sur le SVM vs1.example.com qui dispose d'un chemin de jonction /vol/data1:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01
```

```
 Vserver Name: vs1.example.com
 Volume Name: data1
 Qtree Name: qt01
Actual (Non-Junction) Qtree Path: /vol/data1/qt01
 Security Style: unix
 Oplock Mode: enable
 Unix Permissions: ---rwxr-xr-x
 Qtree Id: 2
 Qtree Status: normal
 Export Policy: default
Is Export Policy Inherited: true
```

## Sécurisation de l'accès NFS à l'aide de règles d'exportation

### Sécurisation de l'accès NFS à l'aide de règles d'exportation

Vous pouvez utiliser des règles d'exportation pour restreindre l'accès NFS aux volumes ou aux qtrees aux clients correspondant à des paramètres spécifiques. Lorsque vous provisionnez un nouveau stockage, vous pouvez utiliser une stratégie et des règles existantes, ajouter des règles à une stratégie existante, ou créer une nouvelle règle et de nouvelles règles. Vous pouvez également vérifier la configuration des export-polices



Depuis ONTAP 9.3, vous pouvez activer la vérification de la configuration des règles d'exportation en tant que tâche d'arrière-plan qui enregistre toutes les violations de règles dans une liste de règles d'erreur. Le `vserver export-policy config-checker` Les commandes appellent le vérificateur et affichent les résultats, que vous pouvez utiliser pour vérifier votre configuration et supprimer des règles erronées de la stratégie. Les commandes ne valident que la configuration d'exportation pour les noms d'hôte, les groupes réseau et les utilisateurs anonymes.

### Gérer l'ordre de traitement des règles d'exportation

Vous pouvez utiliser le `vserver export-policy rule setindex` commande permettant de définir manuellement le numéro d'index d'une règle d'exportation existante. Cela vous permet de spécifier la priorité selon laquelle ONTAP applique des règles d'exportation aux requêtes client.

### Description de la tâche

Si le nouveau numéro d'index est déjà utilisé, la commande insère la règle au point spécifié et réorganise la liste en conséquence.

## Étape

1. Modifier le numéro d'index d'une règle d'exportation spécifiée :

```
vserver export-policy rule setindex -vserver virtual_server_name -policyname policy_name -ruleindex integer -newruleindex integer
```

## Exemple

La commande suivante modifie l'index numéro d'une règle d'exportation au niveau de l'index numéro 3 en index numéro 2 dans une export policy nommée rs1 sur le SVM nommée vs1 :

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

## Affectation d'une export-policy à un volume

Chaque volume contenu au SVM doit être associé à une export policy qui contient les export rules auxquelles les clients ont accès les données au sein du volume.

## Description de la tâche

Vous pouvez associer une export policy à un volume lors de la création du volume ou à tout moment après sa création. Vous pouvez associer une export policy au volume, bien qu'une seule policy puisse être associée à de nombreux volumes.

## Étapes

1. Si une export policy n'a pas été spécifiée lors de la création du volume, affectez une export policy au volume :

```
volume modify -vserver vserver_name -volume volume_name -policy export_policy_name
```

2. Vérifiez que la policy a été assignée au volume :

```
volume show -volume volume_name -fields policy
```

## Exemple

Les commandes suivantes affectent l'export policy nfs\_policy vers le volume vol1 sur le SVM vs1 et vérifient l'affectation :

```
cluster::> volume modify -vserver vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume policy

vs1 vol1 nfs_policy
```

## Affecter une export policy à un qtree

Au lieu d'exporter un volume entier, vous pouvez également exporter un qtree spécifique sur un volume afin de le rendre directement accessible aux clients. Vous pouvez exporter un qtree en lui attribuant une export policy. Vous pouvez affecter la export policy lorsque vous créez un qtree ou en modifiant un qtree existant.

### Ce dont vous avez besoin

La export policy doit exister.

### Description de la tâche

Par défaut, les qtrees héritent de la politique d'exportation parent du volume contenant, si elle n'est pas spécifiée au moment de la création.

Vous pouvez associer une export policy à un qtree lors de la création du qtree ou à tout moment après la création du qtree. Vous pouvez associer une export policy au qtree, bien qu'une seule règle puisse être associée à de nombreux qtrees.

### Étapes

1. Si une export policy n'a pas été spécifiée lors de la création du qtree, assigner une export policy au qtree :

```
volume qtree modify -vserver vs1 -qtree-path
/vol/volume_name/qtree_name -export-policy export_policy_name
```

2. Vérifier que la règle a été attribuée au qtree :

```
volume qtree show -qtree qtree_name -fields export-policy
```

### Exemple

Les commandes suivantes affectent l'export policy nfs\_policy au qtree qt1 sur le SVM vs1 et vérifient l'affectation :

```
cluster::> volume modify -vserver vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy

vs1 data1 qt01 nfs_policy
```

### Vérifiez l'accès client NFS depuis le cluster

Vous pouvez donner à certains clients l'accès au partage en définissant les autorisations de fichier UNIX sur un hôte d'administration UNIX. Vous pouvez vérifier l'accès client à l'aide de `vserver export-policy check-access` commande, en ajustant les règles d'exportation si nécessaire.

### Étapes

1. Sur le cluster, vérifiez l'accès des clients aux exportations à l'aide de `vserver export-policy check-access` commande.

La commande suivante vérifie l'accès en lecture/écriture pour un client NFSv3 avec l'adresse IP 1.2.3.4 vers la commande volume home2. La sortie de la commande indique que le volume utilise la export policy exp-home-dir et cet accès est refusé.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
```

| Path       | Policy       | Policy<br>Owner | Policy<br>Owner Type | Rule<br>Index | Access |
|------------|--------------|-----------------|----------------------|---------------|--------|
| /          | default      | vs1_root        | volume               | 1             | read   |
| /eng       | default      | vs1_root        | volume               | 1             | read   |
| /eng/home2 | exp-home-dir | home2           | volume               | 1             | denied |

3 entries were displayed.

2. Examinez la sortie pour déterminer si l'export policy fonctionne comme prévu et si l'accès client se comporte comme prévu.

Plus précisément, vous devez vérifier quelles export policy est utilisée par le volume ou qtree et ce type d'accès par le client.

3. Si nécessaire, reconfigurer les règles d'export policy.

## Testez l'accès NFS à partir des systèmes client

Après avoir vérifié l'accès NFS au nouvel objet de stockage, il est important de tester la configuration en vous connectant à un hôte d'administration NFS et en lisant les données à partir de et en écrivant les données sur la SVM. Vous devez ensuite répéter le processus en tant qu'utilisateur non-root sur un système client.

### Ce dont vous avez besoin

- Le système client doit disposer d'une adresse IP autorisée par la règle d'exportation que vous avez spécifiée précédemment.
- Vous devez disposer des informations de connexion pour l'utilisateur root.

### Étapes

1. Sur le cluster, vérifier l'adresse IP de la LIF qui héberge le nouveau volume :

```
network interface show -vserver svm_name
```

2. Connectez-vous en tant qu'utilisateur racine au système client hôte d'administration.
3. Changez le répertoire pour le dossier de montage :

```
cd /mnt/
```

4. Créer et monter un nouveau dossier en utilisant l'adresse IP de la SVM :

a. Créer un nouveau dossier :

```
mkdir /mnt/folder
```

b. Montez le nouveau volume dans ce nouveau répertoire :

```
mount -t nfs -o hard IPAddress:/volume_name /mnt/folder
```

c. Changez le répertoire pour le nouveau dossier :

```
cd folder
```

Les commandes suivantes créent un dossier nommé test1, montent le volume vol1 à l'adresse IP 192.0.2.130 du dossier de montage tes1 et changent dans le nouveau répertoire tes1 :

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. Créez un nouveau fichier, vérifiez qu'il existe et écrivez du texte :

a. Créer un fichier de test :

```
touch filename
```

b. Vérifiez que le fichier existe :

```
ls -l filename
```

c. Entrez :

```
cat > filename
```

Tapez du texte, puis appuyez sur Ctrl+D pour écrire du texte dans le fichier test.

d. Afficher le contenu du fichier de test.

```
cat filename
```

e. Supprimez le fichier de test :

```
rm filename
```

f. Retour au répertoire parent :

```
cd ..
```



```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. En tant que root, définissez les droits de propriété et les autorisations UNIX souhaités sur le volume monté.
7. Sur un système client UNIX identifié dans vos règles d'exportation, connectez-vous en tant qu'un des utilisateurs autorisés qui ont désormais accès au nouveau volume, puis répétez les procédures des étapes 3 à 5 pour vérifier que vous pouvez monter le volume et créer un fichier.

## Où trouver des informations complémentaires

Après avoir testé l'accès client NFS avec succès, vous pouvez effectuer une configuration NFS supplémentaire ou ajouter un accès SAN. Une fois les protocoles accès terminés, vous devez protéger le volume root de la machine virtuelle de stockage (SVM).

### Configuration NFS

Vous pouvez configurer davantage l'accès NFS à l'aide des informations et rapports techniques suivants :

- ["Gestion NFS"](#)

Décrit comment configurer et gérer l'accès aux fichiers à l'aide de NFS.

- ["Rapport technique NetApp 4067 : Guide des meilleures pratiques et de mise en œuvre de NFS"](#)

Sert de guide opérationnel NFSv3 et NFSv4, et présente le système d'exploitation ONTAP avec un accent sur NFSv4.

- ["Rapport technique NetApp 4073 : authentification unifiée sécurisée"](#)

Explique comment configurer ONTAP pour une utilisation avec des serveurs Kerberos version 5 (krb5) UNIX pour l'authentification du stockage NFS et Windows Server Active Directory (AD) en tant que fournisseur d'identité KDC et Lightweight Directory Access Protocol (LDAP).

- ["Rapport technique NetApp 3580 : Guide des améliorations et des meilleures pratiques NFSv4 implémentation d'Data ONTAP"](#)

Décrit les meilleures pratiques à suivre lors de l'implémentation des composants NFSv4 sur des clients AIX, Linux ou Solaris reliés à des systèmes exécutant ONTAP.

## Configuration de la mise en réseau

Vous pouvez configurer davantage les fonctions de réseau et les services de noms à l'aide des informations et rapports techniques suivants :

- ["Gestion NFS"](#)

Décrit la configuration et la gestion de la mise en réseau ONTAP.

- ["Rapport technique NetApp 4182 : considérations relatives à la conception du stockage Ethernet et meilleures pratiques pour les configurations clustered Data ONTAP"](#)

Décrit l'implémentation des configurations réseau ONTAP et fournit des scénarios de déploiement réseau communs et des recommandations sur les meilleures pratiques.

- ["Rapport technique de NetApp 4668 : name Services Best Practices Guide \(Guide des meilleures pratiques des services de noms\)"](#)

Explique comment configurer LDAP, NIS, DNS et la configuration de fichiers locaux à des fins d'authentification.

## Configuration du protocole SAN

Si vous souhaitez fournir ou modifier un accès SAN au nouveau SVM, vous pouvez utiliser les informations de configuration FC ou iSCSI disponibles pour plusieurs systèmes d'exploitation hôtes.

## Protection du volume racine

Après avoir configuré les protocoles sur le SVM, il faut s'assurer que son volume root est protégé :

- ["Protection des données"](#)

Décrit la procédure de création d'un miroir de partage de charge pour protéger le volume racine du SVM, une pratique recommandée par NetApp pour les SVM compatibles avec NAS. Décrit également la procédure de restauration rapide en cas de défaillances ou de pertes de volumes en promouvant le volume racine du SVM à partir d'un miroir de partage de charge.

## La différence entre les exportations ONTAP et les exportations 7-mode

### La différence entre les exportations ONTAP et les exportations 7-mode

Si vous ne savez pas comment ONTAP implémente les exports NFS, vous pouvez comparer les outils de configuration d'exportation 7-mode et ONTAP, ainsi que les exemples 7-mode `/etc/exports` fichiers avec des règles et règles en cluster.

En ONTAP, il n'y a pas de `/etc/exports` fichier et non `exportfs` commande. Vous devez plutôt définir une export-policy. Les export-polices vous permettent de contrôler l'accès des clients de la même manière que dans 7-mode. Toutefois, vous offrent des fonctionnalités supplémentaires, telles que la possibilité de réutiliser la même export policy pour plusieurs volumes.


### Informations associées

["Gestion NFS"](#)

## Comparaison des exportations dans 7-mode et ONTAP

Dans ONTAP, les exportations sont définies et utilisées différemment des environnements 7-mode.

| Domaines de différence                                                                         | 7-mode                                                                                                                                                                                                                                                                                                                                                                     | ONTAP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Définition des exportations                                                                    | Les exportations sont définies dans le <code>/etc/exports</code> fichier.                                                                                                                                                                                                                                                                                                  | Les exportations sont définies par la création d'une export policy au sein d'un SVM. Un SVM peut inclure plusieurs export policy.                                                                                                                                                                                                                                                                                                                                                                                      |
| Champ d'application de l'exportation                                                           | <ul style="list-style-type: none"><li>• Les exportations s'appliquent à un chemin de fichiers ou à un qtree spécifié.</li><li>• Vous devez créer une entrée séparée dans <code>/etc/exports</code> pour chaque chemin de fichier ou qtree.</li><li>• Les exportations ne sont persistantes que si elles sont définies dans le <code>/etc/exports</code> fichier.</li></ul> | <ul style="list-style-type: none"><li>• Les règles d'exportation s'appliquent à tout un volume, y compris l'ensemble des chemins de fichiers et qtrees contenu dans le volume.</li><li>• Si vous le souhaitez, des règles d'exportation peuvent être appliquées à plusieurs volumes.</li><li>• Toutes les règles d'exportation sont conservées sur l'ensemble des redémarrages du système.</li></ul>                                                                                                                   |
| Escrime (spécification d'un accès différent pour des clients spécifiques aux mêmes ressources) | Pour fournir à des clients spécifiques un accès différent à une seule ressource exportée, vous devez répertorier chaque client et son accès autorisé dans <code>/etc/exports</code> fichier.                                                                                                                                                                               | Les export-polices se composent d'un certain nombre de règles d'exportation individuelles. Chaque règle d'exportation définit des autorisations d'accès spécifiques pour une ressource et répertorie les clients disposant de ces autorisations. Pour spécifier un accès différent pour des clients spécifiques, vous devez créer une règle d'exportation pour chaque ensemble spécifique d'autorisations d'accès, répertorier les clients disposant de ces autorisations, puis ajouter les règles à la export policy. |

|                   |                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Changement de nom | Lorsque vous définissez une exportation, vous pouvez choisir de modifier le nom de l'exportation par rapport au nom du chemin du fichier. Vous devez utiliser le <code>-actual</code> paramètre lors de la définition d'une telle exportation dans le <code>/etc/exports</code> fichier. | <p>Vous pouvez choisir de rendre le nom du volume exporté différent de celui du volume réel. Pour ce faire, il faut monter le volume avec un nom de chemin de jonction personnalisé au sein du namespace du SVM.</p> <div>  <p>Par défaut, les volumes sont montés avec leur nom de volume. Pour personnaliser le chemin de jonction d'un volume, vous devez le démonter, le renommer, puis le remonter.</p> </div> |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Exemples de politiques d'exportation ONTAP

Vous pouvez consulter des exemples de règles d'exportation pour mieux comprendre le fonctionnement des règles d'exportation dans ONTAP.

#### Exemple d'implémentation ONTAP d'une exportation 7-mode

L'exemple suivant montre une exportation 7-mode telle qu'elle s'affiche dans la `/etc/export` fichier :

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

Pour reproduire cet export policy en cluster, il faut créer une export policy avec trois règles d'exportation, puis assigner la export policy au volume vol1.

| Règle                                                                                 | Elément                                                   | Valeur                                              |
|---------------------------------------------------------------------------------------|-----------------------------------------------------------|-----------------------------------------------------|
| Règle 1                                                                               | <code>-clientmatch</code> (spécification client)          | <code>@readonly_netgroup</code>                     |
| <code>-ruleindex</code> (position de la règle d'exportation dans la liste des règles) | 1                                                         | <code>-protocol</code>                              |
| <code>nfs</code>                                                                      | <code>-rorule</code> (autoriser l'accès en lecture seule) | <code>sys</code> (Client authentifié avec AUTH_SYS) |

| Règle                                          | Élément                                   | Valeur                                         |
|------------------------------------------------|-------------------------------------------|------------------------------------------------|
| -rwrule(autoriser l'accès en lecture/écriture) | never                                     | -superuser(autoriser l'accès superutilisateur) |
| none(racine écrasée à anon)                    | Règle 2                                   | -clientmatch                                   |
| @rootaccess_netgroup                           | -ruleindex                                | 2                                              |
| -protocol                                      | nfs                                       | -rorule                                        |
| sys                                            | -rwrule                                   | sys                                            |
| -superuser                                     | sys                                       | Règle 3                                        |
| -clientmatch                                   | @readwrite_netgroup1,@readwrite_netgroup2 | -ruleindex                                     |
| 3                                              | -protocol                                 | nfs                                            |
| -rorule                                        | sys                                       | -rwrule                                        |
| sys                                            | -superuser                                | none                                           |

1. Créez une export policy appelée exp\_vol1 :

```
vserver export-policy create -vserver NewSVM -policyname exp_vol1
```

2. Créer trois règles avec les paramètres suivants pour la commande de base :

° Commande de base :

```
vserver export-policy rule create -vserver NewSVM -policyname exp_vol1
```

° Paramètres de règle :

```
-clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys
-rwrule never -superuser none
```

```
-clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys
-rwrule sys -superuser sys
```

```
-clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3
-protocol nfs -rorule sys -rwrule sys -superuser none
```

3. Affectez la policy au volume vol1 :

```
volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
```

## Exemple de consolidation des exports 7-mode

L'exemple suivant montre 7-mode /etc/export fichier qui inclut une ligne pour chacun des 10 qtrees :

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

Dans ONTAP, une des deux règles est nécessaire pour chaque qtree : l'une avec une règle incluant `-clientmatch host1519s`, ou un avec une règle incluant `-clientmatch host2057s`.

1. Créez deux règles d'exportation appelées `exp_vol1q1` et `exp_vol1q2` :

- `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
- `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`

2. Créer une règle pour chaque règle :

- `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
- `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`

3. Appliquer les règles aux qtrees :

- `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
- [4 qtrees suivants...]
- `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
- [4 qtrees suivants...]

Si vous devez ajouter des qtrees supplémentaires pour ces hôtes, vous utiliserez les mêmes règles d'exportation.

## Gérez NFS avec l'interface de ligne de commande

### Présentation de référence NFS

ONTAP inclut des fonctionnalités d'accès aux fichiers disponibles pour le protocole NFS. Vous pouvez activer un serveur NFS et exporter des volumes ou des qtrees.

Vous effectuez cette procédure dans les cas suivants :

- Vous souhaitez connaître la gamme de fonctionnalités de protocole NFS de ONTAP.
- Vous souhaitez effectuer des tâches de configuration et de maintenance moins courantes, pas une configuration NFS de base.
- Vous souhaitez utiliser l'interface de ligne de commande et non System Manager, ni un outil de création de scripts automatisé.

## Compréhension de l'accès aux fichiers NAS

### Espaces de noms et points de jonction

#### Présentation des espaces de noms et des points de jonction

Un NAS *namespace* est un regroupement logique de volumes regroupés à *Junction points* pour créer une seule hiérarchie de système de fichiers. Un client disposant des autorisations suffisantes peut accéder aux fichiers dans l'espace de noms sans spécifier l'emplacement des fichiers dans le stockage. Des volumes regroupés dans le cluster peuvent se trouver n'importe où.

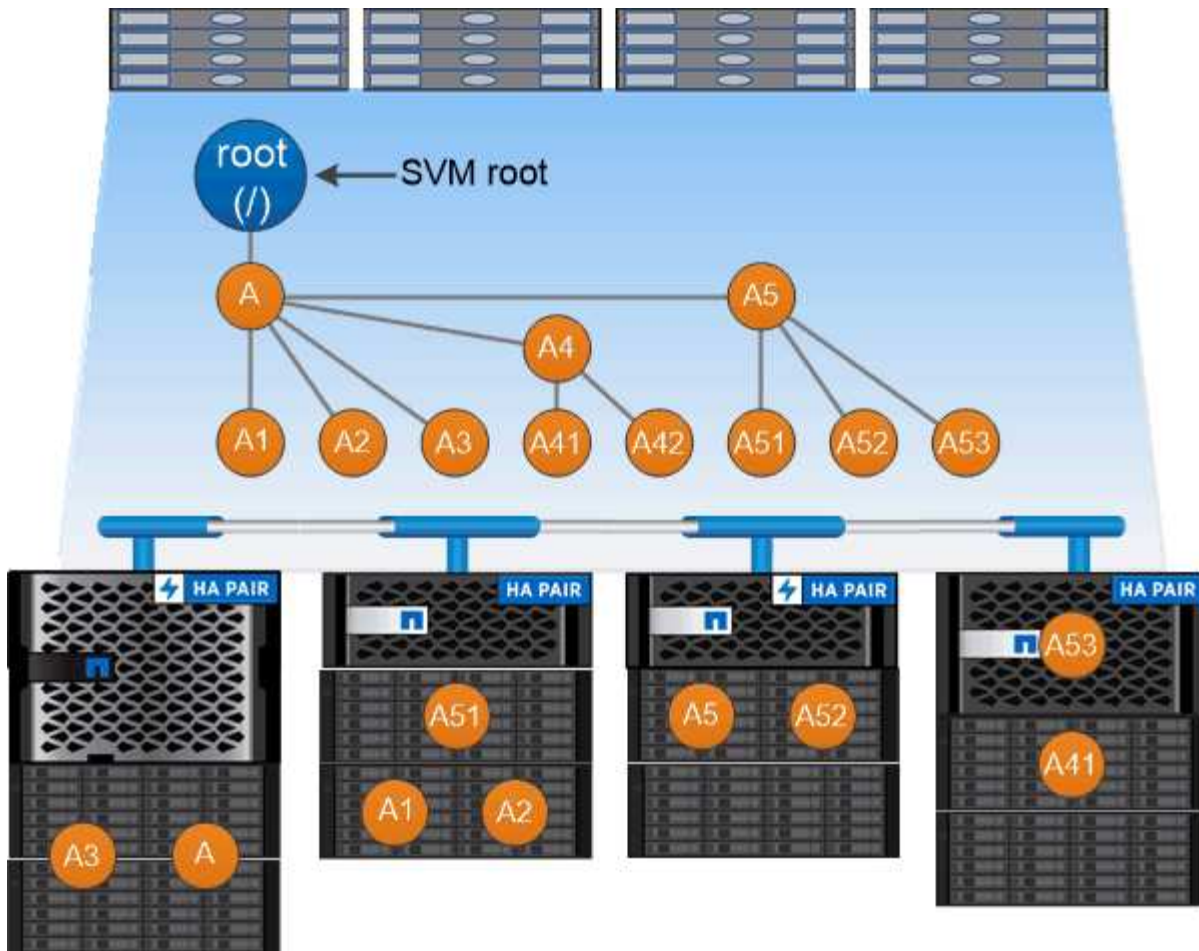
Plutôt que de monter chaque volume contenant un fichier d'intérêt, les clients NAS monter un NFS *export* ou accéder à un partage SMB. L'exportation ou le partage représente l'intégralité de l'espace de noms ou un emplacement intermédiaire dans l'espace de noms. Le client n'accède qu'aux volumes montés sous son point d'accès.

Vous pouvez ajouter des volumes au namespace selon vos besoins. Vous pouvez créer des points de jonction directement en-dessous d'une jonction de volume parent ou sur un répertoire au sein d'un volume. Il se peut qu'un chemin vers une jonction de volume pour un volume nommé « vol3 » soit possible `/vol1/vol2/vol3`, ou `/vol1/dir2/vol3`, ou même `/dir1/dir2/vol3`. Le chemin est appelé *Junction path*.

Chaque SVM possède un espace de noms unique. Le volume root du SVM est le point d'entrée de la hiérarchie de l'espace de noms.



Pour garantir la disponibilité des données en cas de panne du nœud ou de basculement, vous devez créer une copie *load-sharing mirror* pour le volume root du SVM.



*A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.*

### Exemple

L'exemple suivant crée un volume nommé « maison 4 » situé sur le SVM vs1 qui a une Junction path /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

### Caractéristiques des architectures d'espace de noms NAS

Plusieurs architectures d'espace de noms NAS classiques peuvent être utilisées lors de la création d'un espace de noms de SVM. Vous pouvez choisir l'architecture d'espace de noms qui correspond le mieux à vos besoins métiers et de flux de travail.

Le haut du namespace est toujours le volume root, représenté par une barre oblique (/). L'architecture d'espace de noms sous la racine se divise en trois catégories de base :

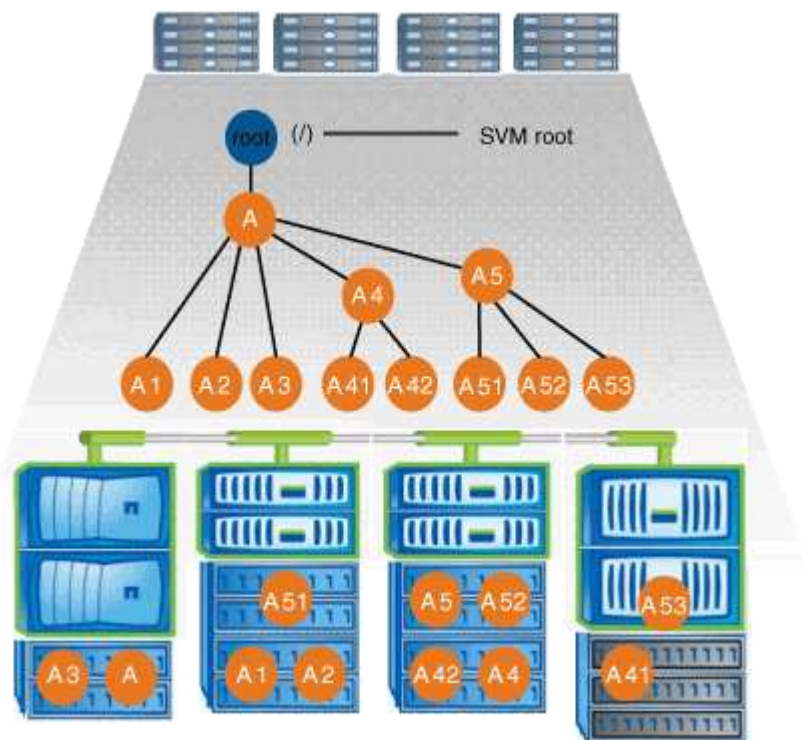
- Arbre branché unique, avec une seule jonction à la racine de l'espace de noms



- Plusieurs arborescences ramifiées, avec plusieurs points de jonction à la racine de l'espace de noms
- Plusieurs volumes autonomes, chacun avec un point de jonction séparé à la racine de l'espace de noms

### Espace de noms avec une seule arborescence ramifiée

Une architecture avec une seule arborescence de branche possède un point d'insertion unique à la racine du namespace du SVM. Le point d'insertion unique peut être un volume relié par jonction ou un répertoire sous la racine. Tous les autres volumes sont montés aux points de jonction sous le point d'insertion unique (qui peut être un volume ou un répertoire).

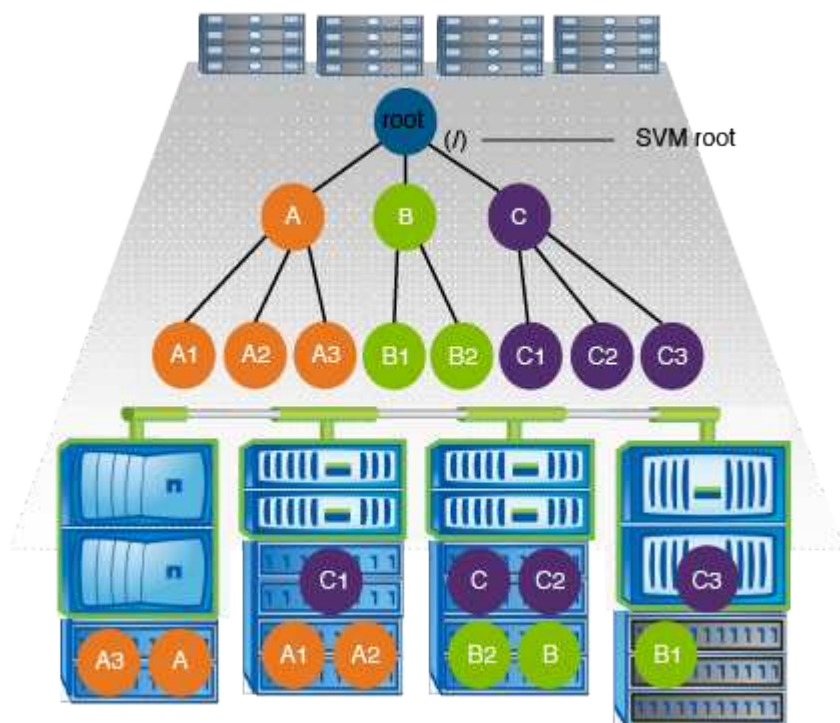


Par exemple, une configuration de jonction de volume typique avec l'architecture de namespace ci-dessus peut ressembler à la configuration suivante, où tous les volumes sont reliés sous le point d'insertion unique, qui est un répertoire nommé « `data` » :

| Vserver | Volume   | Junction Active | Junction Path     | Junction Path Source |
|---------|----------|-----------------|-------------------|----------------------|
| vs1     | corp1    | true            | /data/dir1/corp1  | RW_volume            |
| vs1     | corp2    | true            | /data/dir1/corp2  | RW_volume            |
| vs1     | data1    | true            | /data/data1       | RW_volume            |
| vs1     | eng1     | true            | /data/data1/eng1  | RW_volume            |
| vs1     | eng2     | true            | /data/data1/eng2  | RW_volume            |
| vs1     | sales    | true            | /data/data1/sales | RW_volume            |
| vs1     | vol1     | true            | /data/vol1        | RW_volume            |
| vs1     | vol2     | true            | /data/vol2        | RW_volume            |
| vs1     | vol3     | true            | /data/vol3        | RW_volume            |
| vs1     | vs1_root | -               | /                 | -                    |

### Espace de noms avec plusieurs arborescences ramifiées

Une architecture avec plusieurs arbres ramifiés a plusieurs points d'insertion à la racine du namespace du SVM. Les points d'insertion peuvent être des volumes ou des répertoires sous la racine. Tous les autres volumes sont montés aux points de jonction sous les points d'insertion (qui peuvent être des volumes ou des répertoires).

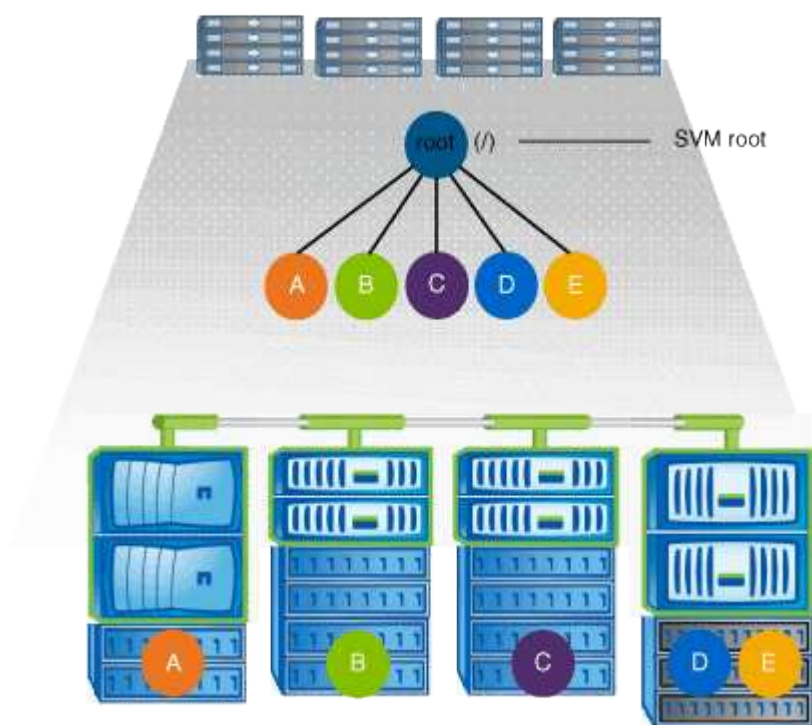


Par exemple, une configuration de jonction de volume standard avec l'architecture de namespace ci-dessus peut ressembler à la configuration suivante, où il existe trois points d'insertion pour le volume racine de la SVM. Deux points d'insertion sont des répertoires nommés "data" et "projets". Un point d'insertion est un volume relié par jonction nommé « audit » :

| Vserver | Volume      | Junction Active | Junction Path      | Junction Path Source |
|---------|-------------|-----------------|--------------------|----------------------|
| vs1     | audit       | true            | /audit             | RW_volume            |
| vs1     | audit_logs1 | true            | /audit/logs1       | RW_volume            |
| vs1     | audit_logs2 | true            | /audit/logs2       | RW_volume            |
| vs1     | audit_logs3 | true            | /audit/logs3       | RW_volume            |
| vs1     | eng         | true            | /data/eng          | RW_volume            |
| vs1     | mktg1       | true            | /data/mktg1        | RW_volume            |
| vs1     | mktg2       | true            | /data/mktg2        | RW_volume            |
| vs1     | project1    | true            | /projects/project1 | RW_volume            |
| vs1     | project2    | true            | /projects/project2 | RW_volume            |
| vs1     | vs1_root    | -               | /                  | -                    |

### Espace de noms avec plusieurs volumes autonomes

Dans une architecture avec des volumes autonomes, chaque volume a un point d'insertion à la racine de l'espace de noms SVM ; cependant, le volume n'est pas relié par jonction sous un autre volume. Chaque volume a un chemin unique, avec une jonction directe sous la racine ou sous un répertoire sous la racine.



Par exemple, une configuration de jonction de volume standard avec l'architecture de l'espace de noms ci-dessus peut ressembler à la configuration suivante, où il existe cinq points d'insertion pour le volume racine de la SVM, avec chaque point d'insertion représentant un chemin vers un volume.

| Vserver | Volume   | Junction |           | Junction Path | Junction Source |
|---------|----------|----------|-----------|---------------|-----------------|
|         |          | Active   |           |               |                 |
| vs1     | eng      | true     | /eng      |               | RW_volume       |
| vs1     | mktg     | true     | /vol/mktg |               | RW_volume       |
| vs1     | project1 | true     | /project1 |               | RW_volume       |
| vs1     | project2 | true     | /project2 |               | RW_volume       |
| vs1     | sales    | true     | /sales    |               | RW_volume       |
| vs1     | vs1_root | -        | /         |               | -               |

## Comment ONTAP contrôle l'accès aux fichiers

### Présentation des contrôles d'accès aux fichiers par ONTAP

ONTAP contrôle l'accès aux fichiers en fonction des restrictions basées sur l'authentification et les fichiers que vous avez spécifiées.

Lorsqu'un client se connecte au système de stockage pour accéder aux fichiers, ONTAP doit effectuer deux tâches :

- Authentification

ONTAP doit authentifier le client en vérifiant l'identité avec une source de confiance. De plus, le type d'authentification du client est une méthode qui peut être utilisée pour déterminer si un client peut accéder aux données lors de la configuration des export policies (facultatif pour CIFS).

- Autorisation

ONTAP doit autoriser l'utilisateur en comparant les informations d'identification de l'utilisateur avec les autorisations configurées sur le fichier ou le répertoire et en déterminant le type d'accès à fournir, le cas échéant.

Pour gérer correctement le contrôle d'accès aux fichiers, ONTAP doit communiquer avec des services externes tels que des serveurs NIS, LDAP et Active Directory. La configuration d'un système de stockage pour l'accès aux fichiers via CIFS ou NFS nécessite la configuration des services appropriés, en fonction de votre environnement dans ONTAP.

### Restrictions basées sur l'authentification

En cas de restrictions basées sur l'authentification, vous pouvez spécifier les ordinateurs clients et les utilisateurs autorisés à se connecter à la machine virtuelle de stockage (SVM).

ONTAP prend en charge l'authentification Kerberos depuis des serveurs UNIX et Windows.

### Restrictions basées sur des fichiers

ONTAP évalue trois niveaux de sécurité pour déterminer si une entité est autorisée à effectuer une action demandée sur les fichiers et répertoires résidant sur une SVM.

L'accès est déterminé par les autorisations effectives après évaluation des trois niveaux de sécurité.

Tout objet de stockage peut contenir jusqu'à trois types de couches de sécurité :

- Sécurité des exportations (NFS) et des partages (SMB)

La sécurité des exportations et des partages s'applique à l'accès client à une exportation NFS ou à un partage SMB donné. Les utilisateurs disposant de privilèges d'administration peuvent gérer la sécurité au niveau de l'exportation et du partage à partir des clients SMB et NFS.

- Sécurité des fichiers et répertoires Access Guard du niveau de stockage

La sécurité Access Guard du niveau de stockage s'applique aux accès des clients SMB et NFS pour les volumes SVM. Seules les autorisations d'accès NTFS sont prises en charge. Pour que ONTAP puisse effectuer des vérifications de sécurité sur les utilisateurs UNIX afin d'accéder aux données sur les volumes pour lesquels Storage-Level Access Guard a été appliqué, l'utilisateur UNIX doit mapper un utilisateur Windows sur le SVM propriétaire du volume.



Si vous affichez les paramètres de sécurité d'un fichier ou d'un répertoire à partir d'un client NFS ou SMB, vous ne verrez pas la sécurité de Storage-Level Access Guard. La sécurité Access Guard au niveau du stockage ne peut pas être révoquée d'un client, même par un administrateur système (Windows ou UNIX).

- Sécurité native au niveau des fichiers NTFS, UNIX et NFSv4

La sécurité native au niveau du fichier existe sur le fichier ou le répertoire qui représente l'objet de stockage. Vous pouvez définir la sécurité au niveau des fichiers à partir d'un client. Les autorisations liées aux fichiers sont efficaces, que SMB ou NFS soit utilisé pour accéder aux données.

## Comment ONTAP gère l'authentification client NFS

### Comment ONTAP gère l'authentification client NFS

Les clients NFS doivent être authentifiés correctement avant que leur système puisse accéder aux données sur la SVM. ONTAP authentifie les clients en comparant leurs informations d'identification UNIX aux services de nom que vous configurez.

Lorsqu'un client NFS se connecte au SVM, ONTAP obtient les identifiants UNIX pour l'utilisateur en cochant différents services de noms selon la configuration des services de noms du SVM. ONTAP peut vérifier les informations d'identification des comptes UNIX locaux, des domaines NIS et des domaines LDAP. Au moins l'un d'entre eux doit être configuré de manière à ce que ONTAP puisse authentifier l'utilisateur avec succès. Vous pouvez spécifier plusieurs services de noms et l'ordre dans lequel ONTAP les recherche.

Dans un environnement NFS pur avec des styles de sécurité de volume UNIX, cette configuration suffit à authentifier et à fournir l'accès approprié aux fichiers pour un utilisateur connecté à partir d'un client NFS.

Si vous utilisez des styles de sécurité de volumes mixtes, NTFS ou Unified, ONTAP doit obtenir un nom d'utilisateur SMB pour l'utilisateur UNIX pour l'authentification avec un contrôleur de domaine Windows. Cela peut se produire soit en mappant des utilisateurs individuels à l'aide de comptes UNIX locaux ou de domaines LDAP, soit en utilisant un utilisateur SMB par défaut. Vous pouvez spécifier le nom des services que ONTAP recherche dans l'ordre ou spécifier un utilisateur SMB par défaut.

ONTAP utilise les services de noms pour obtenir des informations sur les utilisateurs et les clients. ONTAP utilise ces informations pour authentifier les utilisateurs qui accèdent aux données sur ou administrent le système de stockage, et mapper les identifiants des utilisateurs dans un environnement mixte.

Lorsque vous configurez le système de stockage, vous devez spécifier les services de nom que vous souhaitez que ONTAP utilise pour obtenir les identifiants utilisateur pour l'authentification. ONTAP prend en charge les noms suivants :

- Utilisateurs locaux (fichier)
- Domaines NIS externes (NIS)
- Domaines LDAP externes (LDAP)

Vous utilisez le `vserver services name-service ns-switch` Famille de commandes afin de configurer les SVM avec les sources pour rechercher les informations relatives au réseau et l'ordre dans lequel les rechercher. Ces commandes fournissent l'équivalent des fonctionnalités de `/etc/nsswitch.conf` Fichier sur les systèmes UNIX.

Lorsqu'un client NFS se connecte au SVM, ONTAP vérifie les services de nom spécifiés pour obtenir les informations d'identification UNIX pour l'utilisateur. Si les services de nom sont correctement configurés et que ONTAP peut obtenir les informations d'identification UNIX, ONTAP authentifie l'utilisateur avec succès.

Dans un environnement avec des styles de sécurité mixtes, ONTAP peut avoir à mapper les informations d'identification de l'utilisateur. Vous devez configurer les services de noms de manière appropriée pour votre environnement afin que ONTAP puisse correctement mapper les identifiants des utilisateurs.

ONTAP utilise également des services de noms pour l'authentification des comptes d'administrateur des SVM. Vous devez garder cela à l'esprit lors de la configuration ou de la modification du commutateur de service de nom afin d'éviter toute désactivation accidentelle de l'authentification pour les comptes d'administrateur SVM. Pour plus d'informations sur les utilisateurs d'administration des SVM, voir ["Authentification de l'administrateur et RBAC"](#).

### Comment ONTAP permet aux clients NFS d'accéder aux fichiers SMB

ONTAP utilise la sémantique de sécurité du système de fichiers NTFS (Windows NT File System) pour déterminer si un utilisateur UNIX, sur un client NFS, a accès à un fichier avec des autorisations NTFS.

Pour ce faire, ONTAP convertit l'ID utilisateur UNIX (UID) de l'utilisateur en informations d'identification SMB, puis utilise les informations d'identification SMB pour vérifier que l'utilisateur dispose des droits d'accès au fichier. Un identifiant SMB se compose d'un identificateur de sécurité principal (SID), généralement le nom d'utilisateur Windows de l'utilisateur, et d'un ou plusieurs SID de groupe qui correspondent à des groupes Windows dont l'utilisateur est membre.

Le temps ONTAP nécessaire à la conversion de l'UID UNIX en identifiants SMB peut être de plusieurs dizaines de millisecondes à des centaines de millisecondes, car le processus implique de contacter un contrôleur de domaine. ONTAP mappe l'UID sur les identifiants SMB et entre le mappage dans un cache d'identifiants afin de réduire le temps de vérification provoqué par la conversion.

Lorsqu'un utilisateur NFS demande l'accès aux exports NFS sur le système de stockage, ONTAP doit récupérer les identifiants de l'utilisateur à partir de serveurs de noms externes ou de fichiers locaux afin de l'authentifier. ONTAP stocke ensuite ces informations d'identification dans un cache d'informations d'identification interne pour référence ultérieure. Il est donc essentiel de comprendre le fonctionnement des caches d'identifiants NFS pour gérer les problèmes de performance et d'accès qui peuvent survenir.

Sans le cache des informations d'identification, ONTAP devra interroger les services de noms chaque fois qu'un utilisateur NFS a demandé l'accès. Sur un système de stockage surchargé auquel de nombreux utilisateurs accèdent, cela peut rapidement entraîner des problèmes de performance graves, entraînant des retards non désirés ou même des dénis de l'accès client NFS.

Avec le cache des informations d'identification, ONTAP récupère les informations d'identification de l'utilisateur, puis les stocke pendant un délai prédéterminé pour un accès rapide et facile en cas d'envoi d'une autre demande par le client NFS. Cette méthode offre les avantages suivants :

- Il facilite la charge du système de stockage en gérant moins de requêtes vers des serveurs de noms externes (par exemple NIS ou LDAP).
- Il facilite la charge sur les serveurs de noms externes en leur envoyant moins de demandes.
- Il accélère l'accès des utilisateurs en éliminant le temps d'attente pour obtenir des informations d'identification de sources externes avant que l'utilisateur puisse être authentifié.

ONTAP stocke les informations d'identification positives et négatives dans le cache des informations d'identification. Des informations d'identification positives signifient que l'utilisateur a été authentifié et a accordé l'accès. Les identifiants négatifs signifient que l'utilisateur n'a pas été authentifié et a refusé l'accès.

Par défaut, ONTAP stocke des identifiants positifs pendant 24 heures. Ainsi, après l'authentification initiale d'un utilisateur, ONTAP utilise les identifiants mis en cache pour toutes les demandes d'accès de cet utilisateur pendant 24 heures. Si l'utilisateur demande l'accès après 24 heures, le cycle commence : ONTAP supprime les informations d'identification mises en cache et obtient à nouveau les informations d'identification à partir de la source de service de noms appropriée. Si les informations d'identification ont été modifiées sur le serveur de noms au cours des 24 dernières heures, ONTAP met en cache les informations d'identification mises à jour pour les 24 prochaines heures.

Par défaut, ONTAP stocke les informations d'identification négatives pendant deux heures. Ainsi, après avoir initialement refusé l'accès à un utilisateur, ONTAP continue à refuser toute demande d'accès à cet utilisateur pendant deux heures. Si l'utilisateur demande l'accès au bout de 2 heures, le cycle commence : ONTAP obtient à nouveau les informations d'identification à partir de la source de service de noms appropriée. Si les informations d'identification ont été modifiées sur le serveur de noms au cours des deux heures précédentes, ONTAP met en cache les informations d'identification mises à jour pour les deux heures suivantes.

## Création et gestion des volumes de données dans les espaces de noms NAS

### Créez des volumes de données avec des points de jonction spécifiés

Vous pouvez spécifier le point de jonction lorsque vous créez un volume de données. Le volume ainsi obtenu est automatiquement monté au point de jonction et est immédiatement disponible pour la configuration pour l'accès NAS.



## Avant de commencer

- L'agrégat dans lequel vous souhaitez créer le volume doit déjà exister.
- À partir de ONTAP 9.13.1, vous pouvez créer des volumes dont l'analyse de la capacité et le suivi des activités sont activés. Pour activer le suivi de la capacité ou des activités, exécutez le `volume create` commande avec `-analytics-state` ou `-activity-tracking-state` réglé sur `on`.

Pour en savoir plus sur l'analyse de la capacité et le suivi des activités, reportez-vous à la section "[Activez l'analyse du système de fichiers](#)".



Les caractères suivants ne peuvent pas être utilisés dans le chemin de jonction : \* # " > < | ? \

+

De plus, la longueur du chemin de jonction ne peut pas dépasser 255 caractères.

## Étapes

1. Créer le volume avec un point de jonction :

```
volume create -vserver vs1 -volume volume_name -aggregate
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path junction_path
```

Le chemin de jonction doit commencer par la racine (/) et peut contenir à la fois des répertoires et des volumes reliés. Il n'est pas nécessaire que la Junction path contienne le nom du volume. Les Junction paths sont indépendants du nom du volume.

La spécification d'un style de sécurité de volume est facultative. Si vous ne spécifiez pas de style de sécurité, ONTAP crée le volume avec le même style de sécurité que celui appliqué au volume racine de la machine virtuelle de stockage (SVM). Cependant, le style de sécurité du volume racine n'est peut-être pas celui que vous souhaitez appliquer au volume de données que vous créez. Il est recommandé de spécifier le style de sécurité lors de la création du volume afin de minimiser les problèmes d'accès aux fichiers difficiles à résoudre.

Le chemin de jonction n'est pas sensible à la casse ; /ENG est identique à /eng. Si vous créez un partage CIFS, Windows traite le chemin de jonction comme s'il est sensible à la casse. Par exemple, si la jonction est de /ENG, Le chemin d'un partage SMB doit commencer par /ENG`pas `/eng.

De nombreux paramètres facultatifs peuvent être utilisés pour personnaliser un volume de données. Pour en savoir plus, consultez les pages de manuel pour le `volume create` commande.

2. Vérifier que le volume a été créé avec le point de jonction souhaité :

```
volume show -vserver vs1 -volume volume_name -junction
```

## Exemple

L'exemple suivant crée un volume nommé « maison 4 » situé sur le SVM vs1 qui a une Junction path /eng/home:



```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -volume home4 -junction
```

| Vserver | Volume | Active | Junction Path | Junction Path Source |
|---------|--------|--------|---------------|----------------------|
| vs1     | home4  | true   | /eng/home     | RW_volume            |

## Créez des volumes de données sans spécifier de points de jonction

Vous pouvez créer un volume de données sans spécifier de point de jonction. Le volume résultant n'est pas monté automatiquement et n'est pas disponible pour configurer l'accès NAS. Vous devez monter le volume avant de configurer les partages SMB ou les exportations NFS pour ce volume.

### Avant de commencer

- L'agrégat dans lequel vous souhaitez créer le volume doit déjà exister.
- À partir de ONTAP 9.13.1, vous pouvez créer des volumes dont l'analyse de la capacité et le suivi des activités sont activés. Pour activer le suivi de la capacité ou des activités, exécutez le `volume create` commande avec `-analytics-state` ou `-activity-tracking-state` réglés sur `on`.

Pour en savoir plus sur l'analyse de la capacité et le suivi des activités, reportez-vous à la section ["Activez l'analyse du système de fichiers"](#).

### Étapes

1. Créer le volume sans point de jonction en utilisant la commande suivante :

```
volume create -vserver vserver_name -volume volume_name -aggregate
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed}
```

La spécification d'un style de sécurité de volume est facultative. Si vous ne spécifiez pas de style de sécurité, ONTAP crée le volume avec le même style de sécurité que celui appliqué au volume racine de la machine virtuelle de stockage (SVM). Toutefois, le style de sécurité du volume racine n'est peut-être pas celui que vous souhaitez appliquer au volume de données. Il est recommandé de spécifier le style de sécurité lors de la création du volume afin de minimiser les problèmes d'accès aux fichiers difficiles à résoudre.

De nombreux paramètres facultatifs peuvent être utilisés pour personnaliser un volume de données. Pour en savoir plus, consultez les pages de manuel pour le `volume create` commande.

2. Vérifier que le volume a été créé sans point de jonction :

```
volume show -vserver vserver_name -volume volume_name -junction
```

### Exemple

L'exemple suivant crée un volume nommé « sales » situé sur la SVM vs1 qui n'est pas monté à un point de jonction :

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

| Vserver | Volume   | Junction |  | Junction Path | Junction Path Source |
|---------|----------|----------|--|---------------|----------------------|
|         |          | Active   |  |               |                      |
| vs1     | data     | true     |  | /data         | RW_volume            |
| vs1     | home4    | true     |  | /eng/home     | RW_volume            |
| vs1     | vs1_root | -        |  | /             | -                    |
| vs1     | sales    | -        |  | -             | -                    |

## Montez ou démontez les volumes existants dans l'espace de noms NAS

Un volume doit être monté sur le namespace NAS avant de pouvoir configurer l'accès des clients NAS aux données contenues dans les volumes SVM (Storage Virtual machine). Vous pouvez monter un volume sur un point de jonction s'il n'est pas actuellement monté. Vous pouvez également démonter des volumes.

### Description de la tâche

Si vous démontez et mettez un volume hors ligne, toutes les données du point de jonction, y compris les données des volumes dont les points de jonction se trouvent dans l'espace de noms du volume non monté, sont inaccessibles aux clients NAS.



Pour interrompre l'accès client NAS à un volume, il ne suffit pas de démonter le volume. Vous devez mettre le volume hors ligne ou prendre d'autres mesures pour vous assurer que les caches de descripteur de fichier côté client sont invalidés. Pour plus d'informations, consultez l'article suivant de la base de connaissances :

["Les clients NFSv3 ont toujours accès à un volume après avoir été supprimés du namespace dans ONTAP"](#)

Lorsque vous démontez et mettez hors ligne un volume, les données ne sont pas perdues au sein du volume. En outre, les règles d'exportation de volume et les partages SMB créés sur le volume ou sur des répertoires et des points de jonction au sein du volume démonté sont conservés. Si vous remontez le volume démonté, les clients NAS peuvent accéder aux données contenues dans le volume à l'aide des règles d'exportation et des partages SMB existants.

### Étapes

1. Effectuez l'action souhaitée :

| Les fonctions que vous recherchez... | Entrez les commandes...                                                                                                                                                |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Montez un volume                     | <code>volume mount -vserver <i>svm_name</i> -volume <i>volume_name</i> -junction-path <i>junction_path</i></code>                                                      |
| Démonter un volume                   | <code>volume unmount -vserver <i>svm_name</i> -volume <i>volume_name</i></code><br><br><code>volume offline -vserver <i>svm_name</i> -volume <i>volume_name</i></code> |

## 2. Vérifiez que le volume est dans l'état de montage souhaité :

```
volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active
```

### Exemples

L'exemple suivant monte un volume nommé « ventes » situé sur la SVM « vs1 » au point de jonction « /ventes » :

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active
```

| vserver | volume | state  | junction-path | junction-active |
|---------|--------|--------|---------------|-----------------|
| vs1     | data   | online | /data         | true            |
| vs1     | home4  | online | /eng/home     | true            |
| vs1     | sales  | online | /sales        | true            |

L'exemple suivant démonte et met hors ligne un volume nommé « data » situé sur le SVM « vs1 » :

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-active
```

| vserver | volume | state   | junction-path | junction-active |
|---------|--------|---------|---------------|-----------------|
| vs1     | data   | offline | -             | -               |
| vs1     | home4  | online  | /eng/home     | true            |
| vs1     | sales  | online  | /sales        | true            |

**Affiche les informations sur le montage du volume et le point de jonction**

Vous pouvez afficher des informations sur les volumes montés pour les SVM et les points de jonction auxquels les volumes sont montés. Vous pouvez également déterminer quels volumes ne sont pas montés sur un point de jonction. Vous pouvez utiliser ces informations pour comprendre et gérer votre namespace SVM.

**Étape**

- 1. Effectuez l'action souhaitée :

| Si vous voulez afficher...                                                   | Entrez la commande...                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Récapitulatif des informations sur les volumes montés et démontés sur le SVM | <code>volume show -vserver vs1 -junction</code>                                                                                                                                                                                                                                                                                                  |
| Informations détaillées sur les volumes montés et démontés sur le SVM        | <code>volume show -vserver vs1 -volume volume_name -instance</code>                                                                                                                                                                                                                                                                              |
| Informations spécifiques sur les volumes montés et démontés sur le SVM       | <div>a. Si nécessaire, vous pouvez afficher des champs valides pour l' <code>-fields</code> paramètre via la commande suivante :<br/><code>volume show -fields ?</code></div> <div>b. Afficher les informations souhaitées à l'aide de l' <code>-fields</code> paramètre :<br/><code>volume show -vserver vs1 -fields fieldname,...</code></div> |

**Exemples**

L'exemple suivant affiche un récapitulatif des volumes montés et démontés sur le SVM vs1 :

```
cluster1::> volume show -vserver vs1 -junction
```

| Vserver | Volume   | Active | Junction Path | Junction Path Source |
|---------|----------|--------|---------------|----------------------|
| vs1     | data     | true   | /data         | RW_volume            |
| vs1     | home4    | true   | /eng/home     | RW_volume            |
| vs1     | vs1_root | -      | /             | -                    |
| vs1     | sales    | true   | /sales        | RW_volume            |

L'exemple suivant affiche des informations sur les champs spécifiés pour les volumes situés sur le SVM vs2 :

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume aggregate size state type security-style junction-path
junction-parent node

vs2 data1 aggr3 2GB online RW unix -
node3
vs2 data2 aggr3 1GB online RW ntfs /data2
vs2_root node3
vs2 data2_1 aggr3 8GB online RW ntfs /data2/d2_1
data2 node3
vs2 data2_2 aggr3 8GB online RW ntfs /data2/d2_2
data2 node3
vs2 pubs aggr1 1GB online RW unix /publications
vs2_root node1
vs2 images aggr3 2TB online RW ntfs /images
vs2_root node3
vs2 logs aggr1 1GB online RW unix /logs
vs2_root node1
vs2 vs2_root aggr3 1GB online RW ntfs /
node3
```

## Configurer les styles de sécurité

### Comment les styles de sécurité affectent l'accès aux données

#### Styles de sécurité et leurs effets

Il existe quatre styles de sécurité différents : UNIX, NTFS, mixte et unifié. Chaque style de sécurité a un effet différent sur la façon dont les autorisations sont traitées pour les données. Vous devez comprendre les différents effets pour vous assurer que vous sélectionnez le style de sécurité approprié à vos fins.

Il est important de comprendre que les styles de sécurité ne déterminent pas quels types de clients peuvent ou ne peuvent pas accéder aux données. Les styles de sécurité déterminent uniquement le type d'autorisations que ONTAP utilise pour contrôler l'accès aux données et le type de client pouvant modifier ces autorisations.

Par exemple, si un volume utilise le style de sécurité UNIX, les clients SMB peuvent toujours accéder aux données (à condition qu'ils s'authentifient et autorisent correctement) en raison de la nature multiprotocole de ONTAP. Toutefois, ONTAP utilise des autorisations UNIX que seuls les clients UNIX peuvent modifier à l'aide d'outils natifs.

| Style de sécurité                                                                          | Clients pouvant modifier des autorisations | Autorisations que les clients peuvent utiliser | Un style de sécurité efficace | Clients pouvant accéder aux fichiers |
|--------------------------------------------------------------------------------------------|--------------------------------------------|------------------------------------------------|-------------------------------|--------------------------------------|
| UNIX                                                                                       | NFS                                        | Bits de mode NFSv3                             | UNIX                          | NFS et SMB                           |
|                                                                                            |                                            | Listes de contrôle d'accès NFSv4.x             |                               |                                      |
| NTFS                                                                                       | PME                                        | ALC NTFS                                       | NTFS                          |                                      |
| Mixte                                                                                      | NFS ou SMB                                 | Bits de mode NFSv3                             | UNIX                          |                                      |
|                                                                                            |                                            | ACL.NFSv4                                      |                               |                                      |
|                                                                                            |                                            | ALC NTFS                                       | NTFS                          |                                      |
| Unifiée<br>(Pour Infinite volumes uniquement, dans ONTAP 9.4 et les versions antérieures.) | NFS ou SMB                                 | Bits de mode NFSv3                             | UNIX                          |                                      |
|                                                                                            |                                            | ACL NFSv4.1                                    |                               |                                      |
|                                                                                            |                                            | ALC NTFS                                       | NTFS                          |                                      |

Les volumes FlexVol prennent en charge les styles de sécurité UNIX, NTFS et mixte. Lorsque le style de sécurité est mixte ou unifié, les autorisations effectives dépendent du type de client qui a modifié les autorisations pour la dernière fois, car les utilisateurs définissent le style de sécurité sur une base individuelle. Si le dernier client ayant modifié des autorisations était un client NFSv3, les autorisations sont des bits en mode UNIX NFSv3. Si le dernier client était un client NFSv4, les autorisations sont définies comme listes de contrôle d'accès NFSv4. Si le dernier client était un client SMB, les autorisations sont des listes de contrôle d'accès Windows NTFS.

La méthode de sécurité unifiée est uniquement disponible avec des volumes infinis, qui ne sont plus pris en charge dans ONTAP 9.5 et versions ultérieures. Pour plus d'informations, voir [Présentation de la gestion des volumes FlexGroup](#).

À partir de ONTAP 9.2, le `show-effective-permissions` paramètre au `vserver security file-directory` La commande vous permet d'afficher les autorisations effectives accordées à un utilisateur Windows ou UNIX sur le chemin d'accès au fichier ou au dossier spécifié. De plus, le paramètre facultatif `-share-name` vous permet d'afficher l'autorisation de partage effective.



ONTAP définit au départ certaines autorisations de fichier par défaut. Par défaut, le style de sécurité effectif sur toutes les données des volumes de style de sécurité UNIX, mixte et unifié est UNIX et le type d'autorisation effectif est bits de mode UNIX (0755 sauf indication contraire) jusqu'à ce qu'un client soit configuré comme autorisé par le style de sécurité par défaut. Par défaut, le style de sécurité effectif sur toutes les données des volumes de style de sécurité NTFS est NTFS et dispose d'une liste de contrôle d'accès permettant un contrôle total à tous.

#### Où et quand définir les styles de sécurité

Les styles de sécurité peuvent être définis sur les volumes FlexVol (volumes root ou de données) et les qtrees. Les styles de sécurité peuvent être définis manuellement au moment de la création, hérités automatiquement ou modifiés ultérieurement.

## Choisissez le style de sécurité à utiliser sur les SVM

Pour vous aider à choisir le style de sécurité à utiliser sur un volume, vous devez tenir compte de deux facteurs. Le facteur principal est le type d'administrateur qui gère le système de fichiers. Le facteur secondaire désigne le type d'utilisateur ou de service qui accède aux données du volume.

Lorsque vous configurez le style de sécurité sur un volume, vous devez tenir compte des besoins de votre environnement pour vous assurer que vous sélectionnez le meilleur style de sécurité et éviter les problèmes liés à la gestion des autorisations. Vous pouvez décider des considérations suivantes :

| Style de sécurité | Choisissez si...                                                                                                                                                                                                                                                                     |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UNIX              | <ul style="list-style-type: none"><li>• Le système de fichiers est géré par un administrateur UNIX.</li><li>• La plupart des utilisateurs sont des clients NFS.</li><li>• Une application accédant aux données utilise un utilisateur UNIX comme compte de service.</li></ul>        |
| NTFS              | <ul style="list-style-type: none"><li>• Le système de fichiers est géré par un administrateur Windows.</li><li>• La majorité des utilisateurs sont des clients SMB.</li><li>• Une application accédant aux données utilise un utilisateur Windows comme compte de service.</li></ul> |
| Mixte             | <ul style="list-style-type: none"><li>• Le système de fichiers est géré à la fois par les administrateurs et utilisateurs d'UNIX et de Windows, et il se compose de clients NFS et SMB.</li></ul>                                                                                    |

## Fonctionnement de l'héritage du style de sécurité

Si vous ne spécifiez pas le style de sécurité lors de la création d'un nouveau volume FlexVol ou d'un qtree, il hérite de son style de sécurité de différentes manières.

Les styles de sécurité sont hérités de la manière suivante :

- Un volume FlexVol hérite du style de sécurité du volume root de son SVM contenant.
- Un qtree hérite du style de sécurité de son volume FlexVol.
- Un fichier ou un répertoire hérite du style de sécurité de son volume FlexVol ou qtree.

## Comment ONTAP préserve les autorisations UNIX

Lorsque les fichiers d'un volume FlexVol qui disposent actuellement d'autorisations UNIX sont modifiés et enregistrés par des applications Windows, ONTAP peut préserver les autorisations UNIX.

Lorsque des applications sur des clients Windows modifient et enregistrent des fichiers, elles lisent les propriétés de sécurité du fichier, créent un nouveau fichier temporaire, appliquent ces propriétés au fichier temporaire, puis donnent au fichier temporaire le nom du fichier d'origine.

Lorsque les clients Windows effectuent une requête pour les propriétés de sécurité, ils reçoivent une ACL construite qui représente exactement les autorisations UNIX. Le seul but de cette liste de contrôle d'accès

construite est de préserver les autorisations UNIX du fichier lorsque les fichiers sont mis à jour par les applications Windows pour s'assurer que les fichiers résultants ont les mêmes autorisations UNIX. ONTAP ne définit pas d'ACL NTFS à l'aide de la liste de contrôle d'accès construite.

### Gérez les autorisations UNIX à l'aide de l'onglet sécurité Windows

Si vous souhaitez manipuler les autorisations UNIX de fichiers ou de dossiers dans des volumes ou des qtrees de style sécurité mixtes sur des SVM, vous pouvez utiliser l'onglet sécurité sur les clients Windows. Vous pouvez également utiliser des applications qui peuvent interroger et définir des listes de contrôle d'accès Windows.

- **Modification des autorisations UNIX**

Vous pouvez utiliser l'onglet sécurité Windows pour afficher et modifier les autorisations UNIX pour un volume ou qtree de style de sécurité mixte. Si vous utilisez l'onglet principal sécurité Windows pour modifier les autorisations UNIX, vous devez d'abord supprimer l'ACE que vous souhaitez modifier (ceci définit les bits de mode sur 0) avant d'effectuer vos modifications. Vous pouvez également utiliser l'éditeur avancé pour modifier les autorisations.

Si des autorisations de mode sont utilisées, vous pouvez modifier directement les autorisations de mode pour l'UID, le GID et d'autres (tous les autres utilisateurs disposant d'un compte sur l'ordinateur). Par exemple, si l'UID affiché possède des autorisations r-x, vous pouvez modifier les autorisations UID sur rwx.

- **Modification des autorisations UNIX en autorisations NTFS**

Vous pouvez utiliser l'onglet sécurité Windows pour remplacer les objets de sécurité UNIX par des objets de sécurité Windows sur un volume ou qtree de style de sécurité mixte, où les fichiers et les dossiers ont une méthode de sécurité efficace UNIX.

Vous devez d'abord supprimer toutes les entrées d'autorisation UNIX répertoriées pour pouvoir les remplacer par les objets utilisateur et groupe Windows souhaités. Vous pouvez ensuite configurer des listes de contrôle d'accès NTFS sur les objets utilisateur et groupe Windows. En supprimant tous les objets de sécurité UNIX et en ajoutant uniquement des utilisateurs et des groupes Windows à un fichier ou à un dossier dans un volume ou qtree de style de sécurité mixte, vous modifiez le style de sécurité effectif sur le fichier ou le dossier d'UNIX à NTFS.

Lors de la modification des autorisations sur un dossier, le comportement par défaut de Windows consiste à propager ces modifications à tous les sous-dossiers et fichiers. Par conséquent, vous devez modifier le choix de propagation sur le paramètre souhaité si vous ne souhaitez pas propager de modification du style de sécurité à tous les dossiers, sous-dossiers et fichiers enfants.

### Configurer des styles de sécurité sur les volumes root SVM

Il configure la style de sécurité du volume root de la machine virtuelle de stockage (SVM) afin de déterminer le type d'autorisations utilisées pour les données sur le volume root de la SVM.

#### Étapes

1. Utilisez le `vserver create` commande avec `-rootvolume-security-style` paramètre pour définir le style de sécurité.

Les options possibles pour le style de sécurité du volume racine sont `unix`, `ntfs`, ou `mixed`.



2. Afficher et vérifier la configuration, y compris le style de sécurité du volume root du SVM que vous avez créé :

```
vserver show -vserver vserver_name
```

## Configurer des styles de sécurité sur les volumes FlexVol

Configurez le style de sécurité des volumes FlexVol afin de déterminer le type d'autorisations utilisées pour les données sur des volumes FlexVol de la machine virtuelle de stockage (SVM).

### Étapes

1. Effectuez l'une des opérations suivantes :

| Si le volume FlexVol... | Utilisez la commande...                                                                                              |
|-------------------------|----------------------------------------------------------------------------------------------------------------------|
| N'existe pas encore     | <code>volume create</code> et inclure le <code>-security-style</code> paramètre pour spécifier le style de sécurité. |
| Existe déjà             | <code>volume modify</code> et inclure le <code>-security-style</code> paramètre pour spécifier le style de sécurité. |

Les options possibles pour le style de sécurité du volume FlexVol sont `unix`, `ntfs`, ou `mixed`.

Si vous ne spécifiez pas de style de sécurité lors de la création d'un volume FlexVol, le volume hérite du style de sécurité du volume racine.

Pour plus d'informations sur le `volume create` ou `volume modify` commandes, voir ["Gestion du stockage logique"](#).

2. Pour afficher la configuration, en incluant le style de sécurité du volume FlexVol que vous avez créé, entrez la commande suivante :

```
volume show -volume volume_name -instance
```

## Configurer des styles de sécurité sur les qtrees

Vous configurez le style de sécurité du volume qtree afin de déterminer le type d'autorisations utilisées pour les données sur des qtrees.

### Étapes

1. Effectuez l'une des opérations suivantes :

| Si le qtree...      | Utilisez la commande...                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------------------------------|
| N'existe pas encore | <code>volume qtree create</code> et inclure le <code>-security-style</code> paramètre pour spécifier le style de sécurité. |

|             |                                                                                                               |
|-------------|---------------------------------------------------------------------------------------------------------------|
| Existe déjà | volume qtree modify et inclure le <code>-security-style</code> paramètre pour spécifier le style de sécurité. |
|-------------|---------------------------------------------------------------------------------------------------------------|

Les options possibles pour la méthode de sécurité qtree sont `unix`, `ntfs`, ou `mixed`.

Si vous ne spécifiez pas de style de sécurité lors de la création d'un qtree, le style de sécurité par défaut est `mixed`.

Pour plus d'informations sur le `volume qtree create` ou `volume qtree modify` commandes, voir ["Gestion du stockage logique"](#).

2. Pour afficher la configuration, y compris le style de sécurité du qtree que vous avez créé, entrez la commande suivante : `volume qtree show -qtree qtree_name -instance`

## Configurez l'accès aux fichiers à l'aide de NFS

### Configurez l'accès aux fichiers à l'aide de la présentation de NFS

Vous devez suivre un certain nombre d'étapes pour permettre aux clients d'accéder aux fichiers sur des SVM (Storage Virtual machine) à l'aide de NFS. Certaines étapes supplémentaires sont facultatives en fonction de la configuration actuelle de votre environnement.

Pour que les clients puissent accéder aux fichiers sur des SVM via NFS, vous devez effectuer les tâches suivantes :

1. Activer le protocole NFS sur le SVM.

On doit configurer le SVM de façon à permettre l'accès aux données des clients sur NFS.

2. Créer un serveur NFS sur le SVM.

Un serveur NFS est une entité logique du SVM qui permet à la SVM de transmettre des fichiers via NFS. Vous devez créer le serveur NFS et spécifier les versions de protocole NFS que vous souhaitez autoriser.

3. Configurer les export policy sur le SVM.

Vous devez configurer des règles d'exportation pour que les volumes et les qtrees soient disponibles pour les clients.

4. Configurez le serveur NFS avec les paramètres de sécurité appropriés et d'autres paramètres en fonction du réseau et de l'environnement de stockage.

Cette étape peut inclure la configuration de Kerberos, ["NFS sur TLS"](#), LDAP, NIS, mappages de noms et utilisateurs locaux.

### Sécurisation de l'accès NFS à l'aide de règles d'exportation

#### Comment les règles d'exportation contrôlent l'accès des clients aux volumes ou aux qtrees

Les règles d'exportation contiennent une ou plusieurs *export rules* qui traitent chaque

demande d'accès client. Le résultat du processus détermine si le client est refusé ou accordé et quel niveau d'accès. Un export policy avec règles d'export doit exister sur la machine virtuelle de stockage (SVM) afin que les clients puissent accéder aux données.

Vous associez exactement une export policy à chaque volume ou qtree pour configurer l'accès client au volume ou qtree. Le SVM peut contenir plusieurs export policy. Vous pouvez ainsi effectuer les opérations suivantes pour les SVM avec plusieurs volumes ou qtrees :

- Assigner différentes export policy à chaque volume ou qtree du SVM pour le contrôle d'accès client individuel à chaque volume ou qtree du SVM.
- Assigner la même export policy à plusieurs volumes ou qtrees du SVM pour un contrôle d'accès client identique sans avoir à créer une nouvelle export policy pour chaque volume ou qtree.

Si un client effectue une demande d'accès qui n'est pas autorisée par la stratégie d'exportation applicable, la requête échoue et un message d'autorisation est refusé. Si un client ne correspond à aucune règle de l'export policy, l'accès est refusé. Si une export policy est vide, alors tous les accès sont implicitement refusés.

Vous pouvez modifier une export-policy de manière dynamique sur un système exécutant ONTAP.

### **Export policy par défaut pour SVM**

Chaque SVM dispose d'une export policy par défaut qui ne contient aucune règle. Un export policy avec règles doit exister pour que les clients puissent accéder aux données sur la SVM. Chaque volume FlexVol contenu au SVM doit être associé à une export policy.

Lorsque vous créez un SVM, le système de stockage crée automatiquement une export policy par défaut appelée `default` Pour le volume root du SVM. On doit créer une ou plusieurs règles pour l'export policy par défaut avant que les clients puissent accéder aux données sur la SVM. Vous pouvez également créer une export-policy personnalisée avec des règles. Vous pouvez modifier et renommer l'export policy par défaut, mais vous ne pouvez pas supprimer l'export policy par défaut.

Lorsque vous créez un volume FlexVol dans son SVM contenant, le système de stockage crée le volume et associe le volume avec la export policy par défaut pour le volume root du SVM. Par défaut, chaque volume créé au sein du SVM est associé à l'export policy par défaut pour le volume root. Vous pouvez utiliser l'export policy par défaut pour tous les volumes contenus dans le SVM, ou bien créer une export policy unique pour chaque volume. Vous pouvez associer plusieurs volumes à la même export policy.

### **Fonctionnement des règles d'exportation**

Les règles d'exportation sont les éléments fonctionnels d'une export-policy. Les règles d'exportation correspondent aux demandes d'accès client à un volume par rapport à des paramètres spécifiques que vous configurez pour déterminer comment traiter les demandes d'accès client.

Une export-policy doit contenir au moins une règle d'exportation pour permettre l'accès aux clients. Si une export-policy contient plusieurs règles, celles-ci sont traitées dans l'ordre dans lequel elles apparaissent dans l'export-policy. L'ordre des règles est dicté par le numéro d'index des règles. Si une règle correspond à un client, les autorisations de cette règle sont utilisées et aucune autre règle n'est traitée. Si aucune règle ne correspond, l'accès au client est refusé.

Vous pouvez configurer des règles d'exportation pour déterminer les autorisations d'accès client à l'aide des

critères suivants :

- Protocole d'accès aux fichiers utilisé par le client envoyant la requête, par exemple, NFSv4 ou SMB.
- Identifiant client, par exemple, nom d'hôte ou adresse IP.

La taille maximale du `-clientmatch` le champ est composé de 4096 caractères.

- Type de sécurité utilisé par le client pour l'authentification, par exemple Kerberos v5, NTLM ou AUTH\_SYS.

Si une règle spécifie plusieurs critères, le client doit tous les correspondre pour que la règle s'applique.



Depuis ONTAP 9.3, vous pouvez activer la vérification de la configuration des règles d'exportation en tant que tâche d'arrière-plan qui enregistre toutes les violations de règles dans une liste de règles d'erreur. Le `vserver export-policy config-checker` les commandes invoquent le vérificateur et affichent les résultats, que vous pouvez utiliser pour vérifier votre configuration et supprimer des règles erronées de la stratégie.

Les commandes valident uniquement la configuration d'exportation pour les noms d'hôte, les groupes réseau et les utilisateurs anonymes.

### Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La requête d'accès client est envoyée à l'aide du protocole NFSv3 et le client a l'adresse IP 10.1.17.37.

Bien que le protocole d'accès client corresponde, l'adresse IP du client se trouve dans un sous-réseau différent de celui spécifié dans la règle d'exportation. Par conséquent, la correspondance des clients échoue et cette règle ne s'applique pas à ce client.

### Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La requête d'accès client est envoyée via le protocole NFSv4 et le client a l'adresse IP 10.1.16.54.

Le protocole d'accès client correspond et l'adresse IP du client se trouve dans le sous-réseau spécifié. Par conséquent, la correspondance du client a réussi et cette règle s'applique à ce client. Le client obtient un accès en lecture-écriture quel que soit son type de sécurité.

### Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Le client #1 a l'adresse IP 10.1.16.207, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec AUTH\_SYS.

Le protocole d'accès client et l'adresse IP correspondent pour les deux clients. Le paramètre en lecture seule permet l'accès en lecture seule à tous les clients, quel que soit le type de sécurité auquel ils sont authentifiés. Par conséquent, les deux clients bénéficient d'un accès en lecture seule. Cependant, seul le client #1 obtient l'accès en lecture-écriture car il a utilisé le type de sécurité approuvé Kerberos v5 pour s'authentifier. Le client n° 2 ne dispose pas d'un accès en lecture/écriture.

#### Gérez les clients avec un type de sécurité non répertorié

Lorsqu'un client se présente avec un type de sécurité qui n'est pas répertorié dans un paramètre d'accès d'une règle d'exportation, vous pouvez soit refuser l'accès au client, soit le mapper à l'ID utilisateur anonyme à la place de l'aide de l'option `none` dans le paramètre d'accès.

Un client peut se présenter avec un type de sécurité qui n'est pas répertorié dans un paramètre d'accès car il a été authentifié avec un type de sécurité différent ou n'a pas été authentifié du tout (type de sécurité `AUTH_NONE`). Par défaut, l'accès au client est automatiquement refusé. Toutefois, vous pouvez ajouter l'option `none` au paramètre d'accès. Par conséquent, les clients dont le style de sécurité n'est pas répertorié sont mappés sur l'ID utilisateur anonyme. Le `-anon` Paramètre détermine quel ID utilisateur est attribué à ces clients. ID utilisateur spécifié pour le `-anon` le paramètre doit être un utilisateur valide configuré avec des autorisations appropriées pour l'utilisateur anonyme.

Valeurs valides pour le `-anon` plage de paramètres de 0 à 65535.

| ID utilisateur attribué à <code>-anon</code> | Traitement des demandes d'accès client résultant                                                                                                                                    |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0 - 65533                                    | La demande d'accès client est mappée à l'ID utilisateur anonyme et obtient l'accès en fonction des autorisations configurées pour cet utilisateur.                                  |
| 65534                                        | La demande d'accès client est mappée à l'utilisateur personne et obtient l'accès en fonction des autorisations configurées pour cet utilisateur. Il s'agit de la valeur par défaut. |

| ID utilisateur attribué à <code>-anon</code> | Traitement des demandes d'accès client résultant                                                                                                                                                                                                                                                                                         |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 65535                                        | La demande d'accès de n'importe quel client est refusée lorsqu'elle est mappée à cet ID et que le client se présente avec le type de sécurité <code>AUTH_NONE</code> . La demande d'accès des clients avec l'ID utilisateur 0 est refusée lorsqu'elle est mappée à cet ID et que le client se présente avec tout autre type de sécurité. |

Lorsque vous utilisez l'option `none`, il est important de se rappeler que le paramètre lecture seule est traité en premier. Lors de la configuration des règles d'exportation pour les clients dont les types de sécurité ne sont pas répertoriés, prenez en compte les consignes suivantes :

| La lecture seule inclut <code>none</code> | Lecture-écriture incluse <code>none</code> | Accès résultant pour les clients avec des types de sécurité non répertoriés |
|-------------------------------------------|--------------------------------------------|-----------------------------------------------------------------------------|
| Non                                       | Non                                        | Refusée                                                                     |
| Non                                       | Oui.                                       | Refusé car la lecture seule est traitée en premier                          |
| Oui.                                      | Non                                        | Lecture seule comme anonyme                                                 |
| Oui.                                      | Oui.                                       | Lecture-écriture comme anonyme                                              |

### Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

Le client #1 a l'adresse IP 10.1.16.207, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec `AUTH_SYS`.

Le client #3 a l'adresse IP 10.1.16.234, envoie une demande d'accès à l'aide du protocole NFSv3 et ne s'authentifie pas (ce qui signifie le type de sécurité `AUTH_NONE`).

Le protocole d'accès client et l'adresse IP correspondent pour les trois clients. Le paramètre lecture seule permet l'accès en lecture seule aux clients avec leur propre ID utilisateur authentifié auprès de `AUTH_SYS`. Le paramètre lecture seule permet l'accès en lecture seule en tant qu'utilisateur anonyme avec l'ID utilisateur 70 aux clients authentifiés à l'aide de n'importe quel autre type de sécurité. Le paramètre lecture-écriture permet

l'accès en lecture-écriture à n'importe quel type de sécurité, mais s'applique uniquement aux clients déjà filtrés par la règle en lecture seule.

Par conséquent, les clients n° 1 et n° 3 bénéficient de l'accès en lecture-écriture uniquement en tant qu'utilisateur anonyme avec l'ID utilisateur 70. Le client #2 obtient un accès en lecture-écriture avec son propre ID utilisateur.

### Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

Le client #1 a l'adresse IP 10.1.16.207, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec AUTH\_SYS.

Le client #3 a l'adresse IP 10.1.16.234, envoie une demande d'accès à l'aide du protocole NFSv3 et ne s'authentifie pas (ce qui signifie le type de sécurité AUTH\_NONE).

Le protocole d'accès client et l'adresse IP correspondent pour les trois clients. Le paramètre lecture seule permet l'accès en lecture seule aux clients avec leur propre ID utilisateur authentifié auprès de AUTH\_SYS. Le paramètre lecture seule permet l'accès en lecture seule en tant qu'utilisateur anonyme avec l'ID utilisateur 70 aux clients authentifiés à l'aide de n'importe quel autre type de sécurité. Le paramètre lecture-écriture permet l'accès en lecture-écriture uniquement en tant qu'utilisateur anonyme.

Par conséquent, les clients #1 et le client #3 obtiennent un accès en lecture-écriture uniquement en tant qu'utilisateur anonyme avec l'ID utilisateur 70. Le client #2 obtient un accès en lecture seule avec son propre ID utilisateur, mais il est refusé l'accès en lecture-écriture.

### Comment les types de sécurité déterminent les niveaux d'accès client

Le type de sécurité auquel le client s'est authentifié joue un rôle particulier dans les règles d'exportation. Vous devez comprendre la manière dont le type de sécurité détermine les niveaux d'accès du client à un volume ou à un qtree.

Les trois niveaux d'accès possibles sont les suivants :

1. Lecture seule
2. Lecture-écriture
3. Super-utilisateur (pour les clients ayant l'ID utilisateur 0)

Dans la mesure où le niveau d'accès par type de sécurité est évalué dans cet ordre, vous devez respecter les règles suivantes lors de la construction de paramètres de niveau d'accès dans les règles d'exportation :

| Pour qu'un client puisse obtenir le niveau d'accès... | Ces paramètres d'accès doivent correspondre au type de sécurité du client...                                   |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Lecture seule normale par l'utilisateur               | Lecture seule ( <code>-rorule</code> )                                                                         |
| Lecture-écriture utilisateur normale                  | Lecture seule ( <code>-rorule</code> ) et lecture-écriture ( <code>-rwrule</code> )                            |
| Super-utilisateur en lecture seule                    | Lecture seule ( <code>-rorule</code> ) et <code>-superuser</code>                                              |
| Super-utilisateur lecture-écriture                    | Lecture seule ( <code>-rorule</code> ) et lecture-écriture ( <code>-rwrule</code> ) et <code>-superuser</code> |

Les types de sécurité suivants sont valides pour chacun de ces trois paramètres d'accès :

- `any`
- `none`
- `never`

Ce type de sécurité n'est pas valide pour une utilisation avec `-superuser` paramètre.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Lorsque vous faites correspondre le type de sécurité d'un client à chacun des trois paramètres d'accès, trois résultats sont possibles :

| Si le type de sécurité du client...                                                                  | Ensuite, le client...                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Correspond à celui spécifié dans le paramètre d'accès.                                               | Obtient l'accès à ce niveau avec son propre ID utilisateur.                                                                                                                       |
| Ne correspond pas à celui spécifié, mais le paramètre d'accès inclut l'option <code>none</code> .    | Obtient l'accès pour ce niveau, mais en tant qu'utilisateur anonyme avec l'ID utilisateur spécifié par le <code>-anon</code> paramètre.                                           |
| Ne correspond pas à celui spécifié et le paramètre d'accès n'inclut pas l'option <code>none</code> . | Ne dispose d'aucun accès pour ce niveau. cela ne s'applique pas à l' <code>-superuser</code> paramètre car il inclut toujours <code>none</code> même si elle n'est pas spécifiée. |

### Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :



- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule sys,krb5`
- `-superuser krb5`

Le client #1 a l'adresse IP 10.1.16.207, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec AUTH\_SYS.

Le client #3 a l'adresse IP 10.1.16.234, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et n'a pas authentifié (AUTH\_NONE).

Le protocole d'accès client et l'adresse IP correspondent aux trois clients. Le paramètre lecture seule permet un accès en lecture seule à tous les clients, quel que soit leur type de sécurité. Le paramètre lecture-écriture permet l'accès en lecture-écriture aux clients avec leur propre ID utilisateur authentifié par AUTH\_SYS ou Kerberos v5. Le paramètre superuser permet un accès superuser aux clients avec l'ID utilisateur 0 authentifié avec Kerberos v5.

Par conséquent, le client #1 obtient l'accès en lecture-écriture superutilisateur car il correspond aux trois paramètres d'accès. Le client #2 obtient un accès en lecture-écriture mais pas un accès super-utilisateur. Le client #3 obtient un accès en lecture seule mais pas un accès super-utilisateur.

#### Gérer les demandes d'accès superutilisateur

Lorsque vous configurez des stratégies d'exportation, vous devez tenir compte de ce que vous voulez faire si le système de stockage reçoit une demande d'accès client avec l'ID utilisateur 0, c'est-à-dire en tant que superutilisateur, et définir vos règles d'exportation en conséquence.

Dans le monde UNIX, un utilisateur avec l'ID utilisateur 0 est appelé superutilisateur, généralement appelé root, qui dispose de droits d'accès illimités sur un système. L'utilisation des privilèges de superutilisateur peut être dangereuse pour plusieurs raisons, y compris une violation du système et de la sécurité des données.

Par défaut, ONTAP mappe les clients présentant l'ID utilisateur 0 à l'utilisateur anonyme. Toutefois, vous pouvez spécifier le `-superuser` Paramètre dans les règles d'exportation pour déterminer comment gérer les clients présentant l'ID utilisateur 0 en fonction de leur type de sécurité. Les options suivantes sont valides pour le `-superuser` paramètre :

- `any`
- `none`

Il s'agit du paramètre par défaut si vous ne spécifiez pas le `-superuser` paramètre.

- `krb5`
- `ntlm`
- `sys`

Il existe deux façons différentes de gérer les clients présentant l'ID utilisateur 0, selon le `-superuser` configuration des paramètres :

| Si le <code>-superuser</code> et le type de sécurité du client... | Ensuite, le client...                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Correspondance                                                    | Obtient l'accès superutilisateur avec l'ID utilisateur 0.                                                                                                                                                                                                           |
| Ne correspondent pas                                              | Obtient l'accès en tant qu'utilisateur anonyme avec l'ID utilisateur spécifié par le <code>-anon</code> paramètre et ses autorisations attribuées. Cette option est précise si le paramètre lecture seule ou lecture-écriture spécifie l'option <code>none</code> . |

Si un client se présente avec l'ID utilisateur 0 pour accéder à un volume avec le style de sécurité NTFS et le `-superuser` le paramètre est défini sur `none`, ONTAP utilise le mappage de noms pour l'utilisateur anonyme afin d'obtenir les informations d'identification appropriées.

### Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

Le client n° 1 a l'adresse IP 10.1.16.207, a l'ID utilisateur 746, envoie une demande d'accès à l'aide du protocole NFSv3 et s'authentifie avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec AUTH\_SYS.

Le protocole d'accès client et l'adresse IP correspondent pour les deux clients. Le paramètre en lecture seule permet l'accès en lecture seule à tous les clients, quel que soit le type de sécurité auquel ils sont authentifiés. Cependant, seul le client #1 obtient l'accès en lecture-écriture car il a utilisé le type de sécurité approuvé Kerberos v5 pour s'authentifier.

Le client #2 ne dispose pas d'un accès super-utilisateur. Au lieu de cela, il est mappé sur anonyme car le `-superuser` paramètre non spécifié. Cela signifie que la valeur par défaut est `none` Et mappe automatiquement l'ID utilisateur 0 sur anonyme. Le client #2 obtient également un accès en lecture seule car son type de sécurité ne correspond pas au paramètre lecture-écriture.

### Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`

- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

Le client #1 a l'adresse IP 10.1.16.207, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec AUTH\_SYS.

Le protocole d'accès client et l'adresse IP correspondent pour les deux clients. Le paramètre en lecture seule permet l'accès en lecture seule à tous les clients, quel que soit le type de sécurité auquel ils sont authentifiés. Cependant, seul le client #1 obtient l'accès en lecture-écriture car il a utilisé le type de sécurité approuvé Kerberos v5 pour s'authentifier. Le client n° 2 ne dispose pas d'un accès en lecture/écriture.

La règle d'exportation permet l'accès superutilisateur pour les clients avec l'ID utilisateur 0. Le client #1 obtient l'accès superutilisateur car il correspond à l'ID utilisateur et au type de sécurité pour la lecture seule et `-superuser` paramètres. Le client #2 ne dispose pas d'un accès en lecture-écriture ou super-utilisateur, car son type de sécurité ne correspond pas au paramètre en lecture-écriture ou au `-superuser` paramètre. Au lieu de cela, le client #2 est mappé à l'utilisateur anonyme, qui a dans ce cas l'ID utilisateur 0.

#### Utilisation des caches de règles d'exportation par ONTAP

Pour améliorer les performances système, ONTAP utilise des caches locaux pour stocker des informations telles que les noms d'hôtes et les groupes de réseaux. Cela permet à ONTAP de traiter les règles des export-policy plus rapidement que de récupérer les informations à partir de sources externes. Comprendre ce qu'sont les caches et ce qu'ils font pour vous aider à résoudre les problèmes d'accès client.

Vous configurez les export policy pour contrôler l'accès client aux exports NFS. Chaque export policy contient des règles, et chaque règle contient des paramètres qui correspondent à la règle avec les clients demandant un accès. Certains de ces paramètres exigent que ONTAP contacte une source externe, telle que des serveurs DNS ou NIS, pour résoudre des objets tels que des noms de domaine, des noms d'hôtes ou des groupes réseau.

Ces communications avec des sources externes prennent peu de temps. Afin d'améliorer les performances, ONTAP réduit le temps nécessaire à la résolution des objets de règles d'exportation en stockant les informations localement sur chaque nœud dans plusieurs caches.

| Nom du cache | Type d'information stockée                                                                                   |
|--------------|--------------------------------------------------------------------------------------------------------------|
| L'accès      | Mise en correspondance des clients avec les règles d'exportation correspondantes                             |
| Nom          | Mappage des noms d'utilisateur UNIX avec les ID utilisateur UNIX correspondants                              |
| ID           | Mappage des ID utilisateur UNIX avec les ID utilisateur UNIX correspondants et les ID de groupe UNIX étendus |

| Nom du cache  | Type d'information stockée                                             |
|---------------|------------------------------------------------------------------------|
| Hôte          | Mappages de noms d'hôtes sur les adresses IP correspondantes           |
| Groupe réseau | Mappages de groupes réseau aux adresses IP correspondantes des membres |
| Showmount     | Liste des répertoires exportés depuis le namespace du SVM              |

Si vous modifiez les informations sur les serveurs de noms externes de votre environnement après la récupération et le stockage en local par ONTAP, les caches peuvent désormais contenir des informations obsolètes. Bien que les mises à jour ONTAP se placent automatiquement après certaines périodes, différents caches ont des temps d'expiration et d'actualisation et des algorithmes différents.

Une autre raison possible pour que les caches contiennent des informations obsolètes est le moment où ONTAP tente d'actualiser les informations en cache mais rencontre un échec lors de tentatives de communication avec des serveurs de noms. Dans ce cas, ONTAP continue d'utiliser les informations actuellement stockées dans les caches locaux pour éviter toute perturbation du client.

Par conséquent, les demandes d'accès des clients qui sont censées réussir risquent d'échouer et les demandes d'accès des clients qui sont censées échouer pourraient réussir. Vous pouvez afficher et vider manuellement certains caches de règles d'exportation lors du dépannage de tels problèmes d'accès client.

#### Fonctionnement du cache d'accès

ONTAP utilise un cache d'accès pour stocker les résultats de l'évaluation de la règle d'export policy pour les opérations d'accès client à un volume ou à un qtree. Il en résulte une amélioration des performances, car les informations peuvent être récupérées beaucoup plus rapidement depuis le cache d'accès qu'un processus d'évaluation des règles d'export-policy à chaque fois qu'un client envoie une requête d'E/S.

Lorsqu'un client NFS envoie une requête d'E/S pour accéder aux données d'un volume ou qtree, ONTAP doit évaluer chaque demande d'E/S afin de déterminer s'il faut accorder ou refuser la demande d'E/S. Cette évaluation implique de vérifier chaque règle d'export policy de la export policy associée au volume ou à qtree. Si le chemin vers le volume ou qtree implique de franchir un ou plusieurs points de jonction, cette vérification peut s'avérer nécessaire pour rechercher plusieurs règles d'exportation le long du chemin.

Notez que cette évaluation est effectuée pour chaque demande d'E/S envoyée depuis un client NFS, par exemple pour la lecture, l'écriture, la liste, la copie et d'autres opérations. Il ne s'agit pas uniquement de demandes de montage initiales.

Une fois que ONTAP a identifié les règles d'export policy applicables et a décidé d'autoriser ou de refuser la requête, ONTAP crée ensuite une entrée dans le cache d'accès pour stocker ces informations.

Lorsqu'un client NFS envoie une requête d'E/S, ONTAP note l'adresse IP du client, l'ID de la SVM et la export policy associée au volume cible ou au qtree, et recherche d'abord une entrée correspondante dans le cache d'accès. S'il existe une entrée correspondante dans le cache d'accès, ONTAP utilise les informations stockées pour autoriser ou refuser la demande d'E/S. Si aucune entrée correspondante n'existe, ONTAP passe par le processus normal d'évaluation de toutes les règles de politique applicables, comme expliqué ci-dessus.

Les entrées du cache d'accès qui ne sont pas utilisées activement ne sont pas actualisées. Cela permet de réduire les communications inutiles et inutiles avec des services de noms externes.

La récupération des informations à partir du cache d'accès est bien plus rapide qu'au cours de l'intégralité du processus d'évaluation des règles des règles d'export-policy pour chaque demande d'E/S. Par conséquent, l'utilisation du cache d'accès améliore nettement les performances en réduisant la surcharge liée aux vérifications d'accès client.

#### Fonctionnement des paramètres de cache d'accès

Plusieurs paramètres contrôlent les périodes d'actualisation des entrées dans le cache d'accès. Le fonctionnement de ces paramètres vous permet de les modifier pour régler le cache d'accès et équilibrer les performances avec la récente information stockée.

Le cache d'accès stocke des entrées composées d'une ou plusieurs règles d'exportation qui s'appliquent aux clients qui essaient d'accéder aux volumes ou aux qtrees. Ces entrées sont stockées pendant un certain temps avant leur actualisation. La durée d'actualisation est déterminée par les paramètres du cache d'accès et dépend du type d'entrée du cache d'accès.

Vous pouvez spécifier les paramètres du cache d'accès pour chaque SVM. Cela permet aux paramètres de différer en fonction des exigences d'accès des SVM. Les entrées de cache d'accès qui ne sont pas utilisées activement ne sont pas réactualisées, ce qui réduit les communications inutiles et inutiles avec le nom externe sert.

| Accès au type d'entrée du cache | Description                                                                       | Période d'actualisation en secondes                           |
|---------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------|
| Entrées positives               | Les entrées du cache d'accès qui n'ont pas entraîné de refus d'accès aux clients. | Minimum: 300<br>Maximum : 86,400<br>Valeur par défaut : 3,600 |
| Entrées négatives               | Les entrées du cache d'accès qui ont entraîné un refus d'accès aux clients.       | Minimum : 60<br>Maximum : 86,400<br>Valeur par défaut : 3,600 |

#### Exemple

Un client NFS tente d'accéder à un volume sur un cluster. ONTAP mappe le client sur une règle export policy et détermine que le client accède à cette règle en fonction de la configuration de la règle export policy. ONTAP stocke la règle d'export policy dans le cache d'accès sous forme d'entrée positive. Par défaut, ONTAP conserve l'entrée positive dans le cache d'accès pendant une heure (3,600 secondes), puis actualise automatiquement l'entrée pour maintenir les informations à jour.

Pour éviter que le cache d'accès ne se remplit inutilement, il existe un paramètre supplémentaire pour effacer les entrées existantes du cache d'accès qui n'ont pas été utilisées pendant une certaine période pour décider de l'accès client. C'est ça `-harvest-timeout` le paramètre a une plage autorisée de 60 à 2,592,000 secondes et un réglage par défaut de 86,400 secondes.

**Supprimer une export policy d'un qtree**

Si vous décidez de ne plus vouloir attribuer une export policy spécifique à un qtree, vous pouvez supprimer la export policy en modifiant le qtree de manière à hériter de la export policy du volume contenant. Pour ce faire, utilisez le `volume qtree modify` commande avec `-export-policy` paramètre et chaîne de nom vide ("").

**Étapes**

- 1. Pour supprimer une export policy d'un qtree, entrez la commande suivante :

```
volume qtree modify -vserver vservice_name -qtree-path
/vol/volume_name/qtree_name -export-policy ""
```

- 2. Vérifier que le qtree a été modifié en conséquence :

```
volume qtree show -qtree qtree_name -fields export-policy
```

**Valider les ID de qtree pour les opérations sur les fichiers qtree**

ONTAP peut procéder à une validation supplémentaire facultative des ID de qtree. Cette validation garantit que les demandes d'opérations de fichiers client utilisent un ID qtree valide et que les clients ne peuvent déplacer que les fichiers au sein du même qtree. Vous pouvez activer ou désactiver cette validation en modifiant le `-validate-qtree-export` paramètre. Ce paramètre est activé par défaut.

**Description de la tâche**

Ce paramètre n'est efficace que lorsque vous avez attribué une export policy directement à un ou plusieurs qtrees sur la machine virtuelle de stockage (SVM).

**Étapes**

- 1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

- 2. Effectuez l'une des opérations suivantes :

| Pour que la validation de l'ID qtree soit... | Saisissez la commande suivante...                                                      |
|----------------------------------------------|----------------------------------------------------------------------------------------|
| Activé                                       | <code>vserver nfs modify -vserver vservice_name -validate-qtree-export enabled</code>  |
| Désactivé                                    | <code>vserver nfs modify -vserver vservice_name -validate-qtree-export disabled</code> |

- 3. Retour au niveau de privilège admin :

```
set -privilege admin
```

## Restrictions des export policy et jonctions imbriquées pour volumes FlexVol

Si vous avez configuré des stratégies d'exportation pour définir une stratégie moins restrictive sur une jonction imbriquée mais une règle plus restrictive sur une jonction de niveau supérieur, l'accès à la jonction de niveau inférieur peut échouer.

Vous devez vous assurer que les jonctions de niveau supérieur disposent de règles d'exportation moins restrictives que les jonctions de niveau inférieur.

## Utilisation de Kerberos avec NFS pour une sécurité renforcée

### Prise en charge de ONTAP pour Kerberos

Kerberos fournit une authentification sécurisée renforcée pour les applications client/Server. L'authentification permet de vérifier les identités des utilisateurs et des processus à un serveur. Dans l'environnement ONTAP, Kerberos assure une authentification entre les SVM (Storage Virtual machine) et les clients NFS.

Dans ONTAP 9, les fonctionnalités Kerberos suivantes sont prises en charge :

- Authentification Kerberos 5 avec contrôle d'intégrité (krb5i)

Krb5i utilise des checksums pour vérifier l'intégrité de chaque message NFS transféré entre le client et le serveur. Cette fonction est utile pour des raisons de sécurité (par exemple pour s'assurer que les données n'ont pas été falsifiées) et pour des raisons d'intégrité des données (par exemple, pour empêcher la corruption des données lors de l'utilisation de NFS sur des réseaux non fiables).

- Authentification Kerberos 5 avec vérification de la confidentialité (krb5p)

Krb5p utilise des checksums pour chiffrer l'ensemble du trafic entre le client et le serveur. Ceci est plus sûr et entraîne également plus de charge.

- Chiffrement AES 128 bits et 256 bits

Advanced Encryption Standard (AES) est un algorithme de cryptage permettant de sécuriser les données électroniques. ONTAP prend en charge AES avec des clés 128 bits (AES-128) et AES avec des clés 256 bits (AES-256) pour Kerberos pour une sécurité renforcée.

- Les configurations de Royaume Kerberos au niveau du SVM

Les administrateurs des SVM peuvent désormais créer des configurations de domaine Kerberos au niveau du SVM. Les administrateurs des SVM n'ont plus besoin de se reposer sur l'administrateur du cluster pour la configuration des royaumes Kerberos. Ils peuvent donc créer des configurations de Royaume Kerberos individuelles dans un environnement mutualisé.

### Conditions requises pour la configuration de Kerberos avec NFS

Avant de configurer Kerberos avec NFS sur votre système, vous devez vérifier que certains éléments de votre réseau et de votre environnement de stockage sont correctement configurés.



Les étapes de configuration de votre environnement dépendent de la version et du type du système d'exploitation client, du contrôleur de domaine, de Kerberos, DNS, etc. Que vous utilisez. La documentation de toutes ces variables dépasse le cadre de ce document. Pour plus d'informations, reportez-vous à la documentation correspondante pour chaque composant.

Pour obtenir un exemple détaillé de la configuration de ONTAP et de Kerberos 5 avec NFSv3 et NFSv4 dans un environnement utilisant des hôtes Windows Server 2008 R2 Active Directory et Linux, consultez le rapport technique 4073.

Les éléments suivants doivent d'abord être configurés :

### Conditions requises pour l'environnement réseau

- Kerberos

Vous devez avoir une configuration Kerberos fonctionnant avec un centre de distribution de clés (KDC), tel que Windows Active Directory Based Kerberos ou MIT Kerberos.

Les serveurs NFS doivent utiliser `nfs` en tant que composant principal de leur machine principale.

- Service d'annuaire

Vous devez utiliser un service d'annuaire sécurisé dans votre environnement, tel qu'Active Directory ou OpenLDAP, configuré pour utiliser LDAP sur SSL/TLS.

- NTP

Vous devez disposer d'un serveur de temps de travail exécutant NTP. Cette opération est nécessaire pour éviter l'échec de l'authentification Kerberos en raison de l'inclinaison du temps.

- Résolution des noms de domaine (DNS)

Chaque client UNIX et chaque LIF de SVM doivent avoir un enregistrement de service (SRV) correct enregistré auprès du KDC dans des zones de recherche avant et arrière. Tous les participants doivent être résolus correctement via DNS.

- Comptes d'utilisateur

Chaque client doit disposer d'un compte utilisateur dans le domaine Kerberos. Les serveurs NFS doivent utiliser « `nfs` » comme composant principal de leur machine principale.

### Exigences du client NFS

- NFS

Chaque client doit être correctement configuré pour communiquer sur le réseau en utilisant NFSv3 ou NFSv4.

Les clients doivent prendre en charge les RFC1964 et RFC2203.

- Kerberos

Chaque client doit être correctement configuré pour utiliser l'authentification Kerberos, avec les informations suivantes :



- Le chiffrement pour les communications TGS est activé.

AES-256 pour une sécurité optimale.

- Le type de cryptage le plus sécurisé pour les communications TGT est activé.
- Le domaine et le domaine Kerberos sont configurés correctement.
- GSS est activé.

Lors de l'utilisation des informations d'identification de la machine

- Ne pas exécuter `gssd` avec le `-n` paramètre.
- Ne pas exécuter `kinit` en tant qu'utilisateur root.

- Chaque client doit utiliser la version la plus récente et la plus récente du système d'exploitation.

Cela offre la meilleure compatibilité et fiabilité pour le chiffrement AES avec Kerberos.

- DNS

Chaque client doit être correctement configuré pour utiliser DNS pour la résolution correcte du nom.

- NTP

Chaque client doit être en cours de synchronisation avec le serveur NTP.

- Informations sur l'hôte et le domaine

Chaque client `/etc/hosts` et `/etc/resolv.conf` Les fichiers doivent contenir le nom d'hôte et les informations DNS correctes, respectivement.

- Fichiers keytab

Chaque client doit avoir un fichier keytab du KDC. Le Royaume doit être en majuscules. Le type de chiffrement doit être AES-256 pour une sécurité optimale.

- Facultatif : pour des performances optimales, les clients bénéficient d'au moins deux interfaces réseau : l'une pour communiquer avec le réseau local et l'autre pour communiquer avec le réseau de stockage.

## Configuration requise pour le système de stockage

- Licence NFS

Une licence NFS valide doit être installée sur le système de stockage.

- Licence CIFS

La licence CIFS est facultative. Il n'est nécessaire de vérifier les informations d'identification Windows que lors de l'utilisation du mappage de noms multiprotocole. Elle n'est pas requise dans un environnement UNIX strict.

- SVM

Au moins un SVM doit être configuré sur le système.

- DNS sur le SVM

On doit avoir configuré DNS sur chaque SVM.

- Serveur NFS

Vous devez avoir configuré NFS sur le SVM.

- Cryptage AES

Pour une sécurité optimale, vous devez configurer le serveur NFS de sorte qu'il n'autorise que le chiffrement AES-256 pour Kerberos.

- Serveur SMB

Si vous exécutez un environnement multiprotocole, vous devez avoir configuré SMB sur le SVM. Le serveur SMB est requis pour le mappage de noms multiprotocole.

- Volumes

On doit disposer d'un volume root et d'au moins un volume de données configuré pour une utilisation par la SVM.

- Volume racine

Le volume root du SVM doit avoir la configuration suivante :

| Nom                | Réglage        |
|--------------------|----------------|
| Style de sécurité  | UNIX           |
| UID                | Racine ou ID 0 |
| GIDS               | Racine ou ID 0 |
| Autorisations UNIX | 776            |

Contrairement au volume racine, les volumes de données peuvent avoir n'importe quel style de sécurité.

- Groupes UNIX

La SVM doit avoir les groupes UNIX suivants configurés :

| Nom du groupe | ID de groupe                                                      |
|---------------|-------------------------------------------------------------------|
| démon         | 1                                                                 |
| racine        | 0                                                                 |
| pcuser        | 65534 (créé automatiquement par ONTAP lors de la création du SVM) |

- Utilisateurs UNIX

Le SVM doit avoir les utilisateurs UNIX suivants configurés :

| Nom d'utilisateur | ID d'utilisateur | ID de groupe principal | Commentaire                                                                                                                                                 |
|-------------------|------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| nfs               | 500              | 0                      | Requis pour la phase INITIALE GSS<br><br>Le premier composant de l'utilisateur client NFS SPN est utilisé comme utilisateur.                                |
| pcuser            | 65534            | 65534                  | Obligatoire pour une utilisation multiprotocole NFS et CIFS<br><br>Créé et ajouté au groupe pcuser automatiquement par ONTAP lors de la création de la SVM. |
| racine            | 0                | 0                      | Nécessaire pour le montage                                                                                                                                  |

L'utilisateur nfs n'est pas requis si un mappage de nom Kerberos-UNIX existe pour le SPN de l'utilisateur client NFS.

- Export-polices et rules

Vous devez avoir configuré des export policy avec les règles d'exportation nécessaires pour les volumes root et de données et les qtrees. Si tous les volumes du SVM sont accessibles via Kerberos, vous pouvez définir les options des règles d'exportation `-rorule`, `-rwrule`, et `-superuser` pour le volume racine à `krb5`, `krb5i`, ou `krb5p`.

- Mapping de noms Kerberos-UNIX

Si vous souhaitez que l'utilisateur identifié par l'utilisateur client NFS SPN dispose d'autorisations root, vous devez créer un mappage de nom à la racine.

#### Informations associées

["Rapport technique NetApp 4073 : authentification unifiée sécurisée"](#)

["Matrice d'interopérabilité NetApp"](#)

["Administration du système"](#)

["Gestion du stockage logique"](#)

## Spécifiez le domaine ID utilisateur pour NFSv4

Pour spécifier le domaine d'ID utilisateur, vous pouvez définir le `-v4-id-domain` option.

### Description de la tâche

Par défaut, ONTAP utilise le domaine NIS pour le mappage d'ID utilisateur NFSv4, si un est défini. Si aucun domaine NIS n'est défini, le domaine DNS est utilisé. Vous devrez peut-être définir le domaine d'ID utilisateur si, par exemple, vous disposez de plusieurs domaines d'ID utilisateur. Le nom de domaine doit correspondre à la configuration de domaine sur le contrôleur de domaine. Elle n'est pas requise pour NFSv3.

### Étape

1. Saisissez la commande suivante :

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

## Utilisation de TLS avec NFS pour une sécurité renforcée

### Présentation de l'utilisation de TLS avec NFS pour une sécurité renforcée

TLS permet des communications réseau chiffrées avec une sécurité équivalente et moins complexe que Kerberos et IPsec. En tant qu'administrateur, vous pouvez activer, configurer et désactiver TLS pour une sécurité renforcée avec les connexions NFSv3 et NFSv4.x via System Manager, l'interface de ligne de commande ONTAP ou l'API REST ONTAP.



NFS over TLS est disponible dans ONTAP 9.15.1 en tant que préversion publique. À titre de préversion, NFS over TLS n'est pas pris en charge pour les workloads de production dans ONTAP 9.15.1.

ONTAP utilise TLS 1.3 pour les connexions NFS sur TLS.

### De formation

NFS sur TLS nécessite des certificats X.509. Vous pouvez soit créer un certificat de serveur d'installation signé par une autorité de certification sur le cluster ONTAP, soit installer un certificat que le service NFS utilise directement. Vos certificats doivent être conformes aux directives suivantes :

- Chaque certificat doit être configuré avec le nom de domaine complet (FQDN) du serveur NFS (la LIF de données sur laquelle TLS sera activé/configuré) en tant que nom commun (CN).
- Chaque certificat doit être configuré avec l'adresse IP ou le nom de domaine complet du serveur NFS (ou les deux) en tant que nom secondaire de l'objet (SAN). Si l'adresse IP et le nom de domaine complet sont configurés, les clients NFS peuvent se connecter à l'aide de l'adresse IP ou du nom de domaine complet.
- Vous pouvez installer plusieurs certificats de service NFS pour la même LIF, mais un seul d'entre eux peut être utilisé à la fois dans le cadre de la configuration NFS TLS.

### Activez ou désactivez TLS pour les clients NFS

Vous pouvez améliorer la sécurité des connexions NFS en configurant NFS sur TLS de manière à chiffrer toutes les données envoyées sur le réseau entre le client NFS et ONTAP. Cela augmente la sécurité des connexions NFS. Vous pouvez le configurer sur

une VM de stockage existante activée pour "NFS".



NFS over TLS est disponible dans ONTAP 9.15.1 en tant que préversion publique. À titre de préversion, NFS over TLS n'est pas pris en charge pour les workloads de production dans ONTAP 9.15.1.

## Activez TLS

Vous pouvez activer le chiffrement TLS pour les clients NFS afin d'augmenter la sécurité des données en transit.

### Avant de commencer

- Reportez-vous à la ["de formation"](#) Pour NFS sur TLS avant de commencer.
- Reportez-vous aux pages de manuel ONTAP pour plus d'informations sur la commande dans cette procédure.

### Étapes

1. Il convient de choisir une machine virtuelle de stockage et une interface logique (LIF) sur laquelle activer TLS.
2. Activez TLS pour les connexions NFS sur cette machine virtuelle et cette interface de stockage.

```
vserver nfs tls interface enable -vserver <STORAGE_VM> -lif <LIF_NAME>
-certificate-name <CERTIFICATE_NAME>
```

3. Utilisez le `vserver nfs tls interface show` pour afficher les résultats :

```
vserver nfs tls interface show
```

### Exemple

La commande suivante active NFS sur TLS sur le data1 LIF du vs1 VM de stockage :

```
vserver nfs tls interface enable -vserver vs1 -lif data1 -certificate-name
cert_vs1
```

```
vserver nfs tls interface show
```

| Vserver<br>Name           | Logical<br>Interface | Address  | TLS Status | TLS Certificate |
|---------------------------|----------------------|----------|------------|-----------------|
| -----                     | -----                | -----    | -----      |                 |
| vs1                       | data1                | 10.0.1.1 | enabled    | cert_vs1        |
| vs2                       | data2                | 10.0.1.2 | disabled   | -               |
| 2 entries were displayed. |                      |          |            |                 |

## Désactiver TLS

Vous pouvez désactiver TLS pour les clients NFS si vous n'avez plus besoin de la sécurité améliorée pour les données en transit.

### Avant de commencer

Reportez-vous aux pages de manuel ONTAP pour plus d'informations sur la commande dans cette procédure.

### Étapes

1. Choisissez une VM de stockage et une interface logique (LIF) sur laquelle désactiver TLS.
2. Désactivez TLS pour les connexions NFS sur cette VM et cette interface de stockage.

```
vserver nfs tls interface disable -vserver <STORAGE_VM> -lif <LIF_NAME>
```

3. Utilisez le `vserver nfs tls interface show` pour afficher les résultats :

```
vserver nfs tls interface show
```

### Exemple

La commande suivante désactive NFS sur TLS sur le data1 LIF du vs1 VM de stockage :

```
vserver nfs tls interface disable -vserver vs1 -lif data1
```

```
vserver nfs tls interface show
```

| Vserver<br>Name           | Logical<br>Interface | Address  | TLS Status | TLS Certificate |
|---------------------------|----------------------|----------|------------|-----------------|
| -----                     | -----                | -----    | -----      |                 |
| vs1                       | data1                | 10.0.1.1 | disabled   | -               |
| vs2                       | data2                | 10.0.1.2 | disabled   | -               |
| 2 entries were displayed. |                      |          |            |                 |

## Modifier une configuration TLS

Vous pouvez modifier les paramètres d'une configuration NFS sur TLS existante. Par exemple, vous pouvez utiliser cette procédure pour mettre à jour le certificat TLS.

### Avant de commencer

Reportez-vous aux pages de manuel ONTAP pour plus d'informations sur la commande dans cette procédure.

### Étapes

1. Choisir une VM de stockage et une interface logique (LIF) sur laquelle modifier la configuration TLS pour les clients NFS.
2. Modifier la configuration. Si vous spécifiez un `status` de `enable`, vous devez également spécifier le `certificate-name` paramètre. Remplacez les valeurs entre parenthèses <> par les informations de votre environnement :

```
vserver nfs tls interface modify -vserver <STORAGE_VM> -lif <LIF_NAME>
-status <STATUS> -certificate-name <CERTIFICATE_NAME>
```

3. Utilisez le `vserver nfs tls interface show` pour afficher les résultats :

```
vserver nfs tls interface show
```

### Exemple

La commande suivante modifie la configuration NFS sur TLS sur le `data2` LIF du `vs2` VM de stockage :

```
vserver nfs tls interface modify -vserver vs2 -lif data2 -status enable
-certificate-name new_cert
```

```
vserver nfs tls interface show
```

| Vserver<br>Name           | Logical<br>Interface | Address  | TLS Status | TLS Certificate |
|---------------------------|----------------------|----------|------------|-----------------|
| -----                     | -----                | -----    | -----      |                 |
| vs1                       | data1                | 10.0.1.1 | disabled   | -               |
| vs2                       | data2                | 10.0.1.2 | enabled    | new_cert        |
| 2 entries were displayed. |                      |          |            |                 |

## Configurer NAME-services

### Fonctionnement de la configuration du commutateur de service name ONTAP

ONTAP stocke les informations de configuration du service de noms dans un tableau équivalent à `/etc/nsswitch.conf` Fichier sur les systèmes UNIX. Vous devez connaître les fonctions du tableau et savoir comment ONTAP l'utilise pour que vous puissiez le configurer de façon appropriée pour votre environnement.

La table commutateur de service de nom ONTAP détermine les sources de service de nom auxquelles ONTAP consulte afin de récupérer les informations relatives à un certain type d'informations de service de nom. ONTAP conserve une table de commutateur de service de noms distincte pour chaque SVM.

### Types de base de données

La table stocke une liste de services de noms distincte pour chacun des types de bases de données suivants :

| Type de base de données | Définit les sources de service de noms pour...            | Les sources valides sont... |
|-------------------------|-----------------------------------------------------------|-----------------------------|
| hôtes                   | Conversion des noms d'hôte en adresses IP                 | fichiers, dns               |
| groupe                  | Recherche des informations sur les groupes d'utilisateurs | fichiers, nis, ldap         |
| passwd                  | Recherche des informations utilisateur                    | fichiers, nis, ldap         |
| groupe réseau           | Recherche des informations de groupe réseau               | fichiers, nis, ldap         |
| carte de nom            | Mappage des noms d'utilisateur                            | fichiers, ldap              |

### Types de source

Les sources indiquent quelle source de service de nom utiliser pour récupérer les informations appropriées.



| Spécifiez le type de source... | Pour rechercher des informations dans...                                             | Géré par les familles de commande...                                                                                                                                            |
|--------------------------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fichiers                       | Fichiers source locaux                                                               | <pre>vserver services name- service unix-user vserver services name-service unix-group  vserver services name- service netgroup  vserver services name- service dns hosts</pre> |
| nis                            | Serveurs NIS externes tels que spécifiés dans la configuration de domaine NIS du SVM | <pre>vserver services name- service nis-domain</pre>                                                                                                                            |
| ldap                           | Serveurs LDAP externes comme spécifié dans la configuration du client LDAP du SVM    | <pre>vserver services name- service ldap</pre>                                                                                                                                  |
| dns                            | Serveurs DNS externes comme spécifié dans la configuration DNS du SVM                | <pre>vserver services name- service dns</pre>                                                                                                                                   |

Même si vous prévoyez d'utiliser NIS ou LDAP pour l'accès aux données et l'authentification d'administration des SVM, vous devez toujours inclure `files` Et configurer des utilisateurs locaux comme un repli en cas d'échec de l'authentification NIS ou LDAP.

### Protocoles utilisés pour accéder à des sources externes

Pour accéder aux serveurs pour des sources externes, ONTAP utilise les protocoles suivants :

| Source de service de nom externe | Protocole utilisé pour l'accès |
|----------------------------------|--------------------------------|
| NIS                              | UDP                            |
| DNS                              | UDP                            |
| LDAP                             | TCP                            |

### Exemple

L'exemple suivant montre la configuration du switch de service de nom pour le SVM `svm svm_1` :

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
```

| Vserver | Database | Source Order  |
|---------|----------|---------------|
| -----   | -----    | -----         |
| svm_1   | hosts    | files,<br>dns |
| svm_1   | group    | files         |
| svm_1   | passwd   | files         |
| svm_1   | netgroup | nis,<br>files |

Pour rechercher les adresses IP des hôtes, ONTAP consulte d'abord les fichiers source locaux. Si la requête ne renvoie aucun résultat, les serveurs DNS sont vérifiés ensuite.

Pour rechercher des informations sur les utilisateurs ou les groupes, ONTAP consulte uniquement les fichiers sources locales. Si la requête ne renvoie aucun résultat, la recherche échoue.

Pour rechercher des informations sur le groupe réseau, ONTAP consulte d'abord les serveurs NIS externes. Si la requête ne renvoie aucun résultat, le fichier netgroup local est coché ensuite.

Il n'y a pas d'entrées de nom de service pour le mappage de noms dans le tableau pour le SVM svm\_1. Par conséquent, ONTAP consulte uniquement les fichiers source locaux par défaut.

### Informations associées

["Rapport technique de NetApp 4668 : name Services Best Practices Guide \(Guide des meilleures pratiques des services de noms\)"](#)

### Utiliser LDAP

#### Présentation LDAP

Un serveur LDAP (Lightweight Directory Access Protocol) vous permet de gérer de manière centralisée les informations utilisateur. Si vous stockez votre base de données utilisateur sur un serveur LDAP dans votre environnement, vous pouvez configurer votre système de stockage pour rechercher les informations utilisateur dans votre base de données LDAP existante.

- Avant de configurer LDAP pour ONTAP, vérifiez que votre déploiement de site respecte les bonnes pratiques en matière de configuration de serveur LDAP et de client. En particulier, les conditions suivantes doivent être remplies :
  - Le nom de domaine du serveur LDAP doit correspondre à l'entrée du client LDAP.
  - Les types de hachage de mot de passe utilisateur LDAP pris en charge par le serveur LDAP doivent inclure ceux pris en charge par ONTAP :
    - CRYPT (tous types) et SHA-1 (SHA, SSHA).
    - Depuis ONTAP 9.8, des hachages SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 et SSHA-512) sont également pris en charge.
  - Si le serveur LDAP nécessite des mesures de sécurité de session, vous devez les configurer dans le

client LDAP.

Les options de sécurité de session suivantes sont disponibles :

- La signature LDAP (fournit un contrôle de l'intégrité des données), la signature et le chiffrement LDAP (assure le contrôle de l'intégrité des données et le chiffrement)
- DÉMARRER TLS
- LDAPS (LDAP sur TLS ou SSL)
- Pour activer les requêtes LDAP signées et scellées, les services suivants doivent être configurés :
  - Les serveurs LDAP doivent prendre en charge le mécanisme GSSAPI (Kerberos) SASL.
  - Les serveurs LDAP doivent avoir des enregistrements DNS A/AAAA ainsi que des enregistrements PTR configurés sur le serveur DNS.
  - Les serveurs Kerberos doivent contenir des enregistrements SRV sur le serveur DNS.
- Pour activer START TLS ou LDAPS, les points suivants doivent être pris en compte.
  - Il s'agit d'une meilleure pratique NetApp d'utiliser Start TLS plutôt que LDAPS.
  - Si LDAPS est utilisé, le serveur LDAP doit être activé pour TLS ou pour SSL dans ONTAP 9.5 et versions ultérieures. SSL n'est pas pris en charge dans ONTAP 9.0-9.4.
  - Un serveur de certificats doit déjà être configuré dans le domaine.
- Pour activer la recherche de recommandation LDAP (dans ONTAP 9.5 et versions ultérieures), les conditions suivantes doivent être remplies :
  - Les deux domaines doivent être configurés avec l'une des relations d'approbation suivantes :
    - Bidirectionnel
    - Aller simple, où le principal fait confiance au domaine de référence
    - Parent-enfant
  - Le DNS doit être configuré pour résoudre tous les noms de serveur mentionnés.
  - Les mots de passe du domaine doivent être identiques pour s'authentifier lorsque `--bind-as-cifs-server` défini sur vrai.

Les configurations suivantes ne sont pas prises en charge avec la recherche de références LDAP.



- Pour toutes les versions de ONTAP :
- Clients LDAP sur un SVM d'admin
- Pour ONTAP 9.8 et versions antérieures (ils sont pris en charge dans la version 9.9.1 et ultérieures) :
- Signature et chiffrement LDAP (le `-session-security` en option)
- Connexions TLS cryptées ( `-use-start-tls` en option)
- Communications via le port LDAPS 636 (le `-use-ldaps-for-ad-ldap` en option)

- Vous pouvez utiliser ONTAP 9.11.1 depuis "[LDAP Fast bind pour l'authentification nsswitch.](#)"
- Vous devez entrer un schéma LDAP lors de la configuration du client LDAP sur le SVM.

Dans la plupart des cas, l'un des schémas ONTAP par défaut sera approprié. Toutefois, si le schéma

LDAP de votre environnement diffère de celui-ci, vous devez créer un nouveau schéma client LDAP pour ONTAP avant de créer le client LDAP. Consultez votre administrateur LDAP pour connaître les conditions requises pour votre environnement.

- L'utilisation de LDAP pour la résolution du nom d'hôte n'est pas prise en charge.

Pour plus d'informations, reportez-vous à la section ["Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP"](#).

## Concepts de signature et d'étanchéité LDAP

Depuis ONTAP 9, vous pouvez configurer la signature et le chiffrement pour activer la sécurité des sessions LDAP sur les requêtes vers un serveur Active Directory (AD). Vous devez configurer les paramètres de sécurité du serveur NFS sur la machine virtuelle de stockage (SVM) de manière à ce qu'ils correspondent à ceux du serveur LDAP.

La signature valide l'intégrité des données LDAP à l'aide d'une technologie à clé secrète. Le chiffrement crypte les données LDAP afin de ne pas transmettre de données sensibles en clair. Une option *LDAP Security Level* indique si le trafic LDAP doit être signé, signé et scellé, ou non. La valeur par défaut est `none`. testez

La signature et le chiffrement LDAP sur le trafic SMB sont activés sur le SVM avec le `-session-security-for-ad-ldap` à la `vserver cifs security modify` commande.

## Concepts LDAPS

Vous devez comprendre certains termes et concepts relatifs à la sécurisation de la communication LDAP par ONTAP. ONTAP peut utiliser START TLS ou LDAPS pour configurer des sessions authentifiées entre des serveurs LDAP intégrés à Active Directory ou des serveurs LDAP basés sur UNIX.

## Terminologie

Il existe certains termes que vous devez comprendre sur la manière dont ONTAP utilise LDAPS pour sécuriser les communications LDAP.

- **LDAP**

(Lightweight Directory Access Protocol) Protocole permettant d'accéder aux répertoires d'informations et de les gérer. LDAP est utilisé comme répertoire d'informations pour le stockage d'objets tels que des utilisateurs, des groupes et des groupes réseau. LDAP fournit également des services d'annuaire qui gèrent ces objets et répondent aux demandes LDAP des clients LDAP.

- **SSL**

(Secure Sockets Layer) Protocole développé pour envoyer des informations en toute sécurité via Internet. Le protocole SSL est pris en charge par ONTAP 9 et versions ultérieures, mais il est obsolète en faveur de TLS.

- **TLS**

(Sécurité de la couche de transport) un protocole de suivi conforme aux normes IETF, basé sur les spécifications SSL précédentes. C'est le successeur de SSL. TLS est pris en charge par ONTAP 9.5 et versions ultérieures.

## • LDAPS (LDAP sur SSL ou TLS)

Protocole utilisant TLS ou SSL pour sécuriser la communication entre les clients LDAP et les serveurs LDAP. Les termes *LDAP sur SSL* et *LDAP sur TLS* sont parfois utilisés de manière interchangeable. LDAPS est pris en charge par ONTAP 9.5 et versions ultérieures.

- Dans ONTAP 9.5-9.8, LDAPS ne peut être activé que sur le port 636. Pour ce faire, utilisez le `-use -ldaps-for-ad-ldap` paramètre avec le `vserver cifs security modify` commande.
- À partir de ONTAP 9.9.1, LDAPS peut être activé sur n'importe quel port, bien que le port 636 reste le port par défaut. Pour ce faire, définissez le `-ldaps-enabled` paramètre à `true` et spécifiez le souhaité `-port` paramètre. Pour plus d'informations, reportez-vous à la section `vserver services name-service ldap client create` page de manuel



Il s'agit d'une meilleure pratique NetApp d'utiliser Start TLS plutôt que LDAPS.

## • Démarrer TLS

(Également appelé *start\_tls*, *STARTTLS* et *StartTLS*) Un mécanisme de communication sécurisée à l'aide des protocoles TLS.

ONTAP utilise STARTTLS pour sécuriser les communications LDAP et utilise le port LDAP par défaut (389) pour communiquer avec le serveur LDAP. Le serveur LDAP doit être configuré de manière à autoriser les connexions via le port LDAP 389 ; sinon, les connexions LDAP TLS du SVM vers le serveur LDAP échouent.

## Comment ONTAP utilise LDAPS

ONTAP prend en charge l'authentification du serveur TLS qui permet au client SVM LDAP de confirmer l'identité du serveur LDAP lors de l'opération BIND. Les clients LDAP compatibles TLS peuvent utiliser des techniques standard de cryptographie à clé publique pour vérifier que le certificat et l'ID public d'un serveur sont valides et ont été émis par une autorité de certification (AC) répertoriée dans la liste des autorités de certification de confiance du client.

LDAP prend en charge STARTTLS pour crypter les communications à l'aide de TLS. STARTTLS commence comme une connexion texte clair sur le port LDAP standard (389), et cette connexion est ensuite mise à niveau vers TLS.

ONTAP supporte les éléments suivants :

- LDAPS pour le trafic lié au SMB entre les serveurs LDAP intégrés à Active Directory et le SVM
- LDAPS pour le trafic LDAP pour le mappage de noms et autres informations UNIX

Les serveurs LDAP intégrés à Active Directory ou les serveurs LDAP basés sur UNIX peuvent être utilisés pour stocker des informations pour le mappage de noms LDAP et d'autres informations UNIX, telles que des utilisateurs, des groupes et des netgroups.

- Certificats CA racine auto-signés

Lors de l'utilisation d'un LDAP intégré à Active-Directory, le certificat racine auto-signé est généré lorsque le service de certificat Windows Server est installé dans le domaine. Lors de l'utilisation d'un serveur LDAP UNIX pour le mappage de noms LDAP, le certificat racine auto-signé est généré et enregistré à l'aide de moyens appropriés à cette application LDAP.

Par défaut, LDAPS est désactivé.

## Activez la prise en charge du protocole LDAP RFC2307bis

Si vous souhaitez utiliser LDAP et que vous avez besoin de la fonctionnalité supplémentaire d'utilisation des appartenances aux groupes imbriqués, vous pouvez configurer ONTAP pour activer la prise en charge de LDAP RFC2307bis.

### Ce dont vous avez besoin

Vous devez avoir créé une copie de l'un des schémas de client LDAP par défaut que vous souhaitez utiliser.

### Description de la tâche

Dans les schémas client LDAP, les objets de groupe utilisent l'attribut memberUID. Cet attribut peut contenir plusieurs valeurs et répertorie les noms des utilisateurs appartenant à ce groupe. Dans les schémas de client LDAP compatibles avec RFC2307bis, les objets de groupe utilisent l'attribut uniqueMember. Cet attribut peut contenir le nom unique complet (DN) d'un autre objet dans le répertoire LDAP. Cela vous permet d'utiliser des groupes imbriqués car les groupes peuvent avoir d'autres groupes en tant que membres.

L'utilisateur ne doit pas être membre de plus de 256 groupes, y compris des groupes imbriqués. ONTAP ignore tous les groupes dépassant la limite de 256 groupes.

Par défaut, le support RFC2307bis est désactivé.



La prise en charge RFC2307bis est activée automatiquement dans ONTAP lorsqu'un client LDAP est créé avec le schéma MS-AD-BIS.

Pour plus d'informations, reportez-vous à la section "[Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP](#)".

### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Modifiez le schéma de client LDAP RFC2307 copié pour activer la prise en charge de RFC2307bis :

```
vserver services name-service ldap client schema modify -vserver vserver_name
-schema schema-name -enable-rfc2307bis true
```

3. Modifiez le schéma pour qu'il corresponde à la classe d'objet prise en charge par le serveur LDAP :

```
vserver services name-service ldap client schema modify -vserver vserver-name
-schema schema_name -group-of-unique-names-object-class object_class
```

4. Modifiez le schéma pour qu'il corresponde au nom d'attribut pris en charge par le serveur LDAP :

```
vserver services name-service ldap client schema modify -vserver vserver-name
-schema schema_name -unique-member-attribute attribute_name
```

5. Retour au niveau de privilège admin :

```
set -privilege admin
```

## Options de configuration pour les recherches d'annuaire LDAP

Vous pouvez optimiser les recherches d'annuaire LDAP, y compris les informations sur les utilisateurs, les groupes et les groupes réseau, en configurant le client LDAP ONTAP pour vous connecter aux serveurs LDAP de la manière la plus appropriée pour votre environnement. Vous devez savoir quand les valeurs de base LDAP et de recherche d'étendue par défaut sont suffisantes et quels paramètres doivent spécifier lorsque les valeurs personnalisées sont plus appropriées.

Les options de recherche du client LDAP pour les informations utilisateur, groupe et groupe réseau permettent d'éviter les requêtes LDAP échouées et, par conséquent, l'échec de l'accès du client aux systèmes de stockage. Ils permettent également de s'assurer que les recherches sont aussi efficaces que possible pour éviter les problèmes de performance du client.

### Valeurs par défaut de recherche de base et de portée

La base LDAP est le DN de base par défaut utilisé par le client LDAP pour effectuer des requêtes LDAP. Toutes les recherches, y compris les recherches d'utilisateur, de groupe et de groupe réseau, sont effectuées à l'aide du DN de base. Cette option est appropriée lorsque votre répertoire LDAP est relativement petit et que toutes les entrées pertinentes se trouvent dans le même DN.

Si vous ne spécifiez pas de NA de base personnalisé, la valeur par défaut est `root`. Cela signifie que chaque requête recherche l'intégralité du répertoire. Bien que cela optimise les chances de réussite de la requête LDAP, elle peut être inefficace et entraîner une baisse significative des performances avec les grands répertoires LDAP.

L'étendue de base LDAP est l'étendue de recherche par défaut utilisée par le client LDAP pour effectuer des requêtes LDAP. Toutes les recherches, y compris les recherches d'utilisateur, de groupe et de groupe réseau, sont effectuées à l'aide de la portée de base. Elle détermine si la requête LDAP recherche uniquement l'entrée nommée, entre un niveau sous le DN ou l'ensemble de la sous-arborescence sous le DN.

Si vous ne spécifiez pas d'étendue de base personnalisée, la valeur par défaut est `subtree`. Cela signifie que chaque requête effectue une recherche dans toute la sous-arborescence située sous le nom unique. Bien que cela optimise les chances de réussite de la requête LDAP, elle peut être inefficace et entraîner une baisse significative des performances avec les grands répertoires LDAP.

### Valeurs de base et d'étendue personnalisées

Vous pouvez éventuellement spécifier des valeurs de base et de portée distinctes pour les recherches utilisateur, groupe et groupe réseau. Limiter la base de recherche et l'étendue des requêtes de cette façon peut améliorer considérablement les performances car elle limite la recherche à une sous-section plus petite de l'annuaire LDAP.

Si vous spécifiez des valeurs de base et d'étendue personnalisées, elles remplacent la base de recherche générale par défaut et la portée pour les recherches utilisateur, groupe et groupe réseau. Les paramètres permettant de spécifier des valeurs de base et d'étendue personnalisées sont disponibles au niveau de privilège avancé.

|                          |                          |
|--------------------------|--------------------------|
| Paramètre client LDAP... | Spécifie personnalisé... |
|--------------------------|--------------------------|

|                 |                                                                                                                                                                                                |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -base-dn        | DN de base pour toutes les valeurs de recherche LDAP il est possible de saisir si nécessaire (par exemple, si la recherche de renvoi LDAP est activée dans ONTAP 9.5 et versions ultérieures). |
| -base-scope     | Portée de base pour toutes les recherches LDAP                                                                                                                                                 |
| -user-dn        | DNS de base pour tous les utilisateurs LDAP. ce paramètre s'applique également aux recherches de mappage de nom d'utilisateur.                                                                 |
| -user-scope     | Portée de base pour toutes les recherches utilisateur LDAP ce paramètre s'applique également aux recherches de mappage de nom d'utilisateur.                                                   |
| -group-dn       | DNS de base pour toutes les recherches de groupes LDAP                                                                                                                                         |
| -group-scope    | Portée de base pour toutes les recherches de groupes LDAP                                                                                                                                      |
| -netgroup-dn    | DNS de base pour toutes les recherches de groupe réseau LDAP                                                                                                                                   |
| -netgroup-scope | Portée de base pour toutes les recherches de groupe réseau LDAP                                                                                                                                |

### Plusieurs valeurs DN de base personnalisées

Si votre structure d'annuaire LDAP est plus complexe, vous devrez peut-être spécifier plusieurs DNS de base pour rechercher des informations dans plusieurs parties de votre annuaire LDAP. Vous pouvez spécifier plusieurs DNS pour les paramètres DN utilisateur, groupe et groupe réseau en les séparant par un point-virgule (;) et en enfermant toute la liste de recherche DN avec des guillemets doubles ("). Si un DN contient un point-virgule, vous devez ajouter un caractère d'échappement (\) immédiatement avant le point-virgule dans le DN.

Notez que le périmètre s'applique à la liste complète de DNS spécifiée pour le paramètre correspondant. Par exemple, si vous spécifiez une liste de trois noms d'utilisateur différents et de sous-arborescence pour l'étendue utilisateur, l'utilisateur LDAP recherche dans l'ensemble de la sous-arborescence pour chacun des trois DNS spécifiés.

Depuis ONTAP 9.5, vous pouvez également spécifier LDAP *recommandation traquer*, qui permet au client LDAP ONTAP de renvoyer des demandes de recherche à d'autres serveurs LDAP si une réponse de recommandation LDAP n'est pas renvoyée par le serveur LDAP principal. Le client utilise ces données de référence pour extraire l'objet cible du serveur décrit dans les données de référence. Pour rechercher des objets présents dans les serveurs LDAP désignés, le dn de base des objets désignés peut être ajouté au dn de base dans le cadre de la configuration du client LDAP. Cependant, les objets renvoyés ne sont examinés que lorsque la recherche de renvoi est activée (à l'aide du `-referral-enabled true`) lors de la création ou de la modification d'un client LDAP.

### Améliorez les performances des recherches LDAP netgroup-par-hôte

Si votre environnement LDAP est configuré pour permettre des recherches netgroup-par-hôte, vous pouvez configurer ONTAP pour en tirer parti et effectuer des recherches netgroup-par-hôte. Cela permet d'accélérer considérablement les recherches sur les



groupes réseau et de réduire les problèmes d'accès aux clients NFS possibles en raison de la latence lors des recherches sur les groupes réseau.

### Ce dont vous avez besoin

Votre annuaire LDAP doit contenir un `netgroup.byhost` carte.

Vos serveurs DNS doivent contenir des enregistrements de recherche avant (A) et arrière (PTR) pour les clients NFS.

Lorsque vous spécifiez des adresses IPv6 dans les groupes réseau, vous devez toujours raccourcir et compresser chaque adresse comme spécifié dans RFC 5952.

### Description de la tâche

Les serveurs NIS stockent les informations de groupe réseau sous trois cartes distinctes appelées `netgroup`, `netgroup.byuser`, et `netgroup.byhost`. Le but du `netgroup.byuser` et `netgroup.byhost` les cartes permettent d'accélérer la recherche de groupes réseau. ONTAP peut effectuer des recherches `netgroup` par hôte sur les serveurs NIS pour améliorer les temps de réponse de montage.

Par défaut, les répertoires LDAP ne possèdent pas ce type de `netgroup.byhost`. Effectuez des mappages comme les serveurs NIS. Il est cependant possible, avec l'aide d'outils tiers, d'importer un NIS `netgroup.byhost`. Effectuez un mappage vers des répertoires LDAP pour permettre des recherches réseau par hôte rapides. Si vous avez configuré votre environnement LDAP pour autoriser des recherches `netgroup-par-hôte`, vous pouvez configurer le client LDAP ONTAP avec le système `netgroup.byhost`. Nom de mappage, DN et étendue de recherche pour des recherches plus rapides avec `netgroup` par hôte.

La réception plus rapide des résultats de recherches `netgroup` par hôte permet à ONTAP de traiter les règles d'exportation plus rapidement lorsque les clients NFS demandent un accès aux exportations. Cela permet de réduire les risques de retard d'accès en raison des problèmes de latence de recherche de groupe réseau.

### Étapes

1. Obtenir le nom distinctif complet exact du NIS `netgroup.byhost` Mapper que vous avez importé dans votre répertoire LDAP.

Le NA de carte peut varier en fonction de l'outil tiers utilisé pour l'importation. Pour des performances optimales, vous devez spécifier le NA correspondant exact.

2. Définissez le niveau de privilège sur avancé : `set -privilege advanced`

3. Activer les recherches `netgroup-by-host` dans la configuration client LDAP de la machine virtuelle de stockage (SVM) : `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost -scope netgroup-by-host_search_scope`

`-is-netgroup-byhost-enabled {true false}` Active ou désactive la recherche `netgroup-par-hôte` pour les répertoires LDAP. La valeur par défaut est `false`.

`-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` spécifie le nom distinctif du `netgroup.byhost` Mapper dans le répertoire LDAP. Il remplace le DN de base pour les recherches `netgroup-par-hôte`. Si vous ne spécifiez pas ce paramètre, ONTAP utilise plutôt le DN de base.

`-netgroup-byhost-scope {base|onelevel subtree}` spécifie l'étendue de recherche pour les recherches `netgroup-par-hôte`. Si vous ne spécifiez pas ce paramètre, le paramètre par défaut est

subtree.

Si la configuration client LDAP n'existe pas encore, vous pouvez activer les recherches netgroup-par-hôte en spécifiant ces paramètres lors de la création d'une nouvelle configuration client LDAP à l'aide de l'`vserver services name-service ldap client create` commande.



À partir de ONTAP 9.2, le champ `-ldap-servers` remplace le champ `-servers`. Ce nouveau champ peut prendre un nom d'hôte ou une adresse IP pour le serveur LDAP.

4. Retour au niveau de privilège admin : `set -privilege admin`

### Exemple

La commande suivante modifie la configuration du client LDAP existante nommée « `ldap_corp` » pour activer les recherches netgroup par hôte à l'aide de l' `netgroup.byhost` Carte nommée `"nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com"` et champ de recherche par défaut `subtree`:

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

### Une fois que vous avez terminé

Le `netgroup.byhost` et `netgroup` les cartes du répertoire doivent être synchronisées en permanence pour éviter tout problème d'accès client.

### Informations associées

["IETF RFC 5952 : une recommandation pour la représentation texte de l'adresse IPv6"](#)

### Utilisez LDAP FAST bind pour l'authentification nsswitch

Depuis ONTAP 9.11.1, vous pouvez bénéficier de la fonctionnalité LDAP *FAST bind* (également appelée *bind* simultanée) pour des requêtes d'authentification client plus rapides et plus simples. Pour utiliser cette fonctionnalité, le serveur LDAP doit prendre en charge la fonctionnalité de liaison rapide.

### Description de la tâche

Sans liaison rapide, ONTAP utilise LDAP simple BIND pour authentifier les utilisateurs admin avec le serveur LDAP. Avec cette méthode d'authentification, ONTAP envoie un nom d'utilisateur ou de groupe au serveur LDAP, reçoit le mot de passe de hachage stocké et compare le code de hachage du serveur avec le code de hachage généré localement à partir du mot de passe de l'utilisateur. S'ils sont identiques, ONTAP accorde l'autorisation de connexion.

Grâce à la fonctionnalité de liaison rapide, ONTAP n'envoie que les informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe) au serveur LDAP via une connexion sécurisée. Le serveur LDAP valide ensuite ces informations d'identification et demande à ONTAP d'accorder des autorisations de connexion.

L'un des avantages de Fast bind est qu'il n'est pas nécessaire que ONTAP prenne en charge chaque nouvel algorithme de hachage pris en charge par les serveurs LDAP, car le hachage du mot de passe est effectué par le serveur LDAP.

["En savoir plus sur l'utilisation de FAST BIND."](#)

Vous pouvez utiliser les configurations client LDAP existantes pour la liaison rapide LDAP. Cependant, il est fortement recommandé de configurer le client LDAP pour TLS ou LDAPS ; dans le cas contraire, le mot de passe est envoyé sur le réseau en texte brut.

Pour activer la liaison rapide LDAP dans un environnement ONTAP, vous devez répondre aux exigences suivantes :

- Les utilisateurs admin ONTAP doivent être configurés sur un serveur LDAP qui prend en charge la liaison rapide.
- Le SVM ONTAP doit être configuré pour LDAP dans la base de données du switch des services de noms (nsswitch).
- Les comptes utilisateur et groupe admin ONTAP doivent être configurés pour l'authentification nsswitch avec le bind rapide.

## Étapes

1. Vérifiez auprès de votre administrateur LDAP que la liaison rapide LDAP est prise en charge sur le serveur LDAP.
2. Assurez-vous que les informations d'identification de l'utilisateur administrateur ONTAP sont configurées sur le serveur LDAP.
3. Vérifier que le SVM admin ou données est configuré correctement pour LDAP FAST BIND.

- a. Pour confirmer que le serveur LDAP FAST BIND est répertorié dans la configuration du client LDAP, entrez :

```
vserver services name-service ldap client show
```

["En savoir plus sur la configuration du client LDAP."](#)

- b. Pour le confirmer ldap est l'une des sources configurées pour le nsswitch passwd base de données, entrez :

```
vserver services name-service ns-switch show
```

["Découvrez la configuration nsswitch."](#)

4. Assurez-vous que les utilisateurs admin s'authentifient auprès de nsswitch et que l'authentification LDAP FAST BIND est activée dans leurs comptes.
  - Pour les utilisateurs existants, entrez `security login modify` et vérifiez les paramètres suivants :

```
-authentication-method nsswitch
```

```
-is-ldap-fastbind true
```
  - Pour les nouveaux utilisateurs admin, voir ["Activez l'accès aux comptes LDAP ou NIS."](#)

## Affiche les statistiques LDAP

Depuis ONTAP 9.2, vous pouvez afficher les statistiques LDAP des serveurs virtuels de stockage (SVM) sur un système de stockage pour surveiller les performances et diagnostiquer les problèmes.

## Ce dont vous avez besoin

- Vous devez avoir configuré un client LDAP sur la SVM.
- Vous devez avoir identifié des objets LDAP à partir desquels vous pouvez afficher des données.

## Étape

1. Afficher les données de performance des objets compteur :

```
statistics show
```

## Exemples

L'exemple suivant montre les données de performances de l'objet `secd_external_service_op`:

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"
```

```
Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
```

| Counter                  | Value                                                                    |
|--------------------------|--------------------------------------------------------------------------|
| instance_name            | vserverName:LDAP (NIS & Name<br>Mapping):GetUserInfoFromName:<br>1.1.1.1 |
| last_modified_time       | 1460610787                                                               |
| node_name                | nodeName                                                                 |
| num_not_found_responses  | 1                                                                        |
| num_request_failures     | 1                                                                        |
| num_requests_sent        | 1                                                                        |
| num_responses_received   | 1                                                                        |
| num_successful_responses | 0                                                                        |
| num_timeouts             | 0                                                                        |
| operation                | GetUserInfoFromName                                                      |
| process_name             | secd                                                                     |
| request_latency          | 52131us                                                                  |

## Configurez les mappages de noms

### Présentation de la configuration des mappages de noms

ONTAP utilise le mappage de noms pour mapper les identités SMB aux identités UNIX, aux identités Kerberos aux identités UNIX et aux identités UNIX aux identités SMB. Il a besoin de ces informations pour obtenir les informations d'identification des utilisateurs et

fournir un accès approprié aux fichiers, qu'ils se connectent depuis un client NFS ou un client SMB.

Il existe deux exceptions lorsque vous n'avez pas besoin d'utiliser le mappage de noms :

- Vous configurez un environnement UNIX pur et ne prévoyez pas d'utiliser l'accès SMB ou le style de sécurité NTFS sur les volumes.
- Vous configurez l'utilisateur par défaut à utiliser à la place.

Dans ce scénario, le mappage de noms n'est pas nécessaire car au lieu de mapper chaque identifiant client individuel, toutes les informations d'identification client sont mappées au même utilisateur par défaut.

Notez que vous pouvez utiliser le mappage de noms uniquement pour les utilisateurs, pas pour les groupes.

Toutefois, vous pouvez mapper un groupe d'utilisateurs individuels à un utilisateur spécifique. Par exemple, vous pouvez mapper tous les utilisateurs AD qui commencent ou se terminent par le mot VENTES à un utilisateur UNIX spécifique et à l'UID de l'utilisateur.

### Fonctionnement du mappage de noms

Lorsque ONTAP doit mapper les informations d'identification d'un utilisateur, il recherche tout d'abord un mappage existant dans la base de données de mappage de noms locaux et le serveur LDAP. Qu'elle vérifie un ou les deux et dans quel ordre est déterminé par la configuration du service de nom du SVM.

- Pour le mappage Windows à UNIX

Si aucun mappage n'est trouvé, ONTAP vérifie si le nom d'utilisateur Windows minuscule est un nom d'utilisateur valide dans le domaine UNIX. Si cela ne fonctionne pas, il utilise l'utilisateur UNIX par défaut à condition qu'il soit configuré. Si l'utilisateur UNIX par défaut n'est pas configuré et que ONTAP ne peut pas obtenir de mappage de cette façon, le mappage échoue et une erreur est renvoyée.

- Pour le mappage d'UNIX à Windows

Si aucun mappage n'est trouvé, ONTAP tente de trouver un compte Windows correspondant au nom UNIX dans le domaine SMB. Si cela ne fonctionne pas, il utilise l'utilisateur SMB par défaut, à condition qu'il soit configuré. Si l'utilisateur SMB par défaut n'est pas configuré et que ONTAP ne peut pas obtenir de mappage de cette façon, le mappage échoue et une erreur est renvoyée.

Par défaut, les comptes machine sont mappés à l'utilisateur UNIX par défaut spécifié. Si aucun utilisateur UNIX par défaut n'est spécifié, les mappages de compte machine échouent.

- À partir de ONTAP 9.5, vous pouvez mapper des comptes machine à des utilisateurs autres que l'utilisateur UNIX par défaut.
- Dans ONTAP 9.4 et versions antérieures, vous ne pouvez pas mapper les comptes machine à d'autres utilisateurs.

Même si des mappages de noms pour des comptes machine sont définis, les mappages sont ignorés.

ONTAP prend en charge les recherches multidomaine lors du mappage d'utilisateurs UNIX aux utilisateurs Windows. Tous les domaines de confiance découverts sont recherchés pour trouver des correspondances avec le modèle de remplacement jusqu'à ce qu'un résultat correspondant soit renvoyé. Vous pouvez également configurer une liste de domaines de confiance préférés, qui est utilisée à la place de la liste de domaines de confiance découverts et est recherchée dans l'ordre jusqu'à ce qu'un résultat correspondant soit renvoyé.

### **La manière dont les approbations de domaine affectent les recherches de mappage de noms d'utilisateur UNIX à des noms d'utilisateur Windows**

Pour comprendre le fonctionnement du mappage de noms d'utilisateur multidomaine, vous devez comprendre comment les approbations de domaine fonctionnent avec ONTAP. Les relations d'approbation Active Directory avec le domaine d'accueil du serveur SMB peuvent être une confiance bidirectionnelle ou l'un des deux types de fiducies unidirectionnelles, soit une confiance entrante, soit une confiance sortante. Le home domain est le domaine auquel le serveur SMB sur le SVM appartient.

- *Confiance bidirectionnelle*

Avec des approbations bidirectionnelles, les deux domaines se font confiance. Si le domaine de base du serveur SMB possède une approbation bidirectionnelle avec un autre domaine, le domaine de base peut authentifier et autoriser un utilisateur appartenant au domaine de confiance, et vice versa.

Les recherches de mappage de noms d'utilisateur UNIX à Windows peuvent être effectuées uniquement sur les domaines avec des approbations bidirectionnelles entre le domaine principal et l'autre domaine.

- *Confiance sortante*

Avec une confiance sortante, le domaine d'origine approuve l'autre domaine. Dans ce cas, le domaine home peut authentifier et autoriser un utilisateur appartenant au domaine de confiance sortant.

Un domaine avec une confiance sortante avec le domaine d'origine est *NOT* recherché lors de l'exécution de recherches de mappage entre utilisateurs UNIX et noms d'utilisateur Windows.

- *Confiance entrante*

Avec une confiance entrante, l'autre domaine fait confiance au domaine d'origine du serveur SMB. Dans ce cas, le domaine personnel ne peut pas authentifier ni autoriser un utilisateur appartenant au domaine de confiance entrant.

Un domaine avec une confiance entrante avec le domaine d'origine est *NOT* recherché lors de l'exécution de recherches de mappage entre utilisateurs UNIX et noms d'utilisateur Windows.

### **Comment les caractères génériques (\*) sont utilisés pour configurer les recherches multidomaines pour le mappage de noms**

Les recherches de mappage de noms de domaines multiples sont facilitées par l'utilisation de caractères génériques dans la section domaine du nom d'utilisateur Windows. Le tableau suivant illustre comment utiliser des caractères génériques dans la partie domaine d'une entrée de mappage de nom pour activer les recherches multidomaine :



## Règles de conversion du mappage de noms

Un système ONTAP conserve un ensemble de règles de conversion pour chaque SVM. Chaque règle se compose de deux éléments : un *pattern* et un *remplacement*. Les conversions commencent au début de la liste appropriée et effectuent une substitution basée sur la première règle correspondante. Le motif est une expression régulière de style UNIX. Le remplacement est une chaîne contenant des séquences d'échappement représentant des sous-expressions du motif, comme dans UNIX `sed` programme.

### Créer un mappage de nom

Vous pouvez utiliser le `vserver name-mapping create` commande permettant de créer un mappage de noms. Vous utilisez les mappages de noms pour permettre aux utilisateurs Windows d'accéder aux volumes du style de sécurité UNIX et les inverser.

### Description de la tâche

Par SVM, ONTAP prend en charge jusqu'à 12,500 mappages de noms dans chaque direction.

### Étape

1. Créer un mappage de noms :

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text
```



Le `-pattern` et `-replacement` les énoncés peuvent être formulés comme des expressions régulières. Vous pouvez également utiliser le `-replacement` instruction pour refuser explicitement un mappage à l'utilisateur en utilisant la chaîne de remplacement nulle " " (le caractère d'espace). Voir la `vserver name-mapping create` page de manuel pour plus de détails.

Lorsque des mappages entre Windows et UNIX sont créés, tous les clients SMB disposant de connexions ouvertes au système ONTAP au moment de la création des nouveaux mappages doivent se déconnecter et se reconnecter pour voir les nouveaux mappages.

### Exemples

La commande suivante crée un nom de mappage sur le SVM nommé `vs1`. Le mappage est un mappage d'UNIX à Windows à la position 1 dans la liste des priorités. Le mappage mappe l'utilisateur UNIX `johnd` à l'utilisateur Windows `ENG\johndoe`.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

La commande suivante crée un autre mappage de nom sur le SVM nommé `vs1`. Le mappage est un mappage de Windows à UNIX à la position 1 dans la liste des priorités. Dans ce cas, le motif et le remplacement incluent des expressions régulières. Le mapping mappe chaque utilisateur CIFS du domaine `ENG` aux utilisateurs du domaine LDAP associé avec la SVM.



```
vs1::> vsserver name-mapping create -vsserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\\1"
```

La commande suivante crée un autre mappage de nom sur le SVM nommé vs1. Ici, le schéma inclut "\$" comme élément du nom d'utilisateur Windows qui doit être échappé. Le mappage mappe l'utilisateur Windows ENG\john\$OPS à l'utilisateur UNIX john\_OPS.

```
vs1::> vsserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

### Configurez l'utilisateur par défaut

Vous pouvez configurer un utilisateur par défaut à utiliser si toutes les autres tentatives de mappage échouent pour un utilisateur, ou si vous ne souhaitez pas mapper des utilisateurs individuels entre UNIX et Windows. Si vous souhaitez que l'authentification des utilisateurs non mappés échoue, vous ne devez pas configurer un utilisateur par défaut.

### Description de la tâche

Pour l'authentification CIFS, si vous ne souhaitez pas mapper chaque utilisateur Windows à un utilisateur UNIX individuel, vous pouvez spécifier un utilisateur UNIX par défaut.

Pour l'authentification NFS, si vous ne souhaitez pas mapper chaque utilisateur UNIX à un utilisateur Windows individuel, vous pouvez spécifier un utilisateur Windows par défaut.

### Étape

1. Effectuez l'une des opérations suivantes :

| Les fonctions que vous recherchez...        | Saisissez la commande suivante...                                      |
|---------------------------------------------|------------------------------------------------------------------------|
| Configurez l'utilisateur UNIX par défaut    | <code>vsserver cifs options modify -default-unix-user user_name</code> |
| Configurez l'utilisateur Windows par défaut | <code>vsserver nfs modify -default-win-user user_name</code>           |

### Commandes permettant de gérer les mappages de noms

Il existe des commandes ONTAP spécifiques permettant de gérer les mappages de noms.

| Les fonctions que vous recherchez... | Utilisez cette commande... |
|--------------------------------------|----------------------------|
|--------------------------------------|----------------------------|

|                                                                                                                                                                        |                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Créer un mappage de nom                                                                                                                                                | <code>vserver name-mapping create</code>                                                                                          |
| Insérez un mappage de nom à une position spécifique                                                                                                                    | <code>vserver name-mapping insert</code>                                                                                          |
| Afficher les mappages de noms                                                                                                                                          | <code>vserver name-mapping show</code>                                                                                            |
| Échangez la position de deux mappages de noms<br>REMARQUE : un échange n'est pas autorisé lorsque le mappage de noms est configuré avec une entrée de qualificatif ip. | <code>vserver name-mapping swap</code>                                                                                            |
| Modifier un mappage de noms                                                                                                                                            | <code>vserver name-mapping modify</code>                                                                                          |
| Supprime un mappage de noms                                                                                                                                            | <code>vserver name-mapping delete</code>                                                                                          |
| Valider le mappage de nom correct                                                                                                                                      | <code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code> |

Consultez la page man pour chaque commande pour plus d'informations.

## Activez l'accès aux clients Windows NFS

ONTAP prend en charge l'accès aux fichiers à partir de clients Windows NFSv3. Cela signifie que les clients exécutant des systèmes d'exploitation Windows avec prise en charge de NFSv3 peuvent accéder aux fichiers lors des exports NFSv3 sur le cluster. Pour utiliser correctement cette fonctionnalité, vous devez configurer correctement le serveur virtuel de stockage (SVM) et connaître certaines exigences et limites.

### Description de la tâche

Par défaut, la prise en charge du client Windows NFSv3 est désactivée.

### Avant de commencer

NFSv3 doit être activé sur le SVM.

### Étapes

1. Activer la prise en charge des clients Windows NFSv3 :

```
vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rotonly disabled
```

2. Sur tous les SVM qui prennent en charge les clients Windows NFSv3, désactivez le `-enable-ejukebox` et `-v3-connection-drop` paramètres :

```
vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection
```

```
-drop disabled
```

Les clients Windows NFSv3 peuvent désormais monter des exportations sur le système de stockage.

3. Assurez-vous que chaque client Windows NFSv3 utilise des montages durs en spécifiant le `-o mtype=hard` option.

Ceci est nécessaire pour garantir la fiabilité des supports.

```
mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
```

## Activer l'affichage des exportations NFS sur les clients NFS

Les clients NFS peuvent utiliser le `showmount -e` Commande pour afficher la liste des exportations disponibles à partir d'un serveur NFS ONTAP. Cela peut aider les utilisateurs à identifier le système de fichiers qu'ils souhaitent monter.

Depuis ONTAP 9.2, ONTAP permet aux clients NFS d'afficher la liste d'export par défaut. Dans les versions précédentes, le `showmount` de la `vserver nfs modify` la commande doit être activée explicitement. Pour afficher la liste d'export, NFSv3 doit être activé sur le SVM.

### Exemple

La commande suivante présente la fonctionnalité `showmount` sur le SVM nommé `vs1` :

```
cluster1 : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount

vs1 enabled
```

La commande suivante exécutée sur un client NFS affiche la liste des exportations sur un serveur NFS avec l'adresse IP 10.63.21.9 :

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix (everyone)
/unix/unix1 (everyone)
/unix/unix2 (everyone)
/ (everyone)
```

## Gérer l'accès aux fichiers à l'aide de NFS

### Activer ou désactiver NFSv3

Vous pouvez activer ou désactiver NFSv3 en modifiant le `-v3` option. Cette fonctionnalité permet aux clients d'accéder aux fichiers via le protocole NFSv3. NFSv3 est activé par défaut.

## Étape

1. Effectuez l'une des opérations suivantes :

| Les fonctions que vous recherchez... | Entrez la commande...                                              |
|--------------------------------------|--------------------------------------------------------------------|
| Activez NFSv3                        | <code>vserver nfs modify -vserver vserver_name -v3 enabled</code>  |
| Désactiver NFSv3                     | <code>vserver nfs modify -vserver vserver_name -v3 disabled</code> |

## Activez ou désactivez NFSv4.0

Vous pouvez activer ou désactiver NFSv4.0 en modifiant le `-v4.0` option. Cela permet d'accéder aux fichiers pour les clients utilisant le protocole NFSv4.0. Dans ONTAP 9.9.1, NFSv4.0 est activé par défaut ; dans les versions antérieures, il est désactivé par défaut.

## Étape

1. Effectuez l'une des opérations suivantes :

| Les fonctions que vous recherchez... | Saisissez la commande suivante...                                    |
|--------------------------------------|----------------------------------------------------------------------|
| Activer NFSv4.0                      | <code>vserver nfs modify -vserver vserver_name -v4.0 enabled</code>  |
| Désactivez NFSv4.0                   | <code>vserver nfs modify -vserver vserver_name -v4.0 disabled</code> |

## Activer ou désactiver NFSv4.1

Vous pouvez activer ou désactiver NFSv4.1 en modifiant `-v4.1` option. Ainsi, les clients bénéficient d'un accès aux fichiers à l'aide du protocole NFSv4.1. Dans ONTAP 9.9.1, NFSv4.1 est activé par défaut. Dans les versions antérieures, il est désactivé par défaut.

## Étape

1. Effectuez l'une des opérations suivantes :

| Les fonctions que vous recherchez... | Saisissez la commande suivante...                                    |
|--------------------------------------|----------------------------------------------------------------------|
| Activation de NFSv4.1                | <code>vserver nfs modify -vserver vserver_name -v4.1 enabled</code>  |
| Désactiver NFSv4.1                   | <code>vserver nfs modify -vserver vserver_name -v4.1 disabled</code> |

## Gestion des limites des pools de stockage NFSv4

À partir de ONTAP 9.13, les administrateurs peuvent activer leurs serveurs NFSv4 pour refuser des ressources aux clients NFSv4 lorsqu'ils ont atteint les limites de ressources de pool de stockage par client. Lorsque les clients consomment trop de ressources de pool de stockage NFSv4, cela peut entraîner le blocage d'autres clients NFSv4 en raison de l'indisponibilité des ressources de pool de stockage NFSv4.

L'activation de cette fonction permet également aux clients d'afficher la consommation de ressources du pool de stockage actif par chaque client. Cela facilite l'identification des clients qui épuise les ressources système et permet d'imposer des limites de ressources par client.

### Afficher les ressources de pool de stockage consommées

Le `vserver nfs storepool show` affiche le nombre de ressources de pool de stockage utilisées. Un pool de stockage est un pool de ressources utilisé par les clients NFSv4.

#### Étape

1. En tant qu'administrateur, exécutez `vserver nfs storepool show` Commande permettant d'afficher les informations de réserve des clients NFSv4.

#### Exemple

Cet exemple affiche les informations relatives au pool de stockage des clients NFSv4.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-IP: 10.0.1.1

Client-IP Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

10.0.2.1 nfs4.1 true 2 1 0 4

10.0.2.2 nfs4.2 true 2 1 0 4

2 entries were displayed.
```

### Activer ou désactiver les contrôles de limite de pool de stockage

Les administrateurs peuvent utiliser les commandes suivantes pour activer ou désactiver les contrôles de limite de pool de stockage.

#### Étape

1. En tant qu'administrateur, effectuez l'une des opérations suivantes :

| Les fonctions que vous recherchez...                   | Saisissez la commande suivante...                                        |
|--------------------------------------------------------|--------------------------------------------------------------------------|
| Activer les contrôles de limite de pool de stockage    | <code>vserver nfs storepool config modify -limit-enforce enabled</code>  |
| Désactiver les contrôles de limite de pool de stockage | <code>vserver nfs storepool config modify -limit-enforce disabled</code> |

#### Afficher la liste des clients bloqués

Si la limite de réserve est activée, les administrateurs peuvent voir quels clients ont été bloqués lorsqu'ils ont atteint leur seuil de ressources par client. Les administrateurs peuvent utiliser la commande suivante pour voir quels clients ont été marqués comme des clients bloqués.

#### Étapes

1. Utilisez le `vserver nfs storepool blocked-client show` Commande permettant d'afficher la liste des clients bloqués par NFSv4.

#### Supprimer un client de la liste des clients bloqués

Les clients qui atteignent leur seuil par client seront déconnectés et ajoutés au cache client-bloc. Les administrateurs peuvent utiliser la commande suivante pour supprimer le client du cache du client de bloc. Cela permettra au client de se connecter au serveur ONTAP NFSV4.

#### Étapes

1. Utilisez le `vserver nfs storepool blocked-client flush -client-ip <ip address>` commande permettant de vider le cache client bloqué du pool de stockage.
2. Utilisez le `vserver nfs storepool blocked-client show` commande permettant de vérifier que le client a été supprimé du cache du client en mode bloc.

#### Exemple

Cet exemple affiche un client bloqué dont l'adresse IP "10.2.1.1" est vidée de tous les nœuds.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP

10.1.1.1

1 entries were displayed.
```

## Activer ou désactiver pNFS

pNFS améliore les performances en permettant aux clients NFS d'effectuer des opérations de lecture/écriture sur les périphériques de stockage directement et en parallèle, en contournant le serveur NFS comme un goulot d'étranglement potentiel. Pour activer ou désactiver pNFS (Parallel NFS), vous pouvez modifier le `-v4.1-pnfs` option.

| Si la version de ONTAP est... | La norme pNFS par défaut est... |
|-------------------------------|---------------------------------|
| 9.8 ou ultérieure             | désactivé                       |
| 9.7 ou antérieure             | activé                          |

### Ce dont vous avez besoin

La prise en charge de NFSv4.1 est requise pour pouvoir utiliser pNFS.

Si vous souhaitez activer pNFS, vous devez d'abord désactiver les référencements NFS. Les deux ne peuvent pas être activées en même temps.

Si vous utilisez pNFS avec Kerberos sur des SVM, il faut activer Kerberos sur chaque LIF de la SVM.

### Étape

1. Effectuez l'une des opérations suivantes :

| Les fonctions que vous recherchez... | Entrez la commande...                                                       |
|--------------------------------------|-----------------------------------------------------------------------------|
| Activez pNFS                         | <pre>vserver nfs modify -vserver<br/>vserver_name -v4.1-pnfs enabled</pre>  |
| Désactiver pNFS                      | <pre>vserver nfs modify -vserver<br/>vserver_name -v4.1-pnfs disabled</pre> |

### Informations associées

- [Présentation de l'agrégation NFS](#)

### Contrôle de l'accès NFS sur TCP et UDP

Vous pouvez activer ou désactiver l'accès NFS aux serveurs virtuels de stockage (SVM) via TCP et UDP en modifiant le `-tcp` et `-udp` paramètres, respectivement. Vous pouvez ainsi contrôler l'accès des clients NFS aux données via TCP ou UDP dans votre environnement.

### Description de la tâche

Ces paramètres s'appliquent uniquement à NFS. Ils n'affectent pas les protocoles auxiliaires. Par exemple, si NFS sur TCP est désactivé, les opérations de montage sur TCP ont toujours réussi. Pour bloquer complètement le trafic TCP ou UDP, vous pouvez utiliser des règles d'export-policy.



Vous devez désactiver le serveur RPC SnapDiff avant de désactiver TCP pour NFS pour éviter une erreur de commande. Vous pouvez désactiver TCP en utilisant la commande `vserver snapdiff-rpc-server off -vserver vserver name`.

## Étape

1. Effectuez l'une des opérations suivantes :

| Si vous souhaitez obtenir un accès NFS... | Entrez la commande...                                               |
|-------------------------------------------|---------------------------------------------------------------------|
| Activé sur TCP                            | <code>vserver nfs modify -vserver vserver_name -tcp enabled</code>  |
| Désactivé sur TCP                         | <code>vserver nfs modify -vserver vserver_name -tcp disabled</code> |
| Activé sur UDP                            | <code>vserver nfs modify -vserver vserver_name -udp enabled</code>  |
| Désactivé sur UDP                         | <code>vserver nfs modify -vserver vserver_name -udp disabled</code> |

## Contrôlez les demandes NFS à partir de ports non réservés

Vous pouvez rejeter les demandes de montage NFS à partir de ports non réservés en activant le `-mount-rootonly` option. Pour rejeter toutes les demandes NFS de ports non réservés, vous pouvez activer le `-nfs-rootonly` option.

### Description de la tâche

Par défaut, l'option `-mount-rootonly` est enabled.

Par défaut, l'option `-nfs-rootonly` est disabled.

Ces options ne s'appliquent pas à la procédure NULL.

## Étape

1. Effectuez l'une des opérations suivantes :

| Les fonctions que vous recherchez...                                 | Entrez la commande...                                                           |
|----------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Autoriser les demandes de montage NFS à partir de ports non réservés | <code>vserver nfs modify -vserver vserver_name -mount -rootonly disabled</code> |
| Rejeter les demandes de montage NFS à partir de ports non réservés   | <code>vserver nfs modify -vserver vserver_name -mount -rootonly enabled</code>  |
| Autoriser toutes les demandes NFS à partir de ports non réservés     | <code>vserver nfs modify -vserver vserver_name -nfs -rootonly disabled</code>   |



|                                                       |                                                                              |
|-------------------------------------------------------|------------------------------------------------------------------------------|
| Rejeter toutes les demandes NFS de ports non réservés | <code>vserver nfs modify -vserver vserver_name -nfs -rootonly enabled</code> |
|-------------------------------------------------------|------------------------------------------------------------------------------|

Gérer l'accès NFS aux volumes NTFS ou aux qtrees pour les utilisateurs UNIX inconnus

Si ONTAP ne peut pas identifier les utilisateurs UNIX qui tentent de se connecter à des volumes ou des qtrees avec le style de sécurité NTFS, il ne peut donc pas mapper l'utilisateur de façon explicite à un utilisateur Windows. Vous pouvez configurer ONTAP de manière à refuser l'accès à ces utilisateurs pour une sécurité plus stricte ou les mapper à un utilisateur Windows par défaut afin d'assurer un niveau d'accès minimum pour tous les utilisateurs.

Ce dont vous avez besoin

Un utilisateur Windows par défaut doit être configuré si vous souhaitez activer cette option.

Description de la tâche

Si un utilisateur UNIX tente d'accéder aux volumes ou aux qtrees avec un style de sécurité NTFS, l'utilisateur UNIX doit d'abord être mappé à un utilisateur Windows afin que ONTAP puisse correctement évaluer les autorisations NTFS. Cependant, si ONTAP ne peut pas rechercher le nom de l'utilisateur UNIX dans les sources de service de nom d'informations utilisateur configurées, il ne peut pas explicitement mapper l'utilisateur UNIX à un utilisateur Windows spécifique. Vous pouvez décider comment gérer ces utilisateurs UNIX inconnus de la manière suivante :

- Refuser l'accès aux utilisateurs UNIX inconnus.
- Ceci met en œuvre une sécurité plus stricte en nécessitant un mappage explicite pour tous les utilisateurs UNIX afin d'accéder aux volumes ou aux qtrees NTFS.
- Mapper des utilisateurs UNIX inconnus à un utilisateur Windows par défaut.

Cette fonctionnalité offre moins de sécurité et davantage de commodité, en veillant à ce que tous les utilisateurs aient un niveau d'accès minimal aux volumes NTFS ou aux qtrees par l'intermédiaire d'un utilisateur Windows par défaut.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Effectuez l'une des opérations suivantes :

|                                                                                            |                                                                                                         |
|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Si vous voulez que l'utilisateur Windows par défaut pour les utilisateurs UNIX inconnus... | Entrez la commande...                                                                                   |
| Activé                                                                                     | <code>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled</code> |

|           |                                                                                                          |
|-----------|----------------------------------------------------------------------------------------------------------|
| Désactivé | <code>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled</code> |
|-----------|----------------------------------------------------------------------------------------------------------|

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

### Considérations relatives aux clients qui montent des exportations NFS à l'aide d'un port non réservé

Le `-mount-rootonly` L'option doit être désactivée sur un système de stockage qui doit prendre en charge les clients qui montent des exportations NFS à l'aide d'un port non réservé, même lorsque l'utilisateur est connecté en tant que root. Ces clients comprennent les clients Hummingbird et les clients Solaris NFS/IPv6.

Si le `-mount-rootonly` ONTAP n'autorise pas les clients NFS utilisant des ports non réservés. Ainsi, les ports dont les numéros sont supérieurs à 1,023, ne permettent pas le montage des exports NFS.

### Effectuer des contrôles d'accès plus stricts pour les groupes réseau en vérifiant les domaines

Par défaut, ONTAP effectue une vérification supplémentaire lors de l'évaluation de l'accès client pour un groupe réseau. Cette vérification supplémentaire garantit que le domaine du client correspond à la configuration de domaine de la machine virtuelle de stockage (SVM). Sinon, ONTAP refuse l'accès client.

#### Description de la tâche

Lorsque ONTAP évalue les règles d'export policy pour l'accès client et qu'une règle d'export policy contient un netgroup, ONTAP doit déterminer si l'adresse IP d'un client appartient au netgroup. Pour ce faire, ONTAP convertit l'adresse IP du client en un nom d'hôte à l'aide du DNS et obtient un nom de domaine complet (FQDN).

Si le fichier netgroup répertorie uniquement un nom court pour l'hôte et que le nom court de l'hôte existe dans plusieurs domaines, il est possible qu'un client d'un domaine différent obtienne un accès sans cette vérification.

Pour empêcher cela, ONTAP compare le domaine renvoyé par DNS pour l'hôte avec la liste des noms de domaine DNS configurés pour le SVM. Si la correspondance correspond, l'accès est autorisé. Si ce n'est pas le cas, l'accès est refusé.

Cette vérification est activée par défaut. Vous pouvez le gérer en modifiant le `-netgroup-dns-domain-search` paramètre, disponible au niveau de privilège avancé.

#### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Effectuez l'action souhaitée :

| Si vous voulez que la vérification de domaine pour les groupes réseau soit... | Entrer...                                                                                   |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Activé                                                                        | <code>vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled</code>  |
| Désactivé                                                                     | <code>vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled</code> |

3. Définissez le niveau de privilège sur admin :

```
set -privilege admin
```

### Modifier les ports utilisés pour les services NFSv3

Le serveur NFS du système de stockage utilise des services tels que le démon de montage et Network Lock Manager pour communiquer avec les clients NFS sur des ports réseau par défaut spécifiques. Dans la plupart des environnements NFS, les ports par défaut fonctionnent correctement et ne nécessitent pas de modification, mais si vous souhaitez utiliser différents ports réseau NFS dans votre environnement NFSv3, vous pouvez le faire.

#### Ce dont vous avez besoin

La modification des ports NFS sur le système de stockage requiert que tous les clients NFS se connectent au système. Il est donc important de communiquer ces informations aux utilisateurs avant de faire la modification.

#### Description de la tâche

Vous pouvez définir les ports utilisés par les services du démon de montage NFS, Network Lock Manager, Network Status Monitor et NFS quota daemon pour chaque machine virtuelle de stockage (SVM). La modification du numéro de port affecte l'accès des clients NFS aux données via TCP et UDP.

Les ports pour NFSv4 et NFSv4.1 ne peuvent pas être modifiés.

#### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Désactivation de l'accès à NFS :

```
vserver nfs modify -vserver vserver_name -access false
```

3. Définissez le port NFS pour le service NFS spécifique :

```
vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
```

| Paramètre du port NFS | Description                         | Port par défaut |
|-----------------------|-------------------------------------|-----------------|
| -mountd-port          | Démon de montage NFS                | 658             |
| -nlm-port             | Gestionnaire de verrouillage réseau | 4045            |
| -nsm-port             | Moniteur d'état du réseau           | 4046            |
| -rquotad-port         | Démon de quota NFS                  | 4049            |

Outre le port par défaut, la plage autorisée de numéros de port est comprise entre 1024 et 65535. Chaque service NFS doit utiliser un port unique.

#### 4. Activation de l'accès au NFS :

```
vserver nfs modify -vserver vserver_name -access true
```

#### 5. Utilisez le `network connections listening show` pour vérifier que le numéro de port change.

#### 6. Retour au niveau de privilège admin :

```
set -privilege admin
```

### Exemple

Les commandes suivantes définissent le port NFS Mount Daemon sur 1113 sur le SVM nommé vs1 :

```

vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
 them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name Interface Name:Local Port Protocol/Service


Node: cluster1-01
Cluster cluster1-01_clus_1:7700 TCP/ctlopcp
vs1 data1:4046 TCP/sm
vs1 data1:4046 UDP/sm
vs1 data1:4045 TCP/nlm-v4
vs1 data1:4045 UDP/nlm-v4
vs1 data1:1113 TCP/mount
vs1 data1:1113 UDP/mount
...
vs1::*> set -privilege admin

```

## Commandes pour la gestion des serveurs NFS

Il existe des commandes ONTAP spécifiques pour gérer les serveurs NFS.

| Les fonctions que vous recherchez... | Utilisez cette commande...      |
|--------------------------------------|---------------------------------|
| Créez un serveur NFS                 | <code>vserver nfs create</code> |
| Affichez les serveurs NFS            | <code>vserver nfs show</code>   |
| Modifier un serveur NFS              | <code>vserver nfs modify</code> |
| Supprimer un serveur NFS             | <code>vserver nfs delete</code> |

|                                                                                                                                                                                                                                    |                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| <p>Masquer le <code>.snapshot</code> Liste de répertoires sous points de montage NFSv3</p>                                                                                                                                         | <p><code>vserver nfs</code> commandes avec le <code>-v3-hide-snapshot</code> option activée</p> |
| <div> <div></div> <div> <p>Accès explicite au <code>.snapshot</code> le répertoire reste autorisé même si l'option est activée.</p> </div> </div> |                                                                                                 |

Consultez la page man pour chaque commande pour plus d'informations.

## Résoudre les problèmes de service de noms

Lorsque les clients rencontrent des échecs d'accès en raison de problèmes de service de nom, vous pouvez utiliser le `vserver services name-service getxxbyyy` famille de commandes pour effectuer manuellement différentes recherches de services de noms et examiner les détails et les résultats de la recherche pour faciliter le dépannage.

### Description de la tâche

- Pour chaque commande, vous pouvez spécifier les éléments suivants :

- Nom du nœud ou de la machine virtuelle de stockage (SVM) à effectuer la recherche.

Cela vous permet de tester les recherches de service de noms pour un nœud ou un SVM spécifique afin de limiter la recherche de problèmes potentiels de configuration du service de noms.

- Indique si la source utilisée pour la recherche doit être utilisée.

Cela vous permet de vérifier si la source correcte a été utilisée.

- ONTAP sélectionne le service pour effectuer la recherche en fonction de l'ordre de commutation de service de noms configuré.
- Ces commandes sont disponibles au niveau de privilège avancé.

### Étapes

1. Effectuez l'une des opérations suivantes :

| Pour récupérer...                    | Utilisez la commande...                                                                                                                                           |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Adresse IP d'un nom d'hôte           | <code>vserver services name-service getxxbyyy getaddrinfo</code><br><code>vserver services name-service getxxbyyy gethostbyname</code> (Adresses IPv4 uniquement) |
| Membres d'un groupe par ID de groupe | <code>vserver services name-service getxxbyyy getgrbygid</code>                                                                                                   |

|                                                                                        |                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Membres d'un groupe par nom de groupe                                                  | <code>vserver services name-service getxxbyyy getgrbyname</code>                                                                                                                                                |
| Liste des groupes auxquels un utilisateur appartient                                   | <code>vserver services name-service getxxbyyy getgrlist</code>                                                                                                                                                  |
| Nom d'hôte d'une adresse IP                                                            | <code>vserver services name-service getxxbyyy getnameinfo</code><br><code>vserver services name-service getxxbyyy gethostbyaddr</code> (Adresses IPv4 uniquement)                                               |
| Informations sur l'utilisateur par nom d'utilisateur                                   | <code>vserver services name-service getxxbyyy getpwbyname</code><br>Vous pouvez tester la résolution des noms des utilisateurs RBAC en spécifiant le <code>-use -rbac</code> ens. paramètre <code>true</code> . |
| Informations utilisateur par ID utilisateur                                            | <code>vserver services name-service getxxbyyy getpwbyuid</code><br>Vous pouvez tester la résolution des noms des utilisateurs RBAC en spécifiant le <code>-use -rbac</code> ens. paramètre <code>true</code> .  |
| Appartenance au groupe réseau d'un client                                              | <code>vserver services name-service getxxbyyy netgrp</code>                                                                                                                                                     |
| Appartenance à un groupe réseau d'un client à l'aide de la recherche netgroup par hôte | <code>vserver services name-service getxxbyyy netgrpbyhost</code>                                                                                                                                               |

L'exemple suivant montre un test de recherche DNS pour le SVM vs1 en essayant d'obtenir l'adresse IP pour l'hôte `acast1.eng.example.com` :

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

L'exemple suivant montre un test de recherche NIS pour le SVM vs1 en essayant de récupérer les informations utilisateur pour un utilisateur avec l'UID 501768 :

```
cluster1::~*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: 1y8rA4XX7$/DDOXAvC2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

L'exemple suivant montre un test de recherche LDAP pour le SVM vs1 en tentant de récupérer les informations utilisateur d'un utilisateur portant le nom ldap1 :

```
cluster1::~*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

L'exemple suivant montre un test de recherche de groupe réseau pour le SVM vs1 en essayant de déterminer si le client dnshost0 est membre du groupe netgroup136 :

```
cluster1::~*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. Analysez les résultats du test que vous avez effectué et prenez les mesures nécessaires.

| Si...                                                                                     | Vérifiez le...                                    |
|-------------------------------------------------------------------------------------------|---------------------------------------------------|
| La recherche de nom d'hôte ou d'adresse IP a échoué ou a produit des résultats incorrects | Configuration DNS                                 |
| Recherche interrogea une source incorrecte                                                | Nommer la configuration du commutateur de service |



| Si...                                                                                                                     | Vérifiez le...                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| La recherche d'utilisateur ou de groupe a échoué ou a produit des résultats incorrects                                    | <ul style="list-style-type: none"> <li>• Nommer la configuration du commutateur de service</li> <li>• Configuration source (fichiers locaux, domaine NIS, client LDAP)</li> <li>• Configuration du réseau (par exemple, LIFs et routes)</li> </ul> |
| La recherche de nom d'hôte a échoué ou a expiré et le serveur DNS ne résout pas les noms courts DNS (par exemple, host1). | Configuration DNS pour les requêtes de domaine de premier niveau (TLD). Vous pouvez désactiver les requêtes TLD à l'aide du <code>-is-tld-query-enabled false</code> à la <code>vserver services name-service dns modify</code> commande.          |

### Informations associées

["Rapport technique de NetApp 4668 : name Services Best Practices Guide \(Guide des meilleures pratiques des services de noms\)"](#)

### Vérifiez le nom des connexions de service

Depuis ONTAP 9.2, vous pouvez vérifier les serveurs de noms DNS et LDAP pour vous assurer qu'ils sont connectés à ONTAP. Ces commandes sont disponibles au niveau de privilège admin.

### Description de la tâche

Vous pouvez vérifier que la configuration du service de noms DNS ou LDAP est valide selon les besoins à l'aide du vérificateur de configuration du service de noms. Cette vérification de validation peut être lancée en ligne de commande ou dans System Manager.

Pour les configurations DNS, tous les serveurs sont testés et doivent fonctionner pour que la configuration soit considérée comme valide. Pour les configurations LDAP, tant qu'un serveur est en service, la configuration est valide. Les commandes `name service` appliquent le vérificateur de configuration sauf `skip-config-validation` le champ est vrai (la valeur par défaut est faux).

### Étape

1. Utiliser la commande appropriée pour vérifier la configuration du service de noms. L'interface utilisateur affiche l'état des serveurs configurés.

| Pour vérifier...              | Utilisez cette commande...                            |
|-------------------------------|-------------------------------------------------------|
| État de la configuration DNS  | <code>vserver services name-service dns check</code>  |
| État de la configuration LDAP | <code>vserver services name-service ldap check</code> |

```
cluster1::> vserver services name-service dns check -vserver vs0
```

| Vserver | Name Server | Status | Status Details           |
|---------|-------------|--------|--------------------------|
| vs0     | 10.11.12.13 | up     | Response time (msec): 55 |
| vs0     | 10.11.12.14 | up     | Response time (msec): 70 |
| vs0     | 10.11.12.15 | down   | Connection refused.      |

```
cluster1::> vserver services name-service ldap check -vserver vs0
```

```
| Vserver: vs0 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
"10.11.12.13". |
```

La validation de la configuration est réussie si au moins un des serveurs configurés (name-Server/ldap-servers) est accessible et fournit le service. Un avertissement est affiché si certains serveurs sont inaccessibles.

## Commandes permettant de gérer les entrées des commutateurs de service de noms

Vous pouvez gérer les entrées de commutateur de service de noms en les créant, en les affichant, en les modifiant et en les supprimant.

| Les fonctions que vous recherchez...                   | Utilisez cette commande...                                  |
|--------------------------------------------------------|-------------------------------------------------------------|
| Créer une entrée de commutateur de service de nom      | <code>vserver services name-service ns-switch create</code> |
| Afficher les entrées du commutateur d'entretien du nom | <code>vserver services name-service ns-switch show</code>   |
| Modifier une entrée de commutateur de service de nom   | <code>vserver services name-service ns-switch modify</code> |
| Supprimer une entrée de commutateur de service de nom  | <code>vserver services name-service ns-switch delete</code> |

Consultez la page man pour chaque commande pour plus d'informations.

## Informations associées

["Rapport technique de NetApp 4668 : name Services Best Practices Guide \(Guide des meilleures pratiques des services de noms\)"](#)

## Commandes permettant de gérer le cache du service de noms

Vous pouvez gérer le cache du service de noms en modifiant la valeur TTL (Time to live). La valeur TTL détermine la persistance des informations de service de noms longs dans le cache.

| Si vous souhaitez modifier la valeur TTL pour... | Utilisez cette commande...                                                 |
|--------------------------------------------------|----------------------------------------------------------------------------|
| Utilisateurs UNIX                                | <code>vserver services name-service cache unix-user settings</code>        |
| Groupes UNIX                                     | <code>vserver services name-service cache unix-group settings</code>       |
| Netgroups UNIX                                   | <code>vserver services name-service cache netgroups settings</code>        |
| Hôtes                                            | <code>vserver services name-service cache hosts settings</code>            |
| Appartenance à un groupe                         | <code>vserver services name-service cache group-membership settings</code> |

### Informations associées

["Référence de commande ONTAP"](#)

## Commandes permettant de gérer les mappages de noms

Il existe des commandes ONTAP spécifiques permettant de gérer les mappages de noms.

| Les fonctions que vous recherchez...                                                                                                                                   | Utilisez cette commande...               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| Créer un mappage de nom                                                                                                                                                | <code>vserver name-mapping create</code> |
| Insérez un mappage de nom à une position spécifique                                                                                                                    | <code>vserver name-mapping insert</code> |
| Afficher les mappages de noms                                                                                                                                          | <code>vserver name-mapping show</code>   |
| Échangez la position de deux mappages de noms<br>REMARQUE : un échange n'est pas autorisé lorsque le mappage de noms est configuré avec une entrée de qualificatif ip. | <code>vserver name-mapping swap</code>   |

|                                   |                                                                                                                                   |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Modifier un mappage de noms       | <code>vserver name-mapping modify</code>                                                                                          |
| Supprime un mappage de noms       | <code>vserver name-mapping delete</code>                                                                                          |
| Valider le mappage de nom correct | <code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code> |

Consultez la page man pour chaque commande pour plus d'informations.

### Commandes permettant de gérer les utilisateurs UNIX locaux

Il existe des commandes ONTAP spécifiques pour gérer les utilisateurs UNIX locaux.

| Les fonctions que vous recherchez...                      | Utilisez cette commande...                                         |
|-----------------------------------------------------------|--------------------------------------------------------------------|
| Créer un utilisateur UNIX local                           | <code>vserver services name-service unix-user create</code>        |
| Chargement des utilisateurs UNIX locaux à partir d'un URI | <code>vserver services name-service unix-user load-from-uri</code> |
| Afficher les utilisateurs UNIX locaux                     | <code>vserver services name-service unix-user show</code>          |
| Modifier un utilisateur UNIX local                        | <code>vserver services name-service unix-user modify</code>        |
| Supprimer un utilisateur UNIX local                       | <code>vserver services name-service unix-user delete</code>        |

Consultez la page man pour chaque commande pour plus d'informations.

### Commandes permettant de gérer les groupes UNIX locaux

Il existe des commandes ONTAP spécifiques pour gérer les groupes UNIX locaux.

| Les fonctions que vous recherchez...                 | Utilisez cette commande...                                          |
|------------------------------------------------------|---------------------------------------------------------------------|
| Créer un groupe UNIX local                           | <code>vserver services name-service unix-group create</code>        |
| Ajouter un utilisateur à un groupe UNIX local        | <code>vserver services name-service unix-group adduser</code>       |
| Chargement des groupes UNIX locaux à partir d'un URI | <code>vserver services name-service unix-group load-from-uri</code> |
| Afficher les groupes UNIX locaux                     | <code>vserver services name-service unix-group show</code>          |

|                                                 |                                                               |
|-------------------------------------------------|---------------------------------------------------------------|
| Modifier un groupe UNIX local                   | <code>vserver services name-service unix-group modify</code>  |
| Supprimer un utilisateur d'un groupe UNIX local | <code>vserver services name-service unix-group deluser</code> |
| Supprimer un groupe UNIX local                  | <code>vserver services name-service unix-group delete</code>  |

Consultez la page man pour chaque commande pour plus d'informations.

### Limites pour les utilisateurs, groupes et membres UNIX locaux

ONTAP a introduit des limites au nombre maximal d'utilisateurs et de groupes UNIX dans le cluster, et des commandes pour gérer ces limites. Ces limites peuvent aider à éviter les problèmes de performances en empêchant les administrateurs de créer un trop grand nombre d'utilisateurs et de groupes UNIX locaux au sein du cluster.

Il existe une limite pour le nombre combiné de groupes d'utilisateurs UNIX locaux et de membres de groupe. Il existe une limite distincte pour les utilisateurs UNIX locaux. Les limites portent à l'échelle du cluster. Chacune de ces nouvelles limites est définie sur une valeur par défaut que vous pouvez modifier jusqu'à une limite stricte préaffectée.

| Base de données                           | Limite par défaut | Limitation stricte |
|-------------------------------------------|-------------------|--------------------|
| Utilisateurs UNIX locaux                  | 32,768            | 65,536             |
| Groupes UNIX locaux et membres de groupes | 32,768            | 65,536             |

### Gérez les limites des utilisateurs et groupes UNIX locaux

Il existe des commandes ONTAP spécifiques permettant de gérer les limites des utilisateurs et groupes UNIX locaux. Les administrateurs du cluster peuvent utiliser ces commandes pour résoudre les problèmes de performances qui, selon eux, seraient liés à un nombre excessif d'utilisateurs et de groupes UNIX locaux.

#### Description de la tâche

Ces commandes sont disponibles pour l'administrateur du cluster au niveau de privilège avancé.

#### Étape

1. Effectuez l'une des opérations suivantes :

| Les fonctions que vous recherchez...                                  | Utilisez la commande...                                |
|-----------------------------------------------------------------------|--------------------------------------------------------|
| Affiche des informations sur les limites des utilisateurs UNIX locaux | <code>vserver services unix-user max-limit show</code> |

| Les fonctions que vous recherchez...                            | Utilisez la commande...                                   |
|-----------------------------------------------------------------|-----------------------------------------------------------|
| Affiche des informations sur les limites de groupe UNIX locales | <code>vserver services unix-group max-limit show</code>   |
| Modifier les limites des utilisateurs UNIX locaux               | <code>vserver services unix-user max-limit modify</code>  |
| Modifier les limites du groupe UNIX local                       | <code>vserver services unix-group max-limit modify</code> |

Consultez la page man pour chaque commande pour plus d'informations.

### Commandes de gestion des groupes réseau locaux

Vous pouvez gérer les groupes réseau locaux en les chargeant à partir d'un URI, en vérifiant leur état sur les nœuds, en les affichant et en les supprimant.

| Les fonctions que vous recherchez...             | Utilisez la commande...                                                                                                            |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Charger des groupes réseau à partir d'un URI     | <code>vserver services name-service netgroup load</code>                                                                           |
| Vérifiez l'état des groupes réseau sur les nœuds | <code>vserver services name-service netgroup status</code><br><br>Disponible au niveau de privilège avancé et au niveau supérieur. |
| Afficher les groupes réseau locaux               | <code>vserver services name-service netgroup file show</code>                                                                      |
| Supprimer un groupe réseau local                 | <code>vserver services name-service netgroup file delete</code>                                                                    |

Consultez la page man pour chaque commande pour plus d'informations.

### Commandes pour la gestion des configurations de domaine NIS

Il existe des commandes ONTAP spécifiques pour gérer les configurations de domaine NIS.

| Les fonctions que vous recherchez...      | Utilisez cette commande...                                   |
|-------------------------------------------|--------------------------------------------------------------|
| Créez une configuration de domaine NIS    | <code>vserver services name-service nis-domain create</code> |
| Affiche les configurations de domaine NIS | <code>vserver services name-service nis-domain show</code>   |

|                                                                |                                                                                                                                                        |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Affiche l'état de liaison d'une configuration de domaine NIS   | <code>vserver services name-service nis-domain show-bound</code>                                                                                       |
| Affiche les statistiques NIS                                   | <code>vserver services name-service nis-domain show-statistics</code> Disponible au niveau de privilège avancé et au niveau supérieur.                 |
| Effacer les statistiques NIS                                   | <code>vserver services name-service nis-domain clear-statistics</code> Disponible au niveau de privilège avancé et au niveau supérieur.                |
| Modifier une configuration de domaine NIS                      | <code>vserver services name-service nis-domain modify</code>                                                                                           |
| Supprimer une configuration de domaine NIS                     | <code>vserver services name-service nis-domain delete</code>                                                                                           |
| Activer la mise en cache pour les recherches netgroup-par-hôte | <code>vserver services name-service nis-domain netgroup-database config modify</code> Disponible au niveau de privilège avancé et au niveau supérieur. |

Consultez la page man pour chaque commande pour plus d'informations.

### Commandes permettant de gérer les configurations du client LDAP

Il existe des commandes ONTAP spécifiques pour gérer les configurations du client LDAP.



Les administrateurs du SVM ne peuvent ni modifier ni supprimer les configurations du client LDAP créées par les administrateurs du cluster.

| Les fonctions que vous recherchez...               | Utilisez cette commande...                                                  |
|----------------------------------------------------|-----------------------------------------------------------------------------|
| Créez une configuration client LDAP                | <code>vserver services name-service ldap client create</code>               |
| Affiche les configurations du client LDAP          | <code>vserver services name-service ldap client show</code>                 |
| Modifier une configuration client LDAP             | <code>vserver services name-service ldap client modify</code>               |
| Modifiez le mot de passe DE LIAISON du client LDAP | <code>vserver services name-service ldap client modify-bind-password</code> |
| Supprimez une configuration client LDAP            | <code>vserver services name-service ldap client delete</code>               |

Consultez la page man pour chaque commande pour plus d'informations.

### Commandes pour la gestion des configurations LDAP

Il existe des commandes ONTAP spécifiques pour gérer les configurations LDAP.

| Les fonctions que vous recherchez... | Utilisez cette commande...                             |
|--------------------------------------|--------------------------------------------------------|
| Créez une configuration LDAP         | <code>vserver services name-service ldap create</code> |
| Afficher les configurations LDAP     | <code>vserver services name-service ldap show</code>   |
| Modifier une configuration LDAP      | <code>vserver services name-service ldap modify</code> |
| Supprimez une configuration LDAP     | <code>vserver services name-service ldap delete</code> |

Consultez la page man pour chaque commande pour plus d'informations.

### Commandes de gestion des modèles de schéma client LDAP

Il existe des commandes ONTAP spécifiques pour gérer les modèles de schéma client LDAP.



Les administrateurs SVM ne peuvent ni modifier ni supprimer les schémas des clients LDAP qui ont été créés par les administrateurs du cluster.

| Les fonctions que vous recherchez...     | Utilisez cette commande...                                                                                                            |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Copier un modèle de schéma LDAP existant | <code>vserver services name-service ldap client schema copy</code> Disponible au niveau de privilège avancé et au niveau supérieur.   |
| Afficher les modèles de schéma LDAP      | <code>vserver services name-service ldap client schema show</code>                                                                    |
| Modifier un modèle de schéma LDAP        | <code>vserver services name-service ldap client schema modify</code> Disponible au niveau de privilège avancé et au niveau supérieur. |
| Supprimer un modèle de schéma LDAP       | <code>vserver services name-service ldap client schema delete</code> Disponible au niveau de privilège avancé et au niveau supérieur. |

Consultez la page man pour chaque commande pour plus d'informations.

### Commandes permettant de gérer les configurations de l'interface Kerberos NFS

Il existe des commandes ONTAP spécifiques pour gérer les configurations de l'interface



## Kerberos NFS.

| Les fonctions que vous recherchez...                   | Utilisez cette commande...                          |
|--------------------------------------------------------|-----------------------------------------------------|
| Activez NFS Kerberos sur une LIF                       | <code>vserver nfs kerberos interface enable</code>  |
| Affiche les configurations de l'interface Kerberos NFS | <code>vserver nfs kerberos interface show</code>    |
| Modifiez une configuration d'interface Kerberos NFS    | <code>vserver nfs kerberos interface modify</code>  |
| Désactivation de NFS Kerberos sur une LIF              | <code>vserver nfs kerberos interface disable</code> |

Consultez la page man pour chaque commande pour plus d'informations.

### Commandes de gestion des configurations de domaine NFS Kerberos

Il existe des commandes ONTAP spécifiques pour gérer les configurations de Royaume Kerberos NFS.

| Les fonctions que vous recherchez...                | Utilisez cette commande...                     |
|-----------------------------------------------------|------------------------------------------------|
| Créez une configuration de domaine NFS Kerberos     | <code>vserver nfs kerberos realm create</code> |
| Affiche les configurations de domaine NFS Kerberos  | <code>vserver nfs kerberos realm show</code>   |
| Modifiez une configuration de domaine NFS Kerberos  | <code>vserver nfs kerberos realm modify</code> |
| Supprimez une configuration de domaine NFS Kerberos | <code>vserver nfs kerberos realm delete</code> |

Consultez la page man pour chaque commande pour plus d'informations.

### Commandes permettant de gérer les export-polices

Il existe des commandes ONTAP spécifiques pour gérer les export-polices.

| Les fonctions que vous recherchez...           | Utilisez cette commande...              |
|------------------------------------------------|-----------------------------------------|
| Affiche des informations sur les export-policy | <code>vserver export-policy show</code> |

|                            |                                           |
|----------------------------|-------------------------------------------|
| Renommez une export-policy | <code>vserver export-policy rename</code> |
| Copier une export-policy   | <code>vserver export-policy copy</code>   |
| Supprime une export-policy | <code>vserver export-policy delete</code> |

Consultez la page man pour chaque commande pour plus d'informations.

### Commandes permettant de gérer les règles d'exportation

Il existe des commandes ONTAP spécifiques pour gérer les règles d'exportation.

| Les fonctions que vous recherchez...                  | Utilisez cette commande...                     |
|-------------------------------------------------------|------------------------------------------------|
| Créer une règle d'exportation                         | <code>vserver export-policy rule create</code> |
| Affiche des informations sur les règles d'exportation | <code>vserver export-policy rule show</code>   |
| Modifier une règle d'exportation                      | <code>vserver export-policy rule modify</code> |
| Supprimer une règle d'exportation                     | <code>vserver export-policy rule delete</code> |



Si vous avez configuré plusieurs règles d'exportation identiques correspondant à différents clients, veillez à les garder synchronisées lors de la gestion des règles d'exportation.

Consultez la page man pour chaque commande pour plus d'informations.

### Configurez le cache des informations d'identification NFS

#### Raisons de la modification du temps de mise en cache des identifiants NFS

ONTAP utilise un cache d'identifiants pour stocker les informations nécessaires à l'authentification utilisateur pour l'accès aux exportations NFS afin d'accélérer l'accès et d'améliorer les performances. Vous pouvez configurer la durée de stockage des informations d'identification dans le cache des informations d'identification pour les personnaliser en fonction de votre environnement.

La modification du TTL (Time-to-Live) du cache d'identifiants NFS permet de résoudre certains problèmes. Vous devez comprendre ce que sont ces scénarios ainsi que les conséquences de ces modifications.

#### Raisons

Envisagez de modifier le TTL par défaut dans les cas suivants :

| Problème                                                                                                                                      | Action corrective                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Les noms de serveurs de votre environnement subissent une dégradation des performances en raison d'une charge élevée de requêtes de ONTAP.    | Augmentez le TTL des identifiants positifs et négatifs en cache afin de réduire le nombre de requêtes de ONTAP vers les serveurs de noms.                                                                                                                                         |
| L'administrateur du serveur de noms a apporté des modifications pour autoriser l'accès aux utilisateurs NFS qui étaient précédemment refusés. | Réduisez le TTL des identifiants négatifs en cache afin de réduire le temps que les utilisateurs NFS doivent attendre que ONTAP demande de nouvelles informations d'identification à partir de serveurs de noms externes afin qu'ils puissent obtenir un accès.                   |
| L'administrateur du serveur de noms a apporté des modifications pour refuser l'accès aux utilisateurs NFS précédemment autorisés.             | Réduisez le TTL des identifiants positifs qui ont été mis en cache afin de réduire le temps avant que ONTAP ne demande de nouvelles informations d'identification auprès de serveurs de noms externes, de sorte que les utilisateurs NFS ne puissent plus accéder à ces derniers. |

## Conséquences

Vous pouvez modifier la durée individuellement pour la mise en cache des informations d'identification positives et négatives. Cependant, vous devriez être conscient à la fois des avantages et des inconvénients de le faire.

| Si...                                                                   | L'avantage, c'est...                                                                                                                                | L'inconvénient est...                                                                                                                                    |
|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Augmenter la durée du cache des informations d'identification positives | ONTAP envoie moins souvent des demandes d'informations d'identification pour nommer des serveurs, ce qui réduit la charge sur les serveurs de noms. | Il faut plus de temps pour refuser l'accès aux utilisateurs NFS, mais qui étaient auparavant autorisés à y accéder.                                      |
| Réduisez la durée du cache des informations d'identification positives  | Le refus d'accès aux utilisateurs NFS, qui étaient auparavant autorisés, prend moins de temps.                                                      | ONTAP envoie plus fréquemment des demandes d'informations d'identification pour nommer des serveurs, ce qui augmente la charge sur les serveurs de noms. |
| Augmenter la durée du cache des informations d'identification négatives | ONTAP envoie moins souvent des demandes d'informations d'identification pour nommer des serveurs, ce qui réduit la charge sur les serveurs de noms. | Il faut plus de temps pour accorder l'accès aux utilisateurs NFS qui n'étaient auparavant pas autorisés mais qui le sont maintenant.                     |
| Réduisez le temps négatif du cache des informations d'identification    | Il faut moins de temps pour accorder l'accès aux utilisateurs NFS qui n'étaient auparavant pas autorisés mais qui le sont maintenant.               | ONTAP envoie plus fréquemment des demandes d'informations d'identification pour nommer des serveurs, ce qui augmente la charge sur les serveurs de noms. |

**Configurez le délai de mise en service pour les informations d'identification de l'utilisateur NFS en cache**

Vous pouvez configurer la durée pendant laquelle ONTAP stocke les identifiants des utilisateurs NFS dans son cache interne (TTL ou délai avant activation) en modifiant le serveur NFS de la machine virtuelle de stockage (SVM). Vous pourrez ainsi remédier à certains problèmes liés à une charge élevée sur les serveurs de noms ou à des modifications d'identifiants qui affectent l'accès des utilisateurs NFS.

**Description de la tâche**

Ces paramètres sont disponibles au niveau de privilège avancé.

**Étapes**

- 1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

- 2. Effectuez l'action souhaitée :

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Si vous souhaitez modifier le TTL pour le cache... | Utilisez la commande...                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Références positives                               | <div><pre>vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live</pre></div> <div>Le TTL est mesuré en millisecondes. À partir de ONTAP 9.10.1 et versions ultérieures, la valeur par défaut est 1 heure (3,600,000 millisecondes). Dans ONTAP 9.9.1 et les versions antérieures, la valeur par défaut est de 24 heures (86,400,000 millisecondes). La plage autorisée pour cette valeur est de 1 minute (60000 millisecondes) à 7 jours (604,800,000 millisecondes).</div> |
| Références négatives                               | <div><pre>vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live</pre></div> <div>Le TTL est mesuré en millisecondes. La valeur par défaut est 2 heures (7,200,000 millisecondes). La plage autorisée pour cette valeur est de 1 minute (60000 millisecondes) à 7 jours (604,800,000 millisecondes).</div>                                                                                                                                                                  |

- 3. Retour au niveau de privilège admin :

```
set -privilege admin
```

**Gestion des caches de règles d'exportation**

**Vider les caches des règles d'exportation**

ONTAP utilise plusieurs caches de règles d'exportation pour stocker les informations relatives aux règles d'exportation afin d'accélérer les accès. Vidage manuel des caches des règles d'exportation (`vserver export-policy cache flush`) Supprime les

informations potentiellement obsolètes et force ONTAP à extraire les informations actuelles des ressources externes appropriées. Cela peut aider à résoudre de nombreux problèmes liés à l'accès client aux exportations NFS.

### Description de la tâche

Les informations du cache de la politique d'exportation peuvent être obsolètes pour les raisons suivantes :

- Modification récente des règles d'export-policy
- Modification récente des enregistrements de nom d'hôte dans les serveurs de noms
- Modification récente des entrées de groupe réseau dans les serveurs de noms
- Récupération suite à une panne réseau qui a empêché le chargement complet des groupes réseau

### Étapes

1. Si le cache du service de noms n'est pas activé, effectuez l'une des opérations suivantes en mode privilèges avancés :

| Si vous voulez rincer...                                  | Entrez la commande...                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tous les caches des règles d'exportation (sauf showmount) | <code>vserver export-policy cache flush<br/>-vserver vserver_name</code>                                                                                                                                                                                                                       |
| Cache d'accès aux règles export-policy                    | <code>vserver export-policy cache flush<br/>-vserver vserver_name -cache access</code><br>Vous pouvez inclure l'option <code>-node</code> paramètre pour spécifier le nœud sur lequel vous souhaitez vider le cache d'accès.                                                                   |
| Cache de nom d'hôte                                       | <code>vserver export-policy cache flush<br/>-vserver vserver_name -cache host</code>                                                                                                                                                                                                           |
| Le cache netgroup                                         | <code>vserver export-policy cache flush<br/>-vserver vserver_name -cache netgroup</code><br>Le traitement des groupes réseau est intensif en ressources. Vous ne devez vider le cache netgroup que si vous essayez de résoudre un problème d'accès client causé par un groupe réseau obsolète. |
| Le cache showmount                                        | <code>vserver export-policy cache flush<br/>-vserver vserver_name -cache showmount</code>                                                                                                                                                                                                      |

2. Si le cache du service de nom est activé, effectuez l'une des opérations suivantes :

| Si vous voulez rincer...               | Entrez la commande...                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cache d'accès aux règles export-policy | <code>vserver export-policy cache flush</code><br><code>-vserver vserver_name -cache access</code><br>Vous pouvez inclure l'option <code>-node</code> paramètre pour spécifier le nœud sur lequel vous souhaitez vider le cache d'accès.                                                                                                                                                                 |
| Cache de nom d'hôte                    | <code>vserver services name-service cache</code><br><code>hosts forward-lookup delete-all</code>                                                                                                                                                                                                                                                                                                         |
| Le cache netgroup                      | <code>vserver services name-service cache</code><br><code>netgroups ip-to-netgroup delete-all</code><br><code>vserver services name-service cache</code><br><code>netgroups members delete-all</code> Le traitement des groupes réseau est intensif en ressources. Vous ne devez vider le cache netgroup que si vous essayez de résoudre un problème d'accès client causé par un groupe réseau obsolète. |
| Le cache showmount                     | <code>vserver export-policy cache flush</code><br><code>-vserver vserver_name -cache showmount</code>                                                                                                                                                                                                                                                                                                    |

#### Affiche la file d'attente et le cache de groupe réseau de la politique d'export

ONTAP utilise la file d'attente du groupe réseau lors de l'importation et de la résolution des groupes réseau et utilise le cache du groupe réseau pour stocker les informations obtenues. Lors de la résolution des problèmes liés à la stratégie d'exportation netgroup, vous pouvez utiliser le `vserver export-policy netgroup queue show` et `vserver export-policy netgroup cache show` commandes permettant d'afficher l'état de la file d'attente netgroup et le contenu du cache netgroup.

#### Étape

1. Effectuez l'une des opérations suivantes :

|                                                       |                                                                                              |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Pour afficher le groupe réseau de la export policy... | Entrez la commande...                                                                        |
| File d'attente                                        | <code>vserver export-policy netgroup queue show</code>                                       |
| Cache                                                 | <code>vserver export-policy netgroup cache show -vserver</code><br><code>vserver_name</code> |

Consultez la page man pour chaque commande pour plus d'informations.

## Vérifiez si une adresse IP client est membre d'un groupe réseau

Lors du dépannage des problèmes d'accès client NFS liés aux netgroups, vous pouvez utiliser le `vserver export-policy netgroup check-membership` Commande permettant de déterminer si une adresse IP client est membre d'un certain groupe réseau.

### Description de la tâche

La vérification de l'appartenance à un groupe réseau vous permet de déterminer si ONTAP est conscient qu'un client est ou non membre d'un groupe réseau. Il vous permet également de savoir si le cache ONTAP netgroup est à l'état transitoire lors de l'actualisation des informations de groupe réseau. Ces informations peuvent vous aider à comprendre pourquoi un client peut être accordé ou refusé de façon inattendue.

### Étape

1. Vérifiez l'appartenance d'un groupe réseau à une adresse IP client : `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

La commande peut renvoyer les résultats suivants :

- Le client est membre du groupe réseau.

Cette opération a été confirmée par une analyse de recherche inversée ou une recherche netgroup-par-hôte.

- Le client est membre du groupe réseau.

Elle a été trouvée dans le cache du groupe réseau ONTAP.

- Le client n'est pas membre du groupe réseau.
- L'appartenance du client ne peut pas encore être déterminée car ONTAP actualisant actuellement la mémoire cache du groupe réseau.

Jusqu'à ce que cela soit fait, l'adhésion ne peut être explicitement exclue. Utilisez le `vserver export-policy netgroup queue show` commande permettant de surveiller le chargement du groupe réseau et de relancer la vérification une fois la vérification terminée.

### Exemple

L'exemple suivant vérifie si un client avec l'adresse IP 172.17.16.72 est membre du netgroup Mercury sur la SVM vs1 :

```
cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup mercury -client-ip 172.17.16.72
```

### Optimisez les performances du cache d'accès

Vous pouvez configurer plusieurs paramètres afin d'optimiser le cache d'accès et trouver le juste équilibre entre les performances et la mise à jour des informations stockées dans le cache d'accès.

## Description de la tâche

Lorsque vous configurez les périodes d'actualisation du cache d'accès, gardez les éléments suivants à l'esprit :

- Des valeurs plus élevées signifient que les entrées restent plus longues dans le cache d'accès.

Ses performances sont meilleures, car ONTAP consacre moins de ressources à l'actualisation des entrées du cache d'accès. L'inconvénient est que si les règles d'export-policy changent et que les entrées de cache d'accès deviennent obsolètes, il faut donc plus de temps pour les mettre à jour. Par conséquent, il est possible que les clients qui devraient obtenir un accès soient refusés et que les clients qui devraient en être refusés aient un accès.

- Les valeurs faibles signifient que ONTAP actualise les entrées du cache d'accès plus souvent.

L'avantage est que les entrées sont plus récentes et que les clients sont plus susceptibles d'obtenir correctement ou de refuser l'accès. L'inconvénient est que les performances sont diminueraient, car ONTAP dépense davantage de ressources lors de la mise à jour des entrées du cache d'accès.

## Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Effectuez l'action souhaitée :

| Pour modifier...                                 | Entrer...                                                                                                                  |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Actualiser la période pour les entrées positives | <code>vserver export-policy access-cache<br/>config modify-all-vservers -refresh<br/>-period-positive timeout_value</code> |
| Actualiser la période pour les entrées négatives | <code>vserver export-policy access-cache<br/>config modify-all-vservers -refresh<br/>-period-negative timeout_value</code> |
| Délai d'expiration pour les anciennes entrées    | <code>vserver export-policy access-cache<br/>config modify-all-vservers -harvest<br/>-timeout timeout_value</code>         |

3. Vérifiez les nouveaux paramètres :

```
vserver export-policy access-cache config show-all-vservers
```

4. Retour au niveau de privilège admin :

```
set -privilege admin
```

## Gérer les verrous de fichier



## A propos du verrouillage de fichier entre les protocoles

Le verrouillage de fichier est une méthode utilisée par les applications client pour empêcher un utilisateur d'accéder à un fichier précédemment ouvert par un autre utilisateur. Le mode de verrouillage des fichiers par ONTAP dépend du protocole du client.

Si le client est un client NFS, les verrouillages sont consultatifs ; si le client est un client SMB, les verrous sont obligatoires.

En raison des différences entre les verrouillages de fichiers NFS et SMB, un client NFS peut ne pas accéder à un fichier précédemment ouvert par une application SMB.

Ce qui suit se produit lorsqu'un client NFS tente d'accéder à un fichier verrouillé par une application SMB :

- Dans les volumes mixtes ou NTFS, les opérations de manipulation de fichiers telles que `rm`, `rmdir`, et `mv` Peut entraîner l'échec de l'application NFS.
- Les opérations de lecture et d'écriture NFS sont refusées par les modes SMB Deny-read et deny-write open, respectivement.
- Les opérations d'écriture NFS échouent lorsque la plage d'écriture du fichier est verrouillée par un bytelock SMB exclusif.

Dans les volumes de style de sécurité UNIX, les opérations de dissociation NFS et de renommage ignorent l'état du verrouillage SMB et permettent l'accès au fichier. Toutes les autres opérations NFS sur des volumes de type sécurité UNIX respectent l'état de verrouillage SMB.

### Comment ONTAP traite les bits en lecture seule

Le bit de lecture seule est défini fichier par fichier pour indiquer si un fichier est inscriptible (désactivé) ou en lecture seule (activé).

Les clients SMB qui utilisent Windows peuvent définir un bit en lecture seule par fichier. Les clients NFS ne définissent pas de bit en lecture seule par fichier, car les clients NFS ne disposent d'aucune opération de protocole utilisant un bit en lecture seule par fichier.

ONTAP peut définir un bit en lecture seule sur un fichier lorsqu'un client SMB utilisant Windows crée ce fichier. ONTAP peut également définir un bit en lecture seule lorsqu'un fichier est partagé entre les clients NFS et les clients SMB. Certains logiciels, lorsqu'ils sont utilisés par des clients NFS et SMB, nécessitent l'activation du bit en lecture seule.

Pour que ONTAP garde les autorisations appropriées en lecture et écriture sur un fichier partagé entre les clients NFS et les clients SMB, il traite le bit en lecture seule conformément aux règles suivantes :

- NFS traite tous les fichiers dont le bit de lecture seule est activé comme s'il n'a pas de bits d'autorisation d'écriture activés.
- Si un client NFS désactive tous les bits d'autorisation d'écriture et qu'au moins un de ces bits avait été précédemment activé, ONTAP active le bit en lecture seule pour ce fichier.
- Si un client NFS active un bit d'autorisation d'écriture, ONTAP désactive le bit en lecture seule pour ce fichier.
- Si le bit de lecture seule d'un fichier est activé et qu'un client NFS tente de détecter les autorisations pour le fichier, les bits d'autorisation du fichier ne sont pas envoyés au client NFS. ONTAP envoie les bits d'autorisation au client NFS avec les bits d'autorisation d'écriture masqués.

- Si le bit de lecture seule d'un fichier est activé et qu'un client SMB désactive le bit de lecture seule, ONTAP active le bit d'autorisation d'écriture du propriétaire pour le fichier.
- Les fichiers dont le bit de lecture seule est activé sont accessibles en écriture uniquement par root.



Les modifications des autorisations liées aux fichiers sont immédiatement appliquées aux clients SMB, mais elles peuvent ne pas être immédiatement appliquées aux clients NFS si le client NFS active la mise en cache des attributs.

#### La différence entre ONTAP et Windows en ce qui concerne la gestion des verrous sur les composants de chemin de partage

Contrairement à Windows, ONTAP ne verrouille pas chaque composant du chemin d'accès à un fichier ouvert lorsque le fichier est ouvert. Ce comportement affecte également les chemins de partage SMB.

Étant donné que ONTAP ne verrouille pas chaque composant du chemin d'accès, il est possible de renommer un composant de chemin au-dessus du fichier ou du partage ouvert, ce qui peut causer des problèmes pour certaines applications ou peut rendre le chemin de partage dans la configuration SMB invalide. Cela peut rendre le partage inaccessible.

Pour éviter les problèmes causés par le changement de nom des composants du chemin d'accès, vous pouvez appliquer des paramètres de sécurité de la liste de contrôle d'accès Windows (ACL) qui empêchent les utilisateurs ou les applications de renommer les répertoires critiques.

En savoir plus sur ["Comment empêcher le changement de nom des répertoires lorsque les clients y accèdent"](#).

#### Affiche des informations sur les verrous

Vous pouvez afficher des informations sur les verrous de fichier en cours, y compris les types de verrous qui sont conservés et l'état de verrouillage, les détails sur les verrous de plage d'octets, les modes de verrouillage de sharelock, les verrous de délégation et les verrous opportunistes, et si les verrous sont ouverts avec des poignées durables ou persistantes.

#### Description de la tâche

L'adresse IP du client ne peut pas être affichée pour les verrouillages établis via NFS V4 ou NFS v4.1.

Par défaut, la commande affiche des informations relatives à tous les verrouillages. Vous pouvez utiliser les paramètres de la commande pour afficher des informations sur les verrous d'une machine virtuelle de stockage (SVM) spécifique ou pour filtrer les résultats de la commande par d'autres critères.

Le `vserver locks show` la commande affiche des informations sur quatre types de verrous :

- Les verrous de plage d'octets, qui verrouillent uniquement une partie d'un fichier.
- Verrous de partage, qui verrouillent les fichiers ouverts.
- Verrouillages opportunistes, qui contrôlent la mise en cache côté client sur SMB.
- Des délégations qui contrôlent la mise en cache côté client sur NFSv4.x.

En spécifiant des paramètres facultatifs, vous pouvez déterminer des informations importantes sur chaque type de verrou. Consultez la page man pour la commande pour plus d'informations.

Étape

- 1. Affiche des informations sur les verrous à l'aide de `vserver locks show` commande.

Exemples

L'exemple suivant présente un récapitulatif des informations relatives à un verrouillage NFSv4 sur un fichier avec le chemin d'accès `/vol1/file1`. Le mode d'accès de sharelock est `Write-deny_none` et le verrou a été accordé avec la délégation d'écriture :

```
cluster1::> vserver locks show

Vserver: vs0
Volume Object Path LIF Protocol Lock Type Client

vol1 /vol1/file1 lif1 nfsv4 share-level -
 Sharelock Mode: write-deny_none
 delegation -
 Delegation Type: write
```

L'exemple suivant affiche des informations détaillées sur le verrou SMB d'un fichier avec le chemin d'accès `/data2/data2_2/intro.pptx`. Un descripteur durable est accordé sur le fichier avec un mode d'accès à verrouillage de partage `Write-Deny_none` à un client dont l'adresse IP est `10.3.1.3`. Un oplock de location est accordé avec un niveau de oplock de lot :

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/intro.pptx
Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
Lock Protocol: cifs
Lock Type: share-level
Node Holding Lock State: node3
Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
Bytelock is Superlock: -
Bytelock is Soft: -
Oplock Level: -
Shared Lock Access Mode: write-deny_none
Shared Lock is Soft: false
Delegation Type: -
Client Address: 10.3.1.3
```

```

 SMB Open Type: durable
 SMB Connect State: connected
SMB Expiration Time (Secs): -
 SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

 Vserver: vs1
 Volume: data2_2
 Logical Interface: lif2
 Object Path: /data2/data2_2/test.pptx
 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
 Lock Protocol: cifs
 Lock Type: op-lock
 Node Holding Lock State: node3
 Lock State: granted
Bytelock Starting Offset: -
 Number of Bytes Locked: -
 Bytelock is Mandatory: -
 Bytelock is Exclusive: -
 Bytelock is Superlock: -
 Bytelock is Soft: -
 Oplock Level: batch
 Shared Lock Access Mode: -
 Shared Lock is Soft: -
 Delegation Type: -
 Client Address: 10.3.1.3
 SMB Open Type: -
 SMB Connect State: connected
SMB Expiration Time (Secs): -
 SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

```

## Serrures de sécurité

Lorsque des verrous de fichier empêchent l'accès client aux fichiers, vous pouvez afficher des informations sur les verrous actuellement mis en attente, puis interrompre des verrous spécifiques. Les applications de débogage sont des exemples de scénarios dans lesquels vous devrez peut-être interrompre les verrous.

## Description de la tâche

Le `vserver locks break` la commande n'est disponible que au niveau de privilège avancé et supérieur. La page man de la commande contient des informations détaillées.

## Étapes

1. Pour trouver les informations dont vous avez besoin pour interrompre un verrouillage, utilisez le `vserver locks show` commande.

La page man de la commande contient des informations détaillées.

2. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

3. Effectuez l'une des opérations suivantes :

|                                                                           |                                                                                                |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Si vous voulez rompre un verrou en spécifiant...                          | Entrez la commande...                                                                          |
| Le nom du SVM, le nom du volume, le nom de la LIF et le chemin de fichier | <code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code> |
| L'ID de verrouillage                                                      | <code>vserver locks break -lockid UUID</code>                                                  |

4. Retour au niveau de privilège admin :

```
set -privilege admin
```

## Fonctionnement des filtres FPolicy de première lecture et de première écriture avec NFS

Les clients NFS bénéficient d'un temps de réponse élevé lors du trafic important de requêtes en lecture/écriture lorsque FPolicy est activé à l'aide d'un serveur FPolicy externe avec des opérations de lecture/écriture sous forme d'événements surveillés. Pour les clients NFS, l'utilisation de filtres de première lecture et de première écriture dans FPolicy réduit le nombre de notifications FPolicy et améliore les performances.

Dans NFS, le client effectue des E/S sur un fichier en récupérant son descripteur. Cet descripteur peut rester valide entre les redémarrages du serveur et du client. Par conséquent, le client est libre de mettre en cache le descripteur et d'y envoyer des requêtes sans récupérer de nouveau les poignées. Dans une session ordinaire, un grand nombre de requêtes de lecture/écriture sont envoyées au serveur de fichiers. Si des notifications sont générées pour toutes ces demandes, cela peut entraîner les problèmes suivants :

- Une charge plus importante grâce à un traitement supplémentaire des notifications et des temps de réponse plus courts.
- Envoi de nombreuses notifications au serveur FPolicy même si toutes les notifications ne sont pas affectées.

Après réception de la première demande de lecture/écriture d'un client pour un fichier particulier, une entrée de cache est créée et le nombre de lectures/écritures est incrémenté. Cette requête est marquée comme opération de première lecture/écriture et un événement FPolicy est généré. Avant de planifier et de créer les filtres FPolicy pour un client NFS, il est important de connaître les principes de base du fonctionnement des filtres FPolicy.

- Première lecture : filtre les demandes de lecture du client pour la première lecture.

Lorsque ce filtre est utilisé pour les événements NFS, le `-file-session-io-grouping-count` et `-file-session-io-grouping-duration` Les paramètres déterminent la demande de première lecture pour laquelle FPolicy est traité.

- Première écriture : filtre les demandes d'écriture du client pour la première écriture.

Lorsque ce filtre est utilisé pour les événements NFS, le `-file-session-io-grouping-count` et `-file-session-io-grouping-duration` Les paramètres déterminent la première requête d'écriture pour laquelle FPolicy a traité.

Les options suivantes sont ajoutées dans la base de données des serveurs NFS.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

### Modifier l'ID d'implémentation du serveur NFSv4.1

Le protocole NFSv4.1 inclut un ID de mise en œuvre du serveur qui documente le domaine, le nom et la date du serveur. Vous pouvez modifier les valeurs par défaut de l'ID d'implémentation du serveur. La modification des valeurs par défaut peut être utile, par exemple, lors de la collecte des statistiques d'utilisation ou de la résolution des problèmes d'interopérabilité. Pour plus d'informations, consultez RFC 5661.

#### Description de la tâche

Les valeurs par défaut des trois options sont les suivantes :

| Option                                | Nom de l'option                          | Valeur par défaut          |
|---------------------------------------|------------------------------------------|----------------------------|
| Domaine d'ID d'implémentation NFSv4.1 | <code>-v4.1-implementation-domain</code> | netapp.com                 |
| Nom de l'ID de mise en œuvre NFSv4.1  | <code>-v4.1-implementation-name</code>   | Nom de version du cluster  |
| Date ID mise en œuvre NFSv4.1         | <code>-v4.1-implementation-date</code>   | Date de version du cluster |

#### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Effectuez l'une des opérations suivantes :

| Si vous voulez modifier l'ID d'implémentation NFSv4.1... | Entrez la commande...                                                   |
|----------------------------------------------------------|-------------------------------------------------------------------------|
| Domaine                                                  | <code>vserver nfs modify -v4.1<br/>-implementation-domain domain</code> |
| Nom                                                      | <code>vserver nfs modify -v4.1<br/>-implementation-name name</code>     |
| Date                                                     | <code>vserver nfs modify -v4.1<br/>-implementation-date date</code>     |

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

## Gérer les listes de contrôle d'accès NFSv4

### Avantages des listes de contrôle d'accès NFSv4

Il existe de nombreux avantages pour activer les listes de contrôle d'accès NFSv4.

Voici quelques-uns des avantages majeurs apportés par les ACL NFSv4 :

- Contrôle plus précis de l'accès des utilisateurs aux fichiers et aux répertoires
- Sécurité NFS renforcée
- Interopérabilité accrue avec CIFS
- Suppression de la limitation NFS de 16 groupes par utilisateur

### Fonctionnement des listes de contrôle d'accès NFSv4

Un client utilisant des listes de contrôle d'accès NFSv4 peut définir et afficher des listes de contrôle d'accès sur les fichiers et les répertoires du système. Lorsqu'un nouveau fichier ou sous-répertoire est créé dans un répertoire comportant une liste de contrôle d'accès, le nouveau fichier ou sous-répertoire hérite de toutes les entrées ACL (ACE) de la liste de contrôle d'accès qui ont été marquées avec les indicateurs d'héritage appropriés.

Lorsqu'un fichier ou un répertoire est créé à la suite d'une requête NFSv4, l'ACL du fichier ou répertoire résultant dépend du fait que la demande de création de fichier inclut une ACL ou uniquement les autorisations d'accès aux fichiers UNIX standard, et si le répertoire parent possède une ACL :

- Si la requête inclut une liste de contrôle d'accès, cette liste de contrôle d'accès est utilisée.
- Si la demande comprend uniquement des autorisations d'accès aux fichiers UNIX standard mais que le répertoire parent possède une ACL, les ACE de l'ACL du répertoire parent sont hérités par le nouveau fichier ou répertoire tant que les ACE ont été balisés avec les indicateurs d'héritage appropriés.



Une ACL parent est héritée même si `-v4.0-acl` est défini sur `off`.

- Si la requête inclut uniquement les autorisations d'accès aux fichiers UNIX standard et que le répertoire parent ne dispose pas d'ACL, le mode fichier client est utilisé pour définir les autorisations d'accès aux fichiers UNIX standard.
- Si la requête inclut uniquement les autorisations d'accès aux fichiers UNIX standard et que le répertoire parent dispose d'une ACL non héritable, le nouvel objet est créé uniquement avec des bits de mode.



Si le `-chown-mode` le paramètre a été défini sur `restricted` à l'aide des commandes dans `vserver nfs` ou `vserver export-policy rule Familles`, la propriété des fichiers ne peut être modifiée que par le superutilisateur, même si les autorisations sur disque définies avec les ACL NFSv4 permettent à un utilisateur non-root de modifier la propriété des fichiers. Pour plus d'informations, consultez les pages de manuel correspondantes.

#### Activer ou désactiver la modification des listes de contrôle d'accès NFSv4

Lorsque ONTAP reçoit un `chmod` Commande pour un fichier ou un répertoire avec une liste de contrôle d'accès, la liste de contrôle d'accès est par défaut conservée et modifiée pour refléter le changement de bit de mode. Vous pouvez désactiver le `-v4-acl` `-preserve` Paramètre pour modifier le comportement si vous souhaitez que la liste de contrôle d'accès soit supprimée.

#### Description de la tâche

Lors de l'utilisation d'un style de sécurité unifié, ce paramètre indique également si les autorisations de fichier NTFS sont conservées ou supprimées lorsqu'un client envoie une commande `chmod`, `chgroup` ou `chown` pour un fichier ou un répertoire.

La valeur par défaut de ce paramètre est activée.

#### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Effectuez l'une des opérations suivantes :

| Les fonctions que vous recherchez...                                                                    | Saisissez la commande suivante...                                                |
|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Activer la conservation et la modification des listes de contrôle d'accès NFSv4 existantes (par défaut) | <code>vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled</code>  |
| Désactivez la conservation et déposez les ACL NFSv4 lors du changement de bits de mode                  | <code>vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled</code> |

3. Retour au niveau de privilège admin :

```
set -privilege admin
```



## Comment ONTAP utilise les listes de contrôle d'accès NFSv4 pour déterminer si elles peuvent supprimer un fichier

Pour déterminer s'il peut supprimer un fichier, ONTAP utilise une combinaison du bit DE SUPPRESSION du fichier et du bit DE SUPPRESSION\_ENFANT du répertoire contenant. Pour plus d'informations, consultez le document NFS 4.1 RFC 5661.

### Activer ou désactiver les ACL NFSv4

Pour activer ou désactiver les ACL NFSv4, vous pouvez modifier le `-v4.0-acl` et `-v4.1-acl` options. Ces options sont désactivées par défaut.

#### Description de la tâche

Le `-v4.0-acl` ou `-v4.1-acl` Option contrôle la définition et l'affichage des ACL NFSv4 ; elle ne contrôle pas l'application de ces listes de contrôle d'accès pour la vérification de l'accès.

#### Étape

1. Effectuez l'une des opérations suivantes :

| Les fonctions que vous recherchez...              | Alors...                                                                                                       |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Activez les listes de contrôle d'accès NFSv4.0    | Saisissez la commande suivante :<br><br><pre>vserver nfs modify -vserver vserver_name -v4.0-acl enabled</pre>  |
| Désactivez les listes de contrôle d'accès NFSv4.0 | Saisissez la commande suivante :<br><br><pre>vserver nfs modify -vserver vserver_name -v4.0-acl disabled</pre> |
| Activer les ACL NFSv4.1                           | Saisissez la commande suivante :<br><br><pre>vserver nfs modify -vserver vserver_name -v4.1-acl enabled</pre>  |
| Désactiver les listes de contrôle d'accès NFSv4.1 | Saisissez la commande suivante :<br><br><pre>vserver nfs modify -vserver vserver_name -v4.1-acl disabled</pre> |

### Modifier la limite ACE maximale pour les listes de contrôle d'accès NFSv4

Vous pouvez modifier le nombre maximal d'ACE autorisés pour chaque ACL NFSv4 en modifiant le paramètre `-v4-acl-max-aces`. Par défaut, la limite est définie sur 400 ACE pour chaque ACL. L'augmentation de cette limite peut permettre de réussir la migration des données avec des listes de contrôle d'accès contenant plus de 400 ACE vers les systèmes de stockage exécutant ONTAP.

**Description de la tâche**

L'augmentation de cette limite peut avoir un impact sur les performances des clients accédant aux fichiers avec des listes de contrôle d'accès NFSv4.

**Étapes**

- 1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

- 2. Modifier la limite ACE maximale pour les listes de contrôle d'accès NFSv4 :

```
vserver nfs modify -v4-acl-max-aces max_ace_limit
```

Plage valide de

```
max_ace_limit est 192 à 1024.
```

- 3. Retour au niveau de privilège admin :

```
set -privilege admin
```

**Gérer les délégations de fichiers NFSv4**

**Activer ou désactiver les délégations des fichiers de lecture NFSv4**

Pour activer ou désactiver les délégations de fichiers en lecture NFSv4, vous pouvez modifier `-v4.0-read-delegation` option. En activant les délégations de fichiers de lecture, vous pouvez éliminer une grande partie de la surcharge de messages associée à l'ouverture et à la fermeture des fichiers.

**Description de la tâche**

Par défaut, les délégations des fichiers lus sont désactivées.

L'inconvénient de l'activation des délégations de fichiers en lecture est que le serveur et ses clients doivent restaurer des délégations après le redémarrage ou le redémarrage du serveur, qu'un client redémarre ou qu'une partition réseau se produit.

**Étape**

- 1. Effectuez l'une des opérations suivantes :

|                                                |                                                                                                                |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Les fonctions que vous recherchez...           | Alors...                                                                                                       |
| Activer les délégations des fichiers lus NFSv4 | Saisissez la commande suivante :<br><br>vserver nfs modify -vserver vserver_name -v4.0-read-delegation enabled |

|                                                           |                                                                                                                              |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Activer les délégations des fichiers de lecture NFSv4.1   | <p>Saisissez la commande suivante :</p> <pre>+ vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled</pre> |
| Désactiver les délégations des fichiers de lecture NFSv4  | <p>Saisissez la commande suivante :</p> <pre>vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled</pre>  |
| Désactiver les délégations de fichiers de lecture NFSv4.1 | <p>Saisissez la commande suivante :</p> <pre>vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled</pre>  |

## Résultat

Les options de délégation de fichiers prennent effet dès qu'elles sont modifiées. Il n'est pas nécessaire de redémarrer ou de redémarrer NFS.

## Activer ou désactiver les délégations de fichiers d'écriture NFSv4

Pour activer ou désactiver les délégations de fichiers d'écriture, vous pouvez modifier le `-v4.0-write-delegation` option. En activant les délégations de fichiers d'écriture, vous pouvez éliminer la majeure partie des surcharges de messages associées au verrouillage des fichiers et des enregistrements, en plus de l'ouverture et de la fermeture des fichiers.

## Description de la tâche

Par défaut, les délégations des fichiers d'écriture sont désactivées.

L'inconvénient de l'activation des délégations de fichiers d'écriture est que le serveur et ses clients doivent effectuer des tâches supplémentaires pour restaurer des délégations après le redémarrage ou le redémarrage du serveur, qu'un client redémarre ou qu'une partition réseau se produit.

## Étape

1. Effectuez l'une des opérations suivantes :

| Les fonctions que vous recherchez...                   | Alors...                                                                                                             |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Activer les délégations des fichiers d'écriture NFSv4  | Saisissez la commande suivante : <pre>vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled</pre> |
| Activer les délégations de fichiers d'écriture NFSv4.1 | Saisissez la commande suivante : <pre>vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled</pre> |

| Les fonctions que vous recherchez...                      | Alors...                                                                                                                |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Désactiver les délégations des fichiers d'écriture NFSv4  | Saisissez la commande suivante : <code>vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled</code> |
| Désactiver les délégations de fichiers d'écriture NFSv4.1 | Saisissez la commande suivante : <code>vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled</code> |

## Résultat

Les options de délégation de fichiers prennent effet dès qu'elles sont modifiées. Il n'est pas nécessaire de redémarrer ou de redémarrer NFS.

## Configurez le verrouillage des fichiers NFSv4 et des enregistrements

### À propos du verrouillage des fichiers et des enregistrements NFSv4

Pour les clients NFSv4, ONTAP supporte le mécanisme de verrouillage des fichiers NFSv4, tout en conservant l'état de tous les verrouillages de fichiers sous un modèle basé sur la location.

["Rapport technique NetApp 3580 : Guide des améliorations et des meilleures pratiques NFSv4 implémentation d'Data ONTAP"](#)

### Spécifier la période de bail du verrouillage NFSv4

Pour spécifier la période de verrouillage NFSv4 (c'est-à-dire la période pendant laquelle ONTAP accorde irrévocablement un verrouillage à un client), vous pouvez modifier le `-v4-lease-seconds` option. Des délais de location plus courts accélèrent la restauration des serveurs, tandis que des périodes de location plus longues sont avantageuses pour les serveurs qui gèrent un nombre très important de clients.

### Description de la tâche

Par défaut, cette option est définie sur 30. La valeur minimale de cette option est 10. La valeur maximale pour cette option est le délai de grâce de verrouillage, que vous pouvez définir avec l' `locking.lease_seconds` option.

### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Saisissez la commande suivante :

```
vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
```

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

### Spécifier la période de grâce du verrouillage NFSv4

Pour spécifier la période de grâce de verrouillage NFSv4 (c'est-à-dire le délai durant lequel les clients tentent de récupérer leur état de verrouillage à partir de ONTAP lors de la restauration du serveur), vous pouvez modifier le `-v4-grace-seconds` option.

### Description de la tâche

Par défaut, cette option est définie sur 45.

### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Saisissez la commande suivante :

```
vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
```

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

### Fonctionnement des référencements NFSv4

Lorsque vous activez les référencements NFSv4, ONTAP fournit des référencements « intra-SVM » aux clients NFSv4. La référence intra-SVM est utilisée lorsqu'un nœud de cluster recevant la requête NFSv4 fait référence au client NFSv4 à une autre interface logique (LIF) sur la machine virtuelle de stockage (SVM).

Le client NFSv4 doit accéder au chemin qui a reçu la recommandation au niveau du LIF cible à partir de ce point. Le nœud de cluster d'origine fournit une telle recommandation lorsqu'il détermine qu'il existe une LIF dans le SVM qui réside sur le nœud de cluster sur lequel réside le volume de données, ce qui permet aux clients d'accéder plus rapidement aux données et d'éviter toute communication supplémentaire du cluster.

### Activez ou désactivez les référencements NFSv4

Vous pouvez activer les référencements NFSv4 sur les machines virtuelles de stockage (SVM) en activant les options `-v4-fsid-change` et `-v4.0-referrals`. L'activation des référencements NFSV4 peut entraîner un accès plus rapide aux données pour les clients NFSv4 qui prennent en charge cette fonctionnalité.

### Ce dont vous avez besoin

Si vous souhaitez activer les référencements NFS, vous devez d'abord désactiver Parallel NFS. Vous ne pouvez pas activer les deux en même temps.

### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Effectuez l'une des opérations suivantes :

| Les fonctions que vous recherchez...  | Entrez la commande...                                                                                                                           |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Activez les référencements NFSv4      | <code>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled</code> |
| Désactiver les référencements NFSv4   | <code>vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled</code>                                                                 |
| Activer les référencements NFSv4.1    | <code>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled</code> |
| Désactiver les référencements NFSv4.1 | <code>vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled</code>                                                                 |

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

## Affiche les statistiques NFS

Pour surveiller les performances et diagnostiquer les problèmes, vous pouvez afficher les statistiques NFS des serveurs virtuels de stockage (SVM) sur le système de stockage.

### Étapes

1. Utilisez le `statistics catalog object show` Commande permettant d'identifier les objets NFS à partir desquels vous pouvez afficher les données.

```
statistics catalog object show -object nfs*
```

2. Utilisez le `statistics start` et en option `statistics stop` commandes permettant de collecter un échantillon de données à partir d'un ou de plusieurs objets.
3. Utilisez le `statistics show` commande pour afficher les exemples de données.

### Exemple : contrôle des performances NFSv3

L'exemple suivant montre les données de performances pour le protocole NFSv3.

La commande suivante démarre la collecte de données pour un nouvel échantillon :

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

La commande suivante affiche les données de l'échantillon en spécifiant des compteurs qui indiquent le

nombre de demandes de lecture et d'écriture réussies par rapport au nombre total de demandes de lecture et d'écriture :

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success
```

```
Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1
```

| Counter       | Value   |
|---------------|---------|
| read_success  | 40042   |
| read_total    | 40042   |
| write_success | 1492052 |
| write_total   | 1492052 |

#### Informations associées

["Configuration du contrôle des performances"](#)

#### Affiche les statistiques DNS

Vous pouvez afficher les statistiques DNS des ordinateurs virtuels de stockage (SVM) sur le système de stockage afin de surveiller les performances et de diagnostiquer les problèmes.

#### Étapes

1. Utilisez le `statistics catalog object show` Commande permettant d'identifier les objets DNS à partir desquels vous pouvez afficher les données.

```
statistics catalog object show -object external_service_op*
```

2. Utilisez le `statistics start` et `statistics stop` commandes permettant de collecter un échantillon de données à partir d'un ou de plusieurs objets.
3. Utilisez le `statistics show` commande pour afficher les exemples de données.

#### Surveillance des statistiques DNS

Les exemples suivants présentent les données de performances des requêtes DNS. Les commandes suivantes permettent de lancer la collecte de données pour un nouvel échantillon :

```

vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2

```

La commande suivante affiche les données de l'échantillon en spécifiant des compteurs qui affichent le nombre de requêtes DNS envoyées par rapport au nombre de requêtes DNS reçues, échouées ou expirées :

```

vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

```

```

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

```

| Counter                  | Value |
|--------------------------|-------|
| num_not_found_responses  | 0     |
| num_request_failures     | 0     |
| num_requests_sent        | 1     |
| num_responses_received   | 1     |
| num_successful_responses | 1     |
| num_timeouts             | 0     |

6 entries were displayed.

La commande suivante affiche les données de l'échantillon en spécifiant des compteurs qui affichent le nombre de fois qu'une erreur spécifique a été reçue pour une requête DNS sur le serveur particulier :



```
vs1:*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count
```

Object: external\_service\_op\_error

Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109

Start-time: 3/8/2016 11:23:21

End-time: 3/8/2016 11:24:25

Elapsed-time: 64s

Scope: vs1

| Counter           | Value         |
|-------------------|---------------|
| count             | 1             |
| error_string      | NXDOMAIN      |
| server_ip_address | 10.72.219.109 |

3 entries were displayed.

## Informations associées

["Configuration du contrôle des performances"](#)

## Affiche les statistiques NIS

Pour surveiller les performances et diagnostiquer les problèmes, vous pouvez afficher les statistiques NIS des machines virtuelles de stockage (SVM) sur le système de stockage.

### Étapes

1. Utilisez le `statistics catalog object show` Pour identifier les objets NIS à partir desquels vous pouvez afficher des données.

```
statistics catalog object show -object external_service_op*
```

2. Utilisez le `statistics start` et `statistics stop` commandes permettant de collecter un échantillon de données à partir d'un ou de plusieurs objets.
3. Utilisez le `statistics show` commande pour afficher les exemples de données.

## Surveillance des statistiques NIS

Les exemples suivants affichent des données de performances pour les requêtes NIS. Les commandes suivantes permettent de lancer la collecte de données pour un nouvel échantillon :

```
vs1:*> statistics start -object external_service_op -sample-id
nis_sample1
vs1:*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

La commande suivante affiche les données de l'échantillon en spécifiant des compteurs indiquant le nombre

de requêtes NIS envoyées par rapport au nombre de requêtes NIS reçues, en échec ou en expiration :

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses
```

```
Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1
```

| Counter                  | Value |
|--------------------------|-------|
| num_not_found_responses  | 0     |
| num_request_failures     | 1     |
| num_requests_sent        | 2     |
| num_responses_received   | 1     |
| num_successful_responses | 1     |
| num_timeouts             | 0     |

6 entries were displayed.

La commande suivante affiche les données de l'échantillon en spécifiant des compteurs indiquant le nombre de fois où une erreur spécifique a été reçue pour une requête NIS sur le serveur particulier :

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count
```

```
Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1
```

| Counter           | Value         |
|-------------------|---------------|
| count             | 1             |
| error_string      | YP_NOTFOUND   |
| server_ip_address | 10.227.13.221 |

3 entries were displayed.

#### Informations associées

["Configuration du contrôle des performances"](#)

## Prise en charge de VMware vStorage over NFS

ONTAP prend en charge certaines fonctionnalités VMware vStorage APIs for Array Integration (VAAI) dans un environnement NFS.

### Fonctionnalités prises en charge

Les fonctionnalités suivantes sont prises en charge :

- Copie auxiliaire

Permet à un hôte ESXi de copier des machines virtuelles ou des disques de machines virtuelles directement entre les emplacements de datastore source et de destination sans impliquer l'hôte. Cela permet d'économiser les cycles du processeur de l'hôte ESXi et la bande passante du réseau. Le déchargement des copies préserve l'efficacité de l'espace si le volume source est faible.

- Réservation d'espace

Garantit l'espace de stockage d'un fichier VMDK en réservant de l'espace pour celui-ci.

### Limites

VMware vStorage over NFS présente les limites suivantes :

- Les opérations de déchargement des copies peuvent échouer dans les scénarios suivants :
  - Lors de l'exécution de waffer sur le volume source ou de destination, car il met temporairement le volume hors ligne
  - Pendant le déplacement du volume source ou de destination
  - Lors du déplacement de LIF source ou de destination
  - Lors des opérations de basculement ou de rétablissement
  - Lors des opérations de basculement ou de rétablissement
- La copie côté serveur peut échouer en raison des différences de format de descripteur de fichier dans le scénario suivant :

Tentative de copie des données à partir des SVM dont les qtrees n'ont pas encore été exportés vers des SVM, ou qui ont déjà été exportés. Pour contourner cette limitation, vous pouvez exporter au moins un qtree sur le SVM de destination.

### Informations associées

["Quelles opérations VAAI Offloaded sont prises en charge par Data ONTAP ?"](#)

## Activation ou désactivation de VMware vStorage sur NFS

Vous pouvez activer ou désactiver la prise en charge de VMware vStorage sur NFS sur des SVM (Storage Virtual machines) à l'aide du `vserver nfs modify` commande.

### Description de la tâche

Par défaut, la prise en charge de VMware vStorage over NFS est désactivée.

### Étapes

1. Afficher l'état actuel de la prise en charge de vStorage pour les SVM :

```
vserver nfs show -vserver vserver_name -instance
```

2. Effectuez l'une des opérations suivantes :

| Les fonctions que vous recherchez...             | Saisissez la commande suivante...                                          |
|--------------------------------------------------|----------------------------------------------------------------------------|
| Prise en charge de VMware vStorage               | <pre>vserver nfs modify -vserver<br/>vserver_name -vstorage enabled</pre>  |
| Désactivez la prise en charge de VMware vStorage | <pre>vserver nfs modify -vserver<br/>vserver_name -vstorage disabled</pre> |

### Une fois que vous avez terminé

Vous devez installer le plug-in NFS pour VMware VAAI avant de pouvoir utiliser cette fonctionnalité. Pour plus d'informations, consultez *installation du plug-in NetApp NFS pour VMware VAAI*.

### Informations associées

["Documentation NetApp : plug-in NetApp NFS pour VMware VAAI"](#)

### Activer ou désactiver la prise en charge de rquota

ONTAP supporte le protocole de quota distant version 1 (rquota v1). Le protocole rquota permet aux clients NFS d'obtenir des informations de quotas pour les utilisateurs à partir d'une machine distante. Vous pouvez activer rquota sur des machines virtuelles de stockage (SVM) à l'aide du `vserver nfs modify` commande.

### Description de la tâche

Par défaut, rquota est désactivé.

### Étape

1. Effectuez l'une des opérations suivantes :

| Les fonctions que vous recherchez...                 | Saisissez la commande suivante...                                       |
|------------------------------------------------------|-------------------------------------------------------------------------|
| Activer la prise en charge de rquota pour les SVM    | <pre>vserver nfs modify -vserver<br/>vserver_name -rquota enable</pre>  |
| Désactiver la prise en charge de rquota pour les SVM | <pre>vserver nfs modify -vserver<br/>vserver_name -rquota disable</pre> |

Pour plus d'informations sur les quotas, reportez-vous à la section ["Gestion du stockage logique"](#).

### Amélioration des performances de NFSv3 et NFSv4 en modifiant la taille du transfert TCP

Vous pouvez améliorer les performances des clients NFSv3 et NFSv4 qui se connectent aux systèmes de stockage sur un réseau à latence élevée en modifiant la taille maximale

## du transfert TCP.

Lorsque les clients accèdent aux systèmes de stockage sur un réseau à latence élevée, tel qu'un réseau WAN (Wide Area Network) ou un réseau MAN (Metro Area Network) avec une latence supérieure à 10 millisecondes, vous pouvez améliorer les performances de connexion en modifiant la taille maximale du transfert TCP. Les clients qui accèdent aux systèmes de stockage dans un réseau à faible latence, tel qu'un réseau local (LAN), ne peuvent guère bénéficier de la modification de ces paramètres. Si l'amélioration du débit ne l'emporte pas sur l'impact sur la latence, vous ne devez pas utiliser ces paramètres.

Pour déterminer si votre environnement de stockage peut tirer parti de la modification de ces paramètres, vous devez d'abord effectuer une évaluation complète des performances d'un client NFS peu performant. Vérifiez si les faibles performances sont à cause d'une latence aller-retour excessive et d'une petite demande sur le client. Dans ces conditions, le client et le serveur ne peuvent pas utiliser pleinement la bande passante disponible parce qu'ils passent la majorité de leurs cycles de service en attente de petites demandes et réponses à transmettre par le biais de la connexion.

En augmentant la taille des requêtes NFSv3 et NFSv4, le client et le serveur peuvent utiliser la bande passante disponible plus efficacement pour déplacer plus de données par unité de temps, ce qui accroît l'efficacité globale de la connexion.

N'oubliez pas que la configuration entre le système de stockage et le client peut varier. Le système de stockage et le client prennent en charge une taille maximale de 1 Mo pour les opérations de transfert. Cependant, si vous configurez le système de stockage pour prendre en charge une taille de transfert maximale de 1 Mo mais que le client ne prend en charge que 64 Ko, la taille de transfert de montage est limitée à 64 Ko ou moins.

Avant de modifier ces paramètres, notez qu'il entraîne une consommation de mémoire supplémentaire sur le système de stockage pendant la durée nécessaire à l'assemblage et à la transmission d'une réponse importante. Plus les connexions à latence élevée sont nombreuses, plus la consommation de mémoire supplémentaire augmente. Les systèmes de stockage dont la capacité de mémoire est élevée ne subissent que très peu d'effet. Les systèmes de stockage dont la capacité de mémoire est faible peuvent constater une dégradation notable des performances.

La réussite de l'utilisation de ces paramètres repose sur la capacité à récupérer les données provenant de plusieurs nœuds d'un cluster. La latence inhérente au réseau du cluster peut augmenter la latence globale de la réponse. La latence globale a tendance à augmenter lors de l'utilisation de ces paramètres. Ainsi, les charges de travail sensibles à la latence peuvent avoir un impact négatif.

### Modifier la taille maximale du transfert TCP NFSv3 et NFSv4

Vous pouvez modifier le `-tcp-max-xfer-size` Option permettant de configurer les tailles de transfert maximales pour toutes les connexions TCP en utilisant les protocoles NFSv3 et NFSv4.x.

#### Description de la tâche

Vous pouvez modifier ces options individuellement pour chaque serveur virtuel de stockage (SVM).

À partir de ONTAP 9, le `v3-tcp-max-read-size` et `v3-tcp-max-write-size` les options sont obsolètes. Vous devez utiliser le `-tcp-max-xfer-size` à la place.

#### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Effectuez l'une des opérations suivantes :

| Les fonctions que vous recherchez...                        | Entrez la commande...                                                                                |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Modifier la taille maximale du transfert TCP NFSv3 ou NFSv4 | <pre>vserver nfs modify -vserver<br/>vserver_name -tcp-max-xfer-size<br/>integer_max_xfer_size</pre> |

| Option             | Gamme                 | Valeur par défaut |
|--------------------|-----------------------|-------------------|
| -tcp-max-xfer-size | 8192 à 1048576 octets | 65536 octets      |



La taille de transfert maximale que vous saisissez doit être un multiple de 4 Ko (4096 octets). Les demandes qui ne sont pas correctement alignées ont un impact négatif sur les performances.

3. Utilisez le `vserver nfs show -fields tcp-max-xfer-size` pour vérifier les modifications.
4. Si des clients utilisent des montages statiques, démontez et remontez la nouvelle taille de paramètre pour prendre effet.

### Exemple

La commande suivante définit la taille maximale du transfert NFSv3 et NFSv4.x TCP à 1048576 octets sur le SVM nommé vs1 :

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

### Configurez le nombre d'ID de groupe autorisé pour les utilisateurs NFS

Par défaut, ONTAP prend en charge jusqu'à 32 ID de groupe lors du traitement des informations d'identification des utilisateurs NFS à l'aide de l'authentification Kerberos (RPCSEC\_GSS). Lors de l'utilisation de l'authentification AUTH\_SYS, le nombre maximal par défaut d'ID de groupe est de 16, comme défini dans RFC 5531. Vous pouvez augmenter le maximum jusqu'à 1,024 si vous avez des utilisateurs qui sont membres de plus que le nombre par défaut de groupes.

### Description de la tâche

Si un utilisateur a plus que le nombre par défaut d'ID de groupe dans ses informations d'identification, les ID de groupe restants sont tronqués et l'utilisateur peut recevoir des erreurs lorsqu'il tente d'accéder aux fichiers du système de stockage. Vous devez définir le nombre maximal de groupes par SVM sur un nombre qui représente le maximum de groupes dans votre environnement.

Le tableau suivant montre les deux paramètres du `vserver nfs modify` Commande qui détermine le nombre maximal d'ID de groupe dans trois exemples de configuration :

| Paramètres                | Paramètres                           | Limite des ID de groupe résultant |
|---------------------------|--------------------------------------|-----------------------------------|
| -extended-groups-limit    | 32                                   | RPCSEC_GSS : 32                   |
| -auth-sys-extended-groups | disabled                             | AUTH_SYS : 16                     |
|                           | Il s'agit des paramètres par défaut. |                                   |
| -extended-groups-limit    | 256                                  | RPCSEC_GSS : 256                  |
| -auth-sys-extended-groups | disabled                             | AUTH_SYS : 16                     |
| -extended-groups-limit    | 512                                  | RPCSEC_GSS : 512                  |
| -auth-sys-extended-groups | enabled                              | AUTH_SYS : 512                    |

## Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Effectuez l'action souhaitée :

|                                                                                 |                                                                                                                                     |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Si vous souhaitez définir le nombre maximum de groupes auxiliaires autorisés... | Entrez la commande...                                                                                                               |
| Uniquement pour RPCSEC_GSS et laissez AUTH_SYS à la valeur par défaut 16        | <pre>vserver nfs modify -vserver<br/>vserver_name -extended-groups-limit<br/>{32-1024} -auth-sys-extended-groups<br/>disabled</pre> |
| Pour RPCSEC_GSS et AUTH_SYS                                                     | <pre>vserver nfs modify -vserver<br/>vserver_name -extended-groups-limit<br/>{32-1024} -auth-sys-extended-groups<br/>enabled</pre>  |

3. Vérifiez le -extended-groups-limit Et vérifiez si AUTH\_SYS utilise des groupes étendus : 

```
vserver
nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-
groups-limit
```
4. Retour au niveau de privilège admin :

```
set -privilege admin
```

## Exemple

L'exemple suivant active les groupes étendus pour l'authentification AUTH\_SYS et définit le nombre maximal de groupes étendus sur 512 pour l'authentification AUTH\_SYS et RPCSEC\_GSS. Ces modifications sont effectuées uniquement pour les clients qui accèdent à la SVM nommée vs1 :

```

vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
 them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit

vs1 enabled 512

vs1::*> set -privilege admin

```

## Contrôler l'accès utilisateur root aux données de style de sécurité NTFS

Vous pouvez configurer ONTAP de manière à permettre aux clients NFS d'accéder aux données de type sécurité NTFS et aux clients NTFS pour accéder aux données de type sécurité NFS. Lorsque vous utilisez le style de sécurité NTFS dans un magasin de données NFS, vous devez décider comment traiter l'accès par l'utilisateur root et configurer la machine virtuelle de stockage (SVM) en conséquence.

### Description de la tâche

Lorsqu'un utilisateur root accède aux données de style de sécurité NTFS, vous disposez de deux options :

- Mappez l'utilisateur root à un utilisateur Windows comme tout autre utilisateur NFS et gérez l'accès en fonction des listes de contrôle d'accès NTFS.
- Ignorez les listes de contrôle d'accès NTFS et offrez un accès complet à la racine.

### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Effectuez l'action souhaitée :

| Si vous voulez que l'utilisateur root...                   | Entrez la commande...                                                                  |
|------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Être mappé à un utilisateur Windows                        | <code>vserver nfs modify -vserver vserver_name -ignore-nt-acl-for-root disabled</code> |
| Ignorer la vérification de la liste de contrôle d'accès NT | <code>vserver nfs modify -vserver vserver_name -ignore-nt-acl-for-root enabled</code>  |



Par défaut, ce paramètre est désactivé.

Si ce paramètre est activé mais qu'il n'y a pas de mappage de noms pour l'utilisateur root, ONTAP utilise les informations d'identification d'administrateur SMB par défaut pour l'audit.

### 3. Retour au niveau de privilège admin :

```
set -privilege admin
```

## Versions NFS et clients pris en charge

### Présentation des clients et des versions NFS prises en charge

Avant d'utiliser NFS dans votre réseau, vous devez connaître les versions NFS et les clients pris en charge par ONTAP.

Ce tableau indique lorsque des versions majeures et mineures des protocoles NFS sont prises en charge par défaut dans ONTAP. Par défaut, la prise en charge n'indique pas qu'il s'agit de la version la plus ancienne de ONTAP prenant en charge ce protocole NFS.

| Version | Pris en charge | Introduction                 |
|---------|----------------|------------------------------|
| NFSv3   | Oui.           | Toutes les versions de ONTAP |
| NFSv4.0 | Oui.           | ONTAP 8                      |
| NFSv4.1 | Oui.           | ONTAP 8,1                    |
| NFSv4.2 | Oui.           | ONTAP 9.8                    |
| PNFS    | Oui.           | ONTAP 8,1                    |

Pour obtenir les dernières informations sur les clients NFS pris en charge par ONTAP, consultez la matrice d'interopérabilité.

["Matrice d'interopérabilité NetApp"](#)

### Fonctionnalité NFSv4.0 prise en charge par ONTAP

ONTAP prend en charge toutes les fonctionnalités obligatoires dans NFSv4.0, à l'exception des mécanismes de sécurité SPKM3 et LIPKEY.

Les fonctionnalités NFSV4 suivantes sont prises en charge :

- **COMPOSÉ**

Permet à un client de demander plusieurs opérations de fichier dans une seule demande RPC (Remote Procedure Call).

- **Délégation de fichiers**

Permet au serveur de déléguer le contrôle de fichiers à certains types de clients pour l'accès en lecture et en écriture.

- **Pseudo-fs**

Utilisé par les serveurs NFSv4 pour déterminer les points de montage sur le système de stockage. Il n'y a pas de protocole de montage dans NFSv4.

- **Verrouillage**

Basé sur la location. Il n'existe pas de protocoles NLM (Network Lock Manager) ou NSM (Network Status Monitor) distincts dans NFSv4.

Pour plus d'informations sur le protocole NFSv4.0, voir RFC 3530.

### **Limites de la prise en charge d'ONTAP pour NFSv4**

Vous devez tenir compte de plusieurs restrictions liées à la prise en charge de ONTAP pour NFSv4.

- La fonction de délégation n'est pas prise en charge par tous les types de clients.
- Dans ONTAP 9.4 et versions antérieures, le système de stockage rejette les noms comportant des caractères non ASCII sur des volumes autres que les volumes UTF8.

Dans ONTAP 9.5 et versions ultérieures, les volumes créés avec le paramètre de langue utf8mb4 et montés via NFS v4 ne sont plus soumis à cette restriction.

- Tous les descripteurs de fichier sont persistants ; le serveur ne fournit pas de descripteurs de fichier volatiles.
- La migration et la réplication ne sont pas prises en charge.
- Les clients NFSv4 ne sont pas pris en charge par les miroirs de partage de charge en lecture seule.

ONTAP achemine les clients NFSv4 vers la source du miroir de partage de charge pour un accès en lecture et en écriture directs.

- Les attributs nommés ne sont pas pris en charge.
- Tous les attributs recommandés sont pris en charge, à l'exception des éléments suivants :
  - archive
  - hidden
  - homogeneous
  - mimetype
  - quota\_avail\_hard
  - quota\_avail\_soft
  - quota\_used
  - system
  - time\_backup



Même s'il ne prend pas en charge le `quota*` Attributs, ONTAP prend en charge les quotas d'utilisateurs et de groupes via le protocole de bande latérale RQUOTA.

## Prise en charge de ONTAP pour NFSv4.1

Depuis ONTAP 9.8, la fonctionnalité `nconnect` est disponible par défaut lorsque NFSv4.1 est activé.

Les implémentations de clients NFS antérieures n'utilisent qu'une connexion TCP unique avec un montage. En ONTAP, une connexion TCP unique peut former un goulot d'étranglement lorsque le nombre d'IOPS augmente. Cependant, un client `nconnect-enabled` peut avoir plusieurs connexions TCP (jusqu'à 16) associées à un seul montage NFS. Un client NFS multiplexe les opérations de fichiers sur plusieurs connexions TCP selon une séquence périodique et obtient ainsi un débit plus élevé à partir de la bande passante réseau disponible. NConnect est recommandé uniquement pour les montages NFS v3 et NFS v4.1.

Consultez la documentation de votre client NFS pour vérifier si `nconnect` est pris en charge dans la version de votre client.

NFSv4.1 est activé par défaut dans ONTAP 9.9.1 et versions ultérieures. Dans les versions antérieures, vous pouvez l'activer en spécifiant le `-v4.1` et le définir sur `enabled` Lors de la création d'un serveur NFS sur la machine virtuelle de stockage (SVM).

ONTAP ne prend pas en charge les délégations au niveau des fichiers et des répertoires NFSv4.1.

## Prise en charge de ONTAP pour NFSv4.2

À partir de ONTAP 9.8, ONTAP prend en charge le protocole NFSv4.2 pour permettre l'accès aux clients compatibles NFSv4.2.

NFSv4.2 est activé par défaut dans ONTAP 9.9.1 et versions ultérieures. Dans ONTAP 9.8, vous devez activer manuellement la version 4.2 en spécifiant le `-v4.1` et le définir sur `enabled` Lors de la création d'un serveur NFS sur la machine virtuelle de stockage (SVM). L'activation de NFSv4.1 permet également aux clients d'utiliser les fonctionnalités NFSv4.1 lorsqu'ils sont montés en tant que v4.2.

Les versions successives de ONTAP étendent la prise en charge des fonctionnalités facultatives NFSv4.2.

| À commencer par... | NFSv4.2 fonctionnalités facultatives comprennent ...                                                                             |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------|
| ONTAP 9.12.1       | <ul style="list-style-type: none"><li>• Attributs étendus NFS</li><li>• Fichiers épars</li><li>• Réservations d'espace</li></ul> |
| ONTAP 9.9.1        | Contrôle d'accès obligatoire (MAC) nommé NFS                                                                                     |

## Étiquettes de sécurité NFS v4.2

Depuis ONTAP 9.9.1, les étiquettes de sécurité NFS peuvent être activées. Ils sont désactivés par défaut.

Avec les étiquettes de sécurité NFS v4.2, les serveurs NFS ONTAP prennent en charge le contrôle d'accès obligatoire (MAC), en stockant et en récupérant les attributs `sec_label` envoyés par les clients.

Pour plus d'informations, voir ["RFC 7240"](#).

Depuis la version ONTAP 9.12.1, les étiquettes de sécurité NFS v4.2 sont prises en charge pour les opérations de dump NDMP. Si des étiquettes de sécurité sont rencontrées sur des fichiers ou des répertoires dans des versions antérieures, le vidage échoue.

### Étapes

1. Modifiez le paramètre de privilège sur avancé :

```
set -privilege advanced
```

2. Activer les étiquettes de sécurité :

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

### Attributs étendus NFS

Depuis ONTAP 9.12.1, les attributs étendus NFS (xattrs) sont activés par défaut.

Les attributs étendus sont des attributs NFS standard définis par ["RFC 8276"](#) Et compatible avec les clients NFS modernes. Elles peuvent servir à associer des métadonnées définies par l'utilisateur à des objets de système de fichiers et présentent un intérêt dans des déploiements de sécurité avancés.

Les attributs étendus NFS ne sont actuellement pas pris en charge pour les opérations de dump NDMP. Si des attributs étendus sont rencontrés sur des fichiers ou des répertoires, le vidage procède mais ne sauvegarde pas les attributs étendus sur ces fichiers ou répertoires.

Si vous devez désactiver les attributs étendus, utilisez le `vserver nfs modify -v4.2-xattrs disabled` commande.

### Prise en charge de ONTAP pour Parallel NFS

ONTAP prend en charge Parallel NFS (pNFS). Le protocole pNFS améliore les performances en offrant aux clients un accès direct aux données d'un ensemble de fichiers distribués sur plusieurs nœuds d'un cluster. Elle aide les clients à trouver le chemin optimal vers un volume.

### Utilisation de supports durs

Lors du dépannage des problèmes de montage, veillez à utiliser le type de montage approprié. NFS prend en charge deux types de montage : les montages souples et les montages durs. Pour des raisons de fiabilité, n'utilisez que des supports durs.

Vous ne devez pas utiliser de montages souples, en particulier en cas de retards NFS fréquents. Ces délais peuvent entraîner la corruption des données.

## Dépendances de nommage des fichiers et des répertoires NFS et SMB

### Présentation des dépendances de nommage des fichiers et des répertoires NFS et SMB

Les conventions d'appellation des fichiers et des répertoires dépendent à la fois des systèmes d'exploitation des clients réseau et des protocoles de partage de fichiers, en plus des paramètres de langue sur le cluster ONTAP et les clients.

Le système d'exploitation et les protocoles de partage de fichiers déterminent ce qui suit :

- Caractères un nom de fichier peut utiliser
- Sensibilité à la casse d'un nom de fichier

ONTAP prend en charge les caractères multi-octets dans les noms de fichier, de répertoire et de qtree, en fonction de la version de ONTAP utilisée.

### Caractères un nom de fichier ou de répertoire peut utiliser

Si vous accédez à un fichier ou à un répertoire à partir de clients ayant différents systèmes d'exploitation, vous devez utiliser des caractères valides dans les deux systèmes d'exploitation.

Par exemple, si vous utilisez UNIX pour créer un fichier ou un répertoire, n'utilisez pas de deux-points (:) dans le nom car le deux-points n'est pas autorisé dans les noms de fichiers ou de répertoires MS-DOS. Comme les restrictions sur les caractères valides varient d'un système d'exploitation à l'autre, consultez la documentation de votre système d'exploitation client pour plus d'informations sur les caractères interdits.

### Sensibilité à la casse des noms de fichiers et de répertoires dans un environnement multiprotocole

Les noms de fichiers et de répertoires sont sensibles à la casse pour les clients NFS et non sensibles à la casse, mais ils préservent la casse pour les clients SMB. Vous devez comprendre les implications dans un environnement multiprotocole et les actions nécessaires lorsque vous spécifiez le chemin lors de la création des partages SMB et lors de l'accès aux données au sein des partages.

Si un client SMB crée un répertoire nommé `testdir`, Les clients SMB et NFS affichent le nom de fichier comme `testdir`. Toutefois, si un utilisateur SMB tente par la suite de créer un nom de répertoire `TESTDIR`, Le nom n'est pas autorisé car, pour le client SMB, ce nom existe actuellement. Si un utilisateur NFS crée par la suite un répertoire nommé `TESTDIR`, Les clients NFS et SMB affichent le nom du répertoire différemment, comme suit :

- Sur les clients NFS, vous voyez les deux noms de répertoire tels qu'ils ont été créés, par exemple `testdir` et `TESTDIR`, car les noms de répertoire sont sensibles à la casse.
- Les clients SMB utilisent les 8.3 noms pour faire la distinction entre les deux répertoires. Un répertoire porte le nom du fichier de base. Un nom de fichier 8.3 est attribué aux répertoires supplémentaires.
  - Sur les clients SMB, vous voyez `testdir` et `TESTDI~1`.
  - ONTAP crée le `TESTDI~1` nom du répertoire pour différencier les deux répertoires.

Dans ce cas, vous devez utiliser le nom 8.3 lorsque vous spécifiez un chemin de partage lors de la création ou de la modification d'un partage sur un SVM (Storage Virtual machine).

De la même manière pour les fichiers, si un client SMB crée `test.txt`, Les clients SMB et NFS affichent le nom de fichier comme `test.txt`. Toutefois, si un utilisateur SMB tente par la suite de le créer `Test.txt`, Le nom n'est pas autorisé car, pour le client SMB, ce nom existe actuellement. Si un utilisateur NFS crée par la suite un fichier nommé `Test.txt`, Les clients NFS et SMB affichent le nom de fichier différemment, comme suit :

- Sur les clients NFS, les deux noms de fichiers sont ceux qu'ils ont créés, `test.txt` et `Test.txt`, car les noms de fichiers sont sensibles à la casse.
- Les clients SMB utilisent les 8.3 noms pour distinguer les deux fichiers. Un fichier porte le nom du fichier de base. Un nom de fichier 8.3 est attribué aux fichiers supplémentaires.
  - Sur les clients SMB, vous voyez `test.txt` et `TEST~1.TXT`.
  - ONTAP crée le `TEST~1.TXT` nom de fichier pour différencier les deux fichiers.



Si un mappage de caractères a été créé à l'aide des commandes de mappage de caractères CIFS du Vserver, une recherche Windows qui ne serait normalement pas sensible à la casse peut être sensible à la casse. Cela signifie que les recherches de nom de fichier ne seront sensibles à la casse que si le mappage de caractères a été créé et que le nom de fichier utilise ce mappage de caractères.

### Comment ONTAP crée des noms de fichiers et de répertoires

ONTAP crée et conserve deux noms pour les fichiers ou les répertoires de tout répertoire ayant accès à partir d'un client SMB : le nom long et le nom d'origine au format 8.3.

Pour les noms de fichier ou de répertoire dépassant le nom de huit caractères ou la limite d'extension de trois caractères (pour les fichiers), ONTAP génère un nom de format 8.3 comme suit :

- Il tronque le nom de fichier ou de répertoire d'origine à six caractères, si le nom dépasse six caractères.
- Il ajoute un tilde (~) et un nombre, un à cinq, aux noms de fichier ou de répertoire qui ne sont plus uniques après être tronqués.

S'il manque des nombres parce qu'il y a plus de cinq noms similaires, il crée un nom unique qui n'a aucune relation avec le nom original.

- Dans le cas des fichiers, il tronque l'extension du nom de fichier à trois caractères.

Par exemple, si un client NFS crée un fichier nommé `specifications.html`, Le nom de fichier au format 8.3 créé par ONTAP est `specif~1.htm`. Si ce nom existe déjà, ONTAP utilise un numéro différent à la fin du nom du fichier. Par exemple, si un client NFS crée un autre fichier nommé `specifications_new.html`, le format 8.3 de `specifications_new.html` est `specif~2.htm`.

### Comment ONTAP gère les noms de fichier, de répertoire et de qtree à plusieurs octets

À partir de ONTAP 9.5, la prise en charge des noms codés UTF-8 de 4 octets permet la création et l'affichage des noms de fichier, de répertoire et d'arborescence qui incluent des caractères supplémentaires Unicode à l'extérieur du plan multilingue de base (BMP). Dans les versions précédentes, ces caractères supplémentaires ne s'affichent pas correctement dans les environnements multiprotocoles.

Pour activer la prise en charge des noms codés UTF-8 à 4 octets, un nouveau code de langue `utf8mb4` est

disponible pour l' `vserver` et `volume` familles de commandement.

- Vous devez créer un volume de l'une des manières suivantes :
- Réglage du volume `-language` explicitement option :

```
volume create -language utf8mb4 {...}
```

- Hériter du volume `-language` Option d'un SVM qui a été créé avec ou modifié pour l'option :

```
vserver [create|modify] -language utf8mb4 {...}``volume create {...}
```

- Si vous utilisez ONTAP 9.6 et des versions antérieures, vous ne pouvez pas modifier les volumes existants pour le support `utf8mb4` ; vous devez créer un nouveau volume prêt à `utf8mb4`, puis migrer les données à l'aide d'outils de copie basés sur le client.

Si vous utilisez ONTAP 9.7P1 ou une version ultérieure, vous pouvez modifier les volumes existants pour `utf8mb4` avec une demande de support. Pour plus d'informations, voir ["Est-il possible de modifier la langue du volume après sa création dans ONTAP ?"](#).

Vous pouvez mettre à jour les SVM pour la prise en charge de `utf8mb4`, mais les volumes existants conservent leurs codes de langue d'origine.



Les noms de LUN portant des caractères UTF-8 de 4 octets ne sont pas pris en charge actuellement.

- Les données de caractères Unicode sont généralement représentées dans les applications de systèmes de fichiers Windows utilisant le format de transformation Unicode 16 bits (UTF-16) et dans les systèmes de fichiers NFS utilisant le format de transformation Unicode 8 bits (UTF-8).

Dans les versions antérieures à ONTAP 9.5, les noms, y compris les caractères supplémentaires UTF-16 créés par les clients Windows, étaient correctement affichés sur d'autres clients Windows mais n'étaient pas traduits correctement en UTF-8 pour les clients NFS. De même, les noms comportant des caractères supplémentaires UTF-8 par les clients NFS créés n'ont pas été correctement traduits en UTF-16 pour les clients Windows.

- Lorsque vous créez des noms de fichier sur des systèmes exécutant ONTAP 9.4 ou une version antérieure contenant des caractères supplémentaires valides ou non valides, ONTAP rejette le nom de fichier et renvoie une erreur de nom de fichier non valide.

Pour éviter ce problème, utilisez uniquement des caractères BMP dans les noms de fichiers et évitez d'utiliser des caractères supplémentaires, ou mettez à niveau vers ONTAP 9.5 ou version ultérieure.

Les caractères Unicode sont autorisés dans les noms de `qtree`.

- Vous pouvez utiliser le `volume qtree` Famille de commandes ou System Manager pour définir ou modifier les noms des `qtree`.
- Les noms des `qtrees` peuvent inclure des caractères multi-octets au format Unicode, comme les caractères japonais et chinois.
- Dans les versions antérieures à ONTAP 9.5, seuls les caractères BMP (c'est-à-dire ceux qui pouvaient être représentés en 3 octets) étaient pris en charge.



Dans les versions antérieures à ONTAP 9.5, le Junction-path du volume parent du qtree peut contenir des noms de qtree et de répertoire avec des caractères Unicode. Le `volume show` La commande affiche ces noms correctement lorsque le volume parent a un paramètre de langue UTF-8. Cependant, si la langue du volume parent n'est pas l'un des paramètres de langue UTF-8, certaines parties du chemin de jonction sont affichées à l'aide d'un nom de remplacement NFS numérique.

- Dans les versions 9.5 et ultérieures, les noms des qtree prennent en charge des caractères de 4 octets, à condition que le qtree se trouve dans un volume activé pour utf8m4.

## Configurez le mappage de caractères pour la conversion de nom de fichier SMB sur des volumes

Les clients NFS peuvent créer des noms de fichiers contenant des caractères non valides pour les clients SMB et certaines applications Windows. Vous pouvez configurer le mappage de caractères pour la conversion de noms de fichiers sur des volumes pour permettre aux clients SMB d'accéder aux fichiers avec des noms NFS qui ne seraient autrement pas valides.

### Description de la tâche

Lorsque les fichiers créés par des clients NFS sont accessibles par des clients SMB, ONTAP recherche le nom du fichier. Si le nom n'est pas un nom de fichier SMB valide (par exemple, s'il comporte un caractère «:»") inclus, ONTAP renvoie le nom de fichier 8.3 qui est conservé pour chaque fichier. Cependant, cela cause des problèmes pour les applications qui codent des informations importantes dans des noms de fichiers longs.

Par conséquent, si vous partagez un fichier entre des clients sur des systèmes d'exploitation différents, vous devez utiliser des caractères dans les noms de fichiers valides dans les deux systèmes d'exploitation.

Cependant, si vous avez des clients NFS qui créent des noms de fichier contenant des caractères qui ne sont pas des noms de fichier valides pour les clients SMB, vous pouvez définir une carte qui convertit les caractères NFS non valides en caractères Unicode acceptés par SMB et certaines applications Windows. Par exemple, cette fonctionnalité prend en charge les applications CATIA MCAD et Mathematica, ainsi que d'autres applications qui ont cette exigence.

Vous pouvez configurer le mappage de caractères sur une base volume par volume.

Lors de la configuration du mappage de caractères sur un volume, vous devez garder à l'esprit les éléments suivants :

- Le mappage de caractères n'est pas appliqué à travers les points de jonction.

Vous devez configurer explicitement le mappage de caractères pour chaque volume de jonction.

- Vous devez vous assurer que les caractères Unicode utilisés pour représenter des caractères non valides ou illégaux sont des caractères qui n'apparaissent normalement pas dans les noms de fichiers ; sinon, des mappages indésirables se produisent.

Par exemple, si vous essayez de mapper un deux-points (:) à un tiret (-) mais que le tiret (-) a été utilisé correctement dans le nom de fichier, un client Windows essayant d'accéder à un fichier nommé ""a-b" aurait sa demande mappée au nom NFS de ""a:b" (pas le résultat souhaité).

- Après l'application du mappage de caractères, si le mappage contient toujours un caractère Windows non valide, ONTAP revient aux noms de fichier Windows 8.3.



- Dans les notifications FPolicy, les journaux d'audit NAS et les messages de suivi de sécurité, les noms de fichiers mappés sont affichés.
- Lors de la création d'une relation SnapMirror de type DP, le mappage de caractères du volume source n'est pas répliqué sur le volume DP de destination.
- Sensibilité à la casse : comme les noms Windows mappés se transforment en noms NFS, la recherche des noms suit la sémantique NFS. Ainsi, les recherches NFS sont sensibles à la casse. Cela signifie que les applications qui accèdent aux partages mappés ne doivent pas se fier au comportement non sensible à la casse de Windows. Cependant, le nom 8.3 est disponible, et cela n'est pas sensible à la casse.
- Mappages partiels ou non valides : après le mappage d'un nom pour revenir aux clients faisant une énumération de répertoire (« dir »), le nom Unicode obtenu est vérifié pour la validité de Windows. Si ce nom contient toujours des caractères non valides ou s'il n'est pas valide pour Windows (par exemple, il se termine par "." ou vierge), le nom 8.3 est renvoyé à la place du nom non valide.

## Étape

### 1. Configurer le mappage de caractères :

```
vserver cifs character-mapping create -vserver vserver_name -volume
volume_name -mapping mapping_text, ...
```

Le mappage se compose d'une liste de paires de caractères source-cible séparées par «»:». Les caractères sont des caractères Unicode saisis à l'aide de chiffres hexadécimaux. Par exemple : 3C:E03C.

La première valeur de chaque `mapping_text` La paire séparée par deux-points est la valeur hexadécimale du caractère NFS que vous souhaitez traduire, et la seconde est la valeur Unicode utilisée par SMB. Les paires de mappage doivent être uniques (un mappage un-à-un doit exister).

#### ◦ Mappage de source

Le tableau suivant montre le jeu de caractères Unicode autorisé pour le mappage de source :

| Caractère Unicode | Caractère imprimé | Description                            |
|-------------------|-------------------|----------------------------------------|
| 0x01-0x19         | Sans objet        | Caractères de contrôle sans impression |
| 0x5C              | \                 | Barre oblique inversée                 |
| 0x3A              | :                 | Deux-points                            |
| 0x2A              | *                 | Astérisque                             |
| 0x3F              | ?                 | Point d'interrogation                  |
| 0x22              | «                 | Devis                                  |
| 0x3C              | <                 | Inférieur à                            |
| 0x3E              | >                 | Supérieur à                            |
| 0x7C              |                   |                                        |

|                 |      |   |
|-----------------|------|---|
| Ligne verticale | 0xb1 | ± |
|-----------------|------|---|

- Mappage de cible

Vous pouvez spécifier des caractères cibles dans la « zone d'utilisation privée » d'Unicode dans la plage suivante : U+E0000...U+F8FF.

### Exemple

La commande suivante crée un mappage de caractères pour un volume nommé « `dates` » sur la machine virtuelle de stockage (SVM) vs1 :

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show
```

| Vserver | Volume Name | Character Mapping         |
|---------|-------------|---------------------------|
| vs1     | data        | 3c:e17c, 3e:f17d, 2a:f745 |

### Commandes permettant de gérer les mappages de caractères pour la conversion de noms de fichiers SMB

Vous pouvez gérer le mappage de caractères en créant, en modifiant, en affichant des informations sur et en supprimant des mappages de caractères de fichiers utilisés pour la conversion de noms de fichiers SMB sur des volumes FlexVol.

| Les fonctions que vous recherchez...                               | Utilisez cette commande...                         |
|--------------------------------------------------------------------|----------------------------------------------------|
| Créer de nouveaux mappages de caractères de fichier                | <code>vserver cifs character-mapping create</code> |
| Affiche des informations sur les mappages de caractères de fichier | <code>vserver cifs character-mapping show</code>   |
| Modifier les mappages de caractères de fichier existants           | <code>vserver cifs character-mapping modify</code> |
| Supprimer les mappages de caractères de fichier                    | <code>vserver cifs character-mapping delete</code> |

Pour plus d'informations, consultez la page man pour chaque commande

## Gérer l'agrégation NFS

## Présentation de l'agrégation NFS

À partir de ONTAP 9.14.1, les clients NFSv4.1 peuvent exploiter la mise en circuit de session pour ouvrir plusieurs connexions à différentes LIF sur le serveur NFS, augmentant ainsi la vitesse du transfert de données et fournissant de la résilience via les chemins d'accès multiples.

L'agrégation est avantageuse pour l'exportation de volumes FlexVol vers des clients compatibles avec l'agrégation, en particulier des clients VMware et Linux, ou pour NFS via RDMA, TCP ou pNFS.

Dans ONTAP 9.14.1, la mise en circuits est limitée aux LIF sur un seul nœud ; la mise en circuits ne peut pas couvrir des LIF sur plusieurs nœuds.

Les volumes FlexGroup sont pris en charge pour l'agrégation. Bien que cela puisse fournir de meilleures performances, l'accès multivoie à un volume FlexGroup ne peut être configuré que sur un seul nœud.

Dans cette version, seule la mise en circuit de session est prise en charge pour les chemins d'accès multiples.

### Comment utiliser l'agrégation

Pour tirer parti des avantages des chemins d'accès multiples offerts par l'agrégation, vous devez disposer d'un ensemble de LIF, appelé *trunking group*, associées au SVM contenant un serveur NFS à ressources partagées. Les LIF d'un groupe à trunking doivent avoir des ports home sur le même nœud du cluster, et elles doivent résider sur ces ports home. Il est recommandé que toutes les LIFs d'un groupe à ressources partagées appartiennent au même groupe de basculement.

ONTAP prend en charge jusqu'à 16 connexions à ressources partagées par nœud à partir d'un client donné.

Lorsqu'un client monte des exportations à partir d'un serveur à ressources partagées, il spécifie un certain nombre d'adresses IP pour les LIF d'un groupe à ressources partagées. Une fois le client connecté à la première LIF, des LIFs supplémentaires ne sont ajoutées à la session NFSv4.1 et utilisées pour la mise en circuit que si elles sont conformes aux exigences des groupes à ressources partagées. Le client distribue ensuite les opérations NFS sur plusieurs connexions en fonction de son propre algorithme (comme la séquence round-robin).

Pour optimiser les performances, il est conseillé de configurer l'agrégation dans un SVM qui fournit des exportations multivoies, et non des exportations à chemin unique. En d'autres termes, vous devez activer la mise en circuits uniquement sur un serveur NFS d'un SVM dont les exportations sont fournies aux clients à ressources partagées uniquement.

### Clients pris en charge

Le serveur ONTAP NFSv4.1 prend en charge la mise en circuit avec tout client capable de la mise en circuit de session NFSv4.1.

Les clients suivants ont été testés avec ONTAP 9.14.1 :

- VMware - ESXi 7.0U3F et versions ultérieures
- Linux : Red Hat Enterprise Linux (RHEL) 8.8 et 9.3



Lorsque l'agrégation est activée sur un serveur NFS, les utilisateurs qui accèdent à des partages exportés sur des clients NFS qui ne prennent pas en charge l'agrégation peuvent voir une baisse des performances. En effet, une seule connexion TCP est utilisée pour plusieurs montages des LIFs de données du SVM.

## Différence entre l'agrégation NFS et nconnect

Depuis ONTAP 9.8, la fonctionnalité nconnect est disponible par défaut lorsque NFSv4.1 est activé. Sur les clients compatibles nconnect, un seul montage NFS peut avoir plusieurs connexions TCP (jusqu'à 16) sur une seule LIF.

En revanche, l'agrégation est *multipathing* fonctionnalité, qui fournit plusieurs connexions TCP sur plusieurs LIFs. Si vous avez la possibilité d'utiliser des cartes réseau supplémentaires dans votre environnement, l'agrégation offre un parallélisme et des performances supérieurs à ceux de nconnect.

En savoir plus sur ["nconnect."](#)

## Configurer un nouveau serveur NFS et des exportations pour l'agrégation

### Créez un serveur NFS à ressources partagées

À partir de ONTAP 9.14.1, l'agrégation peut être activée sur les serveurs NFS. NFSv4.1 est activé par défaut lors de la création des serveurs NFS.

#### Avant de commencer

La création d'un serveur NFS à ressources partagées nécessite une SVM. La SVM doit être :

- stockage suffisant pour répondre aux besoins en données des clients.
- Activé pour NFS.

Vous pouvez utiliser un SVM existant, mais l'activation de la mise en circuits nécessite le montage de tous les clients NFSv4.x, ce qui peut entraîner des perturbations. Si le remontage n'est pas possible, créer un nouveau SVM pour le serveur NFS.

#### Étapes

1. Si aucun SVM approprié n'existe, en créer un :

```
vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
aggregate_name -rootvolume-security-style unix -language C.UTF-8
```

2. Vérifier la configuration et le statut du nouveau SVM :

```
vserver show -vserver svm_name
```

En savoir plus sur ["Création d'un SVM"](#).

3. Créez le serveur NFS :

```
vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
-v4.1-trunking enabled -v4-id-domain my_domain.com
```

4. Vérifiez que NFS est en cours d'exécution :

```
vserver nfs status -vserver svm_name
```

5. Vérifiez que NFS est configuré comme vous le souhaitez :

```
vserver nfs show -vserver svm_name
```

En savoir plus sur ["Configuration du serveur NFS."](#)

### Une fois que vous avez terminé

Configurez les services suivants si nécessaire :

- ["DNS"](#)
- ["LDAP"](#)
- ["Kerberos"](#)

### Préparez votre réseau pour l'agrégation

Pour tirer parti de la mise en circuit NFSv4.1, les LIFs d'un groupe à agrégation doivent résider sur le même nœud et avoir des ports home sur le même nœud. Les LIFs doivent être configurées dans un failover group sur le même node.

### Description de la tâche

Un mappage un-à-un des LIF et des cartes réseau offre un gain de performance optimal, mais il n'est pas nécessaire d'activer l'agrégation. Avoir au moins deux cartes réseau installées peut offrir un avantage en termes de performances, mais ce n'est pas nécessaire.

Vous pouvez avoir plusieurs Failover Groups, mais le failover group pour trunking doit inclure uniquement les LIFS du groupe trunking.

Vous devez ajuster le groupe de basculement à ressources partagées chaque fois que vous ajoutez ou supprimez des connexions (et des cartes réseau sous-jacentes) d'un groupe de basculement.

### Avant de commencer

- Vous devez connaître les noms de port associés aux cartes réseau si vous souhaitez créer un groupe de basculement.
- Tous les ports doivent se trouver sur le même nœud.

### Étapes

1. Vérifiez les noms et l'état des ports réseau que vous prévoyez d'utiliser :

```
network port status
```

2. Créer le failover group :

```
network interface failover-groups create -vserver svm_name -failover-group failover_group_name -targets ports_list
```



La mise en place d'un groupe de basculement n'est pas obligatoire, mais il est fortement recommandé.

- *svm\_name* Est le nom du SVM contenant le serveur NFS.
- *ports\_list* est la liste des ports qui seront ajoutés au failover group.

Les ports sont ajoutés au format *nom\_nœud:numéro\_port*, par exemple, node1:e0c.

La commande suivante crée le groupe de basculement fg3 pour SVM vs1 et ajoute trois ports :

```
network interface failover-groups create -vserver vs1 -failover-group fg3
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

En savoir plus sur ["groupes de basculement."](#)

### 3. Si nécessaire, créez des LIFs pour les membres du groupe de trunking :

```
network interface create -vserver svm_name -lif lif_name -home-node node_name
-home-port port_name -address IP_address -netmask IP_address [-service-policy
policy] [-auto-revert {true|false}]
```

- *-home-node* - Le nœud auquel la LIF retourne lorsque la commande `network interface revert` est exécutée sur la LIF.

Vous pouvez également indiquer si la LIF doit revenir automatiquement au nœud home et au port home-port avec le *-auto-revert* option.

- *-home-port* Est le port physique ou logique renvoyé par la LIF lorsque la commande `network interface revert` est exécutée sur la LIF.
- Vous pouvez spécifier une adresse IP avec le *-address* et *-netmask* et non avec le *-subnet* option.
- Lorsque vous attribuez des adresses IP, vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un sous-réseau IP différent. Le `network route create` La page man contient des informations sur la création d'une route statique au sein d'un SVM.
- *-service-policy* - La politique de service de la LIF. Si aucune règle n'est spécifiée, une règle par défaut sera attribuée automatiquement. Utilisez le `network interface service-policy show` pour consulter les stratégies de service disponibles.
- *-auto-revert* - Spécifier si une LIF de données est automatiquement rétablie sur son nœud de rattachement dans des circonstances telles que le démarrage, les modifications du statut de la base de données de gestion ou lorsque la connexion réseau est établie. Le paramètre par défaut est FALSE, mais vous pouvez le définir sur TRUE en fonction des stratégies de gestion de réseau de votre environnement.

Répéter cette étape pour chaque LIF du groupe de trunking.

La commande suivante crée lif-A Pour la SVM vs1, sur le port e0c du nœud cluster1\_01:

```
network interface create -vserver vs1 -lif lif-A -service-policy ??? -home
-node cluster1_01 -home-port e0c -address 192.0.2.0
```

En savoir plus sur ["Création de LIF."](#)

### 4. Vérifier que les LIFs ont été créées :

```
network interface show
```

5. Vérifiez que l'adresse IP configurée est accessible :

| Pour vérifier... | Utiliser...                |
|------------------|----------------------------|
| Adresse IPv4     | <code>network ping</code>  |
| Adresse IPv6     | <code>network ping6</code> |

## Exporter les données pour l'accès client

Pour que le client puisse accéder aux partages de données, vous devez créer un ou plusieurs volumes et disposer de règles d'exportation au moins une pour le volume.

Conditions requises pour l'exportation du client :

- Les clients Linux doivent disposer d'un point de montage et d'un point de montage distincts pour chaque connexion à ressources partagées (c'est-à-dire, pour chaque LIF).
- Les clients VMware requièrent un seul point de montage pour un volume exporté, avec plusieurs LIF spécifiées.

Les clients VMware nécessitent un accès racine dans la règle d'export.

## Étapes

1. Créer une export-policy :

```
vserver export-policy create -vserver svm_name -policyname policy_name
```

Le nom de la stratégie peut comporter jusqu'à 256 caractères.

2. Vérifier que l'export policy a été créée :

```
vserver export-policy show -policyname policy_name
```

### Exemple

Les commandes suivantes créent et vérifient la création d'une export policy nommée exp1 sur le SVM nommé vs1:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1
```

3. Créez une règle d'export et ajoutez-la à une export-policy existante :

```
vserver export-policy rule create -vserver svm_name -policyname policy_name
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,..." }
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

Le `-clientmatch` Le paramètre doit identifier les clients Linux ou VMware compatibles avec l'agrégation qui vont monter l'exportation.

En savoir plus sur ["création de règles d'exportation."](#)

#### 4. Créer le volume avec un point de jonction :

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path -policy
export_policy_name
```

Découvrez "[création de volumes](#)".

#### 5. Vérifier que le volume a été créé avec le point de jonction souhaité :

```
volume show -vserver svm_name -volume volume_name -junction-path
```

### Créer des montages clients

Les clients Linux et VMware qui prennent en charge l'agrégation peuvent monter des volumes ou des partages de données à partir d'un serveur ONTAP NFSv4.1 qui est activé pour l'agrégation.

Lorsque vous entrez des commandes de montage sur les clients, vous devez entrer des adresses IP pour chaque LIF du groupe de trunking.

Découvrez "[clients pris en charge](#)".

#### Configuration requise pour le client Linux

Un point de montage distinct est requis pour chaque connexion dans le groupe d'agrégation.

Montez les volumes exportés avec des commandes similaires à celles ci-dessous :

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=16
```

```
mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=16
```

La version (`vers`) la valeur doit être de 4.1 ou ultérieure.

Le `max_connect` la valeur correspond au nombre de connexions dans le groupe d'agrégation.

#### Configuration requise pour le client VMware

Une instruction mount est requise, qui inclut une adresse IP pour chaque connexion du groupe d'agrégation.

Montez le datastore exporté avec une commande similaire à la suivante :

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Le `-H` les valeurs correspondent aux connexions dans le groupe d'agrégation.

### Adaptation des exportations NFS existantes pour l'agrégation



## Présentation de l'adaptation des exportations à chemin unique

Vous pouvez adapter une exportation NFSv4.1 à chemin unique existante (sans ressources partagées) pour utiliser la mise en circuit. Les clients prenant en charge l'agrégation peuvent bénéficier de performances améliorées dès que l'agrégation est activée sur le serveur, à condition que les conditions préalables du serveur et du client aient été satisfaites.

L'adaptation d'une exportation à chemin unique pour l'agrégation vous permet de maintenir les jeux de données exportés dans leurs volumes et SVM existants. Pour ce faire, vous devez activer l'agrégation sur le serveur NFS, mettre à jour la mise en réseau et la configuration d'exportation, et remonter le partage exporté sur les clients.

L'activation de l'agrégation a pour effet de redémarrer le serveur. Les clients VMware doivent ensuite remonter les datastores exportés ; les clients Linux doivent remonter les volumes exportés avec le `max_connect` option.

### Activer l'agrégation sur le serveur NFS

L'agrégation doit être explicitement activée sur les serveurs NFS. NFSv4.1 est activé par défaut lors de la création des serveurs NFS.

Après avoir activé l'agrégation, vérifiez que les services suivants sont configurés selon les besoins.

- ["DNS"](#)
- ["LDAP"](#)
- ["Kerberos"](#)

### Étapes

1. Activez la mise en circuit et assurez-vous que NFSv4.1 est activé :

```
vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
```

2. Vérifiez que NFS est en cours d'exécution :

```
vserver nfs status -vserver svm_name
```

3. Vérifiez que NFS est configuré comme vous le souhaitez :

```
vserver nfs show -vserver svm_name
```

En savoir plus sur ["Configuration du serveur NFS."](#)

.. Si vous êtes affectés à des clients Windows à partir de ce SVM, déplacez les partages puis supprimez le serveur.

```
vserver cifs show -vserver svm_name
```

+

```
vserver cifs delete -vserver svm_name
```

### Mettez à jour votre réseau pour l'agrégation

La mise en circuit NFSv4.1 requiert que les LIF d'un groupe à agrégation résident sur le

même nœud et disposent de ports home sur le même nœud. Toutes les LIFs doivent être configurées dans un groupe de failover sur le même node.

### Description de la tâche

Un mappage un-à-un des LIF et des cartes réseau offre un gain de performance optimal, mais n'est pas requis pour l'agrégation.

Vous pouvez avoir plusieurs failover groups, mais le failover group pour trunking doit inclure uniquement ces LIFS dans le groupe trunking.

Vous devez ajuster le groupe de basculement à ressources partagées chaque fois que vous ajoutez ou supprimez des connexions (et des cartes réseau sous-jacentes) d'un groupe de basculement.

### Avant de commencer

- Vous devez connaître les noms de port associés aux cartes réseau pour créer un groupe de basculement.
- Tous les ports doivent se trouver sur le même nœud.

### Étapes

1. Vérifiez les noms et l'état des ports réseau que vous prévoyez d'utiliser :

```
network port show
```

2. Créez un groupe de basculement à ressources partagées ou modifiez un groupe existant pour la mise en circuits :

```
network interface failover-groups create -vserver svm_name -failover-group failover_group_name -targets ports_list
```

```
network interface failover-groups modify -vserver svm_name -failover-group failover_group_name -targets ports_list
```



La mise en place d'un groupe de basculement n'est pas obligatoire, mais il est fortement recommandé.

- ° *svm\_name* Est le nom du SVM contenant le serveur NFS.
- ° *ports\_list* est la liste des ports qui seront ajoutés au failover group.

Les ports sont ajoutés au format *node\_name:port\_number*, par exemple, *node1:e0c*.

La commande suivante crée le failover group *fg3* Pour SVM *vs1* et ajoute trois ports :

```
network interface failover-groups create -vserver vs1 -failover-group fg3 -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

En savoir plus sur ["groupes de basculement."](#)

3. Créez des LIFs supplémentaires pour les membres du groupe d'agrégation, si nécessaire :

```
network interface create -vserver svm_name -lif lif_name -home-node node_name -home-port port_name -address IP_address -netmask IP_address [-service-policy policy] [-auto-revert {true|false}]
```

- `-home-node` - Le nœud auquel la LIF retourne lorsque la commande `network interface revert` est exécutée sur la LIF.
- Vous pouvez indiquer si la LIF doit automatiquement revenir au nœud de rattachement et au port de rattachement avec le `-auto-revert` option.
- `-home-port` Est le port physique ou logique renvoyé par la LIF lorsque la commande `network interface revert` est exécutée sur la LIF.
  - Vous pouvez spécifier une adresse IP avec le `-address` et `-netmask` options.
  - Lorsque vous attribuez des adresses IP manuellement (sans utiliser de sous-réseau), vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un sous-réseau IP différent. La page `man network route create` contient des informations sur la création d'une route statique au sein d'une SVM.
  - `-service-policy` - La politique de service de la LIF. Si aucune règle n'est spécifiée, une règle par défaut sera attribuée automatiquement. Utilisez le `network interface service-policy show` pour consulter les stratégies de service disponibles.
  - `-auto-revert` - Spécifier si une LIF de données est automatiquement rétablie sur son nœud de rattachement dans des circonstances telles que le démarrage, les modifications du statut de la base de données de gestion ou lorsque la connexion réseau est établie. **Le paramètre par défaut est FALSE**, mais vous pouvez le définir sur TRUE en fonction des stratégies de gestion de réseau de votre environnement.

Répéter cette étape pour chaque LIF supplémentaire nécessaire dans le groupe de trunking.

La commande suivante crée `lif-A` pour le SVM `vs1`, sur le port `e0c` du nœud `cluster1_01` :

```
network interface create -vserver vs1 -lif lif-A -service-policy default-
intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
```

En savoir plus sur "[Création de LIF](#)."

#### 4. Vérifier que les LIFs ont été créées :

```
network interface show
```

#### 5. Vérifiez que l'adresse IP configurée est accessible :

| Pour vérifier... | Utiliser...                |
|------------------|----------------------------|
| Adresse IPv4     | <code>network ping</code>  |
| Adresse IPv6     | <code>network ping6</code> |

### Modifier l'exportation des données pour l'accès client

Pour permettre aux clients de tirer parti de l'agrégation pour les partages de données existants, vous devrez peut-être modifier les règles et règles d'exportation ainsi que les volumes auxquels ils sont rattachés. Les exigences d'exportation pour les clients Linux et les datastores VMware sont différentes.

Conditions requises pour l'exportation du client :

- Les clients Linux doivent disposer d'un point de montage et d'un point de montage distincts pour chaque connexion à ressources partagées (c'est-à-dire, pour chaque LIF).

Si vous effectuez une mise à niveau vers ONTAP 9.14.1 et que vous avez déjà exporté un volume, vous pouvez continuer à utiliser ce volume dans un groupe de ressources partagées.

- Les clients VMware requièrent un seul point de montage pour un volume exporté, avec plusieurs LIF spécifiées.

Les clients VMware nécessitent un accès racine dans la règle d'export.

## Étapes

1. Vérifier qu'une export policy existante est en place :

```
vserver export-policy show
```

2. Vérifiez que les règles d'export policy existantes sont appropriées à la configuration de trunking :

```
vserver export-policy rule show -policyname policy_name
```

En particulier, vérifiez que le `-clientmatch` Le paramètre identifie correctement les clients Linux ou VMware compatibles avec l'agrégation qui vont monter l'exportation.

Si des ajustements sont nécessaires, modifiez la règle à l'aide du `vserver export-policy rule modify` ou créez une nouvelle règle :

```
vserver export-policy rule create -vserver svm_name -policyname policy_name
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,..." }
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

En savoir plus sur ["création de règles d'exportation."](#)

3. Vérifier que les volumes exportés existants sont en ligne :

```
volume show -vserver svm_name
```

## Rétablissez les montages client

Pour convertir les connexions client sans ressources partagées en connexions à ressources partagées, les montages existants sur les clients Linux et VMware doivent être démontés et remontés à l'aide des informations relatives aux LIF.

Lorsque vous entrez des commandes de montage sur les clients, vous devez entrer des adresses IP pour chaque LIF du groupe de trunking.

Découvrez ["clients pris en charge"](#).



Le démontage des clients VMware entraîne des interruptions pour toutes les machines virtuelles du datastore. Une alternative consisterait à créer un nouveau datastore activé pour l'agrégation et à utiliser **Storage vmotion** pour déplacer vos machines virtuelles de l'ancien datastore vers le nouveau. Pour plus de détails, reportez-vous à votre documentation VMware.

### Configuration requise pour le client Linux

Un point de montage distinct est requis pour chaque connexion dans le groupe d'agrégation.

Montez les volumes exportés avec des commandes similaires à celles ci-dessous :

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=2
```

```
mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=2
```

Le `vers` la valeur doit être de 4.1 ou ultérieure.

Le `max_connect` la valeur doit correspondre au nombre de connexions dans le groupe de ressources partagées.

### Configuration requise pour le client VMware

Une instruction `mount` est requise, qui inclut une adresse IP pour chaque connexion du groupe d'agrégation.

Montez le datastore exporté avec une commande similaire à la suivante :

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Le `-H` les valeurs doivent correspondre aux connexions dans le groupe d'agrégation.

## Gestion de NFS sur RDMA

### NFS sur RDMA

NFS sur RDMA utilise des adaptateurs RDMA. Il permet de copier directement les données entre la mémoire du système de stockage et la mémoire du système hôte, ce qui évite les interruptions du processeur et la surconsommation.

Les configurations NFS sur RDMA sont conçues pour les clients qui possèdent des charges de travail sensibles à la latence ou à large bande passante, telles que l'apprentissage machine et l'analytique. NVIDIA a étendu NFS sur RDMA pour permettre au GPU Direct Storage (GDS). Le GDS accélère encore plus les charges de travail grâce aux GPU en contournant complètement le processeur et la mémoire principale, et en utilisant RDMA pour transférer directement les données entre le système de stockage et la mémoire GPU.

Depuis ONTAP 9.10.1, les configurations NFS sur RDMA sont prises en charge pour le protocole NFSv4.0 lorsqu'elles sont utilisées avec l'adaptateur Mellanox CX-5 ou CX-6, qui prend en charge RDMA à l'aide de la version 2 du protocole RoCE. Le GDS est uniquement pris en charge par les processeurs graphiques de la famille NVIDIA Tesla et Ampere avec des cartes NIC Mellanox et le logiciel MOFED. Pour plus d'informations sur la prise en charge de la version NFS dans les versions ONTAP ultérieures, reportez-vous au tableau suivant : conditions requises.



Des tailles de montage NFS supérieures à 64 Ko entraînent des performances instables avec les configurations NFS sur RDMA.

### De formation

- Les systèmes de stockage doivent exécuter ONTAP 9.10.1 ou une version ultérieure.
- Vérifiez que vous exécutez la version correcte de ONTAP pour la version NFS que vous souhaitez utiliser.

| Version NFS | Prise en charge de ONTAP             |
|-------------|--------------------------------------|
| NFSv4.0     | ONTAP 9.10.1 et versions ultérieures |
| NFSv4.1     | ONTAP 9.14.1 et versions ultérieures |
| NFSv3       | ONTAP 9.15.1 et versions ultérieures |

- Il est possible de configurer NFS sur RDMA avec System Manager, à partir de ONTAP 9.12.1. Dans ONTAP 9.10.1 et 9.11.1, vous devez utiliser l'interface de ligne de commande pour configurer NFS sur RDMA.
- Les deux nœuds de la paire HA doivent utiliser la même version.
- Les contrôleurs du système de stockage doivent prendre en charge RDMA

| À partir de ONTAP...                 | Les contrôleurs suivants prennent en charge RDMA...                                                  |
|--------------------------------------|------------------------------------------------------------------------------------------------------|
| 9.10.1 et versions ultérieures       | <ul style="list-style-type: none"> <li>• AFF A400</li> <li>• AFF A700</li> <li>• AFF A800</li> </ul> |
| ONTAP 9.14.1 et versions ultérieures | <ul style="list-style-type: none"> <li>• AFF série C.</li> <li>• AFF A900</li> </ul>                 |

- Dispositif de stockage configuré avec du matériel pris en charge par RDMA (p. ex. Mellanox CX-5 ou CX-6).
- Les LIF de données doivent être configurées pour prendre en charge RDMA.
- Les clients doivent utiliser des cartes réseau compatibles RDMA Mellanox et le logiciel réseau MOFED (Mellanox OFED).



Les groupes d'interface ne sont pas pris en charge avec NFS sur RDMA.

### Étapes suivantes

- [Configurer les cartes réseau pour NFS sur RDMA](#)
- [Configuration des LIF pour NFS sur RDMA](#)
- [Paramètres NFS pour NFS sur RDMA](#)

### Informations associées

- ["RDMA"](#)
- [Présentation de l'agrégation NFS](#)
- ["RFC 7530 : protocole NFS version 4"](#)
- ["RFC 8166 : transport d'accès direct à la mémoire à distance pour l'appel de procédure à distance version 1"](#)

- ["RFC 8167 : appel de procédure bidirectionnelle à distance sur les transports RPC-over-RDMA"](#)
- ["RFC 8267 : liaison de couche supérieure NFS à RPC-over-RDMA version 1"](#)

## Configurer les cartes réseau pour NFS sur RDMA

NFS sur RDMA requiert une configuration de carte réseau pour le système client et la plateforme de stockage.

### Configuration de la plateforme de stockage

Un adaptateur X1148 RDMA doit être installé sur le serveur. Si vous utilisez une configuration HA, vous devez disposer d'un adaptateur X1148 correspondant sur le partenaire de basculement pour que le service RDMA puisse continuer le processus de basculement. La carte réseau doit être compatible ROCE.

Depuis ONTAP 9.10.1, vous pouvez afficher la liste des protocoles de déchargement RDMA avec la commande :

```
network port show -rdma-protocols roce
```

### Configuration du système client

Les clients doivent utiliser des cartes NIC Mellanox compatibles RDMA (par exemple, X1148) et logiciel réseau Mellanox OFED. Consultez la documentation Mellanox pour connaître les modèles et versions pris en charge. Bien que le client et le serveur puissent être connectés directement, l'utilisation de commutateurs est recommandée en raison des performances de basculement améliorées avec un commutateur.

Le client, le serveur, tous les commutateurs et tous les ports des commutateurs doivent être configurés à l'aide de trames Jumbo. S'assurer également que le contrôle de flux prioritaire est en vigueur sur tous les commutateurs.

Une fois cette configuration confirmée, vous pouvez monter le NFS.

## System Manager

Vous devez utiliser ONTAP 9.12.1 ou version ultérieure pour configurer les interfaces réseau avec NFS sur RDMA à l'aide de System Manager.

### Étapes

1. Vérifier si le protocole RDMA est pris en charge. Accédez à **réseau > ports Ethernet** et sélectionnez le nœud approprié dans la vue de groupe. Lorsque vous développez le nœud, examinez le champ **protocoles RDMA** pour un port donné : la valeur **RoCE** indique que RDMA est pris en charge ; un tiret (-) indique qu'il n'est pas pris en charge.
2. Pour ajouter un VLAN, sélectionnez **+ VLAN**. Sélectionnez le nœud approprié. Dans le menu déroulant **Port**, les ports disponibles affichent le texte **RoCE Enabled** s'ils prennent en charge RDMA. Aucun texte ne s'affiche s'ils ne prennent pas en charge RDMA.
3. Suivez le flux de travail dans [Activez le stockage NAS pour les serveurs Linux à l'aide de NFS](#) Pour configurer un nouveau serveur NFS.

Lorsque vous ajoutez des interfaces réseau, vous avez la possibilité de sélectionner **utiliser les ports RoCE**. Sélectionnez cette option pour les interfaces réseau que vous souhaitez utiliser NFS sur RDMA.

### CLI

1. Vérifier si l'accès RDMA est activé sur le serveur NFS avec la commande :

```
vserver nfs show-vserver SVM_name
```

Par défaut, `-rdma` doit être activé. Si ce n'est pas le cas, activer l'accès RDMA sur le serveur NFS :

```
vserver nfs modify -vserver SVM_name -rdma enabled
```

2. Monter le client via NFSv4.0 sur RDMA :
  - a. L'entrée du paramètre `proto` dépend de la version du protocole IP du serveur. S'il s'agit d'IPv4, utilisez `proto=rdma`. S'il s'agit du protocole IPv6, utilisez-le `proto=rdma6`.
  - b. Spécifiez le port cible NFS en tant que `port=20049` au lieu du port standard 2049 :

```
mount -o vers=4,minorversion=0,proto=rdma,port=20049 Server_IP_address
:/volume_path mount_point
```

3. **OPTIONNEL**: Si vous devez démonter le client, exécutez la commande `umount mount_path`

### Plus d'informations

- [Créez un serveur NFS](#)
- [Activez le stockage NAS pour les serveurs Linux à l'aide de NFS](#)

## Configuration des LIF pour NFS sur RDMA

Pour utiliser NFS sur RDMA, vous devez configurer vos LIF (interface réseau) pour qu'elles soient compatibles avec RDMA. La LIF et sa paire de basculement doivent pouvoir prendre en charge RDMA.



## Créer une nouvelle LIF

### System Manager

Vous devez exécuter ONTAP 9.12.1 ou une version ultérieure pour créer une interface réseau pour NFS sur RDMA avec System Manager.

#### Étapes

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez **+ Add**.
3. Lorsque vous sélectionnez **NFS,SMB/CIFS,S3**, vous pouvez **utiliser les ports RoCE**. Cochez la case utiliser les ports RoCE\*.
4. Sélectionnez le VM de stockage et le nœud de rattachement. Attribuez un **Nom**, une **adresse IP** et un **masque de sous-réseau**.
5. Une fois que vous avez saisi l'adresse IP et le masque de sous-réseau, System Manager filtre la liste des domaines de diffusion à ceux qui disposent de ports compatibles RoCE. Sélectionnez un domaine de diffusion. Vous pouvez éventuellement ajouter une passerelle.
6. Sélectionnez **Enregistrer**.

### CLI

#### Étapes

1. Créer une LIF :

```
network interface create -vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

- La politique de service doit être des fichiers de données par défaut ou une règle personnalisée qui inclut le service d'interface réseau Data-nfs.
- Le `-rdma-protocols` paramètre accepte une liste, qui est par défaut vide. Quand `roce` Est une valeur ajoutée, le LIF ne peut être configuré que sur des ports prenant en charge RoCE Offload, affectant la migration et le basculement des LIF bot.

## Modifier une LIF

## System Manager

Vous devez exécuter ONTAP 9.12.1 ou une version ultérieure pour créer une interface réseau pour NFS sur RDMA avec System Manager.

### Étapes

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez **Modifier** en regard de l'interface réseau que vous souhaitez modifier.
3. Cochez **utiliser les ports RoCE** pour activer NFS sur RDMA ou décochez la case pour la désactiver. Si l'interface réseau se trouve sur un port compatible RoCE, la case à cocher située en regard de **Use RoCE ports** s'affiche.
4. Modifiez les autres paramètres si nécessaire.
5. Sélectionnez **Enregistrer** pour confirmer vos modifications.

### CLI

1. Vous pouvez vérifier le statut de vos LIFs à l'aide de `network interface show` commande. La politique de service doit inclure le service de l'interface réseau Data-nfs. Le `-rdma-protocols` la liste doit inclure `roce`. Si l'une de ces conditions est fausse, modifiez la LIF.
2. Pour modifier le LIF, lancer :

```
network interface modify vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```



La modification d'une LIF afin de nécessiter un protocole de déchargement particulier lorsque la LIF n'est pas actuellement attribuée à un port qui prend en charge ce protocole entraînera une erreur.

## Migrer un LIF

ONTAP vous permet également de migrer les interfaces réseau (LIF) afin d'utiliser NFS sur RDMA. Lors de cette migration, vous devez vous assurer que le port de destination est compatible RoCE. Depuis ONTAP 9.12.1, vous pouvez effectuer cette procédure dans System Manager. Lors de la sélection d'un port de destination pour l'interface réseau, System Manager désignera si les ports sont compatibles RoCE.

Vous pouvez migrer un LIF vers une configuration NFS sur RDMA uniquement si :

- Il s'agit d'une interface réseau NFS RDMA (LIF) hébergée sur un port compatible RoCE.
- Il s'agit d'une interface réseau TCP NFS (LIF) hébergée sur un port compatible RoCE.
- Il s'agit d'une interface réseau TCP NFS (LIF) hébergée sur un port non compatible RoCE.

Pour plus d'informations sur la migration d'une interface réseau, reportez-vous à la section [Migrer un LIF](#).

### Plus d'informations

- [Créer une LIF](#)
- [Créer une LIF](#)

- [Modifier une LIF](#)
- [Migrer un LIF](#)

## Modifier la configuration NFS

Dans la plupart des cas, il n'est pas nécessaire de modifier la configuration du serveur virtuel de stockage NFS pour NFS sur RDMA.

Si vous êtes toutefois chargé de résoudre les problèmes liés aux puces Mellanox et à la migration de LIF, il est recommandé d'augmenter la période de grâce au verrouillage NFSv4. Par défaut, le délai de grâce est défini sur 45 secondes. Depuis ONTAP 9.10.1, la valeur maximale du délai de grâce est de 180 (secondes).

### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Saisissez la commande suivante :

```
vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
```

Pour plus d'informations sur cette tâche, voir [Spécifier la période de grâce du verrouillage NFSv4](#).

## Configurez SMB avec l'interface de ligne de commandes

### Présentation de la configuration SMB avec l'interface de ligne de commande

Vous pouvez utiliser les commandes de l'interface de ligne de commande de ONTAP 9 pour configurer l'accès des clients SMB aux fichiers contenus dans un nouveau volume ou qtree dans un SVM nouveau ou existant.



**SMB** (Server message Block) désigne les dialectes modernes du protocole CIFS (Common Internet File System). Vous verrez toujours *CIFS* dans l'interface de ligne de commande (CLI) ONTAP et dans les outils de gestion OnCommand.

Utilisez les procédures suivantes pour configurer l'accès SMB à un volume ou à un qtree de la manière suivante :

- Vous souhaitez utiliser SMB version 2 ou ultérieure.
- Vous ne souhaitez servir que les clients SMB, pas les clients NFS (pas une configuration multiprotocole).
- Les autorisations d'accès au fichier NTFS seront utilisées pour sécuriser le nouveau volume.
- Vous disposez des privilèges d'administrateur de cluster et non des privilèges d'administrateur de SVM.

Les privilèges d'administrateur du cluster sont requis pour créer des SVM et des LIFs. Les privilèges d'administrateur SVM sont suffisants pour d'autres tâches de configuration SMB.

- Vous souhaitez utiliser l'interface de ligne de commandes, et non System Manager ou un outil de script automatisé.

Pour utiliser System Manager pour configurer l'accès multiprotocole NAS, reportez-vous à la section ["Provisionnement de stockage NAS pour Windows et Linux à l'aide des protocoles NFS et SMB"](#).

- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.

Vous trouverez des détails sur la syntaxe des commandes dans l'aide de l'interface de ligne de commande et dans les pages de manuel ONTAP.

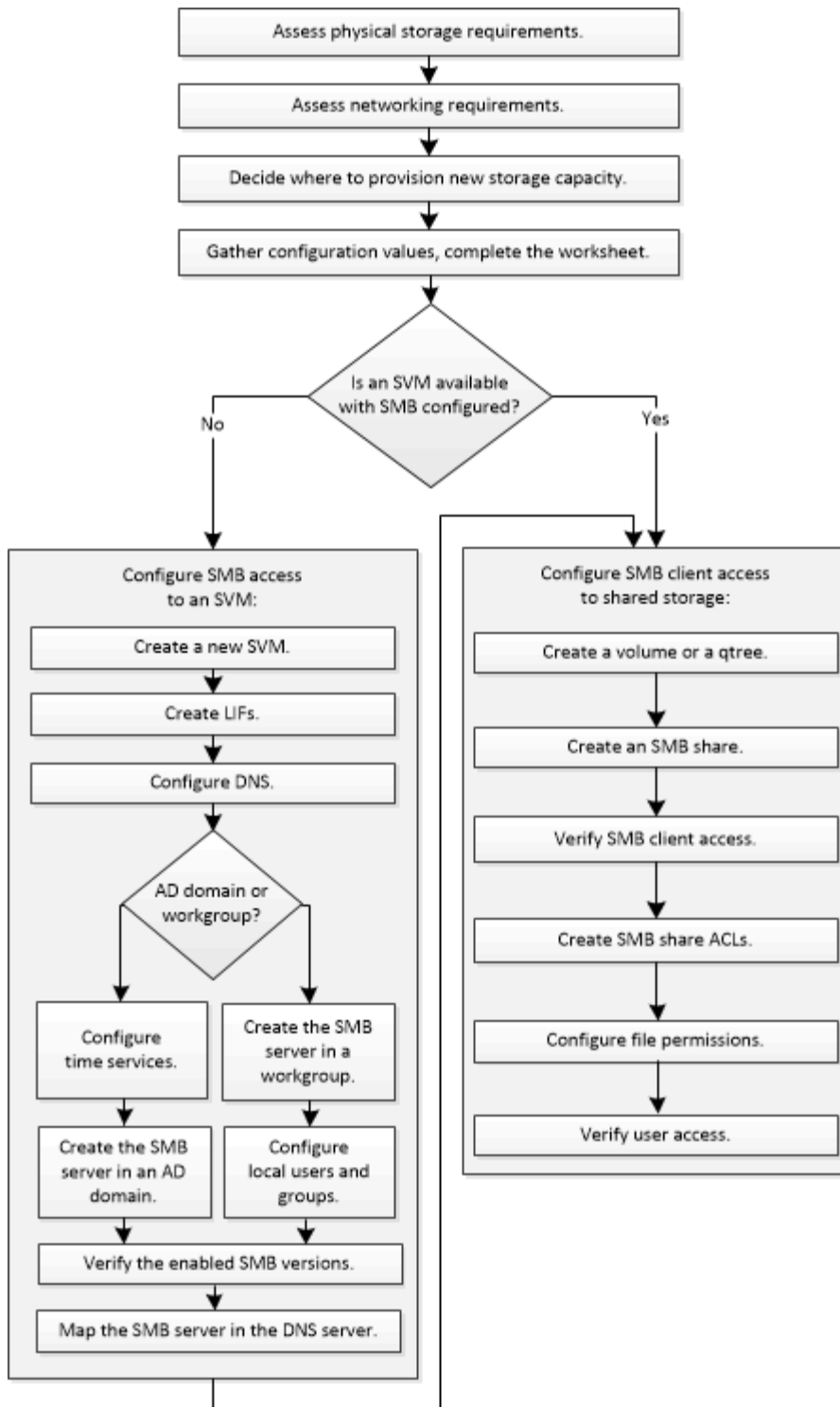
Pour plus d'informations sur la plage de fonctionnalités du protocole SMB de ONTAP, consultez le ["Présentation des références SMB"](#).

### D'autres façons de le faire dans ONTAP

| Pour effectuer ces tâches avec...                                            | Reportez-vous à...                                                                   |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| System Manager redessiné (disponible avec ONTAP 9.7 et versions ultérieures) | <a href="#">"Provisionnement du stockage NAS pour les serveurs Windows avec SMB"</a> |
| System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures)   | <a href="#">"Présentation de la configuration SMB"</a>                               |

### Workflow de configuration SMB

La configuration de SMB implique l'évaluation des besoins en réseau et en stockage physique, puis le choix d'un workflow spécifique à votre objectif ; la configuration de l'accès SMB à un SVM nouveau ou existant ; ou l'ajout d'un volume ou d'un qtree à un SVM existant déjà entièrement configuré pour l'accès SMB.



## Préparation

### Évaluer les besoins en matière de stockage physique

Avant de provisionner le stockage SMB pour les clients, vous devez vérifier que l'espace est suffisant dans un agrégat existant pour le nouveau volume. Si ce n'est pas le cas, vous pouvez ajouter des disques à un agrégat existant ou créer un nouvel agrégat du type souhaité.

## Étapes

1. Afficher l'espace disponible dans les agrégats existants : `storage aggregate show`

Si un agrégat dispose d'un espace suffisant, notez son nom dans la fiche de travail.

```
cluster::> storage aggregate show
Aggregate Size Available Used% State #Vols Nodes RAID Status

aggr_0 239.0GB 11.13GB 95% online 1 node1 raid_dp, normal
aggr_1 239.0GB 11.13GB 95% online 1 node1 raid_dp, normal
aggr_2 239.0GB 11.13GB 95% online 1 node2 raid_dp, normal
aggr_3 239.0GB 11.13GB 95% online 1 node2 raid_dp, normal
aggr_4 239.0GB 238.9GB 95% online 5 node3 raid_dp, normal
aggr_5 239.0GB 239.0GB 95% online 4 node4 raid_dp, normal
6 entries were displayed.
```

2. Si aucun agrégat n'a suffisamment d'espace, ajoutez des disques à un agrégat existant en utilisant le `storage aggregate add-disks` ou créez un nouvel agrégat à l'aide de `storage aggregate create` commande.

## Évaluer les exigences de mise en réseau

Avant de fournir un stockage SMB aux clients, vous devez vérifier que le réseau est correctement configuré pour répondre aux exigences de provisionnement SMB.

### Avant de commencer

Les objets de réseau de cluster suivants doivent être configurés :

- Ports physiques et logiques
- Les domaines de diffusion
- Sous-réseaux (le cas échéant)
- IPspaces (selon les besoins, en plus de l'IPspace par défaut)
- Failover Groups (si nécessaire, en plus du groupe de basculement par défaut pour chaque broadcast domain)
- Pare-feu externes

## Étapes

1. Afficher les ports physiques et virtuels disponibles : `network port show`

- Dans la mesure du possible, vous devez utiliser le port avec la vitesse la plus élevée pour le réseau de données.

- Tous les composants du réseau de données doivent avoir le même paramètre MTU pour optimiser les performances.
- 2. Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, vérifiez que le sous-réseau existe et dispose des adresses suffisantes : `network subnet show`

Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche

3. Les sous-réseaux sont créés à l'aide du `network subnet create` commande.

- 3. Affichez les IPspaces disponibles : `network ipspace show`

Vous pouvez utiliser l'IPspace par défaut ou un IPspace personnalisé.

- 4. Si vous souhaitez utiliser des adresses IPv6, vérifiez que l'IPv6 est activé sur le cluster : `network options ipv6 show`

Si nécessaire, vous pouvez activer IPv6 en utilisant le `network options ipv6 modify` commande.

## Décidez où provisionner la nouvelle capacité de stockage SMB

Avant de créer un nouveau volume SMB ou qtree, vous devez décider de le placer dans un SVM nouveau ou existant, et de la configuration requise par la SVM. Cette décision détermine votre flux de travail.

### Choix

- Si vous souhaitez provisionner un volume ou qtree sur un nouveau SVM, ou sur un SVM existant sur lequel SMB est activé mais non configuré, suivez les étapes des sections « Configuration de l'accès SMB à un SVM » et « Ajout de capacité de stockage à un SVM SMB ».

### Configuration de l'accès SMB à un SVM

### Configuration de l'accès client SMB au stockage partagé

Vous pouvez choisir de créer un nouveau SVM si l'un des cas suivants est vrai :

- Vous activez SMB sur un cluster pour la première fois.
- Un cluster contient des SVM existants dans lequel vous ne souhaitez pas activer la prise en charge SMB.
- Au sein d'un cluster, un ou plusieurs SVM compatibles SMB doivent être connectés :
  - Vers une autre forêt ou groupe de travail Active Directory.
  - Vers un serveur SMB dans un espace de noms isolé (scénario de colocation).  
Vous devez également choisir cette option pour provisionner le stockage sur un SVM existant pour lequel SMB est activé, mais pas configuré. Ce peut être le cas si vous avez créé le SVM pour l'accès SAN ou si aucun protocole n'a été activé au moment de la création de la SVM.

Après l'activation de SMB sur le SVM, procéder au provisionnement d'un volume ou qtree.

- Si vous souhaitez provisionner un volume ou qtree sur un SVM existant entièrement configuré pour l'accès SMB, suivez les étapes de la section « Ajout de capacité de stockage à un SVM compatible SMB ».

### Configuration de l'accès client SMB au stockage partagé

## Fiche de collecte des informations de configuration SMB

La fiche de configuration SMB vous permet de collecter les informations requises pour configurer l'accès SMB pour les clients.

Vous devez remplir une ou les deux sections de la feuille de travail, en fonction de la décision que vous avez prise concernant l'emplacement de stockage :

- Si vous configurez l'accès SMB à un SVM, vous devez compléter les deux sections.

[Configuration de l'accès SMB à un SVM](#)

[Configuration de l'accès client SMB au stockage partagé](#)

- Si vous ajoutez de la capacité de stockage à un SVM compatible SMB, vous ne devez remplir que la deuxième section.

[Configuration de l'accès client SMB au stockage partagé](#)

Les pages de manuel de commande contiennent des informations détaillées sur les paramètres.

### Configuration de l'accès SMB à un SVM

#### Paramètres de création d'un SVM

Ces valeurs sont fournies avec le `vserver create` Commande si vous créez un nouveau SVM.

| Champ                                   | Description                                                                                                                                                                     | Votre valeur         |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <code>-vserver</code>                   | Un nom que vous fournissez pour le nouveau SVM qui est un nom de domaine complet (FQDN) ou suit une autre convention qui applique des noms de SVM uniques au sein d'un cluster. |                      |
| <code>-aggregate</code>                 | Le nom d'un agrégat du cluster disposant d'un espace suffisant pour la nouvelle capacité de stockage SMB.                                                                       |                      |
| <code>-rootvolume</code>                | Un nom unique que vous fournissez pour le volume root du SVM.                                                                                                                   |                      |
| <code>-rootvolume-security-style</code> | Utiliser le style de sécurité NTFS pour le SVM.                                                                                                                                 | <code>ntfs</code>    |
| <code>-language</code>                  | Utilisez le paramètre de langue par défaut de ce flux de travail.                                                                                                               | <code>C.UTF-8</code> |



| Champ   | Description                                                                                       | Votre valeur |
|---------|---------------------------------------------------------------------------------------------------|--------------|
| ipspace | Facultatif : les IPspaces sont des espaces d'adresse IP distincts dans lesquels les SVM résident. |              |

### Paramètres de création d'une LIF

Ces valeurs sont fournies avec le `network interface create` Commande lorsque vous créez des LIFs.

| Champ            | Description                                                                                                                                                 | Votre valeur |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| -lif             | Nom que vous fournissez pour la nouvelle LIF.                                                                                                               |              |
| -role            | Utiliser le rôle LIF de données dans ce workflow                                                                                                            | data         |
| -data-protocol   | Utilisez uniquement le protocole SMB dans ce flux de production.                                                                                            | cifs         |
| -home-node       | Le nœud vers lequel la LIF renvoie lorsque <code>network interface revert</code> La commande est exécutée sur le LIF.                                       |              |
| -home-port       | Le port ou le groupe d'interface sur lequel la LIF renvoie au moment du <code>network interface revert</code> La commande est exécutée sur le LIF.          |              |
| -address         | L'adresse IPv4 ou IPv6 sur le cluster qui seront utilisées pour l'accès aux données par la nouvelle LIF.                                                    |              |
| -netmask         | Le masque de réseau et la passerelle pour le LIF.                                                                                                           |              |
| -subnet          | Un pool d'adresses IP. Utilisé au lieu de <code>-address</code> et <code>-netmask</code> pour attribuer automatiquement des adresses et des masques réseau. |              |
| -firewall-policy | Utilisez la politique de pare-feu de données par défaut dans ce workflow.                                                                                   | data         |

| Champ                     | Description                                                                                                                                                                                             | Votre valeur |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <code>-auto-revert</code> | Facultatif : spécifie si une LIF de données est automatiquement reconvertie vers son nœud de rattachement au démarrage ou dans d'autres circonstances. Le paramètre par défaut est <code>false</code> . |              |

### Paramètres de résolution de nom d'hôte DNS

Ces valeurs sont fournies avec le `vserver services name-service dns create` Commande lorsque vous configurez un DNS.

| Champ                      | Description                                                | Votre valeur |
|----------------------------|------------------------------------------------------------|--------------|
| <code>-domains</code>      | Jusqu'à cinq noms de domaine DNS.                          |              |
| <code>-name-servers</code> | Jusqu'à trois adresses IP pour chaque serveur de noms DNS. |              |

### Configuration d'un serveur SMB dans un domaine Active Directory

#### Paramètres de configuration du service de temps

Ces valeurs sont fournies avec le `cluster time-service ntp server create` commande lorsque vous configurez des services de temps.

| Champ                | Description                                                               | Votre valeur |
|----------------------|---------------------------------------------------------------------------|--------------|
| <code>-server</code> | Nom d'hôte ou adresse IP du serveur NTP pour le domaine Active Directory. |              |

#### Paramètres de création d'un serveur SMB dans un domaine Active Directory

Ces valeurs sont fournies avec le `vserver cifs create` Commande lorsque vous créez un nouveau serveur SMB et spécifiez les informations de domaine.

| Champ                     | Description                                 | Votre valeur |
|---------------------------|---------------------------------------------|--------------|
| <code>-vserver</code>     | Nom du SVM sur lequel créer le serveur SMB. |              |
| <code>-cifs-server</code> | Nom du serveur SMB (15 caractères maximum). |              |

| Champ                         | Description                                                                                                                                                         | Votre valeur |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <code>-domain</code>          | Nom de domaine complet (FQDN) du domaine Active Directory à associer au serveur SMB.                                                                                |              |
| <code>-ou</code>              | Facultatif : unité organisationnelle du domaine Active Directory à associer au serveur SMB. Par défaut, ce paramètre est défini sur CN=Computers.                   |              |
| <code>-netbios-aliases</code> | Facultatif : liste des alias NetBIOS, qui sont des noms alternatifs au nom du serveur SMB.                                                                          |              |
| <code>-comment</code>         | Facultatif : commentaire texte pour le serveur. Les clients Windows peuvent voir cette description du serveur SMB lors de la navigation sur les serveurs du réseau. |              |

### Configuration d'un serveur SMB dans un groupe de travail

#### Paramètres pour la création d'un serveur SMB dans un groupe de travail

Ces valeurs sont fournies avec le `vserver cifs create` Lorsque vous créez un nouveau serveur SMB et spécifiez les versions SMB prises en charge.

| Champ                     | Description                                                                                                                                                         | Votre valeur |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <code>-vserver</code>     | Nom du SVM sur lequel créer le serveur SMB.                                                                                                                         |              |
| <code>-cifs-server</code> | Nom du serveur SMB (15 caractères maximum).                                                                                                                         |              |
| <code>-workgroup</code>   | Nom du groupe de travail (jusqu'à 15 caractères).                                                                                                                   |              |
| <code>-comment</code>     | Facultatif : commentaire texte pour le serveur. Les clients Windows peuvent voir cette description du serveur SMB lors de la navigation sur les serveurs du réseau. |              |

#### Paramètres pour la création d'utilisateurs locaux

Vous fournissez ces valeurs lorsque vous créez des utilisateurs locaux en utilisant le `vserver cifs users-and-groups local-user create` commande. Elles sont requises pour les serveurs SMB des groupes de

travail et facultatives dans les domaines AD.

| Champ                | Description                                                                                                                                                          | Votre valeur |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| -vserver             | Nom du SVM sur lequel créer l'utilisateur local.                                                                                                                     |              |
| -user-name           | Nom de l'utilisateur local (20 caractères maximum).                                                                                                                  |              |
| -full-name           | Facultatif : nom complet de l'utilisateur. Si le nom complet contient un espace, placez le nom complet entre guillemets.                                             |              |
| -description         | Facultatif : description de l'utilisateur local. Si la description contient un espace, placez le paramètre entre guillemets.                                         |              |
| -is-account-disabled | Facultatif : indique si le compte utilisateur est activé ou désactivé. Si ce paramètre n'est pas spécifié, la valeur par défaut est d'activer le compte utilisateur. |              |

### Paramètres de création de groupes locaux

Vous fournissez ces valeurs lorsque vous créez des groupes locaux en utilisant le `vserver cifs users-and-groups local-group create` commande. Elles sont facultatives pour les serveurs SMB dans les domaines AD et les groupes de travail.

| Champ        | Description                                                                                                           | Votre valeur |
|--------------|-----------------------------------------------------------------------------------------------------------------------|--------------|
| -vserver     | Nom du SVM sur lequel créer le groupe local.                                                                          |              |
| -group-name  | Nom du groupe local (256 caractères maximum).                                                                         |              |
| -description | Facultatif : description du groupe local. Si la description contient un espace, placez le paramètre entre guillemets. |              |

### Ajout de capacité de stockage à un SVM compatible SMB

#### Paramètres de création d'un volume

Ces valeurs sont fournies avec le `volume create` commande si vous créez un volume à la place d'un qtrees.

| Champ                        | Description                                                                                  | Votre valeur      |
|------------------------------|----------------------------------------------------------------------------------------------|-------------------|
| <code>-vserver</code>        | Nom d'un SVM nouveau ou existant qui hébergera le nouveau volume.                            |                   |
| <code>-volume</code>         | Un nom descriptif unique que vous fournissez pour le nouveau volume.                         |                   |
| <code>-aggregate</code>      | Nom d'un agrégat dans le cluster disposant d'un espace suffisant pour le nouveau volume SMB. |                   |
| <code>-size</code>           | Un entier que vous fournissez pour la taille du nouveau volume.                              |                   |
| <code>-security-style</code> | Utilisez le style de sécurité NTFS pour ce flux de travail.                                  | <code>ntfs</code> |
| <code>-junction-path</code>  | Emplacement sous la racine (/) où le nouveau volume doit être monté.                         |                   |

### Paramètres pour la création d'un qtree

Ces valeurs sont fournies avec le `volume qtree create` commande si vous créez un qtree à la place d'un volume.

| Champ                    | Description                                                                                                                                                        | Votre valeur |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <code>-vserver</code>    | Nom de la SVM sur lequel réside le volume contenant le qtree.                                                                                                      |              |
| <code>-volume</code>     | Nom du volume qui contiendra le nouveau qtree.                                                                                                                     |              |
| <code>-qtree</code>      | Un nom descriptif unique que vous fournissez pour le nouveau qtree, 64 caractères maximum.                                                                         |              |
| <code>-qtree-path</code> | L'argument de chemin qtree dans le format<br>/vol/volume_name/qtree_name\> peut être spécifié au lieu de spécifier volume et qtree en tant qu'arguments distincts. |              |

### Paramètres de création de partages SMB

Ces valeurs sont fournies avec le `vserver cifs share create` commande.

| Champ                          | Description                                                                                                                                                                                       | Votre valeur |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <code>-vserver</code>          | Nom du SVM sur lequel créer le partage SMB.                                                                                                                                                       |              |
| <code>-share-name</code>       | Nom du partage SMB que vous souhaitez créer (256 caractères maximum).                                                                                                                             |              |
| <code>-path</code>             | Nom du chemin d'accès au partage SMB (256 caractères maximum). Ce chemin doit exister dans un volume avant de créer le partage.                                                                   |              |
| <code>-share-properties</code> | Facultatif : liste des propriétés de partage. Les paramètres par défaut sont <code>oplocks</code> , <code>browsable</code> , <code>changenotify</code> , et <code>show-previous-versions</code> . |              |
| <code>-comment</code>          | Facultatif : commentaire texte pour le serveur (256 caractères maximum). Les clients Windows peuvent voir cette description de partage SMB lors de la navigation sur le réseau.                   |              |

### Paramètres de création de listes de contrôle d'accès de partage SMB (ACL)

Ces valeurs sont fournies avec le `vserver cifs share access-control create` commande.

| Champ                         | Description                                                                                                                         | Votre valeur         |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <code>-vserver</code>         | Nom du SVM sur lequel créer la ACL SMB.                                                                                             |                      |
| <code>-share</code>           | Nom du partage SMB sur lequel créer.                                                                                                |                      |
| <code>-user-group-type</code> | Type de l'utilisateur ou du groupe à ajouter à la liste de contrôle d'accès du partage. Le type par défaut est <code>windows</code> | <code>windows</code> |

| Champ          | Description                                                                                                                                                                    | Votre valeur    |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| -user-or-group | Utilisateur ou groupe à ajouter à la liste ACL du partage. Si vous spécifiez le nom d'utilisateur, vous devez inclure le domaine de l'utilisateur au format "domain\username". |                 |
| -permission    | Spécifie les autorisations pour l'utilisateur ou le groupe.                                                                                                                    | `[ No_access    |
| Read           | Change                                                                                                                                                                         | Full_Control ]` |

## Configuration de l'accès SMB à un SVM

### Configuration de l'accès SMB à un SVM

Si aucune SVM n'est déjà configurée pour l'accès client SMB, vous devez créer et configurer un nouveau SVM ou configurer un SVM existant. La configuration SMB implique l'ouverture d'un accès au volume root du SVM, la création d'un serveur SMB, la création d'une LIF, l'activation de la résolution de nom d'hôte, la configuration des services de noms et, si nécessaire, Activation de la sécurité Kerberos.

### Créer un SVM

Si vous ne disposez pas encore d'au moins un SVM dans un cluster pour fournir un accès aux données aux clients SMB, vous devez en créer un.

#### Avant de commencer

- À partir de la version ONTAP 9.13.1, vous pouvez définir une capacité maximale pour une machine virtuelle de stockage. Vous pouvez également configurer des alertes lorsque la SVM approche un niveau de capacité seuil. Pour plus d'informations, voir [Gestion de la capacité des SVM](#).

### Étapes

1. Création d'un SVM : `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipSpace ipSpace_name`

- Utilisez le paramètre NTFS pour le `-rootvolume-security-style` option.
- Utilisez le paramètre par défaut C.UTF-8 `-language` option.
- Le `ipSpace` le paramètre est facultatif.

2. Vérifier la configuration et le statut du nouveau SVM : `vserver show -vserver vserver_name`

**Le Allowed Protocols** Le champ doit inclure CIFS. Vous pouvez modifier cette liste ultérieurement.

**Le Vserver Operational State** le champ doit afficher `running` état. S'il affiche le `initializing` État, cela signifie qu'une opération intermédiaire telle que la création du volume root a échoué, et vous devez supprimer la SVM et la recréer.

## Exemples

La commande suivante crée un SVM pour l'accès aux données dans l'IPspace `ipspaceA`:

```
cluster1::> vservers create -vservers vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vservers creation completed
```

La commande suivante montre qu'un SVM a été créé avec un volume root de 1 Go, il a été démarré automatiquement et qu'il est en `running` état. Le volume root dispose d'une export policy par défaut qui n'inclut aucune règle et qui ne précise donc pas l'exportation du volume root au moment de sa création.

```
cluster1::> vservers show -vservers vs1.example.com
 Vservers: vs1.example.com
 Vservers Type: data
 Vservers Subtype: default
 Vservers UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736

 Root Volume: root_vs1
 Aggregate: aggr1
 NIS Domain: -
 Root Volume Security Style: ntfs
 LDAP Client: -
 Default Volume Language Code: C.UTF-8
 Snapshot Policy: default
 Comment:
 Quota Policy: default
 List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
 Vservers Admin State: running
 Vservers Operational State: running
Vservers Operational State Stopped Reason: -
 Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
Disallowed Protocols: -
 QoS Policy Group: -
 Config Lock: false
 IPspace Name: ipspaceA
```



À partir de la ONTAP 9.13.1, vous pouvez définir un modèle de groupe de règles de QoS adaptative, en appliquant une limite plafond et un seuil de débit aux volumes du SVM. Vous ne pouvez appliquer cette politique qu'après avoir créé la SVM. Pour en savoir plus sur ce processus, voir [Définissez un modèle de groupe de règles adaptatives](#).



## Vérifier que le protocole SMB est activé sur le SVM

Avant de pouvoir configurer et utiliser SMB sur les SVM, il faut vérifier que le protocole est activé.

### Description de la tâche

Cela s'effectue généralement lors de la configuration d'un SVM, mais si vous n'avez pas activé le protocole lors de l'installation, vous pouvez l'activer plus tard à l'aide du `vserver add-protocols` commande.



Vous ne pouvez pas ajouter ou supprimer un protocole d'une LIF une fois qu'il est créé.

Vous pouvez également désactiver les protocoles sur les SVM à l'aide de `vserver remove-protocols` commande.

### Étapes

1. Vérifier les protocoles actuellement activés et désactivés pour le SVM : `vserver show -vserver vserver_name -protocols`

Vous pouvez également utiliser le `vserver show-protocols` Commande permettant d'afficher les protocoles actuellement activés sur tous les SVM du cluster.

2. Si nécessaire, activer ou désactiver un protocole :

- Pour activer le protocole SMB : `vserver add-protocols -vserver vserver_name -protocols cifs`
- Pour désactiver un protocole : `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`

3. Vérifiez que les protocoles activés et désactivés ont été correctement mis à jour : `vserver show -vserver vserver_name -protocols`

### Exemple

La commande suivante affiche les protocoles actuellement activés et désactivés (autorisés et interdits) sur le SVM nommé vs1 :

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver Allowed Protocols Disallowed Protocols
----- -
vs1.example.com cifs nfs, fcp, iscsi, ndmp
```

La commande suivante permet d'accéder à via SMB par ajout `cifs` Pour la liste des protocoles activés sur le SVM nommé vs1 :

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

## Ouvrir la export policy du volume root du SVM

L'export policy default du volume root du SVM doit inclure une règle afin de permettre à

tous les clients d'y accéder via SMB. Sans cette règle, tous les clients SMB se voient refuser l'accès au SVM et à ses volumes.

### Description de la tâche

Lorsqu'un nouveau SVM est créé, une export policy par défaut (appelée default) est créée automatiquement pour le volume root du SVM. On doit créer une ou plusieurs règles pour l'export policy par défaut avant que les clients puissent accéder aux données sur la SVM.

Vérifiez que tous les accès SMB sont ouverts dans la stratégie d'export par défaut, puis limitez l'accès aux volumes individuels en créant des règles d'export personnalisées pour les volumes individuels ou les qtrees.

### Étapes

1. Si vous utilisez un SVM existant, vérifiez la root volume export policy par défaut : `vserver export-policy rule show`

Le résultat de la commande doit être similaire à ce qui suit :

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

Vserver: vs1.example.com
Policy Name: default
Rule Index: 1
Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
RO Access Rule: any
RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: any
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

Si une telle règle existe et autorise l'accès ouvert, cette tâche est terminée. Si ce n'est pas le cas, passez à l'étape suivante.

2. Créer une règle d'export pour le volume root du SVM: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Vérifiez la création de règles à l'aide du `vserver export-policy rule show` commande.

### Résultats

Tout client SMB peut désormais accéder à n'importe quel volume ou qtree créé sur la SVM.

### Créer une LIF

Une LIF est une adresse IP associée à un port physique ou logique. En cas de panne d'un composant, une LIF peut basculer vers un autre port physique ou la migrer vers un autre port, ce qui continue à communiquer avec le réseau.

### Avant de commencer

- Le port réseau physique ou logique sous-jacent doit avoir été configuré sur l'administrateur `up` état.
- Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, le sous-réseau doit déjà exister.

Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche 3. Ils sont créés à l'aide du `network subnet create` commande.

- Le mécanisme de spécification du type de trafic traité par une LIF a changé. Pour ONTAP 9.5 et versions antérieures, la LIF utilisait des rôles pour spécifier le type de trafic qu'elle entraînerait. Depuis ONTAP 9.6, les LIF utilisent des politiques de service pour spécifier le type de trafic qu'elles seraient à traiter.

### Description de la tâche

- Vous pouvez créer des LIF IPv4 et IPv6 sur le même port réseau.
- Si vous disposez d'un grand nombre de LIF dans le cluster, vous pouvez vérifier la capacité LIF prise en charge sur le cluster à l'aide de `network interface capacity show` Et la capacité LIF prise en charge sur chaque nœud à l'aide de `network interface capacity details show` commande (au niveau de privilège avancé).
- Depuis ONTAP 9.7, si d'autres LIF existent déjà pour le SVM dans le même sous-réseau, il n'est pas nécessaire de spécifier le home port de la LIF. ONTAP choisit automatiquement un port aléatoire sur le nœud de rattachement spécifié dans le même domaine de diffusion que les autres LIFs déjà configurées dans le même sous-réseau.

### Étapes

1. Créer une LIF :

```
network interface create -vserver vservice_name -lif lif_name -role data -data
-protocol cifs -home-node node_name -home-port port_name {-address IP_address
-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
-revert {true|false}
```

| ONTAP 9.5 et versions antérieures                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol cifs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address</code> |
| <code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code>                                                                                                               |
| <code>false}`</code>                                                                                                                                                                          |

| ONTAP 9.6 et ultérieur                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>`network interface create -vserver vservice_name -lif lif_name -service-policy service_policy_name -home -node node_name -home-port port_name {-address IP_address -netmask IP_address</code> |
| <code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code>                                                                                                                     |
| <code>false}`</code>                                                                                                                                                                                |

- Le `-role` Paramètre n'est pas requis lors de la création d'une LIF à l'aide d'une politique de service (à partir de ONTAP 9.6).

- Le `-data-protocol` Paramètre n'est pas requis lors de la création d'une LIF à l'aide d'une politique de service (à partir de ONTAP 9.6). Lors de l'utilisation de ONTAP 9.5 et versions antérieures, le `-data-protocol` Le paramètre doit être spécifié lors de la création de la LIF et ne peut pas être modifié par la suite sans destruction et recréez la LIF de données.
- `-home-node` Est le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.

Vous pouvez également indiquer si la LIF doit revenir automatiquement au nœud home et au port home-port avec le `-auto-revert` option.

- `-home-port` Est le port physique ou logique vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.
- Vous pouvez spécifier une adresse IP avec le `-address` et `-netmask` ou vous activez l'allocation à partir d'un sous-réseau avec le `-subnet_name` option.
- Lors de l'utilisation d'un sous-réseau pour fournir l'adresse IP et le masque de réseau, si le sous-réseau a été défini avec une passerelle, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau.
- Si vous attribuez des adresses IP manuellement (sans utiliser de sous-réseau), vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un autre sous-réseau IP. Le `network route create` La page man contient des informations sur la création d'une route statique au sein d'un SVM.
- Pour le `-firewall-policy` utilisez la même option par défaut `data` Comme le rôle LIF.

Vous pouvez créer et ajouter une stratégie de pare-feu personnalisée ultérieurement si vous le souhaitez.



Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir ["Configuration des politiques de pare-feu pour les LIF"](#).

- `-auto-revert` Vous permet de spécifier si une LIF de données est automatiquement rétablie sur le nœud de rattachement en cas de démarrage, de modifications du statut de la base de données de gestion ou lors de la connexion réseau. Le paramètre par défaut est `false`, mais vous pouvez le définir sur `false` selon les stratégies de gestion de réseau de votre environnement.

## 2. Vérifier que le LIF a été créé correctement :

```
network interface show
```

## 3. Vérifiez que l'adresse IP configurée est accessible :

| Pour vérifier... | Utiliser...                |
|------------------|----------------------------|
| Adresse IPv4     | <code>network ping</code>  |
| Adresse IPv6     | <code>network ping6</code> |

## Exemples

La commande suivante crée une LIF et spécifie les valeurs d'adresse IP et de masque réseau à l'aide de

-address et -netmask paramètres :

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port elc -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

La commande suivante crée une LIF et attribue des valeurs d'adresse IP et de masque réseau à partir du sous-réseau spécifié (nommé client1\_sub) :

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port elc -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

La commande suivante affiche toutes les LIFs du cluster-1. Les LIF de données datalif1 et datalif3 sont configurées avec des adresses IPv4 et le datalif4 est configuré avec une adresse IPv6 :

```
network interface show
```

| Vserver                   | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Is Port |
|---------------------------|-------------------|-------------------|----------------------|--------------|-----------------|
| Home                      |                   |                   |                      |              |                 |
| -----                     | -----             | -----             | -----                | -----        | -----           |
| cluster-1                 |                   |                   |                      |              |                 |
| true                      | cluster_mgmt      | up/up             | 192.0.2.3/24         | node-1       | e1a             |
| node-1                    |                   |                   |                      |              |                 |
| true                      | clus1             | up/up             | 192.0.2.12/24        | node-1       | e0a             |
| true                      | clus2             | up/up             | 192.0.2.13/24        | node-1       | e0b             |
| true                      | mgmt1             | up/up             | 192.0.2.68/24        | node-1       | e1a             |
| node-2                    |                   |                   |                      |              |                 |
| true                      | clus1             | up/up             | 192.0.2.14/24        | node-2       | e0a             |
| true                      | clus2             | up/up             | 192.0.2.15/24        | node-2       | e0b             |
| true                      | mgmt1             | up/up             | 192.0.2.69/24        | node-2       | e1a             |
| vs1.example.com           |                   |                   |                      |              |                 |
| true                      | datalif1          | up/down           | 192.0.2.145/30       | node-1       | e1c             |
| vs3.example.com           |                   |                   |                      |              |                 |
| true                      | datalif3          | up/up             | 192.0.2.146/30       | node-2       | e0c             |
| true                      | datalif4          | up/up             | 2001::2/64           | node-2       | e0c             |
| 5 entries were displayed. |                   |                   |                      |              |                 |

La commande suivante montre comment créer une LIF de données NAS attribuée avec le default-data-files règle de service :

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport e0d -service-policy default-data-files -subnet-name ipspace1
```

## Activez le DNS pour la résolution du nom d'hôte

Vous pouvez utiliser le `vserver services name-service dns` Commande permettant d'activer DNS sur un SVM et de le configurer afin d'utiliser DNS pour la

résolution de nom d'hôte. Les noms d'hôte sont résolus à l'aide de serveurs DNS externes.

**Avant de commencer**


Un serveur DNS au niveau du site doit être disponible pour les recherches de noms d'hôte.

Vous devez configurer plusieurs serveurs DNS pour éviter un point de défaillance unique. Le `vserver services name-service dns create` Commande émet un avertissement si vous entrez un seul nom de serveur DNS.

**Description de la tâche**

Le *Network Management Guide* contient des informations sur la configuration de DNS dynamique sur le SVM.

**Étapes**

1. Activer le DNS sur le SVM : `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`
- La commande suivante permet d'activer les serveurs DNS externes sur le SVM vs1 :
- ```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```
- 

À partir de ONTAP 9.2, le `vserver services name-service dns create` Commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP ne parvient pas à contacter le serveur de noms.
2. Afficher les configurations de domaine DNS à l'aide de `vserver services name-service dns show` commande. ``

La commande suivante affiche les configurations DNS pour tous les SVM du cluster :

```
vserver services name-service dns show
```

			Name
Vserver	State	Domains	Servers
cluster1	enabled	example.com	192.0.2.201, 192.0.2.202
vs1.example.com	enabled	example.com	192.0.2.201, 192.0.2.202

La commande suivante affiche des informations détaillées de configuration DNS pour le SVM vs1 :

```
vserver services name-service dns show -vserver vs1.example.com
Vserver: vs1.example.com
Domains: example.com
Name Servers: 192.0.2.201, 192.0.2.202
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

3. Validez l'état des serveurs de noms à l'aide de la `vserver services name-service dns check` commande.

Le `vserver services name-service dns check` Est disponible à partir de ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com
```

Vserver	Name Server	Status	Status Details
-----	-----	-----	
vs1.example.com	10.0.0.50	up	Response time (msec): 2
vs1.example.com	10.0.0.51	up	Response time (msec): 2

Configurez un serveur SMB dans un domaine Active Directory

Configurer les services de temps

Avant de créer un serveur SMB dans un contrôleur Active Domain, vous devez vous assurer que l'heure du cluster et l'heure sur les contrôleurs de domaine du domaine auquel le serveur SMB appartient correspondent dans les cinq minutes.

Description de la tâche

Vous devez configurer les services NTP du cluster de manière à utiliser les mêmes serveurs NTP pour la synchronisation horaire que le domaine Active Directory.

Depuis ONTAP 9.5, vous pouvez configurer votre serveur NTP avec une authentification symétrique.

Étapes

1. Configurer les services de temps à l'aide du `cluster time-service ntp server create` commande.
 - Pour configurer des services de temps sans authentification symétrique, entrez la commande suivante : `cluster time-service ntp server create -server server_ip_address`
 - Pour configurer des services de temps avec une authentification symétrique, entrez la commande suivante : `cluster time-service ntp server create -server server_ip_address -key-id key_id`
`cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`


2. Vérifiez que les services de temps sont correctement configurés à l'aide du `cluster time-service ntp server show` commande.


```
cluster time-service ntp server show
```

Server	Version
-----	-----
10.10.10.1	auto
10.10.10.2	auto

Commandes de gestion de l'authentification symétrique sur les serveurs NTP

Depuis ONTAP 9.5, le protocole NTP (Network Time Protocol) version 3 est pris en charge. NTPv3 inclut une authentification symétrique à l'aide de clés SHA-1 qui augmente la sécurité du réseau.

Pour cela...	Utilisez cette commande...
Configurer un serveur NTP sans authentification symétrique	<code>cluster time-service ntp server create -server server_name</code>
Configurez un serveur NTP avec une authentification symétrique	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>
Activer l'authentification symétrique pour un serveur NTP existant le serveur NTP existant peut être modifié pour activer l'authentification en ajoutant l'ID de clé requis	<code>cluster time-service ntp server modify -server server_name -key-id key_id</code>
Configurez une clé NTP partagée	<div><code>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</code><div> Les clés partagées sont désignées par un ID. L'ID, son type et la valeur doivent être identiques sur le nœud et le serveur NTP</div></div>
Configurez un serveur NTP avec un ID de clé inconnu	<code>cluster time-service ntp server create -server server_name -key-id key_id</code>

Pour cela...	Utilisez cette commande...
Configurez un serveur dont l'ID de clé n'est pas configuré sur le serveur NTP.	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <div>  <p>L'ID, le type et la valeur de clé doivent être identiques à l'ID, au type et à la valeur de clé configurés sur le serveur NTP.</p> </div>
Désactiver l'authentification symétrique	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

Créez un serveur SMB dans un domaine Active Directory

Vous pouvez utiliser le `vserver cifs create` Commande pour créer un serveur SMB sur le SVM et spécifier le domaine Active Directory (AD) auquel il appartient.

Avant de commencer

Le SVM et les LIF que vous utilisez pour transmettre des données doivent avoir été configurés pour permettre le protocole SMB. Les LIFs doivent pouvoir se connecter aux serveurs DNS configurés sur le SVM et à un contrôleur de domaine AD du domaine auquel vous souhaitez rejoindre le serveur SMB.

Tout utilisateur autorisé à créer des comptes machine dans le domaine AD auquel vous rejoignez le serveur SMB peut créer le serveur SMB sur la SVM. Cela peut inclure des utilisateurs d'autres domaines.

À partir de ONTAP 9.7, votre administrateur AD peut vous fournir un URI vers un fichier keytab comme alternative à vous fournir un nom et un mot de passe à un compte Windows privilégié. Lorsque vous recevez l'URI, l'inclure dans le `-keytab-uri` paramètre avec le `vserver cifs` commandes.

Description de la tâche

Lors de la création d'un serveur SMB dans un domaine d'annuaire d'activités :

- Vous devez utiliser le nom de domaine complet (FQDN) lors de la spécification du domaine.
- Le paramètre par défaut consiste à ajouter le compte de machine du serveur SMB à l'objet CN=Computer Active Directory.
- Vous pouvez choisir d'ajouter le serveur SMB à une autre unité organisationnelle (ou) en utilisant le `-ou` option.
- Vous pouvez choisir d'ajouter une liste délimitée par des virgules d'un ou de plusieurs alias NetBIOS (jusqu'à 200) pour le serveur SMB.

La configuration des alias NetBIOS d'un serveur SMB peut être utile lorsque vous regroupez des données provenant d'autres serveurs de fichiers vers le serveur SMB et que vous souhaitez que le serveur SMB réponde aux noms des serveurs d'origine.

Le `vserver cifs` les pages man contiennent des paramètres facultatifs supplémentaires et des exigences de dénomination.



Depuis ONTAP 9.1, vous pouvez activer SMB version 2.0 pour vous connecter à un contrôleur de domaine (DC). Cela est nécessaire si vous avez désactivé SMB 1.0 sur les contrôleurs de domaine. Depuis ONTAP 9.2, SMB 2.0 est activé par défaut.

Depuis ONTAP 9.8, vous pouvez spécifier le cryptage des connexions aux contrôleurs de domaine. ONTAP nécessite un cryptage pour les communications du contrôleur de domaine lorsque `-encryption-required -for-dc-connection` l'option est définie sur `true`; la valeur par défaut est `false`. Lorsque l'option est définie, seul le protocole SMB3 est utilisé pour les connexions ONTAP-DC, car le chiffrement n'est pris en charge que par SMB3. .

"[Gestion SMB](#)" Contient plus d'informations sur les options de configuration du serveur SMB.

Étapes

1. Vérifiez que la licence SMB est installée sur votre cluster : `system license show -package cifs`

La licence SMB est incluse avec "[ONTAP One](#)". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.

Une licence CIFS n'est pas requise si le serveur SMB sera utilisé uniquement pour l'authentification.

2. Créez le serveur SMB dans un domaine AD : `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit] [-netbios-aliases NetBIOS_name, ...] [-keytab-uri {(ftp|http)://hostname|IP_address}] [-comment text]`

Lorsque vous entrez dans un domaine, cette commande peut prendre plusieurs minutes.

La commande suivante crée le serveur SMB "mb_server01" dans le domaine "example.com":

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
smb_server01 -domain example.com
```

La commande suivante crée le serveur SMB "smb_server02" dans le domaine "mydomain.com" et authentifie l'administrateur ONTAP avec un fichier keytab:

```
cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
smb_server02 -domain mydomain.com -keytab-uri
http://admin.mydomain.com/ontap1.keytab
```

3. Vérifiez la configuration du serveur SMB à l'aide du `vserver cifs show` commande.

Dans cet exemple, le résultat de la commande montre qu'un serveur SMB nommé « `SMB_SERVER01` » a été créé sur la SVM `vs1.example.com` et a été rejoint au domaine « `example.com` » domain.

```
cluster1::> vserver cifs show -vserver vs1
```

```
Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: -
```

4. Si vous le souhaitez, activez la communication chiffrée avec le contrôleur de domaine (ONTAP 9.8 et versions ultérieures): `vserver cifs security modify -vserver svm_name -encryption -required-for-dc-connection true`

Exemples

La commande suivante crée un serveur SMB nommé « 'smb_server02' » sur le SVM `vs2.example.com` dans le domaine « `example.com` » domain. Le compte machine est créé dans le conteneur « `ou=eng,ou=corp,DC=exemple,DC=com` ». Un alias NetBIOS est attribué au serveur SMB.

```
cluster1::> vserver cifs create -vserver vs2.example.com -cifs-server
smb_server02 -domain example.com -ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01
```

```
cluster1::> vserver cifs show -vserver vs1

Vserver: vs2.example.com
CIFS Server NetBIOS Name: SMB_SERVER02
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

La commande suivante permet à un utilisateur d'un domaine différent, dans ce cas un administrateur d'un domaine de confiance, de créer un serveur SMB nommé « 'MB_server03' » sur le SVM `vs3.example.com`. Le `-domain` Option spécifie le nom du domaine de départ (spécifié dans la configuration DNS) dans lequel vous souhaitez créer le serveur SMB. Le `username` spécifie l'administrateur du domaine de confiance.

- Home domain : `example.com`
- Domaine de confiance : `trust.lab.com`
- Nom d'utilisateur du domaine de confiance : `Administrator1`

```
cluster1::> vsyncer cifs create -vsyncer vs3.example.com -cifs-server  
smb_server03 -domain example.com
```

```
Username: Administrator1@trust.lab.com
```

```
Password: . . .
```

Créez des fichiers keytab pour l'authentification SMB

Depuis ONTAP 9.7, ONTAP prend en charge l'authentification des SVM avec des serveurs Active Directory (AD) utilisant des fichiers keytab. Les administrateurs AD génèrent un fichier keytab et le rendent disponible aux administrateurs ONTAP sous la forme d'un URI (Uniform Resource identifier), qui est fourni lorsque `vsyncer cifs` Les commandes exigent une authentification Kerberos avec le domaine AD.

Les administrateurs D'AD peuvent créer les fichiers keytab à l'aide du serveur Windows standard `ktpass` commande. La commande doit être exécutée sur le domaine principal où une authentification est requise. Le `ktpass` la commande peut être utilisée pour générer des fichiers keytab uniquement pour les utilisateurs du domaine principal ; les clés générées à l'aide d'utilisateurs du domaine approuvé ne sont pas prises en charge.

Les fichiers keytab sont générés pour des utilisateurs ONTAP admin spécifiques. Tant que le mot de passe de l'utilisateur administrateur ne change pas, les clés générées pour le type de cryptage et le domaine spécifiques ne changent pas. Par conséquent, un nouveau fichier keytab est requis chaque fois que le mot de passe de l'utilisateur admin est modifié.

Les types de cryptage suivants sont pris en charge :

- AES256-SHA1
- DES-CBC-MD5



ONTAP ne prend pas en charge le type de cryptage DES-CBC-CRC.

- RC4-HMAC

AES256 est le type de cryptage le plus élevé et doit être utilisé si activé sur le système ONTAP.

Les fichiers keytab peuvent être générés en spécifiant le mot de passe admin ou en utilisant un mot de passe généré de manière aléatoire. Toutefois, une seule option de mot de passe peut être utilisée à un moment donné, car une clé privée spécifique à l'utilisateur admin est nécessaire au serveur AD pour déchiffrer les clés à l'intérieur du fichier keytab. Toute modification de la clé privée d'un administrateur spécifique invalidera le fichier keytab.

Configurer un serveur SMB dans un groupe de travail

Configuration d'un serveur SMB dans une présentation d'un groupe de travail

La configuration d'un serveur SMB en tant que membre d'un groupe de travail consiste à créer le serveur SMB, puis à créer des utilisateurs et des groupes locaux.

Vous pouvez configurer un serveur SMB dans un groupe de travail lorsque l'infrastructure de domaine Microsoft Active Directory n'est pas disponible.

Un serveur SMB en mode groupe de travail prend uniquement en charge l'authentification NTLM et ne prend pas en charge l'authentification Kerberos.

Créez un serveur SMB dans un groupe de travail

Vous pouvez utiliser le `vserver cifs create` Commande permettant de créer un serveur SMB sur le SVM et de spécifier le groupe de travail auquel il appartient.

Avant de commencer

Le SVM et les LIF que vous utilisez pour transmettre des données doivent avoir été configurés pour permettre le protocole SMB. Les LIFs doivent pouvoir se connecter aux serveurs DNS configurés sur le SVM.

Description de la tâche

Les serveurs SMB en mode groupe de travail ne prennent pas en charge les fonctions SMB suivantes :

- Protocole SMB3 témoin
- Partages CA SMB3
- SQL sur SMB
- Redirection de dossiers
- Profils d'itinérance
- Objet de stratégie de groupe (GPO)
- Service Snapshot de volume (VSS)

Le `vserver cifs` les pages man contiennent des paramètres de configuration facultatifs supplémentaires et des exigences de dénomination.

Étapes

1. Vérifiez que la licence SMB est installée sur votre cluster : `system license show -package cifs`

La licence SMB est incluse avec ["ONTAP One"](#). Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.

Une licence CIFS n'est pas requise si le serveur SMB sera utilisé uniquement pour l'authentification.

2. Créez le serveur SMB dans un groupe de travail : `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

La commande suivante crée le serveur SMB `"`mb_server01"` dans le groupe de travail `"workgroup01"`:

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
SMB_SERVER01 -workgroup workgroup01
```

3. Vérifiez la configuration du serveur SMB à l'aide du `vserver cifs show` commande.

Dans l'exemple suivant, la sortie de la commande montre qu'un serveur SMB nommé « ``MB_server01'` » a été créé sur SVM `vs1.example.com` dans le groupe de travail « `workgroup01` » :

```
cluster1::> vserver cifs show -vserver vs0

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: workgroup01
Fully Qualified Domain Name: -
Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
Workgroup Name: workgroup01
Authentication Style: workgroup
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -
```

Une fois que vous avez terminé

Pour un serveur CIFS au sein d'un groupe de travail, vous devez créer des utilisateurs locaux, et éventuellement des groupes locaux, sur la SVM.

Informations associées

["Gestion SMB"](#)

Créer des comptes utilisateur locaux

Vous pouvez créer un compte utilisateur local qui peut être utilisé pour autoriser l'accès aux données contenues dans la SVM sur une connexion SMB. Vous pouvez également utiliser les comptes utilisateur locaux pour l'authentification lors de la création d'une session SMB.

Description de la tâche

La fonctionnalité des utilisateurs locaux est activée par défaut lors de la création du SVM.

Lorsque vous créez un compte utilisateur local, vous devez spécifier un nom d'utilisateur et spécifier le SVM avec lequel associer le compte.

Le `vserver cifs users-and-groups local-user` les pages man contiennent des détails sur les paramètres facultatifs et les exigences de dénomination.

Étapes

1. Créez l'utilisateur local : `vserver cifs users-and-groups local-user create -vserver vserver_name -user-name user_name optional_parameters`

Les paramètres facultatifs suivants peuvent s'avérer utiles :

- `-full-name`

Nom complet de l'utilisateur.

- `-description`

Description de l'utilisateur local.

° `-is-account-disabled {true|false}`

Indique si le compte utilisateur est activé ou désactivé. Si ce paramètre n'est pas spécifié, la valeur par défaut est d'activer le compte utilisateur.

La commande demande le mot de passe de l'utilisateur local.

2. Entrez un mot de passe pour l'utilisateur local, puis confirmez le mot de passe.

3. Vérifiez que l'utilisateur a bien été créé : `vserver cifs users-and-groups local-user show -vserver vserver_name`

Exemple

L'exemple suivant crée un utilisateur local « SMB_SERVER01\sue, avec un nom complet « Sue Chang », associé à SVM vs1.example.com :

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                               Full Name  Description
-----  -
vs1      SMB_SERVER01\Administrator                   Built-in administrator
account
vs1      SMB_SERVER01\sue                             Sue Chang
```

Créer des groupes locaux

Vous pouvez créer des groupes locaux qui peuvent être utilisés pour autoriser l'accès aux données associées à la SVM sur une connexion SMB. Vous pouvez également attribuer des privilèges qui définissent les droits d'utilisateur ou les capacités dont dispose un membre du groupe.

Description de la tâche

La fonctionnalité de groupe local est activée par défaut lors de la création du SVM.

Lorsque vous créez un groupe local, vous devez spécifier un nom pour le groupe et vous devez spécifier la SVM avec laquelle associer le groupe. Vous pouvez spécifier un nom de groupe avec ou sans le nom de domaine local, et vous pouvez éventuellement spécifier une description pour le groupe local. Vous ne pouvez pas ajouter un groupe local à un autre groupe local.

Le `vserver cifs users-and-groups local-group` les pages man contiennent des détails sur les paramètres facultatifs et les exigences de dénomination.

Étapes

1. Créez le groupe local : `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

Le paramètre facultatif suivant peut être utile :

- `-description`

Description du groupe local.

2. Vérifiez que le groupe a bien été créé : `vserver cifs users-and-groups local-group show -vserver vserver_name`

Exemple

L'exemple suivant crée un groupe local « `SMB_SERVER01\engineering` » associé à la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering
```

```
cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
```

Vserver	Group Name	Description
vs1.example.com	BUILTIN\Administrators	Built-in Administrators
vs1.example.com	BUILTIN\Backup Operators	Backup Operators group
vs1.example.com	BUILTIN\Power Users	Restricted administrative
vs1.example.com	BUILTIN\Users	All users
vs1.example.com	SMB_SERVER01\engineering	
vs1.example.com	SMB_SERVER01\sales	

Une fois que vous avez terminé

Vous devez ajouter des membres au nouveau groupe.

Gérer l'appartenance à un groupe local

Vous pouvez gérer l'appartenance à un groupe local en ajoutant et en supprimant des utilisateurs locaux ou de domaine, ou en ajoutant et supprimant des groupes de domaines. Cette option est utile si vous souhaitez contrôler l'accès aux données en fonction des contrôles d'accès placés sur le groupe ou si vous souhaitez que les utilisateurs disposent de privilèges associés à ce groupe.

Description de la tâche

Si vous ne souhaitez plus qu'un utilisateur local, un utilisateur de domaine ou un groupe de domaines dispose de droits d'accès ou de privilèges en fonction de l'appartenance à un groupe, vous pouvez supprimer le membre du groupe.

Lorsque vous ajoutez des membres à un groupe local, vous devez garder à l'esprit les éléments suivants :

- Vous ne pouvez pas ajouter d'utilisateurs au groupe spécial *Everyone*.
- Vous ne pouvez pas ajouter un groupe local à un autre groupe local.
- Pour ajouter un utilisateur ou un groupe de domaine à un groupe local, ONTAP doit pouvoir résoudre le nom en SID.

Lorsque vous supprimez des membres d'un groupe local, vous devez garder à l'esprit les éléments suivants :

- Vous ne pouvez pas supprimer des membres du groupe spécial *Everyone*.
- Pour supprimer un membre d'un groupe local, ONTAP doit pouvoir résoudre son nom en SID.

Étapes

1. Ajouter un membre à un groupe ou en supprimer.

- Ajouter un membre : `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

Vous pouvez spécifier une liste délimitée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaine à ajouter au groupe local spécifié.

- Supprimer un membre : `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

Vous pouvez spécifier une liste délimitée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaine à supprimer du groupe local spécifié.

Exemples

L'exemple suivant ajoute un utilisateur local « `SMB_SERVER01\sue` » au groupe local « `SMB_SERVER01\engineering` » sur le SVM vs1.example.com :

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

L'exemple suivant supprime les utilisateurs locaux « SMB_SERVER01\sue » et « SMB_SERVER01\james » du groupe local « `SMB_SERVER01\engineering` » sur la SVM vs1.example.com :

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Vérifiez les versions SMB activées

Votre version de ONTAP 9 détermine quelles versions de SMB sont activées par défaut pour les connexions avec les clients et les contrôleurs de domaine. Vérifiez que le serveur SMB prend en charge les clients et les fonctionnalités requis dans votre environnement.

Description de la tâche

Pour les connexions avec les clients et les contrôleurs de domaine, vous devez activer SMB 2.0 et versions ultérieures autant que possible. Pour des raisons de sécurité, évitez d'utiliser SMB 1.0 et désactivez-le si vous avez vérifié qu'il n'est pas nécessaire dans votre environnement.

Dans ONTAP 9, SMB version 2.0 et ultérieure est activé par défaut pour les connexions client, mais la version de SMB 1.0 activée par défaut dépend de votre version de ONTAP.

- Depuis la version ONTAP 9.1 P8, SMB 1.0 peut être désactivé sur les SVM.

Le `-smb1-enabled` à la `vserver cifs options modify` La commande active ou désactive SMB 1.0.

- Depuis ONTAP 9.3, il est désactivé par défaut sur les nouveaux SVM.

Si votre serveur SMB se trouve dans un domaine Active Directory (AD), vous pouvez activer SMB 2.0 pour vous connecter à un contrôleur de domaine (DC), à partir de ONTAP 9.1. Cela est nécessaire si vous avez désactivé SMB 1.0 sur DCS. Depuis ONTAP 9.2, SMB 2.0 est activé par défaut pour les connexions CC.



Si `-smb1-enabled-for-dc-connections` est défini sur `false` pendant `-smb1-enabled` est défini sur `true`, ONTAP refuse les connexions SMB 1.0 en tant que client, mais continue à accepter les connexions SMB 1.0 entrantes en tant que serveur.

"Gestion SMB" Le contient des détails sur les versions et fonctionnalités SMB prises en charge.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Vérifiez les versions SMB activées :

```
vserver cifs options show
```

Vous pouvez faire défiler la liste pour afficher les versions SMB activées pour les connexions client et si vous configurez un serveur SMB dans un domaine AD, pour les connexions de domaine AD.

3. Activez ou désactivez le protocole SMB pour les connexions client si nécessaire :

- Pour activer une version SMB :

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>  
true
```

Valeurs possibles pour `smb_version`:

- `-smb1-enabled`
- `-smb2-enabled`

- -smb3-enabled
- -smb31-enabled

La commande suivante active SMB 3.1 sur SVM vs1.example.com :

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true
```

- Pour désactiver une version SMB :

```
vserver cifs options modify -vserver <vserver_name> -<smb_version> false
```

4. Si votre serveur SMB se trouve dans un domaine Active Directory, activez ou désactivez le protocole SMB pour les connexions DC selon les besoins :

- Pour activer une version SMB :

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled -for-dc-connections true
```

- Pour désactiver une version SMB :

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled -for-dc-connections false
```

5. Retour au niveau de privilège admin :

```
set -privilege admin
```

Mappez le serveur SMB sur le serveur DNS

Le serveur DNS de votre site doit avoir une entrée pointant sur le nom du serveur SMB, et tous les alias NetBIOS, à l'adresse IP de la LIF de données afin que les utilisateurs Windows puissent mapper un disque au nom du serveur SMB.

Avant de commencer

Vous devez avoir un accès administratif au serveur DNS de votre site. Si vous ne disposez pas d'un accès administratif, vous devez demander à l'administrateur DNS d'effectuer cette tâche.

Description de la tâche

Si vous utilisez des alias NetBIOS pour le nom du serveur SMB, il est recommandé de créer des points d'entrée de serveur DNS pour chaque alias.

Étapes

1. Connectez-vous au serveur DNS.
2. Créer des entrées de recherche de type a - Address record (enregistrement d'adresse A) et inverse (PTR - enregistrement du pointeur) pour mapper le nom du serveur SMB à l'adresse IP de la LIF de données.
3. Si vous utilisez des alias NetBIOS, créez une entrée de recherche alias nom canonique (enregistrement de ressource CNAME) pour mapper chaque alias à l'adresse IP de la LIF de données du serveur SMB.

Résultats

Une fois le mappage propagé sur le réseau, les utilisateurs Windows peuvent mapper un lecteur au nom du serveur SMB ou à ses alias NetBIOS.

Configurez l'accès client SMB au stockage partagé

Configurez l'accès client SMB au stockage partagé

Pour fournir un accès client SMB au stockage partagé d'un SVM, vous devez créer un volume ou qtree pour fournir un conteneur de stockage, puis créer ou modifier un partage pour ce conteneur. Vous pouvez ensuite configurer les autorisations de partage et de fichier, et tester l'accès depuis les systèmes clients.

Avant de commencer

- SMB doit être entièrement configuré sur le SVM.
- Toute mise à jour de la configuration des services de noms doit être terminée.
- Tout ajout ou modification d'un domaine Active Directory ou d'une configuration de groupe de travail doit être effectué.

Créer un volume ou un conteneur de stockage qtree

Créer un volume

Vous pouvez créer un volume et spécifier son point de jonction et d'autres propriétés en utilisant le `volume create` commande.

Description de la tâche

Un volume doit inclure une *Junction path* pour que ses données soient mises à disposition des clients. Vous pouvez spécifier le chemin de jonction lorsque vous créez un nouveau volume. Si vous créez un volume sans spécifier un chemin de jonction, vous devez *mount* le volume du namespace du SVM à l'aide de `volume mount` commande.

Avant de commencer

- SMB doit être configuré et opérationnel.
- La sécurité de type SVM doit être NTFS.
- À partir de ONTAP 9.13.1, vous pouvez créer des volumes dont l'analyse de la capacité et le suivi des activités sont activés. Pour activer le suivi de la capacité ou des activités, exécutez le `volume create` commande avec `-analytics-state` ou `-activity-tracking-state` réglez sur `on`.

Pour en savoir plus sur l'analyse de la capacité et le suivi des activités, reportez-vous à la section ["Activez l'analyse du système de fichiers"](#).

Étapes

1. Créer le volume avec un point de jonction : `volume create -vserver svm_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path junction_path]`

Les choix pour `-junction-path` sont les suivants :

- Directement sous la racine, par exemple, `/new_vol`

Vous pouvez créer un nouveau volume et préciser qu'il peut être monté directement sur le volume root du SVM.

- Sous un répertoire existant, par exemple, `/existing_dir/new_vol`

Vous pouvez créer un nouveau volume et spécifier qu'il doit être monté sur un volume existant (dans une hiérarchie existante), exprimé en tant que répertoire.

Si vous souhaitez créer un volume dans un nouveau répertoire (dans une nouvelle hiérarchie sous un nouveau volume), par exemple, `/new_dir/new_vol`, Ensuite, vous devez d'abord créer un nouveau volume parent qui est relié par une jonction au volume racine de la SVM. Vous devez ensuite créer le nouveau volume enfant dans la Junction path du nouveau volume parent (nouveau répertoire).

2. Vérifier que le volume a été créé avec le point de jonction souhaité : `volume show -vserver svm_name -volume volume_name -junction`

Exemples

La commande suivante crée un nouveau volume nommé `users1` sur le SVM `vs1.example.com` et l'agrégat `aggr1`. Le nouveau volume est disponible sur le site `/users`. Le volume a une taille de 750 Go et sa garantie de volume est de type `volume` (par défaut).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	users1	true	/users	RW_volume

La commande suivante crée un nouveau volume nommé « maison 4 » sur la SVM « `vs1.example.com` » et l'agrégat « `aggr1` ». Le répertoire `/eng/` Existe déjà dans l'espace de nommage de la SVM `vs1`, et le nouveau volume est mis à disposition à `/eng/home`, qui devient le répertoire de base de l' `/eng/` espace de noms. Le volume a une taille de 750 Go et sa garantie de volume est de type `volume` (par défaut).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

Créer un qtree

Vous pouvez créer un qtree pour contenir vos données et spécifier ses propriétés en utilisant le `volume qtree create` commande.

Avant de commencer

- La SVM et le volume qui contiendra le nouveau qtree doivent déjà exister.
- Le style de sécurité du SVM doit être NTFS et SMB doit être configuré et en cours d'exécution.

Étapes

1. Créer le qtree : `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

Vous pouvez spécifier le volume et qtree en tant qu'arguments distincts ou spécifier l'argument du chemin qtree au format `/vol/volume_name/_qtree_name`.

2. Vérifier que le qtree a été créé avec le chemin de jonction souhaité : `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

Exemple

L'exemple suivant crée un qtree nommé qt01 situé sur le SVM vs1.example.com qui dispose d'un chemin de jonction `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path  
/vol/data1/qt01 -security-style ntfs  
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path  
/vol/data1/qt01
```

```
          Vserver Name: vs1.example.com  
          Volume Name: data1  
          Qtree Name: qt01  
Actual (Non-Junction) Qtree Path: /vol/data1/qt01  
          Security Style: ntfs  
          Oplock Mode: enable  
          Unix Permissions: ---rwxr-xr-x  
          Qtree Id: 2  
          Qtree Status: normal  
          Export Policy: default  
Is Export Policy Inherited: true
```

Exigences et considérations relatives à la création d'un partage SMB

Avant de créer un partage SMB, vous devez comprendre les exigences en matière de chemins de partage et de propriétés de partage, en particulier pour les répertoires locaux.

La création d'un partage SMB implique la spécification d'une structure de chemin d'accès au répertoire (à l'aide de `-path` dans le `vserver cifs share create` commande) à laquelle les clients accèdent. Le chemin du répertoire correspond à la Junction path d'un volume ou qtree que vous avez créé dans le SVM namespace. Le chemin du répertoire et le chemin de jonction correspondant doivent exister avant de créer votre partage.

Les chemins de partage ont les exigences suivantes :

- Le chemin d'accès à un répertoire peut comporter jusqu'à 255 caractères.
- Si un espace est présent dans le chemin d'accès, toute la chaîne doit être placée entre guillemets (par exemple, `"/new volume/mount here"`).
- Si le chemin UNC (`\\servername\sharename\filepath`) Du partage contient plus de 256 caractères (à l'exception de la valeur initiale `"\"` dans le chemin UNC), alors l'onglet **Security** de la zone Propriétés de Windows n'est pas disponible.

Il s'agit d'un problème de client Windows plutôt que d'un problème ONTAP. Pour éviter ce problème, ne créez pas de partages avec des chemins UNC de plus de 256 caractères.

Les valeurs par défaut des propriétés de partage peuvent être modifiées :

- Les propriétés initiales par défaut de tous les partages sont `oplocks`, `browsable`, `changenotify`, et `show-previous-versions`.

- Lorsque vous créez un partage, il est facultatif de spécifier des propriétés de partage.

Toutefois, si vous spécifiez des propriétés de partage lorsque vous créez le partage, les valeurs par défaut ne sont pas utilisées. Si vous utilisez le `-share-properties` paramètre lorsque vous créez un partage, vous devez spécifier toutes les propriétés de partage que vous souhaitez appliquer au partage à l'aide d'une liste délimitée par des virgules.

- Pour désigner un partage de répertoire personnel, utilisez le `homedirectory` propriété.

Cette fonctionnalité vous permet de configurer un partage qui correspond à différents répertoires en fonction de l'utilisateur qui se connecte à celui-ci et d'un ensemble de variables. Au lieu de devoir créer des partages distincts pour chaque utilisateur, vous pouvez configurer un partage unique avec quelques paramètres de home Directory afin de définir la relation d'un utilisateur entre un point d'entrée (le partage) et son home Directory (un répertoire sur le SVM).



Vous ne pouvez pas ajouter ou supprimer cette propriété après avoir créé le partage.

Les partages de home Directory présentent les exigences suivantes :

- Avant de créer des home directories SMB, vous devez ajouter au moins un chemin de recherche de répertoire personnel à l'aide de l'`vserver cifs home-directory search-path add` commande.
- Partages de répertoire personnel spécifiés par la valeur de `homedirectory` sur le `-share-properties` le paramètre doit inclure le `%w` (Nom d'utilisateur Windows) variable dynamique dans le nom de partage.

Le nom du partage peut également contenir le `%d` (nom de domaine) variable dynamique (par exemple, `%d/%w`) ou une partie statique dans le nom du partage (par exemple, `home1_%w`).

- Si le partage est utilisé par les administrateurs ou les utilisateurs pour se connecter aux répertoires d'accueil d'autres utilisateurs (à l'aide des options de l'`vserver cifs home-directory modify` commande), le modèle de nom de partage dynamique doit être précédé d'un tilde (`~`).

"[Gestion SMB](#)" et `vserver cifs share` les pages man contiennent des informations supplémentaires.

Créez un partage SMB

Vous devez créer un partage SMB avant de pouvoir partager des données d'un serveur SMB avec des clients SMB. Lorsque vous créez un partage, vous pouvez définir des propriétés de partage, telles que la désignation du partage comme répertoire de base. Vous pouvez également personnaliser le partage en configurant des paramètres facultatifs.

Avant de commencer

Le chemin de répertoire du volume ou `qtree` doit exister dans le namespace du SVM avant de créer le partage.

Description de la tâche

Lorsque vous créez un partage, l'ACL de partage par défaut (autorisations de partage par défaut) est `Everyone / Full Control`. Après avoir testé l'accès au partage, vous devez supprimer la liste ACL de partage par défaut et la remplacer par une alternative plus sécurisée.

Étapes

1. Si nécessaire, créez la structure du chemin d'accès au répertoire pour le partage.

Le `vserver cifs share create` la commande vérifie le chemin d'accès spécifié dans `-path` option pendant la création du partage. Si le chemin spécifié n'existe pas, la commande échoue.

2. Créer un partage SMB associé au SVM spécifié : `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. Vérifiez que le partage a été créé : `vserver cifs share show -share-name share_name`

Exemples

La commande suivante crée un partage SMB nommé « SHARE1 » sur le SVM `vs1.example.com`. Son chemin de répertoire est `/users`, et il est créé avec les propriétés par défaut.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name SHARE1 -path /users
```

```
cluster1::> vserver cifs share show -share-name SHARE1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1.example.com	SHARE1	/users	oplocks	-	Everyone / Full Control
			browsable		
			changenotify		
			show-previous-versions		

Vérifiez l'accès des clients SMB

Vérifiez que SMB est correctement configuré en accédant au partage et en écrivant les données. Vous devez tester l'accès à l'aide du nom du serveur SMB et de tout alias NetBIOS.

Étapes

1. Connectez-vous à un client Windows.
2. Testez l'accès à l'aide du nom du serveur SMB :
 - a. Dans l'Explorateur Windows, mappez un lecteur sur le partage au format suivant : `\\SMB_Server_Name\Share_Name`

Si le mappage ne réussit pas, il est possible que le mappage DNS ne se soit pas encore propagé sur l'ensemble du réseau. Vous devez tester l'accès par la suite à l'aide du nom de serveur SMB.

Si le serveur SMB est nommé `vs1.example.com` et que le partage est nommé `SHARE1`, vous devez entrer ce qui suit : `\\vs0.example.com\SHARE1`

- b. Sur le lecteur nouvellement créé, créez un fichier test, puis supprimez le fichier.

Vous avez vérifié l'accès en écriture au partage à l'aide du nom du serveur SMB.

3. Répétez l'étape 2 pour tous les alias NetBIOS.

Créer des listes de contrôle d'accès pour le partage SMB

La configuration des autorisations de partage en créant des listes de contrôle d'accès (ACL) pour les partages SMB vous permet de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes.

Avant de commencer

Vous devez avoir déterminé quels utilisateurs ou groupes auront accès au partage.

Description de la tâche

Vous pouvez configurer des listes de contrôle d'accès au niveau du partage en utilisant des noms d'utilisateur ou de groupe Windows locaux ou de domaine.

Avant de créer une nouvelle liste de contrôle d'accès, vous devez supprimer la liste de contrôle d'accès de partage par défaut `Everyone / Full Control`, qui pose un risque pour la sécurité.

En mode Workgroup, le nom de domaine local est le nom du serveur SMB.

Étapes

1. Supprimez la liste ACL de partage par défaut :
`vserver cifs share access-control delete -vserver vserver_name -share share_name -user-or-group everyone`
2. Configurer la nouvelle liste de contrôle d'accès :

Si vous souhaitez configurer des listes de contrôle d'accès à l'aide d'un...	Entrez la commande...
Utilisateur Windows	<code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\\user_name -permission access_right</code>
Groupe Windows	<code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right</code>

3. Vérifiez que la liste de contrôle d'accès appliquée au partage est correcte à l'aide de la `vserver cifs share access-control show` commande.

Exemple

La commande suivante donne `Change Autorisations` au groupe Windows "sales Team" pour la part "sales" sur le groupe `"vs1.example.com"SVM`:

```
cluster1::> vsriver cifs share access-control create -vsriver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vsriver cifs share access-control show
```

Vsriver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs1.example.com	sales	DOMAIN\"Sales Team"	windows	Change

Les commandes suivantes fournissent Change L'autorisation au groupe Windows local nommé « Tiger Team » et Full_Control Autorisation à l'utilisateur Windows local nommé "rue Chang" pour le partage "vatavol5" sur le SVM "vs1":

```
cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vsriver cifs share access-control show -vsriver vs1
```

Vsriver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1	c\$	BUILTIN\Administrators	windows	Full_Control
vs1	datavol5	DOMAIN\"Tiger Team"	windows	Change
vs1	datavol5	DOMAIN\"Sue Chang"	windows	Full_Control

Configurez les autorisations de fichier NTFS dans un partage

Pour permettre l'accès aux fichiers aux utilisateurs ou aux groupes qui ont accès à un partage, vous devez configurer les autorisations de fichiers NTFS sur les fichiers et les répertoires de ce partage à partir d'un client Windows.

Avant de commencer

L'administrateur effectuant cette tâche doit disposer d'autorisations NTFS suffisantes pour modifier les autorisations sur les objets sélectionnés.

Description de la tâche

"[Gestion SMB](#)" De plus, votre documentation Windows contient des informations sur la définition des autorisations NTFS standard et avancées.

Étapes

1. Connectez-vous à un client Windows en tant qu'administrateur.
2. Dans le menu **Tools** de l'Explorateur Windows, sélectionnez **Map network drive**.
3. Complétez la boîte **Map Network Drive** :
 - a. Sélectionnez une lettre **lecteur**.
 - b. Dans la zone **dossier**, saisissez le nom du serveur SMB contenant le partage contenant les données auxquelles vous souhaitez appliquer les autorisations, ainsi que le nom du partage.

Si le nom de votre serveur SMB est SMB_SERVER01 et que votre partage est nommé "SHARE1", entrez \\SMB_SERVER01\SHARE1.



Vous pouvez indiquer l'adresse IP de l'interface de données du serveur SMB au lieu du nom du serveur SMB.

- c. Cliquez sur **Terminer**.

Le lecteur sélectionné est monté et prêt avec la fenêtre de l'Explorateur Windows affichant les fichiers et dossiers contenus dans le partage.

4. Sélectionnez le fichier ou le répertoire pour lequel vous souhaitez définir les autorisations de fichier NTFS.
5. Cliquez avec le bouton droit de la souris sur le fichier ou le répertoire, puis sélectionnez **Propriétés**.
6. Sélectionnez l'onglet **sécurité**.

L'onglet sécurité affiche la liste des utilisateurs et des groupes pour lesquels les autorisations NTFS sont définies. La zone autorisations pour <objet> affiche la liste des autorisations Autoriser et refuser en vigueur pour l'utilisateur ou le groupe sélectionné.

7. Cliquez sur **Modifier**.

La case autorisations pour <objet> s'ouvre.

8. Effectuez les opérations souhaitées :

Si vous voulez	Procédez comme suit...
Définissez les autorisations NTFS standard pour un nouvel utilisateur ou un nouveau groupe	<p>a. Cliquez sur Ajouter.</p> <p>La fenêtre Sélectionner un utilisateur, des ordinateurs, des comptes de service ou des groupes s'ouvre.</p> <p>b. Dans la zone Entrez les noms d'objet à sélectionner, saisissez le nom de l'utilisateur ou du groupe sur lequel vous souhaitez ajouter l'autorisation NTFS.</p> <p>c. Cliquez sur OK.</p>
Modifiez ou supprimez des autorisations NTFS standard d'un utilisateur ou d'un groupe	Dans la zone Groupe ou noms d'utilisateur , sélectionnez l'utilisateur ou le groupe que vous souhaitez modifier ou supprimer.

9. Effectuez les opérations souhaitées :

Les fonctions que vous recherchez...	Procédez comme suit
Définissez les autorisations NTFS standard pour un utilisateur ou un groupe existant ou nouveau	Dans la zone permissions pour <objet> , sélectionnez les cases Autoriser ou refuser pour le type d'accès que vous souhaitez autoriser ou non pour l'utilisateur ou le groupe sélectionné.
Supprimer un utilisateur ou un groupe	Cliquez sur Supprimer .



Si certaines ou toutes les zones d'autorisation standard ne sont pas sélectionnables, c'est parce que les autorisations sont héritées de l'objet parent. La case **autorisations spéciales** n'est pas sélectionnable. Si elle est sélectionnée, cela signifie qu'un ou plusieurs des droits avancés granulaires ont été définis pour l'utilisateur ou le groupe sélectionné.

10. Une fois que vous avez terminé d'ajouter, de supprimer ou de modifier des autorisations NTFS sur cet objet, cliquez sur **OK**.

Vérifiez les accès des utilisateurs

Vous devez tester que les utilisateurs que vous avez configurés peuvent accéder au partage SMB et aux fichiers qu'il contient.

Étapes

1. Sur un client Windows, connectez-vous en tant qu'un des utilisateurs qui ont désormais accès au partage.
2. Dans le menu **Tools** de l'Explorateur Windows, sélectionnez **Map network drive**.
3. Complétez la boîte **Map Network Drive** :
 - a. Sélectionnez une lettre **lecteur**.
 - b. Dans la zone **dossier**, saisissez le nom de partage que vous fournissez aux utilisateurs.

Si le nom de votre serveur SMB est SMB_SERVER01 et que votre partage est nommé "SHARE1", entrez \\SMB_SERVER01\share1.

c. Cliquez sur **Terminer**.

Le lecteur sélectionné est monté et prêt avec la fenêtre de l'Explorateur Windows affichant les fichiers et dossiers contenus dans le partage.

4. Créez un fichier de test, vérifiez qu'il existe, écrivez du texte et supprimez le fichier de test.

Gestion de SMB avec l'interface de ligne de commandes

Présentation des références SMB

Les fonctionnalités d'accès aux fichiers ONTAP sont disponibles pour le protocole SMB. Vous pouvez activer un serveur CIFS, créer des partages et activer les services Microsoft.



SMB (Server message Block) désigne les dialectes modernes du protocole CIFS (Common Internet File System). Vous verrez toujours *CIFS* dans l'interface de ligne de commande (CLI) ONTAP et dans les outils de gestion OnCommand.

Vous devez utiliser ces procédures dans les circonstances suivantes :

- Vous souhaitez connaître la plage de fonctionnalités du protocole SMB de ONTAP.
- Vous souhaitez effectuer des tâches de configuration et de maintenance moins courantes, et non pas une configuration SMB de base.
- Vous souhaitez utiliser l'interface de ligne de commande et non System Manager, ni un outil de création de scripts automatisé.

Prise en charge du serveur SMB

Présentation de la prise en charge du serveur SMB

Vous pouvez activer et configurer des serveurs SMB sur des SVM (Storage Virtual machines) pour que les clients SMB puissent accéder aux fichiers du cluster.

- Chaque SVM de données du cluster peut être lié à un domaine Active Directory exactement.
- Les SVM de données n'ont pas besoin d'être liés au même domaine.
- Plusieurs SVM peuvent être liés au même domaine.

Vous devez configurer les SVM et les LIF que vous utilisez pour transmettre des données avant de pouvoir créer un serveur SMB. Si votre réseau de données n'est pas stable, vous devrez peut-être aussi configurer les IPspaces, les domaines de diffusion et les sous-réseaux. Le *Network Management Guide* contient des détails.

Informations associées

["Gestion du réseau"](#)

[Modifier les serveurs SMB](#)

Fonctionnalités et versions SMB prises en charge

Server message Block (SMB) est un protocole de partage de fichiers distant utilisé par les clients et les serveurs Microsoft Windows. Dans ONTAP 9, toutes les versions SMB sont prises en charge, mais la prise en charge par défaut de SMB 1.0 dépend de votre version ONTAP. Vérifiez que le serveur ONTAP SMB prend en charge les clients et les fonctionnalités requis dans votre environnement.

Les dernières informations sur les clients SMB et les contrôleurs de domaine pris en charge par ONTAP sont disponibles dans l'outil *Interoperability Matrix Tool*.

SMB 2.0 et les versions ultérieures sont activées par défaut pour les serveurs SMB ONTAP 9 et peuvent être activées ou désactivées selon les besoins. Le tableau suivant présente le support SMB 1.0 et la configuration par défaut.

Fonctionnalité SMB 1.0 :	Dans ces versions ONTAP 9 :			
	9.0	9.1	9.2	9.3 et versions ultérieures
Est activé par défaut	Oui.	Oui.	Oui.	Non
Peut être activé ou désactivé	Non	Oui*9.1 P8 ou ultérieur requis.	Oui.	Oui.



Les paramètres par défaut des connexions SMB 1.0 et 2.0 aux contrôleurs de domaine dépendent également de la version de ONTAP. Pour plus d'informations, consultez le `vserver cifs security modify` page de manuel. Pour les environnements avec des serveurs CIFS existants exécutant SMB 1.0, vous devez migrer vers une version SMB ultérieure dès que possible pour préparer des améliorations en matière de sécurité et de conformité. Contactez votre représentant NetApp pour plus d'informations.

Le tableau suivant indique les fonctionnalités SMB prises en charge dans chaque version de SMB. Certaines fonctionnalités SMB sont activées par défaut et d'autres requièrent une configuration supplémentaire.

Cette fonctionnalité :	Nécessite une activation:	Est pris en charge dans ONTAP 9 pour ces versions SMB:				
		1.0	2.0	2.1	3.0	3.1.1
Fonctionnalité SMB 1.0 héritée		X	X	X	X	X

Cette fonctionnalité :	Nécessite une activation:	Est pris en charge dans ONTAP 9 pour ces versions SMB:				
Poignées durables			X	X	X	X
Opérations cumulées			X	X	X	X
Opérations asynchrones			X	X	X	X
Tailles de tampon de lecture et d'écriture améliorées			X	X	X	X
Évolutivité optimisée			X	X	X	X
Signature SMB	X	X	X	X	X	X
Autre format de fichier ADS (Data Stream)	X	X	X	X	X	X
MTU important (activé par défaut à partir de ONTAP 9.7)	X			X	X	X
Oplocks de location				X	X	X
Partages disponibles en permanence	X				X	X
Pointeurs permanents					X	X
Témoin					X	X

Cette fonctionnalité :	Nécessite une activation :	Est pris en charge dans ONTAP 9 pour ces versions SMB:					
CHIFFREMENT SMB : AES-128-CCM	X				X		X
Évolutivité horizontale (requis par les partages de CA)					X		X
Basculement transparent					X		X
Multicanal SMB (à partir de ONTAP 9.4)	X				X		X
Intégrité de la pré-authentification							X
Basculement client cluster v.2 (CCFv2)							X
Chiffrement SMB : AES-128-GCM (à partir de ONTAP 9.1)	X						X

Informations associées

[Utilisation de la signature SMB pour améliorer la sécurité du réseau](#)

[Définition du niveau de sécurité d'authentification minimum du serveur SMB](#)

[Configuration du chiffrement SMB requis sur les serveurs SMB pour les transferts de données sur SMB](#)

["Interopérabilité NetApp"](#)

Fonctionnalités Windows non prises en charge

Avant d'utiliser CIFS sur votre réseau, vous devez connaître certaines fonctionnalités Windows que ONTAP ne prend pas en charge.

ONTAP ne prend pas en charge les fonctionnalités Windows suivantes :

- Système de fichiers crypté (EFS)
- Consignation des événements NTFS (NT File System) dans le journal des modifications
- Service FRS (File Replication Service) Microsoft
- Service d'indexation Microsoft Windows
- Stockage distant via HSM (gestion hiérarchique du stockage)
- Gestion des quotas des clients Windows
- Sémantique du quota Windows
- Le fichier LMHOSTS
- Compression native NTFS

Configurer les services de noms NIS ou LDAP sur le SVM

L'accès SMB permet de mapper un utilisateur UNIX, même en cas d'accès aux données d'un volume NTFS de type sécurité. Si vous associez des utilisateurs Windows aux utilisateurs UNIX correspondants dont les informations sont stockées dans des magasins d'annuaire NIS ou LDAP, ou si vous utilisez LDAP pour le mappage de noms, vous devez configurer ces services de noms au cours de l'installation SMB.

Avant de commencer

Vous devez avoir personnalisé la configuration de votre base de données de services de noms afin qu'elle corresponde à votre infrastructure de service de noms.

Description de la tâche

Les SVM utilisent les bases de données de name services ns-switch pour déterminer l'ordre dans lequel rechercher les sources d'une base de données de name-service donnée. La source du commutateur ns peut être n'importe quelle combinaison de « fichiers », « nis » ou « ldap ». Pour la base de données des groupes, ONTAP tente d'obtenir les appartenances de groupe de toutes les sources configurées, puis utilise les informations d'appartenance de groupe consolidées pour les contrôles d'accès. Si l'une de ces sources n'est pas disponible au moment de l'obtention des informations du groupe UNIX, ONTAP ne peut pas obtenir les informations d'identification UNIX complètes et les vérifications d'accès ultérieures peuvent échouer. Par conséquent, vous devez toujours vérifier que toutes les sources du commutateur ns sont configurées pour la base de données du groupe dans les paramètres du commutateur ns.

Par défaut, le serveur SMB doit mapper tous les utilisateurs Windows à l'utilisateur UNIX par défaut stocké dans le serveur local `passwd` base de données. Si vous souhaitez utiliser la configuration par défaut, la configuration des services de nom d'utilisateur et de groupe NIS ou LDAP UNIX ou le mappage d'utilisateur LDAP est facultative pour l'accès SMB.

Étapes

1. Si les informations utilisateur, groupe et groupe de réseau UNIX sont gérées par les services de noms NIS, configurez les services de noms NIS :
 - a. Déterminez la commande actuelle des services de noms à l'aide du `vserver services name-service ns-switch show` commande.

Dans cet exemple, les trois bases de données (`group`, `passwd`, et `netgroup`) qui peut utiliser `nis` en tant que source de service de nom n'utilisent que `files` comme source.

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
-----	-----	-----	-----
vs1	hosts	true	dns, files
vs1	group	true	files
vs1	passwd	true	files
vs1	netgroup	true	files
vs1	namemap	true	files

Vous devez ajouter le `nis` source vers le `group` et `passwd` les bases de données, et éventuellement au `netgroup` base de données.

- b. Réglez l'ordre de la base de données du commutateur `ns-service` de noms en utilisant le `vserver services name-service ns-switch modify` commande.

Pour obtenir des performances optimales, vous ne devez pas ajouter de service de noms à une base de données de services de noms, sauf si vous prévoyez de configurer ce service de noms sur la SVM.

Si vous modifiez la configuration de plusieurs bases de données de service de noms, vous devez exécuter la commande séparément pour chaque base de données de service de noms que vous souhaitez modifier.

Dans cet exemple, `nis` et `files` sont configurés comme sources pour le `group` et `passwd` les bases de données, dans cet ordre. Les bases de données restantes du service de noms ne sont pas modifiées.

```
vserver services name-service ns-switch modify -vserver vs1 -database group  
-sources nis,files vserver services name-service ns-switch modify -vserver  
vs1 -database passwd -sources nis,files
```

- c. Vérifiez que l'ordre des services de noms est correct en utilisant le `vserver services name-service ns-switch show` commande.

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
vs1	hosts	true	dns, files
vs1	group	true	nis, files
vs1	passwd	true	nis, files
vs1	netgroup	true	files
vs1	namemap	true	files

d. Créer la configuration du service de nom NIS :

```
vserver services name-service nis-domain create -vserver vserver_name
-domain NIS_domain_name -servers NIS_server_IPaddress,... -active true+
```

```
vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60 -active true
```



À partir de ONTAP 9.2, le champ `-nis-servers` remplace le champ `-servers`. Ce nouveau champ peut prendre un nom d'hôte ou une adresse IP pour le serveur NIS.

e. Vérifiez que le service de nom NIS est correctement configuré et actif : `vserver services name-service nis-domain show vserver vserver_name`

```
vserver services name-service nis-domain show vserver vs1
```

Vserver	Domain	Active	Server
vs1	example.com	true	10.0.0.60

- Si les informations utilisateur, groupe et groupe de réseau UNIX ou le mappage de nom sont gérés par les services de noms LDAP, configurez les services de noms LDAP à l'aide des informations situées ["Gestion NFS"](#).

Fonctionnement de la configuration du commutateur de service name ONTAP

ONTAP stocke les informations de configuration du service de noms dans un tableau équivalent à `/etc/nsswitch.conf` Fichier sur les systèmes UNIX. Vous devez connaître les fonctions du tableau et savoir comment ONTAP l'utilise pour que vous puissiez le configurer de façon appropriée pour votre environnement.

La table commutateur de service de nom ONTAP détermine les sources de service de nom auxquelles ONTAP consulte afin de récupérer les informations relatives à un certain type d'informations de service de nom. ONTAP conserve une table de commutateur de service de noms distincte pour chaque SVM.

Types de base de données

La table stocke une liste de services de noms distincte pour chacun des types de bases de données suivants :

Type de base de données	Définit les sources de service de noms pour...	Les sources valides sont...
hôtes	Conversion des noms d'hôte en adresses IP	fichiers, dns
groupe	Recherche des informations sur les groupes d'utilisateurs	fichiers, nis, ldap
passwd	Recherche des informations utilisateur	fichiers, nis, ldap
groupe réseau	Recherche des informations de groupe réseau	fichiers, nis, ldap
carte de nom	Mappage des noms d'utilisateur	fichiers, ldap

Types de source

Les sources indiquent quelle source de service de nom utiliser pour récupérer les informations appropriées.

Spécifiez le type de source...	Pour rechercher des informations dans...	Géré par les familles de commande...
fichiers	Fichiers source locaux	<code>vserver services name-service unix-user vserver services name-service unix-group</code> <code>vserver services name-service netgroup</code> <code>vserver services name-service dns hosts</code>
nis	Serveurs NIS externes tels que spécifiés dans la configuration de domaine NIS du SVM	<code>vserver services name-service nis-domain</code>
ldap	Serveurs LDAP externes comme spécifié dans la configuration du client LDAP du SVM	<code>vserver services name-service ldap</code>
dns	Serveurs DNS externes comme spécifié dans la configuration DNS du SVM	<code>vserver services name-service dns</code>

Même si vous prévoyez d'utiliser NIS ou LDAP pour l'accès aux données et l'authentification d'administration des SVM, vous devez toujours inclure `files` Et configurer des utilisateurs locaux comme un repli en cas d'échec de l'authentification NIS ou LDAP.

Protocoles utilisés pour accéder à des sources externes

Pour accéder aux serveurs pour des sources externes, ONTAP utilise les protocoles suivants :

Source de service de nom externe	Protocole utilisé pour l'accès
NIS	UDP
DNS	UDP
LDAP	TCP

Exemple

L'exemple suivant affiche la configuration du commutateur de service de nom pour le SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
```

Vserver	Database	Source
-----	-----	-----
svm_1	hosts	files, dns
svm_1	group	files
svm_1	passwd	files
svm_1	netgroup	nis, files

Pour rechercher des informations sur les utilisateurs ou les groupes, ONTAP consulte uniquement les fichiers sources locales. Si la requête ne renvoie aucun résultat, la recherche échoue.

Pour rechercher des informations sur le groupe réseau, ONTAP consulte d'abord les serveurs NIS externes. Si la requête ne renvoie aucun résultat, le fichier `netgroup` local est coché ensuite.

Il n'y a pas d'entrées de nom de service pour le mappage de noms dans le tableau pour le SVM `svm_1`. Par conséquent, ONTAP consulte uniquement les fichiers source locaux par défaut.

Gérer les serveurs SMB

Modifier les serveurs SMB

Vous pouvez déplacer un serveur SMB d'un groupe de travail vers un domaine Active Directory, d'un groupe de travail vers un autre groupe de travail, ou d'un domaine Active Directory vers un groupe de travail à l'aide de l'`vserver cifs modify` commande.

Description de la tâche

Vous pouvez également modifier d'autres attributs du serveur SMB, tels que le nom du serveur SMB et l'état administratif. Voir la page `man` pour plus de détails.

Choix

- Déplacer le serveur SMB d'un groupe de travail vers un domaine Active Directory :

- a. Définissez l'état administratif du serveur SMB sur down.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Déplacer le serveur SMB du groupe de travail vers un domaine Active Directory : `vserver cifs modify -vserver vserver_name -domain domain_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
```

Pour créer un compte de machine Active Directory pour le serveur SMB, vous devez fournir le nom et le mot de passe d'un compte Windows disposant des privilèges suffisants pour ajouter des ordinateurs à l'`ou=example` ou conteneur dans le ``example`` domaine .com.

À partir de ONTAP 9.7, votre administrateur AD peut vous fournir un URI vers un fichier keytab comme alternative à vous fournir un nom et un mot de passe à un compte Windows privilégié. Lorsque vous recevez l'URI, l'inclure dans le `-keytab-uri` paramètre avec le `vserver cifs` commandes.

- Déplacer le serveur SMB d'un groupe de travail vers un autre groupe de travail :

- a. Définissez l'état administratif du serveur SMB sur down.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Modifiez le groupe de travail pour le serveur SMB : `vserver cifs modify -vserver vserver_name -workgroup new_workgroup_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Déplacer le serveur SMB d'un domaine Active Directory vers un groupe de travail :

- a. Définissez l'état administratif du serveur SMB sur down.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Déplacer le serveur SMB du domaine Active Directory vers un groupe de travail : `vserver cifs modify -vserver vserver_name -workgroup workgroup_name`

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```




Pour passer en mode groupe de travail, toutes les fonctions basées sur un domaine doivent être désactivées et leur configuration doit être supprimée automatiquement par le système, y compris les partages disponibles en continu, les clichés instantanés et AES. Cependant, les listes de contrôle d'accès de partage configurées par domaine telles que « EXAMPLE.COM\userName » ne fonctionneront pas correctement, mais ne peuvent pas être supprimées par ONTAP. Supprimez ces ACL de partage dès que possible à l'aide d'outils externes une fois la commande terminée. Si AES est activé, vous pouvez être invité à fournir le nom et le mot de passe d'un compte Windows disposant de privilèges suffisants pour le désactiver dans le domaine "example.com".

- Modifiez d'autres attributs en utilisant le paramètre approprié de l'`vserver cifs modify` commande.

Utilisez les options pour personnaliser les serveurs SMB

Options de serveur SMB disponibles

Il est utile de connaître les options disponibles lorsque vous envisagez de personnaliser le serveur SMB. Bien que certaines options soient destinées à une utilisation générale sur le serveur SMB, plusieurs sont utilisées pour activer et configurer des fonctionnalités SMB spécifiques. Les options de serveur SMB sont contrôlées avec le `vserver cifs options modify option`.

La liste suivante indique les options du serveur SMB disponibles au niveau de privilège admin :

- **Configuration de la valeur du délai d'expiration de session SMB**

La configuration de cette option vous permet de spécifier le nombre de secondes d'inactivité avant la déconnexion d'une session SMB. Une session inactive est une session dans laquelle un utilisateur ne dispose pas de fichiers ou de répertoires ouverts sur le client. La valeur par défaut est 900 secondes.

- **Configuration de l'utilisateur UNIX par défaut**

La configuration de cette option vous permet de spécifier l'utilisateur UNIX par défaut utilisé par le serveur SMB. ONTAP crée automatiquement un utilisateur par défaut nommé « pcuser » (avec un UID de 65534), crée un groupe nommé « pcuser » (avec un GID de 65534) et ajoute l'utilisateur par défaut au groupe « pcuser ». Lorsque vous créez un serveur SMB, ONTAP configure automatiquement « pcuser » en tant qu'utilisateur UNIX par défaut.

- **Configuration de l'utilisateur UNIX invité**

La configuration de cette option vous permet de spécifier le nom d'un utilisateur UNIX auquel les utilisateurs qui se connectent à partir de domaines non fiables sont mappés, ce qui permet à un utilisateur d'un domaine non fiable de se connecter au serveur SMB. Par défaut, cette option n'est pas configurée (il n'y a pas de valeur par défaut) ; par conséquent, la valeur par défaut ne permet pas aux utilisateurs de domaines non approuvés de se connecter au serveur SMB.

- **Activation ou désactivation de l'exécution d'une subvention en lecture pour les bits de mode**

L'activation ou la désactivation de cette option vous permet de spécifier si les clients SMB doivent autoriser l'exécution de fichiers exécutables avec les bits de mode UNIX auxquels ils ont accès en lecture, même lorsque le bit exécutable UNIX n'est pas défini. Cette option est désactivée par défaut.

- **Activation ou désactivation de la possibilité de supprimer des fichiers en lecture seule des clients NFS**

L'activation ou la désactivation de cette option détermine s'il faut autoriser les clients NFS à supprimer des fichiers ou des dossiers avec l'ensemble d'attributs en lecture seule. La sémantique de suppression NTFS n'autorise pas la suppression d'un fichier ou d'un dossier lorsque l'attribut en lecture seule est défini. La sémantique de suppression UNIX ignore le bit en lecture seule, en utilisant les autorisations du répertoire parent à la place pour déterminer si un fichier ou un dossier peut être supprimé. Le paramètre par défaut est `disabled`, Ce qui entraîne la suppression de la sémantique en NTFS.

- **Configuration des adresses du serveur du service de noms Internet Windows**

La configuration de cette option vous permet de spécifier une liste d'adresses de serveur WINS (Windows Internet Name Service) en tant que liste délimitée par des virgules. Vous devez indiquer des adresses IPv4. Les adresses IPv6 ne sont pas prises en charge. Il n'y a pas de valeur par défaut.

La liste suivante indique les options du serveur SMB disponibles au niveau de privilège avancé :

- **Octroi d'autorisations de groupe UNIX aux utilisateurs CIFS**

La configuration de cette option détermine si l'utilisateur CIFS entrant qui n'est pas le propriétaire du fichier peut obtenir l'autorisation de groupe. Si l'utilisateur CIFS n'est pas le propriétaire du fichier de style de sécurité UNIX et que ce paramètre est défini sur `true`, puis l'autorisation de groupe est accordée pour le fichier. Si l'utilisateur CIFS n'est pas le propriétaire du fichier de style de sécurité UNIX et que ce paramètre est défini sur `false`, Les règles UNIX normales sont alors applicables pour accorder l'autorisation de fichier. Ce paramètre s'applique aux fichiers de style de sécurité UNIX dont l'autorisation est définie sur `mode bits` Et ne s'applique pas aux fichiers utilisant le mode de sécurité NTFS ou NFSv4. Le paramètre par défaut est `false`.

- **Activation ou désactivation de SMB 1.0**

SMB 1.0 est désactivé par défaut sur un SVM pour lequel un serveur SMB est créé dans ONTAP 9.3.



À partir de ONTAP 9.3, SMB 1.0 est désactivé par défaut pour les nouveaux serveurs SMB créés dans ONTAP 9.3. Vous devez migrer vers une version SMB plus récente dès que possible pour préparer des améliorations en matière de sécurité et de conformité. Contactez votre représentant NetApp pour plus d'informations.

- **Activation ou désactivation de SMB 2.x**

SMB 2.0 est la version minimale de SMB qui prend en charge le basculement de LIF. Si vous désactivez SMB 2.x, ONTAP désactive également automatiquement SMB 3.X.

SMB 2.0 est pris en charge uniquement sur les SVM. L'option est activée par défaut sur les SVM

- **Activation ou désactivation de SMB 3.0**

SMB 3.0 est la version minimale de SMB qui prend en charge les partages disponibles en continu. Windows Server 2012 et Windows 8 sont les versions minimales de Windows qui prennent en charge SMB 3.0.

SMB 3.0 n'est pris en charge que sur les SVM. L'option est activée par défaut sur les SVM

- **Activation ou désactivation de SMB 3.1**

Windows 10 est la seule version de Windows qui prend en charge SMB 3.1.

SMB 3.1 n'est pris en charge que sur les SVM. L'option est activée par défaut sur les SVM

- **Activation ou désactivation de l'allègement de charge des copies ODX**

L'allègement de la charge des copies ODX est utilisé automatiquement par les clients Windows qui la prennent en charge. Cette option est activée par défaut.

- **Activation ou désactivation du mécanisme de copie directe pour le déchargement de copies ODX**

Le mécanisme de copie directe augmente les performances de l'opération de déchargement de copie lorsque les clients Windows essaient d'ouvrir le fichier source d'une copie dans un mode qui empêche la modification du fichier pendant la copie. Par défaut, le mécanisme de copie directe est activé.

- **Activation ou désactivation des renvois de nœuds automatiques**

Avec les référencements automatiques des nœuds, le serveur SMB fait automatiquement référence aux clients à une LIF de données locale au nœud qui héberge les données accédées via le partage demandé.

- **Activation ou désactivation des stratégies d'exportation pour SMB**

Cette option est désactivée par défaut.

- **Activation ou désactivation de l'utilisation de points de jonction en tant que points de réanalyse**

Si cette option est activée, le serveur SMB expose les points de jonction aux clients SMB comme points de réanalyse. Cette option n'est valide que pour les connexions SMB 2.x ou SMB 3.0. Cette option est activée par défaut.

Cette option n'est prise en charge que sur les SVM. L'option est activée par défaut sur les SVM

- **Configuration du nombre maximal d'opérations simultanées par connexion TCP**

La valeur par défaut est 255.

- **Activation ou désactivation de la fonctionnalité des groupes et des utilisateurs Windows locaux**

Cette option est activée par défaut.

- **Activation ou désactivation de l'authentification des utilisateurs Windows locaux**

Cette option est activée par défaut.

- **Activation ou désactivation de la fonctionnalité de copie en double VSS**

ONTAP utilise la fonctionnalité Shadow Copy pour effectuer des sauvegardes distantes des données stockées à l'aide de la solution Hyper-V sur SMB.

Cette option n'est prise en charge que sur les SVM et uniquement dans les configurations Hyper-V sur SMB. L'option est activée par défaut sur les SVM

- **Configuration de la profondeur du répertoire de copie en double**

La configuration de cette option vous permet de définir la profondeur maximale des répertoires sur lesquels créer des clichés instantanés lors de l'utilisation de la fonctionnalité copie en double.

Cette option n'est prise en charge que sur les SVM et uniquement dans les configurations Hyper-V sur SMB. L'option est activée par défaut sur les SVM

- **Activation ou désactivation des fonctionnalités de recherche multidomaine pour le mappage de noms**

Si cette option est activée, lorsqu'un utilisateur UNIX est mappé à un utilisateur de domaine Windows à l'aide d'un caractère générique (*) dans la partie domaine du nom d'utilisateur Windows (par exemple *\joe), ONTAP recherche l'utilisateur spécifié dans tous les domaines avec des approbations bidirectionnelles vers le domaine d'origine. Le domaine personnel est le domaine qui contient le compte informatique du serveur SMB.

Vous pouvez également configurer une liste de domaines de confiance préférés en alternative à la recherche de tous les domaines de confiance bidirectionnels. Si cette option est activée et qu'une liste préférée est configurée, la liste préférée est utilisée pour effectuer des recherches de mappage de noms de domaines multiples.

La valeur par défaut est d'activer les recherches de mappage de noms multidomaine.

- **Configuration de la taille du secteur du système de fichiers**

La configuration de cette option vous permet de configurer la taille du secteur du système de fichiers en octets que ONTAP communique aux clients SMB. Cette option comporte deux valeurs valides : 4096 et 512. La valeur par défaut est 4096. Vous devrez peut-être définir cette valeur sur 512 Si l'application Windows ne prend en charge qu'une taille de secteur de 512 octets.

- **Activation ou désactivation du contrôle d'accès dynamique**

L'activation de cette option vous permet de sécuriser les objets sur le serveur SMB à l'aide du contrôle d'accès dynamique (DAC), y compris l'utilisation de l'audit pour définir des règles d'accès centrales et l'utilisation d'objets de stratégie de groupe pour mettre en œuvre des règles d'accès centrales. L'option est désactivée par défaut.

Cette option n'est prise en charge que sur les SVM.

- **Définition des restrictions d'accès pour les sessions non authentifiées (restriction anonyme)**

La définition de cette option détermine les restrictions d'accès pour les sessions non authentifiées. Les restrictions sont appliquées aux utilisateurs anonymes. Par défaut, il n'existe aucune restriction d'accès pour les utilisateurs anonymes.

- **Activation ou désactivation de la présentation des listes de contrôle d'accès NTFS sur des volumes avec sécurité effective UNIX (volumes de type sécurité UNIX ou volumes de type sécurité mixte avec sécurité effective UNIX)**

L'activation ou la désactivation de cette option détermine comment la sécurité des fichiers sur les fichiers et les dossiers avec la sécurité UNIX est présentée aux clients SMB. Lorsqu'elle est activée, ONTAP présente aux clients SMB les fichiers et les dossiers des volumes dotés de la sécurité UNIX comme ayant la sécurité des fichiers NTFS avec les ACL NTFS. S'il est désactivé, ONTAP présente les volumes dont la sécurité UNIX est de type FAT, sans aucun fichier sécurisé. Par défaut, les volumes sont présentés comme ayant la sécurité de fichiers NTFS avec les ACL NTFS.

- **Activation ou désactivation de la fonctionnalité fausse ouverture SMB**

L'activation de cette fonctionnalité améliore les performances de SMB 2.x et de SMB 3.0 en optimisant la

manière dont ONTAP effectue des requêtes ouvertes et fermées lors des requêtes relatives aux attributs des fichiers et des répertoires. Par défaut, la fonctionnalité de faux ouverture SMB est activée. Cette option est utile uniquement pour les connexions effectuées avec SMB 2.x ou version ultérieure.

- **Activation ou désactivation des extensions UNIX**

L'activation de cette option active les extensions UNIX sur un serveur SMB. Les extensions UNIX permettent d'afficher la sécurité du style POSIX/UNIX via le protocole SMB. Par défaut, cette option est désactivée.

Si vous avez des clients SMB basés sur UNIX, tels que des clients Mac OSX, dans votre environnement, vous devez activer les extensions UNIX. L'activation des extensions UNIX permet au serveur SMB de transmettre des informations de sécurité POSIX/UNIX sur SMB au client UNIX, qui convertit ensuite les informations de sécurité en sécurité POSIX/UNIX.

- **Activation ou désactivation du support pour les recherches de noms courts**

L'activation de cette option permet au serveur SMB d'effectuer des recherches sur des noms courts. Une requête de recherche avec cette option activée tente de faire correspondre 8.3 noms de fichier avec des noms de fichier longs. La valeur par défaut de ce paramètre est `false`.

- **Activation ou désactivation de la prise en charge de la publicité automatique des capacités DFS**

L'activation ou la désactivation de cette option détermine si les serveurs SMB annoncent automatiquement les fonctionnalités DFS aux clients SMB 2.x et SMB 3.0 qui se connectent aux partages. ONTAP utilise des référencements DFS dans la mise en œuvre de liens symboliques pour l'accès SMB. Si cette option est activée, le serveur SMB annonce toujours les fonctionnalités DFS, que l'accès à la liaison symbolique soit activé ou non. S'il est désactivé, le serveur SMB annonce les fonctionnalités DFS uniquement lorsque les clients se connectent aux partages où l'accès à la liaison symbolique est activé.

- **Configuration du nombre maximum de crédits SMB**

Depuis ONTAP 9.4, configurer le `-max-credits` Vous permet de limiter le nombre de crédits à accorder sur une connexion SMB lorsque les clients et le serveur exécutent SMB version 2 ou ultérieure. La valeur par défaut est 128.

- **Activation ou désactivation de la prise en charge de SMB Multichannel**

Activation du `-is-multichannel-enabled` Option dans les versions ONTAP 9.4 et ultérieures permet au serveur SMB d'établir plusieurs connexions pour une seule session SMB lorsque les cartes réseau appropriées sont déployées sur le cluster et ses clients. Cela améliore le débit et la tolérance aux pannes. La valeur par défaut de ce paramètre est `false`.

Lorsque SMB Multichannel est activé, vous pouvez également spécifier les paramètres suivants :

- Nombre maximum de connexions autorisées par session multicanal. La valeur par défaut de ce paramètre est 32.
- Nombre maximum d'interfaces réseau annoncées par session multicanal. La valeur par défaut de ce paramètre est 256.

Configuration des options du serveur SMB

Vous pouvez configurer les options du serveur SMB à tout moment après avoir créé un serveur SMB sur une machine virtuelle de stockage (SVM).

Étape

1. Effectuez l'action souhaitée :

Si vous souhaitez configurer les options du serveur SMB...	Entrez la commande...
Au niveau de privilège admin	<code>vserver cifs options modify -vserver vserver_name options</code>
Au niveau de privilège avancé	<ul style="list-style-type: none">a. <code>set -privilege advanced</code>b. <code>vserver cifs options modify -vserver vserver_name options</code>c. <code>set -privilege admin</code>

Pour plus d'informations sur la configuration des options du serveur SMB, reportez-vous à la page de manuel du `vserver cifs options modify` commande.

Configurez l'autorisation d'accorder le groupe UNIX aux utilisateurs SMB

Vous pouvez configurer cette option pour accorder des autorisations de groupe à des fichiers ou des répertoires, même si l'utilisateur SMB entrant n'est pas le propriétaire du fichier.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Configurez l'autorisation Grant UNIX Group comme il convient :

Si vous le souhaitez	Saisissez la commande
Activez l'accès aux fichiers ou répertoires pour obtenir les autorisations de groupe même si l'utilisateur n'est pas le propriétaire du fichier	<code>vserver cifs options modify -grant-unix-group-perms-to-others true</code>
Désactivez l'accès aux fichiers ou répertoires pour obtenir les autorisations de groupe même si l'utilisateur n'est pas le propriétaire du fichier	<code>vserver cifs options modify -grant-unix-group-perms-to-others false</code>

3. Vérifiez que l'option est réglée sur la valeur souhaitée : `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. Retour au niveau de privilège admin : `set -privilege admin`

Configurez les restrictions d'accès pour les utilisateurs anonymes

Par défaut, un utilisateur anonyme et non authentifié (également appelé *null user*) peut accéder à certaines informations sur le réseau. Vous pouvez utiliser une option de serveur SMB pour configurer les restrictions d'accès pour l'utilisateur anonyme.

Description de la tâche

Le `-restrict-anonymous` L'option de serveur SMB correspond au `RestrictAnonymous` Entrée de registre dans Windows.

Les utilisateurs anonymes peuvent lister ou énumérer certains types d'informations système provenant des hôtes Windows sur le réseau, y compris les noms d'utilisateur et les détails, les stratégies de compte et les noms de partage. Vous pouvez contrôler l'accès de l'utilisateur anonyme en spécifiant l'un des trois paramètres de restriction d'accès suivants :

Valeur	Description
<code>no-restriction</code> (valeur par défaut)	Spécifie aucune restriction d'accès pour les utilisateurs anonymes.
<code>no-enumeration</code>	Spécifie que seule l'énumération est restreinte pour les utilisateurs anonymes.
<code>no-access</code>	Spécifie que l'accès est restreint pour les utilisateurs anonymes.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Configurez le paramètre restreindre l'anonymat : `vserver cifs options modify -vserver vserver_name -restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Vérifiez que l'option est réglée sur la valeur souhaitée : `vserver cifs options show -vserver vserver_name`
4. Retour au niveau de privilège admin : `set -privilege admin`

Informations associées

[Options de serveur SMB disponibles](#)

Gérer la manière dont la sécurité des fichiers est présentée aux clients SMB pour les données de type sécurité UNIX

Gérer la manière dont la sécurité des fichiers est présentée aux clients SMB pour une présentation des données de type sécurité UNIX

Vous pouvez choisir comment présenter la sécurité des fichiers aux clients SMB pour les données de style de sécurité UNIX en activant ou désactivant la présentation d'ACL NTFS aux clients SMB. Chaque paramètre présente des avantages, que vous devez comprendre pour choisir le paramètre le mieux adapté aux besoins de votre entreprise.

Par défaut, ONTAP présente des autorisations UNIX sur des volumes de type sécurité UNIX aux clients SMB comme des listes de contrôle d'accès NTFS. Dans certains cas, cette option est souhaitable, notamment :

- Vous souhaitez afficher et modifier les autorisations UNIX à l'aide de l'onglet **sécurité** de la zone Propriétés de Windows.

Vous ne pouvez pas modifier les autorisations d'un client Windows si l'opération n'est pas autorisée par le système UNIX. Par exemple, vous ne pouvez pas modifier la propriété d'un fichier que vous ne possédez

pas, car le système UNIX ne permet pas cette opération. Cette restriction empêche les clients SMB de contourner les autorisations UNIX définies sur les fichiers et dossiers.

- Les utilisateurs modifient et enregistrent des fichiers sur le volume de style de sécurité UNIX en utilisant certaines applications Windows, par exemple Microsoft Office, où ONTAP doit préserver les autorisations UNIX pendant les opérations de sauvegarde.
- Votre environnement compte certaines applications Windows qui doivent lire les listes de contrôle d'accès NTFS sur les fichiers qu'elles utilisent.

Dans certaines circonstances, vous pouvez désactiver la présentation des autorisations UNIX en tant que listes de contrôle d'accès NTFS. Si cette fonctionnalité est désactivée, ONTAP présente les volumes de style de sécurité UNIX en tant que volumes FAT aux clients SMB. Il existe des raisons spécifiques de vouloir présenter des volumes de style sécurité UNIX en tant que volumes FAT aux clients SMB :

- Vous ne modifiez que les autorisations UNIX en utilisant des montages sur des clients UNIX.

L'onglet sécurité n'est pas disponible lorsqu'un volume de style de sécurité UNIX est mappé sur un client SMB. Le lecteur mappé semble être formaté avec le système de fichiers FAT, qui ne dispose pas d'autorisations de fichier.

- Vous utilisez des applications sur SMB qui définissent les listes de contrôle d'accès NTFS sur les fichiers et dossiers auxquels vous accédez, ce qui peut échouer si les données résident sur des volumes de style de sécurité UNIX.

Si ONTAP signale le volume comme FAT, l'application n'essaie pas de modifier une ACL.

Informations associées

[Configuration des styles de sécurité sur les volumes FlexVol](#)

[Configuration des styles de sécurité sur les qtrees](#)

Activez ou désactivez la présentation des listes de contrôle d'accès NTFS pour les données de type de sécurité UNIX

Vous pouvez activer ou désactiver la présentation des listes de contrôle d'accès NTFS aux clients SMB pour les données de style de sécurité UNIX (volumes de style sécurité UNIX et volumes de type sécurité mixte avec sécurité effective UNIX).

Description de la tâche

Si vous activez cette option, ONTAP présente les fichiers et les dossiers sur les volumes avec un style de sécurité UNIX efficace aux clients SMB comme ayant des listes de contrôle d'accès NTFS. Si vous désactivez cette option, les volumes sont présentés en tant que volumes FAT aux clients SMB. Par défaut, cette valeur doit présenter des listes de contrôle d'accès NTFS aux clients SMB.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Configurez le paramètre d'option ACL NTFS UNIX : `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. Vérifiez que l'option est réglée sur la valeur souhaitée : `vserver cifs options show -vserver vserver_name`
4. Retour au niveau de privilège admin : `set -privilege admin`

Comment ONTAP préserve les autorisations UNIX

Lorsque les fichiers d'un volume FlexVol qui disposent actuellement d'autorisations UNIX sont modifiés et enregistrés par des applications Windows, ONTAP peut préserver les autorisations UNIX.

Lorsque des applications sur des clients Windows modifient et enregistrent des fichiers, elles lisent les propriétés de sécurité du fichier, créent un nouveau fichier temporaire, appliquent ces propriétés au fichier temporaire, puis donnent au fichier temporaire le nom du fichier d'origine.

Lorsque les clients Windows effectuent une requête pour les propriétés de sécurité, ils reçoivent une ACL construite qui représente exactement les autorisations UNIX. Le seul but de cette liste de contrôle d'accès construite est de préserver les autorisations UNIX du fichier lorsque les fichiers sont mis à jour par les applications Windows pour s'assurer que les fichiers résultants ont les mêmes autorisations UNIX. ONTAP ne définit pas d'ACL NTFS à l'aide de la liste de contrôle d'accès construite.

Gérez les autorisations UNIX à l'aide de l'onglet sécurité Windows

Si vous souhaitez manipuler les autorisations UNIX de fichiers ou de dossiers dans des volumes ou des qtrees de style sécurité mixtes sur des SVM, vous pouvez utiliser l'onglet sécurité sur les clients Windows. Vous pouvez également utiliser des applications qui peuvent interroger et définir des listes de contrôle d'accès Windows.

- Modification des autorisations UNIX

Vous pouvez utiliser l'onglet sécurité Windows pour afficher et modifier les autorisations UNIX pour un volume ou qtree de style de sécurité mixte. Si vous utilisez l'onglet principal sécurité Windows pour modifier les autorisations UNIX, vous devez d'abord supprimer l'ACE que vous souhaitez modifier (ceci définit les bits de mode sur 0) avant d'effectuer vos modifications. Vous pouvez également utiliser l'éditeur avancé pour modifier les autorisations.

Si des autorisations de mode sont utilisées, vous pouvez modifier directement les autorisations de mode pour l'UID, le GID et d'autres (tous les autres utilisateurs disposant d'un compte sur l'ordinateur). Par exemple, si l'UID affiché possède des autorisations r-x, vous pouvez modifier les autorisations UID sur rwx.

- Modification des autorisations UNIX en autorisations NTFS

Vous pouvez utiliser l'onglet sécurité Windows pour remplacer les objets de sécurité UNIX par des objets de sécurité Windows sur un volume ou qtree de style de sécurité mixte, où les fichiers et les dossiers ont une méthode de sécurité efficace UNIX.

Vous devez d'abord supprimer toutes les entrées d'autorisation UNIX répertoriées pour pouvoir les remplacer par les objets utilisateur et groupe Windows souhaités. Vous pouvez ensuite configurer des listes de contrôle d'accès NTFS sur les objets utilisateur et groupe Windows. En supprimant tous les objets de sécurité UNIX et en ajoutant uniquement des utilisateurs et des groupes Windows à un fichier ou à un dossier dans un volume ou qtree de style de sécurité mixte, vous modifiez le style de sécurité effectif sur le fichier ou le dossier d'UNIX à NTFS.

Lors de la modification des autorisations sur un dossier, le comportement par défaut de Windows consiste à propager ces modifications à tous les sous-dossiers et fichiers. Par conséquent, vous devez modifier le choix de propagation sur le paramètre souhaité si vous ne souhaitez pas propager de modification du style de sécurité à tous les dossiers, sous-dossiers et fichiers enfants.

Gérer les paramètres de sécurité du serveur SMB

Gestion de l'authentification client SMB par ONTAP

Avant que les utilisateurs puissent créer des connexions SMB pour accéder aux données contenues dans la SVM, ils doivent être authentifiés par le domaine auquel le serveur SMB appartient. Le serveur SMB prend en charge deux méthodes d'authentification, Kerberos et NTLM (NTLMv1 ou NTLMv2). Kerberos est la méthode par défaut utilisée pour authentifier les utilisateurs du domaine.

Authentification Kerberos

ONTAP supporte l'authentification Kerberos lors de la création de sessions SMB authentifiées.

Kerberos est le service principal d'authentification pour Active Directory. Le serveur Kerberos, ou le Kerberos Key distribution Center (KDC) service, stocke et récupère des informations sur les principes de sécurité dans Active Directory. A la différence du modèle NTLM, les clients Active Directory qui souhaitent établir une session avec un autre ordinateur, tel que le serveur SMB, contactez directement un KDC pour obtenir leurs credentials de session.

Authentification NTLM

L'authentification du client NTLM est effectuée à l'aide d'un protocole de réponse de défi basé sur une connaissance partagée d'un secret spécifique à un utilisateur basé sur un mot de passe.

Si un utilisateur crée une connexion SMB à l'aide d'un compte utilisateur Windows local, l'authentification est effectuée localement par le serveur SMB à l'aide de NTLMv2.

Instructions relatives aux paramètres de sécurité des serveurs SMB dans une configuration de reprise d'activité des SVM

Avant de créer un SVM configuré en tant que destination de reprise d'activité pour laquelle l'identité n'est pas conservée (le `-identity-preserve` l'option est définie sur `false` En configuration SnapMirror), il est important de savoir comment les paramètres de sécurité des serveurs SMB sont gérés sur la SVM de destination.

- Les paramètres de sécurité du serveur SMB non par défaut ne sont pas répliqués sur la destination.

Lorsque vous créez un serveur SMB sur le SVM de destination, tous les paramètres de sécurité du serveur SMB sont définis sur les valeurs par défaut. Lors de l'initialisation, de la destination de reprise après incident du SVM, de la mise à jour ou de la resynchronisation, les paramètres de sécurité du serveur SMB sur la source ne sont pas répliqués sur la destination.

- Vous devez configurer manuellement les paramètres de sécurité du serveur SMB non par défaut.

Si vous avez configuré sur la SVM source des paramètres de sécurité du serveur SMB non par défaut, vous devez configurer manuellement ces mêmes paramètres sur le SVM de destination après que la destination devienne read-write (après une interruption de la relation SnapMirror).

Affiche des informations sur les paramètres de sécurité du serveur SMB

Vous pouvez afficher des informations sur les paramètres de sécurité du serveur SMB

sur vos serveurs virtuels de stockage (SVM). Vous pouvez utiliser ces informations pour vérifier que les paramètres de sécurité sont corrects.

Description de la tâche

Un paramètre de sécurité affiché peut être la valeur par défaut pour cet objet ou une valeur non par défaut configurée à l'aide de l'interface de ligne de commande ONTAP ou à l'aide d'objets de stratégie de groupe Active Directory.

N'utilisez pas le `vserver cifs security show` Commande pour les serveurs SMB en mode groupe de travail, car certaines options ne sont pas valides.

Étape

- 1. Effectuez l'une des opérations suivantes :

Si vous voulez afficher des informations sur...	Entrez la commande...
Tous les paramètres de sécurité sur un SVM spécifié	<code>vserver cifs security show -vserver vserver_name</code>
Un paramètre de sécurité ou des paramètres spécifiques sur la SVM	<code>vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]</code> Vous pouvez entrer <code>-fields ?</code> pour déterminer les champs que vous pouvez utiliser.

Exemple

L'exemple suivant montre tous les paramètres de sécurité pour SVM vs1 :

```
cluster1::> vservers cifs security show -vservers vs1

Vserver: vs1

Kerberos Clock Skew: 5 minutes
Kerberos Ticket Age: 10 hours
Kerberos Renewal Age: 7 days
Kerberos KDC Timeout: 3 seconds
Is Signing Required: false
Is Password Complexity Required: true
Use start_tls For AD LDAP connection: false
Is AES Encryption Enabled: false
LM Compatibility Level: lm-ntlm-ntlmv2-krb
Is SMB Encryption Required: false
Client Session Security: none
SMB1 Enabled for DC Connections: false
SMB2 Enabled for DC Connections: system-default
LDAP Referral Enabled For AD LDAP connections: false
Use LDAPS for AD LDAP connection: false
Encryption is required for DC Connections: false
AES session key enabled for NetLogon channel: false
Try Channel Binding For AD LDAP Connections: false
```

Notez que les paramètres affichés dépendent de la version ONTAP en cours d'exécution.

L'exemple suivant montre l'inclinaison de l'horloge Kerberos pour le SVM vs1 :

```
cluster1::> vservers cifs security show -vservers vs1 -fields kerberos-
clock-skew

vservers kerberos-clock-skew
-----
vs1      5
```

Informations associées

[Affichage des informations sur les configurations GPO](#)

Activez ou désactivez la complexité requise des mots de passe pour les utilisateurs SMB locaux

Au-dessus de vos SVM, la complexité requise par mot de passe renforce la sécurité des utilisateurs SMB locaux. La fonction de complexité de mot de passe requise est activée par défaut. Vous pouvez le désactiver et le réactiver à tout moment.

Avant de commencer

Les utilisateurs locaux, les groupes locaux et l'authentification des utilisateurs locaux doivent être activés sur le

serveur CIFS.



Description de la tâche

Vous ne devez pas utiliser le `vserver cifs security modify` Commande pour un serveur CIFS en mode groupe de travail car certaines options ne sont pas valides.

Étapes

- 1. Effectuez l'une des opérations suivantes :

Si vous voulez que les utilisateurs de PME locales aient besoin de complexité de mot de passe...	Entrez la commande...
Activé	<code>vserver cifs security modify -vserver vserver_name -is-password-complexity -required true</code>
Désactivé	<code>vserver cifs security modify -vserver vserver_name -is-password-complexity -required false</code>

- 2. Vérifiez le paramètre de sécurité pour connaître la complexité requise du mot de passe : `vserver cifs security show -vserver vserver_name`

Exemple

L'exemple suivant montre que la complexité requise des mots de passe est activée pour les utilisateurs SMB locaux pour le SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
-----
vs1      true
```

Informations associées

- [Affichage d'informations sur les paramètres de sécurité du serveur CIFS](#)
- [Utilisation d'utilisateurs et de groupes locaux pour l'authentification et l'autorisation](#)
- [Conditions requises pour les mots de passe des utilisateurs locaux](#)
- [Modification des mots de passe des comptes utilisateur locaux](#)

Modifiez les paramètres de sécurité Kerberos du serveur CIFS

Vous pouvez modifier certains paramètres de sécurité Kerberos pour le serveur CIFS, notamment le temps d’inclinaison maximal autorisé de l’horloge Kerberos, la durée de vie du ticket Kerberos et le nombre maximum de jours de renouvellement de ticket.

Description de la tâche

Modification des paramètres Kerberos du serveur CIFS à l’aide de `vserver cifs security modify` La commande modifie les paramètres uniquement sur la machine virtuelle de stockage (SVM) que vous spécifiez avec le `-vserver` paramètre. Vous pouvez gérer de manière centralisée les paramètres de sécurité Kerberos pour tous les SVM du cluster appartenant au même domaine Active Directory à l’aide des objets de stratégie de groupe Active Directory.

Étapes

- 1. Effectuez une ou plusieurs des opérations suivantes :

Les fonctions que vous recherchez...	Entrer...
Spécifiez le temps maximal autorisé d’inclinaison de l’horloge Kerberos en minutes (9.13.1 et versions ultérieures) ou en secondes (9.12.1 ou versions antérieures).	<pre>vserver cifs security modify -vserver vserver_name -kerberos-clock-skew integer_in_minutes</pre> <p>La valeur par défaut est 5 minutes.</p>
Spécifiez la durée de vie du ticket Kerberos en heures.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-ticket-age integer_in_hours</pre> <p>Le paramètre par défaut est 10 heures.</p>
Spécifiez le nombre maximum de jours de renouvellement de billet.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days</pre> <p>Le paramètre par défaut est 7 jours.</p>
Spécifiez le délai d’expiration des sockets sur les KDC après lequel tous les KDC sont marqués comme inaccessibles.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-kdc-timeout integer_in_seconds</pre> <p>Le réglage par défaut est de 3 secondes.</p>

- 2. Vérifiez les paramètres de sécurité Kerberos :

```
vserver cifs security show -vserver vserver_name
```

Exemple

L'exemple suivant apporte les modifications suivantes à la sécurité Kerberos : « Kerberos Clock Skew » est défini sur 3 minutes et « Kerberos Ticket Age » est défini sur 8 heures pour le SVM vs1 :

```
cluster1::> vservice cifs security modify -vservice vs1 -kerberos-clock-skew 3 -kerberos-ticket-age 8
```

```
cluster1::> vservice cifs security show -vservice vs1
```

Vservice: vs1

Kerberos Clock Skew:	3 minutes
Kerberos Ticket Age:	8 hours
Kerberos Renewal Age:	7 days
Kerberos KDC Timeout:	3 seconds
Is Signing Required:	false
Is Password Complexity Required:	true
Use start_tls For AD LDAP connection:	false
Is AES Encryption Enabled:	false
LM Compatibility Level:	lm-ntlm-ntlmv2-krb
Is SMB Encryption Required:	false

Informations associées

["Affichage d'informations sur les paramètres de sécurité du serveur CIFS"](#)

["Stratégies de groupe prises en charge"](#)

["Application d'objets de stratégie de groupe aux serveurs CIFS"](#)

Définissez le niveau de sécurité d'authentification minimum du serveur SMB

Vous pouvez définir le niveau de sécurité minimum du serveur SMB, également appelé *LMCompatibilityLevel*, sur votre serveur SMB afin de répondre aux besoins de sécurité de votre entreprise pour l'accès client SMB. Le niveau de sécurité minimum est le niveau minimum des jetons de sécurité que le serveur SMB accepte des clients SMB.



Description de la tâche

- Les serveurs SMB en mode groupe de travail prennent uniquement en charge l'authentification NTLM. L'authentification Kerberos n'est pas prise en charge.
- *LMCompatibilityLevel* s'applique uniquement à l'authentification du client SMB, et non à l'authentification de l'administrateur.

Vous pouvez définir le niveau de sécurité d'authentification minimum sur l'un des quatre niveaux de sécurité pris en charge.

Valeur	Description
lm-ntlm-ntlmv2-krb (valeur par défaut)	La machine virtuelle de stockage (SVM) accepte les authentifications LM, NTLM, NTLMv2 et Kerberos.

Valeur	Description
ntlm-ntlmv2-krb	Le SVM accepte la sécurité d'authentification NTLM, NTLMv2, et Kerberos. Le SVM refuse l'authentification LM.
ntlmv2-krb	Le SVM accepte la sécurité d'authentification NTLMv2 et Kerberos. Le SVM refuse l'authentification LM et NTLM.
krb	Le SVM n'accepte que la sécurité d'authentification Kerberos. Le SVM refuse l'authentification LM, NTLM et NTLMv2.

Étapes

1. Définissez le niveau de sécurité d'authentification minimum : `vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Vérifiez que le niveau de sécurité d'authentification est défini sur le niveau souhaité : `vserver cifs security show -vserver vserver_name`

Informations associées

[Activation ou désactivation du chiffrement AES pour les communications basées sur Kerberos](#)

Configurez une sécurité forte pour les communications Kerberos à l'aide du chiffrement AES

Pour une sécurité renforcée avec les communications basées sur Kerberos, vous pouvez activer le chiffrement AES-256 et AES-128 sur le serveur SMB. Par défaut, lorsque vous créez un serveur SMB sur le SVM, le chiffrement Advanced Encryption Standard (AES) est désactivé. Elle doit permettre aux services IT de bénéficier de la sécurité renforcée fournie par le cryptage AES.

La communication Kerberos pour SMB est utilisée lors de la création du serveur SMB sur le SVM, ainsi que lors de la phase d'installation de la session SMB. Le serveur SMB prend en charge les types de chiffrement suivants pour les communications Kerberos :

- AES 256
- AES 128
- DES
- RC4-HMAC

Si vous souhaitez utiliser le type de chiffrement le plus élevé pour les communications Kerberos, vous devez activer le chiffrement AES pour la communication Kerberos sur la SVM.

Lorsque le serveur SMB est créé, le contrôleur de domaine crée un compte de machine informatique dans Active Directory. À l'heure actuelle, le KDC prend connaissance des capacités de cryptage du compte machine particulier. Par la suite, un type de chiffrement particulier est sélectionné pour le chiffrement du ticket de service que le client présente au serveur lors de l'authentification.

À partir de ONTAP 9.12.1, vous pouvez spécifier les types de cryptage à publier sur le KDC Active Directory (AD). Vous pouvez utiliser le `-advertised-enc-types` pour activer les types de cryptage recommandés, vous pouvez l'utiliser pour désactiver les types de cryptage les plus faibles. Découvrez comment ["Activez et désactivez les types de cryptage pour les communications Kerberos"](#).



Intel AES New instructions (Intel AES ni) est disponible dans SMB 3.0. Il améliore l'algorithme AES et accélère le chiffrement des données avec les familles de processeurs prises en charge. À partir de SMB 3.1.1, AES-128-GCM remplace AES-128-CCM en tant qu'algorithme de hachage utilisé par le chiffrement SMB.

Informations associées

[Modification des paramètres de sécurité Kerberos du serveur CIFS](#)

Activez ou désactivez le chiffrement AES pour les communications basées sur Kerberos

Pour bénéficier de la sécurité la plus forte des communications basées sur Kerberos, vous devez utiliser le chiffrement AES-256 et AES-128 sur le serveur SMB. À partir de ONTAP 9.13.1, le chiffrement AES est activé par défaut. Si vous ne souhaitez pas que le serveur SMB sélectionne les types de cryptage AES pour les communications basées sur Kerberos avec le KDC Active Directory (AD), vous pouvez désactiver le cryptage AES.

Le fait que le cryptage AES soit activé par défaut et que vous puissiez spécifier des types de cryptage dépend de votre version de ONTAP.

Version ONTAP	Le cryptage AES est activé ...	Vous pouvez spécifier des types de cryptage ?
9.13.1 et versions ultérieures	Par défaut	Oui.
9.12.1	Manuellement	Oui.
9.11.1 et versions antérieures	Manuellement	Non

Depuis ONTAP 9.12.1, le chiffrement AES est activé et désactivé à l'aide du `-advertised-enc-types`. Cette option permet de spécifier les types de cryptage annoncés dans AD KDC. Le paramètre par défaut est `rc4` et `des`. Mais lorsqu'un type AES est spécifié, le cryptage AES est activé. Vous pouvez également utiliser l'option pour désactiver explicitement les types de cryptage RC4 et DES les plus faibles. Dans ONTAP 9.11.1 et les versions antérieures, vous devez utiliser le `-is-aes-encryption-enabled`. Option permettant d'activer et de désactiver le cryptage AES, et les types de cryptage ne peuvent pas être spécifiés.

Pour renforcer la sécurité, la machine virtuelle de stockage (SVM) modifie le mot de passe de son compte machine dans l'AD à chaque modification de l'option de sécurité AES. La modification du mot de passe peut nécessiter des informations d'identification AD administratives pour l'unité organisationnelle qui contient le compte de la machine.

Si un SVM est configuré en tant que destination de reprise sur incident où l'identité n'est pas conservée (le `-identity-preserve` l'option est définie sur `false` Dans la configuration SnapMirror), les paramètres de sécurité du serveur SMB non par défaut ne sont pas répliqués sur la destination. Si vous avez activé le chiffrement AES sur la SVM source, vous devez l'activer manuellement.

Exemple 5. Étapes

ONTAP 9.12.1 et versions ultérieures

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que les types de cryptage AES soient utilisés pour les communications Kerberos...	Entrez la commande...
Activé	<code>vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256</code>
Désactivé	<code>vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4</code>

Remarque : le `-is-aes-encryption-enabled` Cette option est obsolète dans ONTAP 9.12.1 et peut être supprimée dans une version ultérieure.

2. Vérifiez que le chiffrement AES est activé ou désactivé selon les besoins :
`vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Exemples

L'exemple suivant active les types de chiffrement AES pour le serveur SMB sur SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-----  -
vs1      aes-128,aes-256
```

L'exemple suivant active les types de cryptage AES pour le serveur SMB sur le SVM vs2.
L'administrateur est invité à saisir les informations d'identification AD d'administration pour l'UO contenant le serveur SMB.

```
cluster1::> vsriver cifs security modify -vsriver vs2 -advertised-enc
-types aes-128,aes-256
```

Info: In order to enable SMB AES encryption, the password for the SMB server machine account must be reset. Enter the username and password for the SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

```
cluster1::> vsriver cifs security show -vsriver vs2 -fields advertised-
enc-types
```

```
vsriver  advertised-enc-types
-----  -----
vs2      aes-128,aes-256
```

ONTAP 9.11.1 et versions antérieures

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que les types de cryptage AES soient utilisés pour les communications Kerberos...	Entrez la commande...
Activé	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled true</pre>
Désactivé	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled false</pre>

2. Vérifiez que le chiffrement AES est activé ou désactivé selon les besoins :

```
vsriver cifs
security show -vsriver vsriver_name -fields is-aes-encryption-enabled
```

Le `is-aes-encryption-enabled` s'affiche `true` Si le cryptage AES est activé et `false` s'il est désactivé.

Exemples

L'exemple suivant active les types de chiffrement AES pour le serveur SMB sur SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-----
vs1      true
```

L'exemple suivant active les types de cryptage AES pour le serveur SMB sur le SVM vs2.
L'administrateur est invité à saisir les informations d'identification AD d'administration pour l'UO contenant le serveur SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-----
vs2      true
```

Informations associées

["L'utilisateur du domaine ne parvient pas à se connecter au cluster avec Domain-tunnel"](#)

Utilisez la signature SMB pour améliorer la sécurité du réseau

Utilisez la signature SMB pour améliorer la présentation de la sécurité réseau

La signature SMB contribue à garantir que le trafic réseau entre le serveur SMB et le client n'est pas compromis. Elle empêche les attaques de relecture. Par défaut, ONTAP prend en charge la signature SMB sur demande du client. L'administrateur du stockage peut éventuellement configurer le serveur SMB afin de nécessiter une signature SMB.

Comment les stratégies de signature SMB affectent la communication avec un serveur CIFS

Outre les paramètres de sécurité de signature SMB du serveur CIFS, deux stratégies de signature SMB sur les clients Windows contrôlent la signature numérique des communications entre les clients et le serveur CIFS. Vous pouvez configurer le paramètre qui répond aux besoins de votre entreprise.

Les stratégies SMB du client sont contrôlées via les paramètres de stratégie de sécurité locale de Windows, qui sont configurés à l'aide des stratégies de groupe MMC (Microsoft Management Console) ou Active Directory. Pour plus d'informations sur les problèmes de sécurité et de signature SMB du client, consultez la documentation Microsoft Windows.

Voici les descriptions des deux stratégies de signature SMB sur les clients Microsoft :

- Microsoft network client: Digitally sign communications (if server agrees)

Ce paramètre détermine si la fonctionnalité de signature SMB du client est activée. Elle est activée par défaut. Lorsque ce paramètre est désactivé sur le client, les communications client avec le serveur CIFS dépendent du paramètre de signature SMB sur le serveur CIFS.

- Microsoft network client: Digitally sign communications (always)

Ce paramètre détermine si le client requiert la signature SMB pour communiquer avec un serveur. Elle est désactivée par défaut. Lorsque ce paramètre est désactivé sur le client, le comportement de signature SMB est basé sur le paramètre de stratégie pour Microsoft network client: Digitally sign communications (if server agrees) Et le paramètre sur le serveur CIFS.



Si votre environnement inclut des clients Windows configurés pour exiger une signature SMB, vous devez activer la signature SMB sur le serveur CIFS. Dans le cas contraire, le serveur CIFS ne peut pas transmettre de données à ces systèmes.

Les résultats effectifs des paramètres de signature SMB du client et du serveur CIFS dépendent du fait que les sessions SMB utilisent SMB 1.0 ou SMB 2.x et versions ultérieures.

Le tableau suivant récapitule le comportement de signature SMB efficace si la session utilise SMB 1.0 :

Client	Signature ONTAP : non requise	Signature ONTAP requise
Signature désactivée et non requise	Non signé	Signé
Signature activée et non requise	Non signé	Signé
Signature désactivée et requise	Signé	Signé
Signature activée et requise	Signé	Signé



Les anciens clients Windows SMB 1 et certains clients non Windows SMB 1 peuvent ne pas se connecter si la signature est désactivée sur le client mais requise sur le serveur CIFS.

Le tableau suivant récapitule le comportement de signature SMB efficace si la session utilise SMB 2.x ou SMB 3.0 :



Pour les clients SMB 2.x et SMB 3.0, la signature SMB est toujours activée. Elle ne peut pas être désactivée.

Client	Signature ONTAP : non requise	Signature ONTAP requise
Signature non requise	Non signé	Signé
Signature requise	Signé	Signé

Le tableau suivant récapitule le comportement de signature SMB du serveur et du client Microsoft par défaut :

Protocole	Algorithme de hachage	Peut activer/désactiver	Peut exiger/non requis	Client par défaut	Serveur par défaut	DC par défaut
SMB 1.0	MD5	Oui.	Oui.	Activé (non requis)	Désactivé (non requis)	Obligatoire
SMB 2.x	HMAC SHA-256	Non	Oui.	Non requis	Non requis	Obligatoire
SMB 3.0	AES-CMAC.	Non	Oui.	Non requis	Non requis	Obligatoire



Microsoft ne recommande plus d'utiliser Digitally sign communications (if client agrees) ou Digitally sign communications (if server agrees) Paramètres de stratégie de groupe. Microsoft ne recommande plus par ailleurs l'utilisation du EnableSecuritySignature paramètres du registre. Ces options n'affectent que le comportement du SMB 1 et peuvent être remplacées par le Digitally sign communications (always) Stratégie de groupe ou RequireSecuritySignature paramètre de registre. Vous pouvez également obtenir plus d'informations sur le blog Microsoft.principes de base de la signature SMB [The \(SMB1 et SMB2\)](#)

Impact de la signature SMB sur les performances

Lorsque les sessions SMB utilisent la signature SMB, toutes les communications SMB vers et depuis les clients Windows subissent un impact sur les performances, ce qui affecte à la fois les clients et le serveur (c'est-à-dire les nœuds sur le cluster exécutant le SVM contenant le serveur SMB).

L'impact sur les performances indique que l'utilisation accrue du CPU sur les clients et le serveur est augmentée, même si le volume du trafic réseau ne change pas.

La mesure de l'impact sur les performances dépend de la version de ONTAP 9 que vous utilisez. Depuis ONTAP 9.7, un nouvel algorithme de déchargement du cryptage peut permettre d'améliorer les performances du trafic SMB signé. L'allègement de la charge des signatures SMB est activé par défaut lorsque la signature SMB est activée.

L'amélioration des performances de signature SMB requiert une fonctionnalité de déchargement AES-ni. Consultez le Hardware Universe (HWU) pour vérifier que le déchargement AES-ni est pris en charge par votre plate-forme.

D'autres améliorations des performances sont également possibles si vous pouvez utiliser SMB version 3.11 qui prend en charge l'algorithme GCM beaucoup plus rapide.

Selon votre réseau, la version ONTAP 9, la version SMB et l'implémentation SVM, l'impact de la signature SMB sur les performances peut varier fortement. Vous pouvez la vérifier uniquement par le biais de tests dans l'environnement réseau.

La plupart des clients Windows négocient la signature SMB par défaut si elle est activée sur le serveur. Si vous avez besoin d'une protection SMB pour certains de vos clients Windows et si le SMB Signing génère des problèmes de performances, vous pouvez désactiver la signature SMB sur l'un de vos clients Windows ne nécessitant pas de protection contre les attaques de rejeu. Pour plus d'informations sur la désactivation de la signature SMB sur les clients Windows, consultez la documentation Microsoft Windows.

Recommandations pour la configuration de la signature SMB

Vous pouvez configurer le comportement de signature SMB entre les clients SMB et le serveur CIFS pour répondre à vos exigences de sécurité. Les paramètres que vous choisissez lors de la configuration de la signature SMB sur votre serveur CIFS dépendent de vos exigences de sécurité.

Vous pouvez configurer la signature SMB sur le client ou sur le serveur CIFS. Tenez compte des recommandations suivantes lors de la configuration de la signature SMB :

Si...	Recommandation...
Vous souhaitez augmenter la sécurité de la communication entre le client et le serveur	Assurez-vous que le SMB Signing est requis au niveau du client en activant le <code>Require Option (Sign always)</code> paramètre de sécurité sur le client.
Vous souhaitez que tous les trafics SMB vers une certaine machine virtuelle de stockage (SVM) signée	Configurez les paramètres de sécurité pour exiger la signature SMB sur le serveur CIFS.

Pour plus d'informations sur la configuration des paramètres de sécurité du client Windows, reportez-vous à la documentation Microsoft.

Consignes de signature SMB lorsque plusieurs LIF de données sont configurées

Si vous activez ou désactivez le SMB Signing requis sur le serveur SMB, vous devez connaître les instructions relatives aux configurations de plusieurs LIF de données pour un SVM.

Lorsque vous configurez un serveur SMB, plusieurs LIF de données peuvent être configurées. Si c'est le cas, le serveur DNS contient plusieurs A Entrées d'enregistrement pour le serveur CIFS, toutes utilisant le même nom d'hôte de serveur SMB, mais chacune avec une adresse IP unique. Par exemple, un serveur SMB dont deux LIF de données sont configurées peut avoir le DNS suivant A entrées d'enregistrement :

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

Le comportement normal est qu'après modification du paramètre de signature SMB requis, seules les nouvelles connexions des clients sont affectées par la modification du paramètre de signature SMB. Cependant, il y a une exception à ce comportement. Il existe un cas où un client dispose d'une connexion existante à un partage, et le client crée une nouvelle connexion au même partage après la modification du paramètre, tout en maintenant la connexion d'origine. Dans ce cas, la connexion SMB, nouvelle et existante, adopte les nouvelles exigences de signature SMB.

Prenons l'exemple suivant :

1. Client1 se connecte à un partage sans avoir à signer SMB à l'aide du chemin `o:\`.
2. L'administrateur du stockage modifie la configuration du serveur SMB afin de exiger la signature SMB.
3. Client1 se connecte au même partage avec la signature SMB requise à l'aide du chemin `s:\` (tout en maintenant la connexion à l'aide du chemin `o:\`).
4. Par conséquent, le SMB Signing est utilisé pour accéder aux données sur le système `o:\` et `s:\` disques.

Activer ou désactiver la signature SMB requise pour le trafic SMB entrant

Vous pouvez imposer aux clients l'exigence de signer les messages SMB en activant la signature SMB requise. S'il est activé, ONTAP n'accepte que les messages SMB s'ils ont une signature valide. Si vous souhaitez autoriser la signature SMB, mais pas l'exiger, vous pouvez désactiver la signature SMB requise.

Description de la tâche

Par défaut, le SMB Signing requis est désactivé. Vous pouvez activer ou désactiver la signature SMB requise à tout moment.

La signature SMB n'est pas désactivée par défaut dans les cas suivants :



1. Le signature SMB requis est activé et le cluster est rétabli sur une version d'ONTAP qui ne prend pas en charge la signature SMB.
2. Le cluster est ensuite mis à niveau vers une version de ONTAP qui prend en charge la signature SMB.

Dans ce cas, la configuration de signature SMB qui a été configurée à l'origine sur une version prise en charge de ONTAP est conservée par le biais d'une nouvelle version et d'une mise à niveau ultérieure.

Lorsque vous configurez une relation de reprise d'activité de machine virtuelle de stockage (SVM), la valeur que vous sélectionnez pour le système `-identity-preserve` de la `snapmirror create` La commande détermine les détails de configuration répliqués dans le SVM de destination.

Si vous définissez le `-identity-preserve` option à `true` (ID-preserve), le paramètre de sécurité de signature SMB est répliqué sur la destination.

Si vous définissez le `-identity-preserve` option à `false` (Non-ID-preserve), le paramètre de sécurité de

signature SMB n'est pas répliqué sur la destination. Dans ce cas, les paramètres de sécurité du serveur CIFS sur la destination sont définis sur les valeurs par défaut. Si vous avez activé la signature SMB requise sur le SVM source, vous devez activer manuellement le SMB Signing requis sur le SVM de destination.

Étapes

- 1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que le SMB soit connecté...	Entrez la commande...
Activé	<code>vserver cifs security modify -vserver vserver_name -is-signing-required true</code>
Désactivé	<code>vserver cifs security modify -vserver vserver_name -is-signing-required false</code>

- 2. Vérifiez que la signature SMB requise est activée ou désactivée en déterminant si la valeur dans l' Is Signing Required le champ de la sortie de la commande suivante est défini sur la valeur souhaitée :
`vserver cifs security show -vserver vserver_name -fields is-signing-required`

Exemple

L'exemple suivant active la signature SMB requise pour le SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-required
vserver  is-signing-required
-----  -
vs1      true
```



Les modifications apportées aux paramètres de cryptage prennent effet pour les nouvelles connexions. Les connexions existantes ne sont pas affectées.

Déterminez si les sessions SMB sont signées

Vous pouvez afficher des informations sur les sessions SMB connectées sur le serveur CIFS. Vous pouvez utiliser ces informations pour déterminer si les sessions SMB sont signées. Cela peut être utile pour déterminer si les sessions client SMB se connectent aux paramètres de sécurité souhaités.

Étapes

- 1. Effectuez l'une des opérations suivantes :

Si vous voulez afficher des informations sur...	Entrez la commande...
Toutes les sessions signées sur une machine virtuelle de stockage (SVM) spécifiée	<code>vserver cifs session show -vserver <i>vserver_name</i> -is-session-signed true</code>
Détails d'une session signée avec un ID de session spécifique sur le SVM	<code>vserver cifs session show -vserver <i>vserver_name</i> -session-id integer -instance</code>

Exemples

La commande suivante affiche les informations relatives aux sessions signées sur le SVM vs1. La sortie de résumé par défaut n'affiche pas le champ de sortie « session signée is » :

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:      node1
Vserver: vs1
Connection Session
ID          ID      Workstation      Windows User      Open      Idle
-----
3151272279  1      10.1.1.1      DOMAIN\joe      2      23s
```

La commande suivante affiche des informations détaillées sur la session, notamment si elle est signée, dans une session SMB avec l'ID de session 2 :

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

Informations associées

[Contrôle des statistiques de session signées SMB](#)

Surveiller les statistiques de session signées SMB

Vous pouvez surveiller les statistiques des sessions SMB et déterminer les sessions établies qui sont signées et qui ne le sont pas.

Description de la tâche

Le `statistics` la commande au niveau de privilège avancé fournit le `signed_sessions` Compteur que vous pouvez utiliser pour surveiller le nombre de sessions SMB signées. Le `signed_sessions` le compteur est disponible avec les objets de statistiques suivants :

- `cifs` Permet de surveiller la signature SMB pour toutes les sessions SMB.
- `smb1` Permet de surveiller la signature SMB pour les sessions SMB 1.0.
- `smb2` Permet de surveiller la signature SMB pour les sessions SMB 2.x et SMB 3.0.

Les statistiques SMB 3.0 sont incluses dans les résultats de `smb2` objet.

Si vous souhaitez comparer le nombre de sessions signées au nombre total de sessions, vous pouvez comparer les résultats de la session `signed_sessions` compteur avec la sortie pour le `established_sessions` compteur.

Vous devez démarrer une collecte d'échantillons de statistiques avant de pouvoir afficher les données

résultantes. Vous pouvez afficher les données de l'échantillon si vous n'arrêtez pas la collecte de données. L'arrêt de la collecte de données vous donne un échantillon fixe. L'option ne pas arrêter la collecte de données vous permet d'obtenir des données mises à jour que vous pouvez utiliser pour comparer à des requêtes précédentes. La comparaison vous aide à identifier les tendances.

Étapes

- 1. Définissez le niveau de privilège sur avancé :
`set -privilege advanced`
- 2. Démarrer une collecte de données :
`statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

Si vous ne spécifiez pas le `-sample-id` Paramètre, la commande génère un exemple d'identificateur pour vous et définit cet échantillon comme échantillon par défaut pour la session de l'interface de ligne de commande. La valeur pour `-sample-id` est une chaîne de texte. Si vous exécutez cette commande pendant la même session CLI et ne spécifiez pas le `-sample-id` paramètre, la commande remplace l'échantillon par défaut précédent.

Vous pouvez spécifier le nœud sur lequel vous souhaitez collecter les statistiques. Si vous ne spécifiez pas le nœud, l'exemple collecte les statistiques de tous les nœuds du cluster.

- 3. Utilisez le `statistics stop` commande pour arrêter la collecte des données de l'échantillon.
- 4. Afficher les statistiques de signature SMB :

Si vous souhaitez afficher les informations pour...	Entrer...
Sessions signées	<code>`show -sample-id sample_ID -counter signed_sessions</code>
<code>node_name [-node node_name]</code>	Sessions signées et sessions établies
<code>`show -sample-id sample_ID -counter signed_sessions</code>	<code>established_sessions</code>

Si vous souhaitez afficher les informations pour un seul nœud, spécifiez l'option `-node` paramètre.

- 5. Revenir au niveau de privilège admin :
`set -privilege admin`

Exemples

L'exemple suivant montre comment surveiller les statistiques de signature SMB 2.x et SMB 3.0 sur la machine virtuelle de stockage (SVM) vs1.

La commande suivante permet d'accéder au niveau de privilège avancé :

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by support personnel.
```

```
Do you want to continue? {y|n}: y
```

La commande suivante démarre la collecte de données pour un nouvel échantillon :

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample  
-vserver vs1
```

```
Statistics collection is being started for Sample-id: smbsigning_sample
```

La commande suivante arrête la collecte des données de l'échantillon :

```
cluster1::*> statistics stop -sample-id smbsigning_sample
```

```
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

La commande suivante affiche les sessions SMB signées et les sessions SMB établies par nœud à partir de l'exemple :

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter  
signed_sessions|established_sessions|node_name
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:03:04

Cluster: cluster1

Counter	Value
-----	-----
established_sessions	0
node_name	node1
signed_sessions	0
established_sessions	1
node_name	node2
signed_sessions	1
established_sessions	0
node_name	node3
signed_sessions	0
established_sessions	0
node_name	node4
signed_sessions	0

La commande suivante affiche les sessions SMB signées pour le nœud 2 à partir de l'exemple :

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter  
signed_sessions|node_name -node node2
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:22:43

Cluster: cluster1

Counter	Value
-----	-----
node_name	node2
signed_sessions	1

La commande suivante revient au niveau de privilège admin :

```
cluster1::*> set -privilege admin
```

Informations associées

Détermination de la signature des sessions SMB

"Contrôle des performances et présentation de la gestion"

Configurez le chiffrement SMB requis sur les serveurs SMB pour les transferts de données via SMB

Présentation du chiffrement SMB

Le chiffrement SMB pour les transferts de données via SMB est une amélioration de sécurité que vous pouvez activer ou désactiver sur les serveurs SMB. Vous pouvez également configurer le paramètre de chiffrement SMB souhaité sur une base partage par partage à l'aide d'un paramètre de propriété de partage.

Par défaut, lorsque vous créez un serveur SMB sur la machine virtuelle de stockage (SVM), le chiffrement SMB est désactivé. Vous devez leur permettre de bénéficier de la sécurité améliorée fournie par le chiffrement SMB.

Pour créer une session SMB chiffrée, le client SMB doit prendre en charge le chiffrement SMB. Les clients Windows commençant par Windows Server 2012 et Windows 8 prennent en charge le cryptage SMB.

Le chiffrement SMB sur la SVM est contrôlé par deux paramètres :

- Option de sécurité du serveur SMB qui active la fonctionnalité sur le SVM
- Propriété de partage SMB qui configure le paramètre de chiffrement SMB partage par partage

Vous pouvez décider s'il faut un chiffrement pour accéder à toutes les données de la SVM ou bien demander un chiffrement SMB pour accéder aux données uniquement dans les partages sélectionnés. Les paramètres des SVM prévalent sur les paramètres de niveau partage.

La configuration de cryptage SMB efficace dépend de la combinaison des deux paramètres. Elle est décrite dans le tableau suivant :

Chiffrement SMB du serveur SMB activé	Le paramètre partage des données de chiffrement est activé	Comportement de cryptage côté serveur
Vrai	Faux	Le chiffrement au niveau du serveur est activé pour tous les partages du SVM. Avec cette configuration, le chiffrement s'effectue pour toute la session SMB.
Vrai	Vrai	Le chiffrement au niveau du serveur est activé pour tous les partages de la SVM indépendamment du chiffrement au niveau du partage. Avec cette configuration, le chiffrement s'effectue pour toute la session SMB.

Chiffrement SMB du serveur SMB activé	Le paramètre partage des données de chiffrement est activé	Comportement de cryptage côté serveur
Faux	Vrai	Le chiffrement au niveau du partage est activé pour les partages spécifiques. Avec cette configuration, le chiffrement se produit à partir de l'arborescence à connecter.
Faux	Faux	Aucun chiffrement n'est activé.

Les clients SMB qui ne prennent pas en charge le chiffrement ne peuvent pas se connecter à un serveur SMB ou à un partage qui nécessite un chiffrement.

Les modifications apportées aux paramètres de cryptage prennent effet pour les nouvelles connexions. Les connexions existantes ne sont pas affectées.

Impact du chiffrement SMB sur les performances

Lorsque les sessions SMB utilisent le chiffrement SMB, toutes les communications SMB vers et depuis les clients Windows rencontrent un impact sur les performances, qui affecte à la fois les clients et le serveur (c'est-à-dire les nœuds sur le cluster exécutant le SVM qui contient le serveur SMB).

L'impact sur les performances indique que l'utilisation accrue du CPU sur les clients et le serveur est augmentée, même si le volume du trafic réseau ne change pas.

La mesure de l'impact sur les performances dépend de la version de ONTAP 9 que vous utilisez. Depuis ONTAP 9.7, un nouvel algorithme de désactivation du chiffrement permet d'améliorer les performances du trafic SMB chiffré. Le délestage du chiffrement SMB est activé par défaut lorsque le chiffrement SMB est activé.

L'optimisation des performances de chiffrement SMB requiert une fonctionnalité de déchargement AES-ni. Consultez le Hardware Universe (HWU) pour vérifier que le déchargement AES-ni est pris en charge par votre plate-forme.

D'autres améliorations des performances sont également possibles si vous pouvez utiliser SMB version 3.11 qui prend en charge l'algorithme GCM beaucoup plus rapide.

Selon votre réseau, la version ONTAP 9, la version SMB et l'implémentation SVM, l'impact du cryptage SMB sur les performances peut varier fortement. Vous pouvez le vérifier uniquement par le biais de tests dans l'environnement réseau.

Le chiffrement SMB est désactivé par défaut sur le serveur SMB. Vous devez activer le chiffrement SMB uniquement sur les partages SMB ou les serveurs SMB qui nécessitent un chiffrement. Avec le cryptage SMB, ONTAP effectue un traitement supplémentaire du décryptage des demandes et du cryptage des réponses à chaque demande. Le chiffrement SMB ne doit donc être activé que lorsque cela est nécessaire.

Activez ou désactivez le chiffrement SMB requis pour le trafic SMB entrant

Si vous souhaitez exiger le cryptage SMB pour le trafic SMB entrant, vous pouvez l'activer sur le serveur CIFS ou au niveau du partage. Par défaut, le chiffrement SMB n'est pas requis.

Description de la tâche

Vous pouvez activer le chiffrement SMB sur le serveur CIFS, qui s'applique à tous les partages du serveur CIFS. Si vous ne souhaitez pas utiliser le cryptage SMB requis pour tous les partages du serveur CIFS ou si vous souhaitez activer le cryptage SMB requis pour le trafic SMB entrant, partage par partage, vous pouvez désactiver le cryptage SMB requis sur le serveur CIFS.

Lorsque vous configurez une relation de reprise d'activité de machine virtuelle de stockage (SVM), la valeur que vous sélectionnez pour le système `-identity-preserve` de la `snapmirror create` La commande détermine les détails de configuration répliqués dans le SVM de destination.

Si vous définissez le `-identity-preserve` option à `true` (ID-preserve), le paramètre de sécurité du cryptage SMB est répliqué sur la destination.

Si vous définissez le `-identity-preserve` option à `false` (Non ID-preserve), le paramètre de sécurité du cryptage SMB n'est pas répliqué sur la destination. Dans ce cas, les paramètres de sécurité du serveur CIFS sur la destination sont définis sur les valeurs par défaut. Si vous avez activé le chiffrement SMB sur le SVM source, vous devez activer manuellement le chiffrement SMB du serveur CIFS sur la destination.

Étapes

- 1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que le chiffrement SMB soit requis pour le trafic SMB entrant sur le serveur CIFS...	Entrez la commande...
Activé	<code>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required true</code>
Désactivé	<code>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false</code>

- 2. Vérifiez que le chiffrement SMB requis sur le serveur CIFS est activé ou désactivé, selon les besoins :
`vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required`

Le `is-smb-encryption-required` s'affiche `true` Le cas échéant, le cryptage SMB est activé sur le serveur CIFS et `false` s'il est désactivé.

Exemple

L'exemple suivant permet le cryptage SMB requis pour le trafic SMB entrant pour le serveur CIFS sur le SVM vs1 :

```
cluster1::> vservers cifs security modify -vservers vs1 -is-smb-encryption
-required true

cluster1::> vservers cifs security show -vservers vs1 -fields is-smb-
encryption-required
vservers  is-smb-encryption-required
-----
vs1       true
```

Déterminez si les clients sont connectés à l'aide de sessions SMB cryptées

Vous pouvez afficher des informations sur les sessions SMB connectées pour déterminer si les clients utilisent des connexions SMB chiffrées. Cela peut être utile pour déterminer si les sessions client SMB se connectent aux paramètres de sécurité souhaités.

Description de la tâche

Les sessions client SMB peuvent avoir l'un des trois niveaux de chiffrement suivants :

- `unencrypted`

La session SMB n'est pas chiffrée. Ni le chiffrement au niveau des serveurs virtuels de stockage ou du partage n'est configuré.

- `partially-encrypted`

Le chiffrement est lancé lorsque l'arborescence se connecte. Le chiffrement au niveau du partage est configuré. Le chiffrement au niveau des SVM n'est pas activé.

- `encrypted`

La session SMB est entièrement chiffrée. Le chiffrement au niveau des SVM est activé. Le chiffrement au niveau du partage peut être activé ou non. Le paramètre de cryptage au niveau SVM remplace le paramètre de cryptage au niveau du partage.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous voulez afficher des informations sur...	Entrez la commande...
Sessions avec un paramètre de chiffrement spécifié pour les sessions sur un SVM spécifié	<code>`vservers cifs session show -vservers vservers_name {unencrypted</code>
<code>partially-encrypted</code>	<code>encrypted}` -instance`</code>
Paramètre de chiffrement pour un ID de session spécifique sur un SVM spécifié	<code>vservers cifs session show -vservers vservers_name -session-id integer -instance</code>

Exemples

La commande suivante affiche des informations détaillées sur la session, y compris le paramètre de chiffrement, sur une session SMB avec l’ID de session 2 :

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

Contrôle des statistiques de chiffrement SMB

Vous pouvez surveiller les statistiques de cryptage SMB et déterminer les sessions établies et les connexions de partage qui sont cryptées et qui ne le sont pas.

Description de la tâche

Le `statistics` Le niveau de privilège avancé fournit les compteurs suivants, que vous pouvez utiliser pour surveiller le nombre de sessions SMB chiffrées et de connexions pour le partage :

Nom du compteur	Descriptions
encrypted_sessions	Indique le nombre de sessions SMB 3.0 cryptées
encrypted_share_connections	Indique le nombre de partages cryptés sur lesquels une arborescence s'est connectée
rejected_unencrypted_sessions	Indique le nombre de configurations de session rejetées en raison d'un manque de capacité de chiffrement du client

Nom du compteur	Descriptions
<code>rejected_unencrypted_shares</code>	Indique le nombre de mappages de partage rejetés en raison d'un manque de capacité de chiffrement du client

Ces compteurs sont disponibles avec les objets de statistiques suivants :

- `cifs` Permet de surveiller le chiffrement SMB pour toutes les sessions SMB 3.0.

Les statistiques SMB 3.0 sont incluses dans les résultats de `cifs` objet. Si vous souhaitez comparer le nombre de sessions chiffrées au nombre total de sessions, vous pouvez comparer les résultats de l' `encrypted_sessions` compteur avec la sortie pour le `established_sessions` compteur.

Si vous souhaitez comparer le nombre de connexions de partage chiffrées au nombre total de connexions de partage, vous pouvez comparer la sortie du `encrypted_share_connections` compteur avec la sortie pour le `connected_shares` compteur.

- `rejected_unencrypted_sessions` Indique le nombre de tentatives d'établissement d'une session SMB nécessitant un chiffrement d'un client qui ne prend pas en charge le chiffrement SMB.
- `rejected_unencrypted_shares` Indique combien de fois une tentative de connexion à un partage SMB nécessite un chiffrement d'un client ne prenant pas en charge le chiffrement SMB.

Vous devez démarrer une collecte d'échantillons de statistiques avant de pouvoir afficher les données résultantes. Vous pouvez afficher les données de l'échantillon si vous n'arrêtez pas la collecte de données. L'arrêt de la collecte de données vous donne un échantillon fixe. L'option ne pas arrêter la collecte de données vous permet d'obtenir des données mises à jour que vous pouvez utiliser pour comparer à des requêtes précédentes. La comparaison vous aide à identifier les tendances.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Démarrer une collecte de données :

```
statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]
```

Si vous ne spécifiez pas le `-sample-id` Paramètre, la commande génère un exemple d'identificateur pour vous et définit cet échantillon comme échantillon par défaut pour la session de l'interface de ligne de commande. La valeur pour `-sample-id` est une chaîne de texte. Si vous exécutez cette commande pendant la même session CLI et ne spécifiez pas le `-sample-id` paramètre, la commande remplace l'échantillon par défaut précédent.

Vous pouvez spécifier le nœud sur lequel vous souhaitez collecter les statistiques. Si vous ne spécifiez pas le nœud, l'exemple collecte les statistiques de tous les nœuds du cluster.

3. Utilisez le `statistics stop` commande pour arrêter la collecte des données de l'échantillon.
4. Afficher les statistiques de chiffrement SMB :

Si vous souhaitez afficher les informations pour...	Entrer...
Sessions chiffrées	<code>`show -sample-id <i>sample_ID</i> -counter encrypted_sessions`</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	Sessions chiffrées et sessions établies
<code>`show -sample-id <i>sample_ID</i> -counter encrypted_sessions`</code>	<code>established_sessions</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	Connexions de partage cryptées
<code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections`</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>
Connexions de partage cryptées et partages connectés	<code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections`</code>
<code>connected_shares</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>
Sessions non chiffrées rejetées rejetées	<code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_sessions`</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	Les connexions de partage non chiffrées ont été rejetées
<code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_share`</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>

Si vous souhaitez afficher les informations uniquement pour un seul nœud, spécifiez l'option `-node` paramètre.

- Revenir au niveau de privilège admin :
`set -privilege admin`

Exemples

L'exemple suivant montre comment surveiller les statistiques de cryptage SMB 3.0 sur la machine virtuelle de stockage (SVM) vs1.

La commande suivante permet d'accéder au niveau de privilège avancé :

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by support personnel.
```

```
Do you want to continue? {y|n}: y
```

La commande suivante démarre la collecte de données pour un nouvel échantillon :

```
cluster1::*> statistics start -object cifs -sample-id  
smbencryption_sample -vserver vs1  
Statistics collection is being started for Sample-id:  
smbencryption_sample
```

La commande suivante arrête la collecte des données pour cet échantillon :

```
cluster1::*> statistics stop -sample-id smbencryption_sample  
Statistics collection is being stopped for Sample-id:  
smbencryption_sample
```

La commande suivante affiche les sessions SMB chiffrées et les sessions SMB établies par le nœud à partir de l'exemple :

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name
```

Object: cifs

Instance: [proto_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:45

Scope: vsim2

Counter	Value
established_sessions	1
encrypted_sessions	1

2 entries were displayed

La commande suivante affiche le nombre de sessions SMB non chiffrées rejetées par le nœud à partir de l'exemple :

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions -node node_name
```

Object: cifs

Instance: [proto_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:51

Scope: vsim2

Counter	Value
rejected_unencrypted_sessions	1

1 entry was displayed.

La commande suivante indique le nombre de partages SMB connectés et de partages SMB chiffrés par le nœud à partir de l'exemple :

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name
```

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

Counter	Value
connected_shares	2
encrypted_share_connections	1

2 entries were displayed.

La commande suivante affiche le nombre de connexions de partage SMB non chiffrées rejetées par le nœud à partir de l'exemple :

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name
```

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

Counter	Value
rejected_unencrypted_shares	1

1 entry was displayed.

Informations associées

[Détermination des objets statistiques et des compteurs disponibles](#)

["Contrôle des performances et présentation de la gestion"](#)

Communication de session LDAP sécurisée

Concepts de signature et d'étanchéité LDAP

Depuis ONTAP 9, vous pouvez configurer la signature et le chiffrement pour activer la sécurité des sessions LDAP sur les requêtes vers un serveur Active Directory (AD). Vous

devez configurer les paramètres de sécurité du serveur CIFS sur la machine virtuelle de stockage (SVM) de sorte qu'ils correspondent à ceux du serveur LDAP.

La signature valide l'intégrité des données LDAP à l'aide d'une technologie à clé secrète. Le chiffrement crypte les données LDAP afin de ne pas transmettre de données sensibles en clair. Une option *LDAP Security Level* indique si le trafic LDAP doit être signé, signé et scellé, ou non. La valeur par défaut est `none`.

La signature et le chiffrement LDAP sur le trafic CIFS sont activés sur le SVM avec le `-session-security -for-ad-ldap` à la `vserver cifs security modify` commande.

Activez le chiffrement et la signature LDAP sur le serveur CIFS

Avant que votre serveur CIFS puisse utiliser la signature et le chiffrement pour sécuriser la communication avec un serveur LDAP Active Directory, vous devez modifier les paramètres de sécurité du serveur CIFS pour activer la signature et le chiffrement LDAP.

Avant de commencer

Vous devez consulter votre administrateur de serveur AD pour déterminer les valeurs de configuration de sécurité appropriées.

Étapes

1. Configurez le paramètre de sécurité du serveur CIFS qui autorise le trafic signé et scellé avec les serveurs LDAP Active Directory : `vserver cifs security modify -vserver vserver_name -session -security-for-ad-ldap {none|sign|seal}`

Vous pouvez activer la signature (`sign`, intégrité des données), signature et scellage (`seal`, intégrité et chiffrement des données), ou ni l'un ni l'autre `none`, pas de signature ou d'étanchéité). La valeur par défaut est `none`.

2. Vérifiez que le paramètre de sécurité de signature et de chiffrement LDAP est défini correctement :

```
vserver cifs security show -vserver vserver_name
```



Si le SVM utilise le même serveur LDAP pour effectuer des requêtes name-mapping ou d'autres informations UNIX, comme les utilisateurs, les groupes et les netgroups, alors vous devez activer le paramètre correspondant avec le `-session-security` de la `vserver services name-service ldap client modify` commande.

Configurer LDAP sur TLS

Exporter une copie du certificat de l'autorité de certification racine auto-signé

Pour utiliser LDAP sur SSL/TLS pour sécuriser la communication Active Directory, vous devez d'abord exporter une copie du certificat d'autorité de certification racine auto-signé du service de certificats Active Directory en fichier de certificat et la convertir en fichier texte ASCII. Ce fichier texte est utilisé par ONTAP pour installer le certificat sur la machine virtuelle de stockage (SVM).

Avant de commencer

Le service de certificat Active Directory doit déjà être installé et configuré pour le domaine auquel le serveur CIFS appartient. Vous trouverez des informations sur l'installation et la configuration des services de certificats

Active Director en consultant la bibliothèque Microsoft TechNet.

"Bibliothèque Microsoft TechNet : technet.microsoft.com"

Étape

1. Obtenez un certificat d'autorité de certification racine du contrôleur de domaine qui se trouve dans le .pem format de texte.

"Bibliothèque Microsoft TechNet : technet.microsoft.com"

Une fois que vous avez terminé

Installer le certificat sur le SVM.

Informations associées

"Bibliothèque Microsoft TechNet"

Installer le certificat d'autorité de certification racine auto-signé sur le SVM

Si l'authentification LDAP avec TLS est requise lorsqu'il s'agit de serveurs LDAP, vous devez d'abord installer le certificat AC racine auto-signé sur le SVM.

Description de la tâche

Lorsque LDAP sur TLS est activé, le client LDAP ONTAP sur la SVM ne prend pas en charge les certificats révoqués dans ONTAP 9.0 et 9.1.

Depuis ONTAP 9.2, toutes les applications de ONTAP qui utilisent les communications TLS peuvent vérifier le statut du certificat numérique à l'aide du protocole OCSP (Online Certificate Status Protocol). Si OCSP est activé pour LDAP sur TLS, les certificats révoqués sont rejetés et la connexion échoue.

Étapes

1. Installez le certificat d'autorité de certification racine auto-signé :
 - a. Commencez l'installation du certificat : `security certificate install -vserver vservice_name -type server-ca`

La sortie de la console affiche le message suivant : Please enter Certificate: Press <Enter> when done
 - b. Ouvrez le certificat .pem fichier avec un éditeur de texte, copiez le certificat, y compris les lignes commençant par -----BEGIN CERTIFICATE----- et se terminant par -----END CERTIFICATE-----, puis collez le certificat après l'invite de commande.
 - c. Vérifiez que le certificat s'affiche correctement.
 - d. Terminez l'installation en appuyant sur entrée.
2. Vérifiez que le certificat est installé : `security certificate show -vserver vservice_name`

Activez LDAP sur TLS sur le serveur

Avant que votre serveur SMB puisse utiliser TLS pour sécuriser les communications avec un serveur LDAP Active Directory, vous devez modifier les paramètres de sécurité du serveur SMB pour activer LDAP sur TLS.

Depuis ONTAP 9.10.1, la liaison des canaux LDAP est prise en charge par défaut pour les connexions LDAP Active Directory (AD) et services de noms. ONTAP essaiera la liaison des canaux avec les connexions LDAP uniquement si Start-TLS ou LDAPS est activé avec la sécurité de session définie sur Sign ou SEAL. Pour désactiver ou réactiver la liaison des canaux LDAP avec les serveurs AD, utilisez le `-try-channel-binding-for-ad-ldap` paramètre avec le `vserver cifs security modify` commande.

Pour en savoir plus, voir :

- ["Présentation LDAP"](#)
- ["2020 exigences de liaison des canaux LDAP et de signature LDAP pour Windows"](#).

Étapes

1. Configurez le paramètre de sécurité du serveur SMB permettant une communication LDAP sécurisée avec les serveurs LDAP Active Directory : `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. Vérifiez que le paramètre de sécurité LDAP sur TLS est défini sur `true`: `vserver cifs security show -vserver vserver_name`



Si le SVM utilise le même serveur LDAP pour effectuer des requêtes name-mapping ou d'autres informations UNIX (par exemple, utilisateurs, groupes et netgroups), alors vous devez également modifier `-use-start-tls` à l'aide de `vserver services name-service ldap client modify` commande.

Configurez SMB Multichannel pour des performances et une redondance optimales

Depuis ONTAP 9.4, vous pouvez configurer SMB Multichannel pour fournir plusieurs connexions entre ONTAP et les clients dans une seule session SMB. Cela améliore le débit et la tolérance aux pannes.

Avant de commencer

La fonctionnalité SMB Multichannel ne peut être utilisée que lorsque les clients négocient avec SMB 3.0 ou une version ultérieure. SMB 3.0 et versions ultérieures sont activés par défaut sur le serveur ONTAP SMB.

Description de la tâche

Les clients SMB détectent et utilisent automatiquement plusieurs connexions réseau si une configuration adéquate est identifiée sur le cluster ONTAP.

Le nombre de connexions simultanées dans une session SMB dépend des cartes réseau que vous avez déployées :

- **NIC 1G sur le client et le cluster ONTAP**

Le client établit une connexion par carte réseau et lie la session à toutes les connexions.

- **Cartes réseau 10G et de capacité supérieure sur le client et le cluster ONTAP**

Le client établit jusqu'à quatre connexions par carte réseau et lie la session à toutes les connexions. Le client peut établir des connexions sur plusieurs cartes réseau 10G et supérieures.

Vous pouvez également modifier les paramètres suivants (privilège avancé) :

- `-max-connections-per-session`

Nombre maximum de connexions autorisées par session multicanal. La valeur par défaut est 32 connexions.

Si vous souhaitez activer plus de connexions que la configuration par défaut, vous devez effectuer des ajustements comparables à la configuration client, qui possède également une valeur par défaut de 32 connexions.

- `-max-lifs-per-session`

Nombre maximum d'interfaces réseau annoncées par session multicanal. La valeur par défaut est 256 interfaces réseau.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Activez SMB Multichannel sur le serveur SMB :

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel  
-enabled true
```

3. Vérifiez que ONTAP signale les sessions SMB multicanaux :

```
vserver cifs session show
```

4. Retour au niveau de privilège admin :

```
set -privilege admin
```

Exemple

L'exemple suivant affiche les informations relatives à toutes les sessions SMB, affichant plusieurs connexions pour une seule session :

```

cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                Open
Idle
IDs      ID      Workstation      Windows User      Files
Time
-----
-----
138683,
138684,
138685    1      10.1.1.1      DOMAIN\
4s                                     Administrator

```

L'exemple suivant affiche des informations détaillées sur une session SMB avec l'ID-session 1 :

```

cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -

```

Configurez les mappages utilisateur Windows par défaut sur utilisateur UNIX sur le serveur SMB

Configurez l'utilisateur UNIX par défaut

Vous pouvez configurer l'utilisateur UNIX par défaut à utiliser si toutes les autres tentatives de mappage échouent pour un utilisateur, ou si vous ne souhaitez pas mapper des utilisateurs individuels entre UNIX et Windows. Si vous souhaitez que l'authentification des utilisateurs non mappés échoue, vous ne devez pas configurer l'utilisateur UNIX par défaut.

Description de la tâche

Par défaut, le nom de l'utilisateur UNIX par défaut est `""pcuser""`, ce qui signifie que par défaut, le mappage d'utilisateur à l'utilisateur UNIX par défaut est activé. Vous pouvez spécifier un autre nom à utiliser comme utilisateur UNIX par défaut. Le nom que vous spécifiez doit exister dans les bases de données de service de noms configurées pour la machine virtuelle de stockage (SVM). Si cette option est définie sur une chaîne null, personne ne peut accéder au serveur CIFS en tant qu'utilisateur UNIX par défaut. En d'autres termes, chaque utilisateur doit avoir un compte dans la base de données de mots de passe avant d'accéder au serveur CIFS.

Pour qu'un utilisateur puisse se connecter au serveur CIFS à l'aide du compte utilisateur UNIX par défaut, l'utilisateur doit respecter les conditions préalables suivantes :

- L'utilisateur est authentifié.
- L'utilisateur se trouve dans la base de données utilisateur Windows locale du serveur CIFS, dans le domaine personnel du serveur CIFS ou dans un domaine approuvé (si les recherches de mappage de noms de domaines multiples sont activées sur le serveur CIFS).
- Le nom d'utilisateur n'est pas explicitement mappé à une chaîne nulle.

Étapes

1. Configurez l'utilisateur UNIX par défaut :

Si vous voulez ...	Entrer ...
Utiliser l'utilisateur UNIX par défaut « pcuser »	<code>vserver cifs options modify -default -unix-user pcuser</code>
Utiliser un autre compte utilisateur UNIX comme utilisateur par défaut	<code>vserver cifs options modify -default -unix-user user_name</code>
Désactivez l'utilisateur UNIX par défaut	<code>vserver cifs options modify -default -unix-user ""</code>

```
vserver cifs options modify -default-unix-user pcuser
```

2. Vérifiez que l'utilisateur UNIX par défaut est configuré correctement:`vserver cifs options show -vserver vserver_name`

Dans l'exemple suivant, l'utilisateur UNIX par défaut et l'utilisateur UNIX invité sur le SVM vs1 sont configurés pour utiliser l'utilisateur UNIX « pcuser » :

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1
```

```
Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

Configurer l'utilisateur UNIX invité

Configurer l'option utilisateur UNIX invité signifie que les utilisateurs qui se connectent à partir de domaines non fiables sont mappés à l'utilisateur UNIX invité et peuvent se connecter au serveur CIFS. Si vous souhaitez que l'authentification des utilisateurs de domaines non fiables échoue, vous ne devez pas configurer l'utilisateur UNIX invité. La valeur par défaut est de ne pas autoriser les utilisateurs de domaines non fiables à se connecter au serveur CIFS (le compte UNIX invité n'est pas configuré).

Description de la tâche

Lors de la configuration du compte UNIX invité, vous devez garder à l'esprit les éléments suivants :

- Si le serveur CIFS ne peut pas authentifier l'utilisateur par rapport à un contrôleur de domaine pour le domaine personnel, un domaine approuvé ou la base de données locale et que cette option est activée, le serveur CIFS considère l'utilisateur comme un utilisateur invité et mappe l'utilisateur avec l'utilisateur UNIX spécifié.
- Si cette option est définie sur une chaîne null, l'utilisateur UNIX invité est désactivé.
- Vous devez créer un utilisateur UNIX afin d'utiliser comme utilisateur UNIX invité dans l'une des bases de données de service de nom de la machine virtuelle de stockage (SVM).
- Un utilisateur connecté en tant qu'utilisateur invité est automatiquement membre du groupe BUILTIN\guest sur le serveur CIFS.
- L'option 'homedirs-public' s'applique uniquement aux utilisateurs authentifiés. Un utilisateur connecté en tant qu'utilisateur invité ne dispose pas d'un répertoire personnel et ne peut pas accéder aux répertoires d'accueil des autres utilisateurs.

Étapes

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez...	Entrer...
Configurer l'utilisateur UNIX invité	<pre>vserver cifs options modify -guest -unix-user <i>unix_name</i></pre>
Désactiver l'utilisateur UNIX invité	<pre>vserver cifs options modify -guest -unix-user ""</pre>

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Vérifiez que l'utilisateur UNIX invité est configuré correctement : `vserver cifs options show -vserver vserver_name`

Dans l'exemple suivant, l'utilisateur UNIX par défaut et l'utilisateur UNIX invité sur le SVM vs1 sont configurés pour utiliser l'utilisateur UNIX « pcuser » :

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers           : -
```

Mappez le groupe d'administrateurs à la racine

Si vous ne possédez que des clients CIFS dans votre environnement et que votre machine virtuelle de stockage (SVM) a été configurée comme un système de stockage multiprotocole, vous devez disposer d'au moins un compte Windows disposant de privilège racine pour accéder aux fichiers sur la SVM ; Sinon, vous ne pouvez pas gérer la SVM car vous ne disposez pas de droits d'utilisateur suffisants.

Description de la tâche

Si votre système de stockage a été configuré en NTFS-only, cependant, le `/etc` Le répertoire dispose d'une liste de contrôle d'accès de niveau fichier qui permet au groupe d'administrateurs d'accéder aux fichiers de configuration ONTAP.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Configurez l'option de serveur CIFS qui mappe le groupe d'administrateurs à root, le cas échéant :

Les fonctions que vous recherchez...	Alors...
Associez les membres du groupe d'administrateurs à la racine	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled true</code> Tous les comptes du groupe administrateurs sont considérés comme root, même si vous n'avez pas de <code>/etc/usermap.cfg</code> entrée mappant les comptes à la racine. Si vous créez un fichier à l'aide d'un compte appartenant au groupe d'administrateurs, le fichier est détenu par root lorsque vous affichez le fichier à partir d'un client UNIX.
Désactivez le mappage des membres du groupe d'administrateurs à la racine	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled false</code> Les comptes du groupe d'administrateurs ne sont plus mis en correspondance avec root. Vous ne pouvez mapper explicitement un seul utilisateur qu'à la racine.

- Vérifiez que l'option est réglée sur la valeur souhaitée : `vserver cifs options show -vserver vserver_name`
- Retour au niveau de privilège admin : `set -privilege admin`

Affiche des informations sur les types d'utilisateurs connectés via des sessions SMB

Vous pouvez afficher des informations sur le type d'utilisateurs connectés via des sessions SMB. Cela vous aide à vous assurer que seul le type d'utilisateur approprié est connecté via des sessions SMB sur la machine virtuelle de stockage (SVM).

Description de la tâche

Les types d'utilisateurs suivants peuvent se connecter via des sessions SMB :

- `local-user`

Authentifié en tant qu'utilisateur CIFS local

- `domain-user`

Authentifié en tant qu'utilisateur de domaine (soit à partir du domaine personnel du serveur CIFS ou d'un domaine de confiance)

- `guest-user`

Authentifié en tant qu'utilisateur invité

- `anonymous-user`

Authentifié en tant qu'utilisateur anonyme ou nul

Étapes

1. Déterminez le type d'utilisateur connecté au cours d'une session SMB : `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

Si vous souhaitez afficher les informations de type d'utilisateur pour les sessions établies...	Saisissez la commande suivante...
Pour toutes les sessions avec un type d'utilisateur spécifié	<code>`vserver cifs session show -vserver vserver_name -user-type {local-user</code>
domain-user	guest-user
anonymous-user}`	Pour un utilisateur spécifique

Exemples

La commande suivante affiche des informations sur le type d'utilisateur pour les sessions sur le SVM vs1 établies par l'utilisateur " ipubs\user1":

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user      user-type
-----
pub1node1 pub1      1      3439441860      10.0.0.1      10.1.1.1
IEPUBS\user1      domain-user
```

Options de commande pour limiter la consommation excessive de ressources client Windows

Les options du `vserver cifs options modify` La commande vous permet de contrôler la consommation des ressources pour les clients Windows. Cela peut être utile si un client se trouve en dehors des limites normales de consommation des ressources, par exemple si un nombre inhabituellement élevé de fichiers sont ouverts, si des sessions sont ouvertes ou si des demandes de modification sont envoyées.

Les options suivantes pour le `vserver cifs options modify` La commande a été ajoutée pour contrôler la consommation des ressources client Windows. Si la valeur maximale de l'une de ces options est dépassée, la demande est refusée et un message EMS est envoyé. Un message d'avertissement EMS est également envoyé lorsque 80 % de la limite configurée pour ces options sont atteintes.

- `-max-opens-same-file-per-tree`
Nombre maximum d'ouvertures sur le même fichier par arborescence CIFS
- `-max-same-user-sessions-per-connection`
Nombre maximal de sessions ouvertes par le même utilisateur par connexion

- `-max-same-tree-connect-per-session`

Nombre maximal de connexions d'arborescence sur le même partage par session

- `-max-watches-set-per-tree`

Nombre maximum de montres (également appelé *change notifie*) établi par arbre

Voir les pages de manuel pour les limites par défaut et pour afficher la configuration actuelle.

Depuis ONTAP 9.4, les serveurs exécutant SMB version 2 ou ultérieure peuvent limiter le nombre de requêtes en attente (*crédits SMB*) que le client peut envoyer au serveur sur une connexion SMB. La gestion des crédits SMB est initiée par le client et contrôlée par le serveur.

Le nombre maximal de requêtes en attente pouvant être accordées sur une connexion SMB est contrôlé par le `-max-credits` option. La valeur par défaut de cette option est 128.

Améliorez les performances de vos clients grâce aux oplocks classiques et de location

Améliorez les performances des clients grâce à une vue d'ensemble des oplocks classiques et des baux

Les oplocks traditionnels (verrous opportunistes) et les oplocks de location permettent à un client SMB dans certains scénarios de partage de fichiers d'effectuer une mise en cache côté client des informations de lecture anticipée, d'écriture différée et de verrouillage. Un client peut alors lire ou écrire dans un fichier sans rappeler régulièrement au serveur qu'il a besoin d'accéder au fichier en question. Ceci améliore les performances en réduisant le trafic réseau.

Les oplocks de location sont une forme améliorée de oplocks disponibles avec le protocole SMB 2.1 et les versions ultérieures. Les oplocks de location permettent à un client d'obtenir et de préserver l'état de mise en cache du client sur plusieurs ouvertures SMB en provenance de lui-même.

Les oplocks peuvent être contrôlés de deux façons :

- Par une propriété de partage, en utilisant `vserver cifs share create` lorsque le partage est créé, ou le `vserver share properties` commande après sa création.
- Par une propriété `qtree`, en utilisant le `volume qtree create` commande lors de la création du `qtree`, ou le `volume qtree oplock` commandes après leur création.

Écrire des considérations de perte de données dans le cache lors de l'utilisation de oplocks

Dans certaines circonstances, si un processus possède un oplock exclusif sur un fichier et qu'un deuxième processus tente d'ouvrir le fichier, le premier processus doit invalider les données mises en cache et vider les écritures et les verrous. Le client doit ensuite abandonner le oplock et accéder au fichier. En cas de panne du réseau pendant ce vidage, les données d'écriture mises en cache peuvent être perdues.

- Les possibilités de perte de données

Toute application avec des données en cache d'écriture peut perdre ces données dans les circonstances suivantes :

- La connexion s'effectue à l'aide de SMB 1.0.
- Il a un oplock exclusif sur le fichier.
- Il est dit de briser ce oplock ou de fermer le fichier.
- Lors du vidage du cache d'écriture, le réseau ou le système cible génère une erreur.
- Erreur de gestion et de fin d'écriture

Le cache lui-même n'a pas de traitement d'erreur—les applications le font. Lorsque l'application effectue une écriture dans le cache, l'écriture est toujours terminée. Si le cache, à son tour, effectue une écriture sur le système cible via un réseau, il doit supposer que l'écriture est terminée car si ce n'est pas le cas, les données sont perdues.

Activez ou désactivez les oplocks lors de la création de partages SMB

Les oplocks permettent aux clients de verrouiller des fichiers et de mettre du contenu en cache localement, ce qui peut augmenter les performances des opérations sur les fichiers. Les oplocks sont activés sur des partages SMB résidant sur des SVM (Storage Virtual machine). Dans certaines circonstances, vous pouvez désactiver les oplocks. Vous pouvez activer ou désactiver les oplocks sur une base de partage par partage.



Description de la tâche

Si les oplocks sont activés sur le volume contenant un partage mais que la propriété de partage oplock pour ce partage est désactivée, les oplocks sont désactivés pour ce partage. La désactivation des oplocks sur un partage a priorité sur le paramètre oplock de volume. La désactivation des oplocks sur le partage désactive à la fois les oplocks opportunistes et les oplocks de location.

Vous pouvez spécifier d'autres propriétés de partage en plus de spécifier la propriété de partage oplock à l'aide d'une liste délimitée par des virgules. Vous pouvez également spécifier d'autres paramètres de partage.

Étapes

1. Effectuez l'action appropriée :

Les fonctions que vous recherchez...	Alors...
Activez les oplocks sur un partage lors de la création du partage	<p data-bbox="842 159 1482 338">Saisissez la commande suivante : <code>vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]</code></p> <div data-bbox="873 604 928 667">  </div> <p data-bbox="987 380 1464 898">Si vous souhaitez que le partage n'ait que les propriétés de partage par défaut, c'est-à-dire oplocks, browsable, et changenotify activé, vous n'avez pas besoin de spécifier le <code>-share-properties</code> Paramètre lors de la création d'un partage SMB. Si vous souhaitez utiliser une combinaison de propriétés de partage autre que la valeur par défaut, vous devez spécifier l' <code>-share-properties</code> paramètre avec la liste des propriétés de partage à utiliser pour ce partage.</p>
Désactiver les oplocks sur un partage lors de la création du partage	<p data-bbox="842 961 1482 1140">Saisissez la commande suivante : <code>vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]</code></p> <div data-bbox="873 1255 928 1318">  </div> <p data-bbox="987 1182 1448 1392">Lors de la désactivation des oplocks, vous devez spécifier une liste de propriétés de partage lors de la création du partage, mais vous ne devez pas spécifier le oplocks propriété.</p>

Informations associées

[Activation ou désactivation des oplocks sur des partages SMB existants](#)

[Surveillance de l'état du oplock](#)

Commandes pour l'activation ou la désactivation des oplocks sur des volumes et des qtrees

Les oplocks permettent aux clients de verrouiller des fichiers et de mettre du contenu en cache localement, ce qui peut augmenter les performances des opérations sur les fichiers. Vous devez connaître les commandes permettant d'activer ou de désactiver les oplocks sur des volumes ou des qtrees. Vous devez également savoir quand vous pouvez activer ou désactiver les oplocks sur des volumes et des qtrees.

- Les oplocks sont activés par défaut sur les volumes.
- Vous ne pouvez pas désactiver les oplocks lorsque vous créez un volume.
- Vous pouvez à tout moment activer ou désactiver les oplocks sur des volumes existants pour des SVM.
- Vous pouvez activer les oplocks sur des qtrees pour les SVM.

Le paramètre du mode oplock est une propriété de l’ID qtree 0, le qtree par défaut que tous les volumes ont. Si vous ne spécifiez pas de paramètre oplock lors de la création d’un qtree, le qtree hérite du paramètre oplock du volume parent, qui est activé par défaut. Cependant, si vous spécifiez un paramètre oplock sur le nouveau qtree, il est prioritaire sur le paramètre oplock sur le volume.

Les fonctions que vous recherchez...	Utilisez cette commande...
Activez les oplocks sur des volumes ou des qtrees	<code>volume qtree oplocks</code> avec le <code>-oplock-mode</code> paramètre défini sur <code>enable</code>
Désactiver les oplocks sur des volumes ou des qtrees	<code>volume qtree oplocks</code> avec le <code>-oplock-mode</code> paramètre défini sur <code>disable</code>

Informations associées

[Surveillance de l’état du oplock](#)

Activez ou désactivez les oplocks sur les partages SMB existants



Les oplocks sont activés par défaut sur des partages SMB sur des SVM (Storage Virtual machines). Dans certaines circonstances, vous pouvez désactiver les oplocks. Si vous avez précédemment désactivé les oplocks sur un partage, vous pouvez également réactiver les oplocks.

Description de la tâche

Si les oplocks sont activés sur le volume contenant un partage, mais que la propriété de partage oplock pour ce partage est désactivée, les oplocks sont désactivés pour ce partage. La désactivation des oplocks sur un partage a priorité sur l’activation des oplocks sur le volume. La désactivation des oplocks sur la part désactive les oplocks opportunistes et ceux de location. Vous pouvez à tout moment activer ou désactiver les oplocks sur des partages existants.

Étape

1. Effectuez l’action appropriée :

Les fonctions que vous recherchez...	Alors...
Activez les oplocks sur un partage en modifiant un partage existant	<p>Saisissez la commande suivante : <code>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks</code></p> <div>  <p>Vous pouvez spécifier des propriétés de partage supplémentaires à ajouter à l'aide d'une liste délimitée par des virgules.</p> </div> <p>Les nouvelles propriétés ajoutées sont ajoutées à la liste existante des propriétés de partage. Toutes les propriétés de partage que vous avez précédemment spécifiées restent en vigueur.</p>
Désactivez les oplocks sur un partage en modifiant un partage existant	<p>Saisissez la commande suivante : <code>vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks</code></p> <div>  <p>Vous pouvez spécifier des propriétés de partage supplémentaires à supprimer à l'aide d'une liste délimitée par des virgules.</p> </div> <p>Les propriétés de partage que vous supprimez sont supprimées de la liste existante de propriétés de partage. Cependant, les propriétés de partage configurées précédemment que vous ne supprimez pas restent en vigueur.</p>

Exemples

La commande suivante active les oplocks pour le partage nommé « Ingénierie » sur une machine virtuelle de stockage (SVM, précédemment connue sous le nom de Vserver) vs1 :

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name Engineering -share-properties oplocks
```

```
cluster1::> vserver cifs share properties show
```

Vserver	Share	Properties
vs1	Engineering	oplocks browsable changenotify showsnapshot

La commande suivante désactive les oplocks pour l'action nommée « Engineering » sur le SVM vs1 :

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name Engineering -share-properties oplocks
```

```
cluster1::> vserver cifs share properties show
```

Vserver	Share	Properties
vs1	Engineering	browsable changenotify showsnapshot

Informations associées

[Activation ou désactivation des oplocks lors de la création de partages SMB](#)

[Surveillance de l'état du oplock](#)

[Ajout ou suppression de propriétés de partage sur un partage SMB existant](#)

Surveiller l'état du oplock

Vous pouvez surveiller et afficher des informations sur l'état du oplock. Vous pouvez utiliser ces informations pour déterminer quels fichiers ont des oplocks, ce que sont le niveau de oplock et le niveau d'état de oplock et si le leasing oplock est utilisé. Vous pouvez également déterminer des informations sur les verrous que vous devrez peut-être briser manuellement.

Description de la tâche

Vous pouvez afficher des informations sur tous les oplocks sous forme de résumé ou sous forme de liste détaillée. Vous pouvez également utiliser des paramètres facultatifs pour afficher des informations sur un plus petit sous-ensemble de verrous existants. Par exemple, vous pouvez spécifier que le retour de sortie se verrouille uniquement avec l'adresse IP du client spécifiée ou avec le chemin d'accès spécifié.

Vous pouvez afficher les informations suivantes sur les oplocks classiques et de location :

- SVM, node, volume et LIF sur lequel le oplock est établi
- Verrouiller l'UUID
- Adresse IP du client avec le oplock
- Chemin auquel le oplock est établi
- Protocole de verrouillage (SMB) et type (oplock)
- État de verrouillage
- Niveau oplock
- État de connexion et heure d'expiration SMB
- ID de groupe ouvert si un oplock de bail est accordé

Voir la `vserver oplocks show` page man pour une description détaillée de chaque paramètre.

Étapes

1. Afficher l'état du oplock à l'aide de l' `vserver locks show` commande.

Exemples

La commande suivante affiche des informations par défaut sur tous les verrouillages. Le oplock du fichier affiché est accordé avec un `read-batch` niveau oplock :

```
cluster1::> vserver locks show
```

```
Vserver: vs0
```

Volume	Object Path	LIF	Protocol	Lock Type	Client
vol1	/vol1/notes.txt	node1_data1	cifs	share-level	192.168.1.5
	Sharelock Mode: read_write-deny_delete				
				op-lock	192.168.1.5
	Oplock Level: read-batch				

L'exemple suivant affiche des informations plus détaillées sur le verrouillage d'un fichier avec le chemin d'accès `/data2/data2_2/intro.pptx`. Un oplock de bail est accordé sur le dossier avec un `batch` Niveau oplock vers un client avec une adresse IP de `10.3.1.3`:



Lors de l'affichage d'informations détaillées, la commande fournit une sortie séparée pour les informations oplock et sharelock. Cet exemple montre uniquement la sortie de la section oplock.

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx
```

```

    Vserver: vs1
    Volume: data2_2
  Logical Interface: lif2
    Object Path: /data2/data2_2/intro.pptx
    Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
    Lock Protocol: cifs
    Lock Type: op-lock
  Node Holding Lock State: node3
    Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
    Bytelock is Mandatory: -
    Bytelock is Exclusive: -
    Bytelock is Superlock: -
    Bytelock is Soft: -
    Oplock Level: batch
  Shared Lock Access Mode: -
    Shared Lock is Soft: -
    Delegation Type: -
    Client Address: 10.3.1.3
    SMB Open Type: -
    SMB Connect State: connected
  SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Informations associées

[Activation ou désactivation des oplocks lors de la création de partages SMB](#)

[Activation ou désactivation des oplocks sur des partages SMB existants](#)

[Commandes pour l'activation ou la désactivation des oplocks sur des volumes et des qtrees](#)

Appliquez des objets de stratégie de groupe aux serveurs SMB

Présentation de l'application d'objets de stratégie de groupe aux serveurs SMB

Votre serveur SMB prend en charge les objets de stratégie de groupe (GPO, Group Policy Objects), un ensemble de règles appelées attributs de stratégie de groupe_ qui s'appliquent aux ordinateurs dans un environnement Active Directory. Vous pouvez utiliser des GPO pour gérer centralement les paramètres de toutes les machines virtuelles de stockage (SVM) sur le cluster appartenant au même domaine Active Directory.

Lorsque les stratégies de groupe sont activées sur votre serveur SMB, ONTAP envoie des requêtes LDAP au serveur Active Directory pour demander des informations de stratégie de groupe. Si des définitions de GPO sont applicables à votre serveur SMB, le serveur Active Directory renvoie les informations de GPO suivantes :

- Nom de l'objet GPO
- Version GPO actuelle
- Emplacement de la définition de GPO
- Listes d'UUID (identificateurs uniques universels) pour les jeux de stratégies GPO

Informations associées

[Sécurisation de l'accès aux fichiers à l'aide du contrôle d'accès dynamique \(DAC\)](#)

["Audit et suivi de sécurité SMB et NFS"](#)

Stratégies de groupe prises en charge

Bien que tous les objets de stratégie de groupe (GPO) ne soient pas applicables à vos SVM (Storage Virtual machines) compatibles CIFS, les SVM peuvent reconnaître et traiter l'ensemble des GPO pertinents.

Les GPO suivants sont actuellement pris en charge sur SVM :

- Paramètres de configuration des règles d'audit avancées :

Accès aux objets : staging de stratégie d'accès central

Spécifie le type d'événements à auditer pour l'activation de la stratégie d'accès central (CAP), y compris les paramètres suivants :

- Ne pas auditer
- Vérifier uniquement les événements de réussite
- Audit des événements d'échec uniquement
- Vérifiez à la fois les événements de réussite et d'échec



Si l'une des trois options d'audit est définie (audit uniquement des événements de réussite, audit uniquement des événements d'échec, audit des événements de réussite et d'échec), ONTAP vérifie à la fois les événements de réussite et d'échec.

Réglez à l'aide du `Audit Central Access Policy Staging` réglage dans le `Advanced Audit Policy Configuration/Audit Policies/Object Access GPO`.



Pour utiliser les paramètres de stratégie d'audit avancée, l'audit doit être configuré sur le SVM compatible CIFS auquel vous souhaitez appliquer ce paramètre. Si l'audit n'est pas configuré sur le SVM, les paramètres de GPO ne sont pas appliqués et seront supprimés.

- Paramètres du registre :
 - Intervalle d'actualisation des règles de groupe pour les SVM compatibles CIFS

Réglez à l'aide du `Registry GPO`.

- Actualisation aléatoire de la stratégie de groupe

Réglez à l'aide du Registry GPO.

- Publication de hachage pour BranchCache

La publication Hash pour BranchCache correspond au mode de fonctionnement de BranchCache. Les trois modes de fonctionnement pris en charge sont les suivants :

- Par action
- Tous les partages
- Désactivé

Réglez à l'aide du Registry GPO.

- Prise en charge du hachage pour BranchCache

Les trois paramètres de version de hachage suivants sont pris en charge :

- BranchCache version 1
- BranchCache version 2
- BranchCache versions 1 et 2

Réglez à l'aide du Registry GPO.



Pour utiliser les paramètres de BranchCache, BranchCache doit être configuré sur le SVM compatible CIFS auquel vous souhaitez appliquer ce paramètre. Si BranchCache n'est pas configuré sur le SVM, les paramètres de GPO ne sont pas appliqués et seront supprimés.

- Les paramètres de sécurité

- Règle d'audit et journal des événements

- Audit des événements de connexion

Spécifie le type d'événements de connexion à auditer, notamment les paramètres suivants :

- Ne pas auditer
- Vérifier uniquement les événements de réussite
- Audit sur les événements de panne
- Vérifiez à la fois les événements de réussite et d'échec

Réglez à l'aide du Audit logon events réglage dans le Local Policies/Audit Policy GPO.



Si l'une des trois options d'audit est définie (audit uniquement des événements de réussite, audit uniquement des événements d'échec, audit des événements de réussite et d'échec), ONTAP vérifie à la fois les événements de réussite et d'échec.

- Auditer l'accès aux objets

Spécifie le type d'accès aux objets à auditer, y compris les paramètres suivants :

- Ne pas auditer

- Vérifier uniquement les événements de réussite
- Audit sur les événements de panne
- Vérifiez à la fois les événements de réussite et d'échec
Réglez à l'aide du `Audit object access` réglage dans le `Local Policies/Audit Policy` GPO.



Si l'une des trois options d'audit est définie (audit uniquement des événements de réussite, audit uniquement des événements d'échec, audit des événements de réussite et d'échec), ONTAP vérifie à la fois les événements de réussite et d'échec.

- Méthode de conservation des journaux

Spécifie la méthode de conservation du journal d'audit, y compris les paramètres suivants :

- Remplacez le journal des événements lorsque la taille du fichier journal dépasse la taille maximale du journal
- Ne pas écraser le journal des événements (effacer le journal manuellement)
Réglez à l'aide du `Retention method for security log` réglage dans le `Event Log` GPO.

- Taille maximale du journal

Spécifie la taille maximale du journal d'audit.

Réglez à l'aide du `Maximum security log size` réglage dans le `Event Log` GPO.



Pour utiliser les paramètres de stratégie d'audit et de stratégie GPO du journal des événements, l'audit doit être configuré sur le SVM compatible CIFS auquel vous souhaitez appliquer ce paramètre. Si l'audit n'est pas configuré sur le SVM, les paramètres de GPO ne sont pas appliqués et seront supprimés.

- Sécurité du système de fichiers

Spécifie une liste de fichiers ou de répertoires sur lesquels la sécurité des fichiers est appliquée via un GPO.

Réglez à l'aide du `File System` GPO.



Le chemin d'accès au volume auquel la stratégie de sécurité du système de fichiers est configurée doit exister au sein de la SVM.

- Règle Kerberos

- Inclinaison maximale de l'horloge

Spécifie la tolérance maximale en minutes pour la synchronisation de l'horloge de l'ordinateur.

Réglez à l'aide du `Maximum tolerance for computer clock synchronization` réglage dans le `Account Policies/Kerberos Policy` GPO.

- Âge maximum du billet

Spécifie la durée de vie maximale en heures pour le ticket utilisateur.

Réglez à l'aide du Maximum lifetime for user ticket réglage dans le Account Policies/Kerberos Policy GPO.

- Âge maximum de renouvellement du billet

Spécifie la durée de vie maximale en jours pour le renouvellement du ticket utilisateur.

Réglez à l'aide du Maximum lifetime for user ticket renewal réglage dans le Account Policies/Kerberos Policy GPO.

- Attribution de droits utilisateur (droits de privilège)

- Devenir propriétaire

Indique la liste des utilisateurs et des groupes qui ont le droit de prendre possession de tout objet sécurisé.

Réglez à l'aide du Take ownership of files or other objects réglage dans le Local Policies/User Rights Assignment GPO.

- Privilège de sécurité

Indique la liste des utilisateurs et des groupes qui peuvent spécifier des options d'audit pour l'accès aux objets de ressources individuelles, telles que des fichiers, des dossiers et des objets Active Directory.

Réglez à l'aide du Manage auditing and security log réglage dans le Local Policies/User Rights Assignment GPO.

- Changer le privilège de notification (vérification de la traverse de dérivation)

Indique la liste des utilisateurs et des groupes qui peuvent traverser les arborescences de répertoires, même si les utilisateurs et les groupes ne disposent pas des autorisations sur le répertoire de traversée.

Le même privilège est requis pour que les utilisateurs reçoivent des notifications sur les modifications apportées aux fichiers et aux répertoires. Réglez à l'aide du Bypass traverse checking réglage dans le Local Policies/User Rights Assignment GPO.

- Valeurs de registre

- Paramètre de signature requis

Indique si la signature SMB requise est activée ou désactivée.

Réglez à l'aide du Microsoft network server: Digitally sign communications (always) réglage dans le Security Options GPO.

- Limiter l'anonymat

Indique les restrictions pour les utilisateurs anonymes et inclut les trois paramètres de stratégie de groupe suivants :

- Pas d'énumération des comptes de Security Account Manager (SAM) :

Ce paramètre de sécurité détermine les autorisations supplémentaires accordées pour les connexions anonymes à l'ordinateur. Cette option s'affiche sous la forme `no-enumeration` Dans ONTAP, si elle est activée.

Réglez à l'aide du `Network access: Do not allow anonymous enumeration of SAM accounts` réglage dans le `Local Policies/Security Options` GPO.

- Pas d'énumération des comptes et des partages SAM

Ce paramètre de sécurité détermine si l'énumération anonyme des comptes et partages SAM est autorisée. Cette option s'affiche sous la forme `no-enumeration` Dans ONTAP, si elle est activée.

Réglez à l'aide du `Network access: Do not allow anonymous enumeration of SAM accounts and shares` réglage dans le `Local Policies/Security Options` GPO.

- Limiter l'accès anonyme aux partages et aux canaux nommés

Ce paramètre de sécurité limite l'accès anonyme aux partages et aux tuyaux. Cette option s'affiche sous la forme `no-access` Dans ONTAP, si elle est activée.

Réglez à l'aide du `Network access: Restrict anonymous access to Named Pipes and Shares` réglage dans le `Local Policies/Security Options` GPO.

Lors de l'affichage d'informations sur les stratégies de groupe définies et appliquées, le `Resultant restriction for anonymous user` Le champ sortie fournit des informations sur la restriction résultant des trois paramètres de GPO anonymes de restriction. Les restrictions possibles résultantes sont les suivantes :

- `no-access`

L'utilisateur anonyme refuse l'accès aux partages spécifiés et aux canaux nommés, et ne peut pas utiliser l'énumération des comptes et des partages SAM. Cette restriction résultante est visible si le `Network access: Restrict anonymous access to Named Pipes and Shares` L'objet GPO est activé.

- `no-enumeration`

L'utilisateur anonyme a accès aux partages spécifiés et aux canaux nommés, mais ne peut pas utiliser l'énumération des comptes et partages SAM. Cette restriction résultante est observée si les deux conditions suivantes sont remplies :

- Le `Network access: Restrict anonymous access to Named Pipes and Shares` GPO est désactivé.
- Soit le `Network access: Do not allow anonymous enumeration of SAM accounts` ou le `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Les stratégies de groupe sont activées.

- `no-restriction`

L'utilisateur anonyme dispose d'un accès complet et peut utiliser l'énumération. Cette restriction résultante est observée si les deux conditions suivantes sont remplies :

- **Le Network access:** Restrict anonymous access to Named Pipes and Shares GPO est désactivé.
- **Les deux Network access:** Do not allow anonymous enumeration of SAM accounts et Network access: Do not allow anonymous enumeration of SAM accounts and shares Les GPO sont désactivés.
- Groupes restreints

Vous pouvez configurer des groupes restreints pour gérer de manière centralisée l'appartenance à des groupes intégrés ou définis par l'utilisateur. Lorsque vous appliquez un groupe restreint via une stratégie de groupe, l'appartenance à un groupe local de serveur CIFS est automatiquement définie pour correspondre aux paramètres de liste d'appartenance définis dans la stratégie de groupe appliquée.

Réglez à l'aide du `Restricted Groups GPO`.

- Paramètres de stratégie d'accès centralisé

Spécifie une liste de stratégies d'accès centralisé. Les politiques d'accès central et les règles de politique d'accès central associées déterminent les autorisations d'accès pour plusieurs fichiers sur la SVM.

Informations associées

[Activation ou désactivation de la prise en charge de GPO sur un serveur CIFS](#)

[Sécurisation de l'accès aux fichiers à l'aide du contrôle d'accès dynamique \(DAC\)](#)

["Audit et suivi de sécurité SMB et NFS"](#)

[Modification des paramètres de sécurité Kerberos du serveur CIFS](#)

[Utilisation de BranchCache pour mettre en cache le contenu de partage SMB dans une succursale](#)

[Utilisation de la signature SMB pour améliorer la sécurité du réseau](#)

[Configuration de la vérification de la traverse de dérivation](#)

[Configuration des restrictions d'accès pour les utilisateurs anonymes](#)

Conditions requises pour l'utilisation de stratégies de groupe avec votre serveur SMB

Pour utiliser des stratégies de groupe (GPO, Group Policy Objects) avec votre serveur SMB, votre système doit répondre à plusieurs exigences.

- SMB doit être sous licence sur le cluster. La licence SMB est incluse avec ["ONTAP One"](#). Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.
- Un serveur SMB doit être configuré et joint à un domaine Windows Active Directory.
- L'état admin du serveur SMB doit être on.
- Les GPO doivent être configurés et appliqués à l'unité organisationnelle (ou) Windows Active Directory contenant l'objet ordinateur serveur SMB.
- La prise en charge des GPO doit être activée sur le serveur SMB.

Activer ou désactiver la prise en charge de GPO sur un serveur CIFS

Vous pouvez activer ou désactiver la prise en charge des objets de stratégie de groupe (GPO, Group Policy Object) sur un serveur CIFS. Si vous activez la prise en charge GPO sur un serveur CIFS, les GPO applicables définis sur la stratégie de groupe—la stratégie appliquée à l'unité organisationnelle (ou) qui contient l'objet ordinateur de serveur CIFS—sont appliqués au serveur CIFS.



Description de la tâche

Les GPO ne peuvent pas être activés sur les serveurs CIFS en mode Workgroup.

Étapes

- 1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez...	Entrez la commande...
Activer les stratégies de groupe	<code>vserver cifs group-policy modify -vserver vserver_name -status enabled</code>
Désactiver les stratégies de groupe	<code>vserver cifs group-policy modify -vserver vserver_name -status disabled</code>

- 2. Vérifiez que la prise en charge des stratégies de groupe est dans l'état souhaité : `vserver cifs group-policy show -vserver +vserver_name_`

L'état de la stratégie de groupe pour les serveurs CIFS en mode groupe de travail s'affiche en tant que « désactivé ».

Exemple

L'exemple suivant illustre la prise en charge de GPO sur SVM (Storage Virtual machine) vs1 :

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

Vserver: vs1
Group Policy Status: enabled
```

Informations associées

[Stratégies de groupe prises en charge](#)

[Configuration requise pour l'utilisation des objets de stratégie de groupe avec votre serveur CIFS](#)

[Mise à jour des stratégies de groupe sur le serveur CIFS](#)

[Mise à jour manuelle des paramètres GPO sur le serveur CIFS](#)

[Affichage des informations sur les configurations GPO](#)

Mise à jour des stratégies de groupe sur la présentation du serveur CIFS

Par défaut, ONTAP récupère et applique les modifications des objets de stratégie de groupe (GPO) toutes les 90 minutes. Les paramètres de sécurité sont actualisés toutes les 16 heures. Si vous voulez mettre à jour les GPO pour appliquer de nouveaux paramètres de stratégie GPO avant que ONTAP ne les mette à jour automatiquement, vous pouvez déclencher une mise à jour manuelle sur un serveur CIFS à l'aide d'une commande ONTAP.

- Par défaut, tous les GPO sont vérifiés et mis à jour au besoin toutes les 90 minutes.

Cet intervalle est configurable et peut être défini à l'aide du `Refresh interval` et `Random offset` Paramètres GPO.

ONTAP interroge Active Directory pour les modifications apportées aux stratégies de groupe. Si les numéros de version de GPO enregistrés dans Active Directory sont supérieurs à ceux du serveur CIFS, ONTAP récupère et applique les nouveaux GPO. Si les numéros de version sont identiques, les GPO sur le serveur CIFS ne sont pas mis à jour.

- Les stratégies de sécurité sont actualisées toutes les 16 heures.

ONTAP récupère et applique les stratégies de groupe de paramètres de sécurité toutes les 16 heures, que ces stratégies de groupe aient été modifiées ou non.



La valeur par défaut de 16 heures ne peut pas être modifiée dans la version ONTAP actuelle. Il s'agit d'un paramètre par défaut du client Windows.

- Tous les GPO peuvent être mis à jour manuellement à l'aide d'une commande ONTAP.

Cette commande simule Windows ``gpupdate.exe`` commande `/force`.

Informations associées

[Mise à jour manuelle des paramètres GPO sur le serveur CIFS](#)

Mise à jour manuelle des paramètres GPO sur le serveur CIFS

Si vous souhaitez mettre à jour immédiatement les paramètres des objets GPO (Group Policy Object) sur votre serveur CIFS, vous pouvez mettre à jour les paramètres manuellement. Vous pouvez uniquement mettre à jour les paramètres modifiés ou forcer une mise à jour pour tous les paramètres, y compris les paramètres qui ont été appliqués auparavant mais qui n'ont pas été modifiés.

Étape

1. Effectuez l'action appropriée :

Si vous voulez mettre à jour...	Entrez la commande...
Paramètres de GPO modifiés	<code>vserver cifs group-policy update -vserver vserver_name</code>
Tous les paramètres GPO	<code>vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true</code>

Informations associées

[Mise à jour des stratégies de groupe sur le serveur CIFS](#)

Affiche des informations sur les configurations GPO

Vous pouvez afficher des informations sur les configurations GPO (Group Policy Object) définies dans Active Directory et à propos des configurations GPO appliquées au serveur CIFS.

Description de la tâche

Vous pouvez afficher des informations sur toutes les configurations GPO définies dans Active Directory du domaine auquel appartient le serveur CIFS ou afficher des informations uniquement sur les configurations GPO appliquées à un serveur CIFS.

Étapes

1. Pour afficher des informations sur les configurations GPO, effectuez l'une des opérations suivantes :

Si vous souhaitez afficher des informations sur toutes les configurations de stratégie de groupe...	Entrez la commande...
Défini dans Active Directory	<code>vserver cifs group-policy show-defined -vserver vserver_name</code>
Appliquée à une machine virtuelle de stockage (SVM) compatible CIFS	<code>vserver cifs group-policy show-applied -vserver vserver_name</code>

Exemple

L'exemple suivant présente les configurations GPO définies dans Active Directory à laquelle la SVM compatible CIFS vs1 appartient :

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
-----
      GPO Name: Default Domain Policy
      Level: Domain
      Status: enabled
```

Advanced Audit Settings:

Object Access:

Central Access Policy Staging: failure

Registry Settings:

Refresh Time Interval: 22

Refresh Random Offset: 8

Hash Publication Mode for BranchCache: per-share

Hash Version Support for BranchCache : version1

Security Settings:

Event Audit and Event Log:

Audit Logon Events: none

Audit Object Access: success

Log Retention Method: overwrite-as-needed

Max Log Size: 16384

File Security:

/vol1/home

/vol1/dir1

Kerberos:

Max Clock Skew: 5

Max Ticket Age: 10

Max Renew Age: 7

Privilege Rights:

Take Ownership: usr1, usr2

Security Privilege: usr1, usr2

Change Notify: usr1, usr2

Registry Values:

Signing Required: false

Restrict Anonymous:

No enumeration of SAM accounts: true

No enumeration of SAM accounts and shares: false

Restrict anonymous access to shares and named pipes: true

Combined restriction for anonymous user: no-access

Restricted Groups:

gpr1

gpr2

Central Access Policy Settings:

Policies: cap1

cap2

GPO Name: Resultant Set of Policy

Status: enabled

Advanced Audit Settings:

Object Access:

Central Access Policy Staging: failure

Registry Settings:

Refresh Time Interval: 22

```

Refresh Random Offset: 8
Hash Publication for Mode BranchCache: per-share
Hash Version Support for BranchCache: version1
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
  Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
  Policies: cap1
            cap2

```

L'exemple suivant présente les configurations GPO appliquées au SVM vs1 compatible CIFS :

```

cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
-----
GPO Name: Default Domain Policy
  Level: Domain
  Status: enabled
Advanced Audit Settings:
  Object Access:

```

```
Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
  Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2

GPO Name: Resultant Set of Policy
Level: RSOP
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
```

```
Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
  Restricted Groups:
    gpr1
    gpr2
  Central Access Policy Settings:
    Policies: cap1
              cap2
```

Informations associées

[Activation ou désactivation de la prise en charge de GPO sur un serveur CIFS](#)

Affiche des informations détaillées sur les GPO de groupe restreints

Vous pouvez afficher des informations détaillées sur les groupes restreints qui sont définis comme objets de stratégie de groupe (GPO, Group Policy Objects) dans Active Directory et qui sont appliqués au serveur CIFS.

Description de la tâche

Par défaut, les informations suivantes sont affichées :

- Nom de la stratégie de groupe
- Version de la stratégie de groupe

- Lien

Spécifie le niveau dans lequel la stratégie de groupe est configurée. Les valeurs de sortie possibles sont les suivantes :

- Local Lorsque la stratégie de groupe est configurée dans ONTAP
 - Site lorsque la stratégie de groupe est configurée au niveau du site dans le contrôleur de domaine
 - Domain lorsque la stratégie de groupe est configurée au niveau du domaine dans le contrôleur de domaine
 - OrganizationalUnit Lorsque la stratégie de groupe est configurée au niveau de l'unité organisationnelle (ou) dans le contrôleur de domaine
 - RSOP pour l'ensemble résultant de règles dérivées de toutes les stratégies de groupe définies à différents niveaux
- Nom de groupe restreint
 - Utilisateurs et groupes qui appartiennent à et qui n'appartiennent pas au groupe restreint
 - Liste des groupes auxquels le groupe restreint est ajouté

Un groupe peut être membre de groupes autres que ceux répertoriés ici.

Étape

1. Afficher des informations sur tous les GPO de groupe restreints en effectuant l'une des actions suivantes :

Si vous souhaitez afficher des informations sur tous les GPO de groupe restreints...	Entrez la commande...
Défini dans Active Directory	<code>vserver cifs group-policy restricted-group show-defined -vserver vserver_name</code>
Appliqué à un serveur CIFS	<code>vserver cifs group-policy restricted-group show-applied -vserver vserver_name</code>

Exemple

L'exemple suivant affiche les informations relatives aux stratégies de groupe restreintes définies dans le domaine Active Directory auquel appartient la SVM compatible CIFS nommée vs1 :


```
cluster1::> vsserver cifs group-policy restricted-group show-defined
-vserver vs1
```

```
Vserver: vs1
-----
```

```
    Group Policy Name: gp01
        Version: 16
        Link: OrganizationalUnit
    Group Name: group1
        Members: user1
        MemberOf: EXAMPLE\group9

    Group Policy Name: Resultant Set of Policy
        Version: 0
        Link: RSOP
    Group Name: group1
        Members: user1
        MemberOf: EXAMPLE\group9
```

L'exemple suivant affiche les informations relatives aux groupes restreints GPO appliqués au SVM vs1 activé pour CIFS :

```
cluster1::> vsserver cifs group-policy restricted-group show-applied
-vserver vs1
```

```
Vserver: vs1
-----
```

```
    Group Policy Name: gp01
        Version: 16
        Link: OrganizationalUnit
    Group Name: group1
        Members: user1
        MemberOf: EXAMPLE\group9

    Group Policy Name: Resultant Set of Policy
        Version: 0
        Link: RSOP
    Group Name: group1
        Members: user1
        MemberOf: EXAMPLE\group9
```

Informations associées

Afficher des informations sur les stratégies d'accès central

Vous pouvez afficher des informations détaillées sur les stratégies d'accès central définies dans Active Directory. Vous pouvez également afficher des informations sur les stratégies d'accès central appliquées au serveur CIFS via des objets de stratégie de groupe (GPO).

Description de la tâche

Par défaut, les informations suivantes sont affichées :

- Nom du SVM
- Nom de la stratégie d'accès central
- SID
- Description
- Heure de création
- Heure de modification
- Règles des membres



Les serveurs CIFS en mode groupe de travail ne sont pas affichés car ils ne prennent pas en charge les GPO.

Étape

1. Afficher des informations sur les stratégies d'accès central en effectuant l'une des actions suivantes :

Si vous souhaitez afficher des informations sur toutes les stratégies d'accès central...	Entrez la commande...
Défini dans Active Directory	<code>vserver cifs group-policy central-access-policy show-defined -vserver vserver_name</code>
Appliqué à un serveur CIFS	<code>vserver cifs group-policy central-access-policy show-applied -vserver vserver_name</code>

Exemple

L'exemple suivant affiche les informations pour toutes les stratégies d'accès central définies dans Active Directory :

```
cluster1::> vsriver cifs group-policy central-access-policy show-defined
```

```
Vserver   Name                               SID
-----
-----
vs1       p1                               S-1-17-3386172923-1132988875-3044489393-
3993546205
    Description: policy #1
    Creation Time: Tue Oct 22 09:34:13 2013
    Modification Time: Wed Oct 23 08:59:15 2013
    Member Rules: r1

vs1       p2                               S-1-17-1885229282-1100162114-134354072-
822349040
    Description: policy #2
    Creation Time: Tue Oct 22 10:28:20 2013
    Modification Time: Thu Oct 31 10:25:32 2013
    Member Rules: r1
                r2
```

L'exemple suivant affiche les informations de toutes les règles d'accès central appliquées aux SVM (Storage Virtual machine) sur le cluster :

```
cluster1::> vsriver cifs group-policy central-access-policy show-applied
```

```
Vserver   Name                               SID
-----
-----
vs1       p1                               S-1-17-3386172923-1132988875-3044489393-
3993546205
    Description: policy #1
    Creation Time: Tue Oct 22 09:34:13 2013
    Modification Time: Wed Oct 23 08:59:15 2013
    Member Rules: r1

vs1       p2                               S-1-17-1885229282-1100162114-134354072-
822349040
    Description: policy #2
    Creation Time: Tue Oct 22 10:28:20 2013
    Modification Time: Thu Oct 31 10:25:32 2013
    Member Rules: r1
                r2
```

Informations associées

Afficher des informations sur les règles de stratégie d'accès central

Vous pouvez afficher des informations détaillées sur les règles de stratégie d'accès central associées aux stratégies d'accès central définies dans Active Directory. Vous pouvez également afficher des informations sur les règles d'accès central appliquées au serveur CIFS via des stratégies d'accès centrales (objets de stratégie de groupe).

Description de la tâche

Vous pouvez afficher des informations détaillées sur les règles de stratégie d'accès central définies et appliquées. Par défaut, les informations suivantes sont affichées :

- Nom d'un vserver
- Nom de la règle d'accès central
- Description
- Heure de création
- Heure de modification
- Autorisations en cours
- Autorisations proposées
- Ressources cibles

Si vous souhaitez afficher des informations sur toutes les règles de stratégie d'accès central associées aux stratégies d'accès central...	Entrez la commande...
Défini dans Active Directory	<code>vserver cifs group-policy central-access-rule show-defined -vserver vserver_name</code>
Appliqué à un serveur CIFS	<code>vserver cifs group-policy central-access-rule show-applied -vserver vserver_name</code>

Exemple

L'exemple suivant affiche les informations de toutes les règles de stratégie d'accès central associées aux stratégies d'accès central définies dans Active Directory :

```
cluster1::> vserver cifs group-policy central-access-rule show-defined
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW) (A;;FA;;;BA) (A;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW) (A;;FA;;;BA) (A;;FA;;;SY)
```

L'exemple suivant affiche les informations de toutes les règles d'accès central associées aux règles d'accès central appliquées aux SVM (Storage Virtual machine) sur le cluster :

```
cluster1::> vserver cifs group-policy central-access-rule show-applied
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW) (A;;FA;;;BA) (A;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW) (A;;FA;;;BA) (A;;FA;;;SY)
```

Informations associées

[Sécurisation de l'accès aux fichiers à l'aide du contrôle d'accès dynamique \(DAC\)](#)

[Affichage des informations sur les configurations GPO](#)

[Affichage d'informations sur les règles d'accès central](#)

Commandes pour la gestion des mots de passe de compte d'ordinateur des serveurs SMB

Vous devez connaître les commandes permettant de modifier, de réinitialiser et de désactiver les mots de passe, ainsi que de configurer des planifications de mises à jour automatiques. Vous pouvez également configurer une planification sur le serveur SMB pour la mettre à jour automatiquement.

Les fonctions que vous recherchez...	Utilisez cette commande...
Modifiez ou réinitialisez le mot de passe du compte de domaine et vous connaissez le mot de passe	<code>vserver cifs domain password change</code>
Réinitialisez le mot de passe du compte de domaine et vous ne connaissez pas le mot de passe	<code>vserver cifs domain password reset</code>
Configurez les serveurs SMB pour les changements de mot de passe de compte d'ordinateur automatique	<code>vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true</code>
Désactivez les modifications de mot de passe de compte informatique automatique sur les serveurs SMB	<code>vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false</code>

Consultez la page man pour chaque commande pour plus d'informations.

Gérer les connexions du contrôleur de domaine

Affiche des informations sur les serveurs découverts

Vous pouvez afficher les informations relatives aux serveurs LDAP découverts et aux contrôleurs de domaine sur votre serveur CIFS.

Étape

1. Pour afficher les informations relatives aux serveurs découverts, entrez la commande suivante : `vserver cifs domain discovered-servers show`

Exemple

L'exemple suivant montre les serveurs découverts pour le SVM vs1 :

```
cluster1::> vsserver cifs domain discovered-servers show
```

```
Node: node1  
Vserver: vs1
```

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

Informations associées

[Réinitialisation et détection à nouveau des serveurs](#)

[Arrêt ou démarrage du serveur CIFS](#)

Réinitialiser et redécouvrir les serveurs

La réinitialisation et la redécouverte des serveurs sur votre serveur CIFS permet au serveur CIFS de supprimer les informations stockées sur les serveurs LDAP et les contrôleurs de domaine. Après l'abandon des informations sur le serveur, le serveur CIFS acquiert de nouveau les informations actuelles sur ces serveurs externes. Cela peut être utile lorsque les serveurs connectés ne répondent pas correctement.

Étapes

1. Saisissez la commande suivante : `vsserver cifs domain discovered-servers reset-servers -vsserver vsserver_name`
2. Afficher les informations sur les nouveaux serveurs découverts : `vsserver cifs domain discovered-servers show -vsserver vsserver_name`

Exemple

L'exemple suivant illustre la réinitialisation et la redécouverte des serveurs pour la machine virtuelle de stockage (SVM, anciennement Vserver) vs1 :

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver vs1
```

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1  
Vserver: vs1
```

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

Informations associées

[Affichage des informations sur les serveurs découverts](#)

[Arrêt ou démarrage du serveur CIFS](#)

Gérer la découverte de contrôleurs de domaine

À partir de ONTAP 9.3, vous pouvez modifier le processus par défaut par lequel les contrôleurs de domaine (DCS) sont détectés. Cela vous permet de limiter la détection à votre site ou à un pool de data centers préférés, ce qui peut entraîner des améliorations des performances en fonction de l'environnement.

Description de la tâche

Par défaut, le processus de découverte dynamique détecte tous les DCS disponibles, y compris tous les DCS préférés, tous les DCS du site local et tous les DCS distants. Cette configuration peut entraîner des temps de latence pour l'authentification et l'accès aux partages dans certains environnements. Si vous avez déjà déterminé le pool de DCS que vous souhaitez utiliser ou si les DCS distants sont insuffisants ou inaccessibles, vous pouvez changer la méthode de découverte.

Dans ONTAP 9.3 et versions ultérieures, le `discovery-mode` paramètre du `cifs domain discovered-servers` la commande vous permet de sélectionner l'une des options de découverte suivantes :

- Tous les DCS du domaine sont découverts.
- Seuls les DCS du site local sont découverts.

Le default-site Le paramètre du serveur SMB peut être défini pour utiliser ce mode avec des LIFs qui ne sont pas attribuées à un site dans `sites-et-services`.

- La détection de serveur n'est pas effectuée, la configuration du serveur SMB dépend uniquement des DCS préférés.

Pour utiliser ce mode, vous devez d'abord définir le DCS préféré pour le serveur SMB.

Avant de commencer

Vous devez avoir le niveau de privilège avancé.

Étape

1. Spécifiez l'option de découverte souhaitée : `vserver cifs domain discovered-servers discovery-mode modify -vserver vserver_name -mode {all|site|none}`

Options du mode paramètre :

- ° `all`

Découvrez tous les DCS disponibles (par défaut).

- ° `site`

Limitez la détection de DC à votre site.

- ° `none`

Utilisez uniquement les DCS préférés sans effectuer de découverte.

Ajouter des contrôleurs de domaine préférés

ONTAP détecte automatiquement les contrôleurs de domaine via DNS. Vous pouvez éventuellement ajouter un ou plusieurs contrôleurs de domaine à la liste des contrôleurs de domaine privilégiés pour un domaine spécifique.

Description de la tâche

Si une liste de contrôleurs de domaine privilégiés existe déjà pour le domaine spécifié, la nouvelle liste est fusionnée avec la liste existante.

Étape

1. Pour ajouter à la liste des contrôleurs de domaine privilégiés, entrez la commande suivante :
`vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name -preferred-dc IP_address, ...+`

`-vserver vserver_name` Spécifie le nom de la machine virtuelle de stockage (SVM).

`-domain domain_name` Spécifie le nom Active Directory complet du domaine auquel appartiennent les contrôleurs de domaine spécifiés.

`-preferred-dc IP_address,...` indique une ou plusieurs adresses IP des contrôleurs de domaine préférés, en tant que liste délimitée par des virgules, par ordre de préférence.

Exemple

La commande suivante ajoute des contrôleurs de domaine 172.17.102.25 et 172.17.102.24 à la liste des contrôleurs de domaine préférés que le serveur SMB du SVM vs1 utilise pour gérer l'accès externe au domaine `cifs.lab.example.com`.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain  
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

Informations associées

[Commandes pour la gestion des contrôleurs de domaine privilégiés](#)

Commandes pour la gestion des contrôleurs de domaine privilégiés

Vous devez connaître les commandes permettant d'ajouter, d'afficher et de supprimer les contrôleurs de domaine préférés.

Les fonctions que vous recherchez...	Utilisez cette commande...
Ajouter un contrôleur de domaine préféré	<code>vserver cifs domain preferred-dc add</code>
Afficher les contrôleurs de domaine préférés	<code>vserver cifs domain preferred-dc show</code>
Supprimez un contrôleur de domaine préféré	<code>vserver cifs domain preferred-dc remove</code>

Consultez la page man pour chaque commande pour plus d'informations.

Informations associées

[Ajout de contrôleurs de domaine préférés](#)

Activez les connexions SMB2 vers les contrôleurs de domaine

Depuis ONTAP 9.1, vous pouvez activer SMB version 2.0 pour vous connecter à un contrôleur de domaine. Cela est nécessaire si vous avez désactivé SMB 1.0 sur les contrôleurs de domaine. Depuis ONTAP 9.2, SMB2 est activé par défaut.

Description de la tâche

Le `smb2-enabled-for-dc-connections` L'option de commande active le système par défaut pour la version de ONTAP que vous utilisez. La valeur par défaut du système pour ONTAP 9.1 est activée pour SMB 1.0 et désactivée pour SMB 2.0. La valeur par défaut du système pour ONTAP 9.2 est activée pour SMB 1.0 et activée pour SMB 2.0. Si le contrôleur de domaine ne peut pas négocier au départ SMB 2.0, il utilise SMB 1.0.

SMB 1.0 peut être désactivé de ONTAP vers un contrôleur de domaine. Dans ONTAP 9.1, si SMB 1.0 a été désactivé, SMB 2.0 doit être activé pour communiquer avec un contrôleur de domaine.

En savoir plus sur :

- ["Vérification des versions SMB activées"](#).
- ["Fonctionnalités et versions SMB prises en charge"](#).



Si `-smb1-enabled-for-dc-connections` est défini sur `false` pendant `-smb1-enabled` est défini sur `true`, ONTAP refuse les connexions SMB 1.0 en tant que client, mais continue à accepter les connexions SMB 1.0 entrantes en tant que serveur.

Étapes

1. Avant de modifier les paramètres de sécurité SMB, vérifiez quelles versions SMB sont activées : `vserver cifs security show`
2. Faites défiler la liste pour voir les versions SMB.
3. Exécutez la commande appropriée, à l'aide de `smb2-enabled-for-dc-connections` option.

Si vous voulez que SMB2 soit...	Entrez la commande...
Activé	<code>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true</code>
Désactivé	<code>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false</code>

Activez les connexions cryptées aux contrôleurs de domaine

Depuis ONTAP 9.8, vous pouvez spécifier le cryptage des connexions aux contrôleurs de domaine.

Description de la tâche

ONTAP nécessite un cryptage pour les communications du contrôleur de domaine (DC) lorsque le système `-encryption-required-for-dc-connection` l'option est définie sur `true`; la valeur par défaut est `false`. Lorsque l'option est définie, seul le protocole SMB3 est utilisé pour les connexions ONTAP-DC, car le chiffrement n'est pris en charge que par SMB3.

Lorsque des communications DC cryptées sont requises, le `-smb2-enabled-for-dc-connections` L'option est ignorée, car ONTAP négocie uniquement les connexions SMB3. Si un DC ne prend pas en charge le SMB3 et le chiffrement, ONTAP ne se connecte pas avec lui.

Étape

1. Activer la communication chiffrée avec le DC : `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

Utilisez des sessions null pour accéder au stockage dans des environnements non Kerberos

Utilisez les sessions null pour accéder au stockage dans les environnements non Kerberos

L'accès aux sessions null fournit des autorisations pour les ressources réseau, telles que les données du système de stockage, ainsi que pour les services basés sur les clients s'exécutant sous le système local. Une session null se produit lorsqu'un processus client utilise le compte "système" pour accéder à une ressource réseau. La configuration de session null est spécifique à l'authentification non Kerberos.

Comment le système de stockage fournit un accès de session nul

Comme les partages de session NULL ne nécessitent pas d'authentification, les clients

qui ont besoin d'un accès de session nul doivent avoir leurs adresses IP mappées sur le système de stockage.

Par défaut, les clients de session null non mappés peuvent accéder à certains services système ONTAP, tels que l'énumération de partage, mais l'accès aux données du système de stockage est limité.



ONTAP prend en charge les valeurs des paramètres de registre Windows RestrictAnonymous avec l' `-restrict-anonymous` option. Cela vous permet de contrôler la mesure dans laquelle les utilisateurs nuls non mappés peuvent afficher ou accéder aux ressources système. Par exemple, vous pouvez désactiver l'énumération de partage et l'accès au partage IPC\$ (le partage de tuyauterie nommé masqué). Le `vserver cifs options modify` et `vserver cifs options show` les pages man fournissent plus d'informations sur le `-restrict-anonymous` option.

Sauf configuration contraire, un client exécutant un processus local qui demande l'accès au système de stockage via une session nulle est membre uniquement de groupes non restrictifs, tels que « tout le monde ». Pour limiter l'accès à une session nulle aux ressources du système de stockage sélectionnées, vous pouvez créer un groupe auquel appartiennent tous les clients de session nulle. La création de ce groupe vous permet de limiter l'accès au système de stockage et de définir des autorisations de ressources du système de stockage qui s'appliquent spécifiquement aux clients de session nul.

ONTAP fournit une syntaxe de mappage dans le `vserver name-mapping` Ensemble de commandes permettant de spécifier l'adresse IP des clients autorisés à accéder aux ressources du système de stockage à l'aide d'une session utilisateur null. Une fois que vous avez créé un groupe pour les utilisateurs nuls, vous pouvez spécifier des restrictions d'accès pour les ressources du système de stockage et les autorisations de ressources qui s'appliquent uniquement aux sessions nulles. L'utilisateur null est identifié comme une connexion anonyme. Les utilisateurs null n'ont accès à aucun répertoire personnel.

Les autorisations d'utilisateur mappées sont accordées à tout utilisateur null accédant au système de stockage à partir d'une adresse IP mappée. Prenez les précautions appropriées pour empêcher tout accès non autorisé aux systèmes de stockage mappés avec des utilisateurs nuls. Pour une protection maximale, placez le système de stockage et tous les clients nécessitant un accès nul au système de stockage utilisateur sur un réseau distinct, afin d'éliminer la possibilité d'une adresse IP « couverture ».

Informations associées

[Configuration des restrictions d'accès pour les utilisateurs anonymes](#)

Accorder aux utilisateurs nuls l'accès aux partages de système de fichiers

Vous pouvez autoriser l'accès aux ressources de votre système de stockage par les clients de session null en attribuant un groupe à utiliser par les clients de session null et en enregistrant les adresses IP des clients de session null à ajouter à la liste des clients autorisés à accéder aux données à l'aide de sessions null du système de stockage.

Étapes

1. Utilisez le `vserver name-mapping create` Commande permettant de mapper l'utilisateur null à un utilisateur Windows valide, avec un qualificateur IP.

La commande suivante mappe l'utilisateur null à user1 avec un nom d'hôte valide google.com :

```
vserver name-mapping create -direction win-unix -position 1 -pattern
"ANONYMOUS LOGON" -replacement user1 - hostname google.com
```

La commande suivante mappe l'utilisateur null à utilisateur1 avec une adresse IP valide 10.238.2.54/32 :

```
vserver name-mapping create -direction win-unix -position 2 -pattern
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. Utilisez le `vserver name-mapping show` commande pour confirmer le mappage de nom.

```
vserver name-mapping show

Vserver:    vs1
Direction: win-unix
Position Hostname      IP Address/Mask
-----
1          -           10.72.40.83/32      Pattern: anonymous logon
                                   Replacement: user1
```

3. Utilisez le `vserver cifs options modify -win-name-for-null-user` Commande permettant d'attribuer l'appartenance à Windows à l'utilisateur nul.

Cette option est applicable uniquement lorsqu'il existe un mappage de nom valide pour l'utilisateur nul.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. Utilisez le `vserver cifs options show` Commande pour confirmer le mappage de l'utilisateur null à l'utilisateur ou au groupe Windows.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

Gérer les alias NetBIOS des serveurs SMB

Présentation de la gestion des alias NetBIOS des serveurs SMB

Les alias NetBIOS sont des noms alternatifs pour votre serveur SMB que les clients SMB peuvent utiliser lors de la connexion au serveur SMB. La configuration des alias NetBIOS d'un serveur SMB peut être utile lorsque vous regroupez des données provenant d'autres

serveurs de fichiers vers le serveur SMB et que vous souhaitez que le serveur SMB réponde aux noms des serveurs de fichiers d'origine.

Vous pouvez spécifier une liste d'alias NetBIOS lorsque vous créez le serveur SMB ou à tout moment après avoir créé le serveur SMB. Vous pouvez à tout moment ajouter ou supprimer des alias NetBIOS de la liste. Vous pouvez vous connecter au serveur SMB en utilisant l'un des noms de la liste d'alias NetBIOS.

Informations associées

[Affichage des informations relatives à NetBIOS sur connexions TCP](#)

Ajoutez une liste d'alias NetBIOS au serveur SMB

Si vous souhaitez que les clients SMB se connectent au serveur SMB à l'aide d'un alias, vous pouvez créer une liste d'alias NetBIOS ou ajouter des alias NetBIOS à une liste existante d'alias NetBIOS.

Description de la tâche

- Le nom d'alias NetBIOS peut contenir jusqu'à 15 caractères.
- Vous pouvez configurer jusqu'à 200 alias NetBIOS sur le serveur SMB.
- Les caractères suivants ne sont pas autorisés :

@ # * () = + [] | ; : " , < > \ / ?

Étapes

1. Ajoutez les alias NetBIOS:

```
vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases  
NetBIOS_alias,...
```

```
vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases  
alias_1,alias_2,alias_3
```

- Vous pouvez spécifier un ou plusieurs alias NetBIOS à l'aide d'une liste délimitée par des virgules.
- Les alias NetBIOS spécifiés sont ajoutés à la liste existante.
- Une nouvelle liste d'alias NetBIOS est créée si la liste est actuellement vide.

2. Vérifiez que les alias NetBIOS ont été correctement ajoutés : `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

Informations associées

[Suppression des alias NetBIOS de la liste des alias NetBIOS](#)

Supprimez les alias NetBIOS de la liste d'alias NetBIOS

Si vous n'avez pas besoin d'alias NetBIOS spécifiques pour un serveur CIFS, vous pouvez supprimer ces alias NetBIOS de la liste. Vous pouvez également supprimer tous les alias NetBIOS de la liste.

Description de la tâche

Vous pouvez supprimer plusieurs alias NetBIOS à l'aide d'une liste délimitée par des virgules. Vous pouvez supprimer tous les alias NetBIOS d'un serveur CIFS en spécifiant - comme valeur pour le -netbios -aliases paramètre.

Étapes

- 1. Effectuez l'une des opérations suivantes :

Si vous souhaitez supprimer...	Entrer...
Alias NetBIOS spécifiques dans la liste	<code>vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...</code>
Tous les alias NetBIOS de la liste	<code>vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -</code>

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

- 2. Vérifiez que les alias NetBIOS spécifiés ont été supprimés :`vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

Server Name: CIFS_SERVER
NetBIOS Aliases: ALIAS_2, ALIAS_3
```

Afficher la liste des alias NetBIOS sur les serveurs CIFS

Vous pouvez afficher la liste des alias NetBIOS. Cela peut être utile lorsque vous voulez déterminer la liste des noms sur lesquels les clients SMB peuvent établir des connexions au serveur CIFS.

Étape

- 1. Effectuez l'une des opérations suivantes :

Pour afficher des informations sur...	Entrer...
Alias NetBIOS d'un serveur CIFS	<code>vserver cifs show -display-netbios -aliases</code>
La liste des alias NetBIOS dans le cadre des informations détaillées du serveur CIFS	<code>vserver cifs show -instance</code>

L'exemple suivant affiche des informations sur les alias NetBIOS d'un serveur CIFS :

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

L'exemple suivant affiche la liste des alias NetBIOS dans le cadre des informations détaillées du serveur CIFS :

```
vserver cifs show -instance
```

```

Vserver: vs1
CIFS Server NetBIOS Name: CIFS_SERVER
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

Consultez la page man pour les commandes pour plus d'informations.

Informations associées

[Ajout d'une liste d'alias NetBIOS au serveur CIFS](#)

[Commandes pour la gestion des serveurs CIFS](#)

Déterminez si les clients SMB sont connectés à l'aide d'alias NetBIOS

Vous pouvez déterminer si les clients SMB sont connectés à l'aide d'alias NetBIOS et, si oui, quel alias NetBIOS est utilisé pour établir la connexion. Cela peut être utile lors du dépannage des problèmes de connexion.

Description de la tâche

Vous devez utiliser le `-instance` Paramètre pour afficher l’alias NetBIOS (le cas échéant) associé à une connexion SMB. Si le nom du serveur CIFS ou une adresse IP est utilisé pour établir la connexion SMB, la sortie de l’`NetBIOS Name` c’est `-` (tiret).

Étape

- 1. Effectuez l’action souhaitée :

Si vous souhaitez afficher les informations NetBIOS pour...	Entrer...
Connexions SMB	<code>vserver cifs session show -instance</code>
Connexions utilisant un alias NetBIOS spécifié :	<code>vserver cifs session show -instance -netbios-name <i>netbios_name</i></code>

L’exemple suivant affiche des informations sur l’alias NetBIOS utilisé pour établir la connexion SMB avec l’ID de session 1 :

```
vserver cifs session show -session-id 1 -instance
```

```
Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
Workstation: 10.2.2.50
Authentication Mechanism: NTLMv2
Windows User: EXAMPLE\user1
UNIX User: user1
Open Shares: 2
Open Files: 2
Open Other: 0
Connected Time: 1d 1h 10m 5s
Idle Time: 22s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: ALIAS1
SMB Encryption Status: Unencrypted
```

Gérer diverses tâches de serveur SMB

Arrêtez ou démarrez le serveur CIFS

Vous pouvez arrêter le serveur CIFS sur un SVM, ce qui peut être utile lors d’opérations effectuées lorsque les utilisateurs n’accèdent pas aux données via les partages SMB. Vous pouvez redémarrer l’accès SMB en démarrant le serveur CIFS. En arrêtant le serveur CIFS, vous pouvez également modifier les protocoles autorisés sur la machine virtuelle de stockage (SVM).

Étapes

- 1. Effectuez l’une des opérations suivantes :

Les fonctions que vous recherchez...	Entrez la commande...
Arrêtez le serveur CIFS	<code>`vserver cifs stop -vserver vserver_name [-foreground {true</code>
<code>false}]`</code>	Démarrez le serveur CIFS
<code>`vserver cifs start -vserver vserver_name [-foreground {true</code>	<code>false}]`</code>

-foreground indique si la commande doit s’exécuter au premier plan ou en arrière-plan. Si vous ne saisissez pas ce paramètre, il est défini sur true, et la commande est exécutée au premier plan.

- 2. Vérifiez que l’état administratif du serveur CIFS est correct à l’aide du `vserver cifs show` commande.

Exemple

Les commandes suivantes permettent de démarrer le serveur CIFS sur le SVM vs1 :

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
        NetBIOS Domain/Workgroup Name: DOMAIN
                Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                        Authentication Style: domain
                CIFS Server Administrative Status: up
```

Informations associées

- [Affichage des informations sur les serveurs découverts](#)
- [Réinitialisation et détection à nouveau des serveurs](#)

Déplacement des serveurs CIFS vers différents UO

Le processus de création du serveur CIFS utilise les unités organisationnelles (ou) CN=ordinateurs par défaut lors de la configuration, sauf si vous spécifiez une autre unité administrative. Après l'installation, vous pouvez déplacer les serveurs CIFS vers différents UO.

Étapes

1. Sur le serveur Windows, ouvrez l'arborescence **utilisateurs et ordinateurs Active Directory**.
2. Recherchez l'objet Active Directory pour la machine virtuelle de stockage (SVM).
3. Cliquez avec le bouton droit de la souris sur l'objet et sélectionnez **déplacer**.
4. Sélectionnez l'unité d'organisation que vous souhaitez associer à la SVM

Résultats

L'objet SVM est placé dans l'UO sélectionnée.

Modifier le domaine DNS dynamique sur le SVM avant de déplacer le serveur SMB

Si vous souhaitez que le serveur DNS intégré à Active Directory enregistre de manière dynamique les enregistrements DNS du serveur SMB dans DNS lorsque vous déplacez le serveur SMB vers un autre domaine, vous devez modifier DNS dynamique (DDNS) sur la machine virtuelle de stockage (SVM) avant de déplacer le serveur SMB.

Avant de commencer

Les services de nom DNS doivent être modifiés sur le SVM afin d'utiliser le domaine DNS qui contient les enregistrements d'emplacement de service pour le nouveau domaine qui contiendra le compte ordinateur du serveur SMB. Si vous utilisez Secure DDNS, vous devez utiliser des serveurs de noms DNS intégrés à Active Directory.

Description de la tâche

Bien que DDNS (si configuré sur la SVM) ajoute automatiquement les enregistrements DNS des LIFs de données au nouveau domaine, les enregistrements DNS du domaine d'origine ne sont pas automatiquement supprimés du serveur DNS d'origine. Vous devez les supprimer manuellement.

Pour effectuer les modifications DDNS avant de déplacer le serveur SMB, reportez-vous à la rubrique suivante :

["Configuration des services DNS dynamiques"](#)

Rejoignez un SVM vers un domaine Active Directory

Vous pouvez associer une machine virtuelle de stockage (SVM) à un domaine Active Directory sans supprimer le serveur SMB existant en modifiant le domaine à l'aide de `vserver cifs modify` commande. Vous pouvez rejoindre à nouveau le domaine actuel ou en rejoindre un nouveau.

Avant de commencer

- Le SVM doit déjà disposer d'une configuration DNS.
- La configuration DNS pour le SVM doit pouvoir représenter le domaine cible.

Les serveurs DNS doivent contenir les enregistrements SRV (Service Location Records) pour les serveurs LDAP de domaine et de contrôleur de domaine.

Description de la tâche

- Le statut administratif du serveur CIFS doit être défini sur "deown" pour pouvoir procéder à la modification du domaine Active Directory.
- Si la commande s'exécute avec succès, le statut administratif est automatiquement défini sur « actif ».
- Lorsque vous rejoignez un domaine, cette commande peut prendre plusieurs minutes.

Étapes

1. Relier le SVM au domaine du serveur CIFS : `vserver cifs modify -vserver vserver_name -domain domain_name -status-admin down`

Pour plus d'informations, consultez la page de manuel du `vserver cifs modify` commande. Si vous devez reconfigurer le DNS pour le nouveau domaine, reportez-vous à la page de manuel de l' `vserver dns modify` commande.

Pour créer un compte de machine Active Directory pour le serveur SMB, vous devez fournir le nom et le mot de passe d'un compte Windows disposant des privilèges suffisants pour ajouter des ordinateurs à l' ou= *example* ou conteneur dans le *example* domaine .com.

À partir de ONTAP 9.7, votre administrateur AD peut vous fournir un URI vers un fichier keytab comme alternative à vous fournir un nom et un mot de passe à un compte Windows privilégié. Lorsque vous recevez l'URI, l'inclure dans le `-keytab-uri` paramètre avec le `vserver cifs` commandes.

2. Vérifiez que le serveur CIFS se trouve dans le domaine Active Directory souhaité : `vserver cifs show`

Exemple

Dans l'exemple suivant, le serveur SMB « CIFSSERVER1 » sur le SVM vs1 rejoint le domaine example.com à l'aide de keytab Authentication :

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab
```

```
cluster1::> vserver cifs show
```

	Server	Status	Domain/Workgroup	Authentication
Vserver	Name	Admin	Name	Style
-----	-----	-----	-----	-----
vs1	CIFSSERVER1	up	EXAMPLE	domain

Affiche des informations sur NetBIOS sur connexions TCP

Vous pouvez afficher des informations sur les connexions NetBIOS sur TCP (NBT). Cela peut être utile lors du dépannage des problèmes liés au NetBIOS.

Étape

1. Utilisez le `vserver cifs nbtstat` Commande pour afficher les informations relatives à NetBIOS sur

connexions TCP.



Le service de noms NetBIOS (NNBNS) sur IPv6 n'est pas pris en charge.

Exemple

L'exemple suivant montre les informations relatives au service de nom NetBIOS affichées pour « cluster1 » :

```
cluster1::> vserver cifs nbtstat

Vserver: vs1
Node:    cluster1-01
Interfaces:
          10.10.10.32
          10.10.10.33
Servers:
          17.17.1.2  (active  )
NBT Scope:
          [ ]
NBT Mode:
          [h]
NBT Name      NetBIOS Suffix  State   Time Left   Type
-----
CLUSTER_1     00                wins    57
CLUSTER_1     20                wins    57

Vserver: vs1
Node:    cluster1-02
Interfaces:
          10.10.10.35
Servers:
          17.17.1.2  (active  )
CLUSTER_1     00                wins    58
CLUSTER_1     20                wins    58
4 entries were displayed.
```

Commandes pour la gestion des serveurs SMB

Vous devez connaître les commandes pour créer, afficher, modifier, arrêter, démarrer, Et suppression des serveurs SMB. Il existe également des commandes permettant de réinitialiser et de redécouvrir les serveurs, de modifier ou de réinitialiser les mots de passe des comptes machine, de planifier des modifications pour les mots de passe des comptes machine et d'ajouter ou de supprimer des alias NetBIOS.

Les fonctions que vous recherchez...

Utilisez cette commande...

Créez un serveur SMB	<code>vserver cifs create</code>
Affiche les informations relatives à un serveur SMB	<code>vserver cifs show</code>
Modifier un serveur SMB	<code>vserver cifs modify</code>
Déplacer un serveur SMB vers un autre domaine	<code>vserver cifs modify</code>
Arrêtez un serveur SMB	<code>vserver cifs stop</code>
Démarrez un serveur SMB	<code>vserver cifs start</code>
Supprimez un serveur SMB	<code>vserver cifs delete</code>
Réinitialisez et redécouvrez les serveurs pour le serveur SMB	<code>vserver cifs domain discovered-servers reset-servers</code>
Modifier le mot de passe du compte machine du serveur SMB	<code>vserver cifs domain password change</code>
Réinitialisez le mot de passe du compte machine du serveur SMB	<code>vserver cifs domain password change</code>
Planifier les modifications automatiques du mot de passe pour le compte machine du serveur SMB	<code>vserver cifs domain password schedule modify</code>
Ajoutez des alias NetBIOS pour le serveur SMB	<code>vserver cifs add-netbios-aliases</code>
Supprimez les alias NetBIOS du serveur SMB	<code>vserver cifs remove-netbios-aliases</code>

Consultez la page man pour chaque commande pour plus d'informations.

Informations associées

["Ce qui se passe pour les utilisateurs et les groupes locaux lors de la suppression des serveurs SMB"](#)

Activez le service de noms NetBIOS

À partir de ONTAP 9, le service de noms NetBIOS (NBNS, parfois appelé Windows Internet Name Service ou WINS) est désactivé par défaut. Auparavant, les machines virtuelles de stockage compatibles CIFS (SVM) envoyaient des diffusions d'enregistrement de noms, même si WINS était activé sur un réseau. Pour limiter ces diffusions à des configurations où NBNS est nécessaire, vous devez activer explicitement NBNS pour les nouveaux serveurs CIFS.

Avant de commencer

- Si vous utilisez déjà NBNS et que vous effectuez une mise à niveau vers ONTAP 9, il n'est pas nécessaire d'effectuer cette tâche. NBNS continuera de fonctionner comme précédemment.
- NBNS est activé sur UDP (port 137).
- NBNS sur IPv6 n'est pas pris en charge.

Étapes

1. Définissez le niveau de privilège sur avancé.

```
set -privilege advanced
```

2. Activez NBNS sur un serveur CIFS.

```
vserver cifs options modify -vserver <vserver name> -is-nbns-enabled true
```

3. Revenir au niveau de privilège admin.

```
set -privilege admin
```

Utilisez IPv6 pour l'accès SMB et les services SMB

Conditions d'utilisation d'IPv6

Avant de pouvoir utiliser IPv6 sur votre serveur SMB, vous devez connaître les versions de ONTAP et SMB qui la prennent en charge et les exigences de licence.

Conditions requises pour les licences ONTAP

Aucune licence spéciale n'est requise pour IPv6 lorsque SMB est sous licence. La licence SMB est incluse avec "ONTAP One". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.

Version requise du protocole SMB

- Pour les SVM, ONTAP prend en charge IPv6 sur toutes les versions du protocole SMB.



Le service de noms NetBIOS (NNBNS) sur IPv6 n'est pas pris en charge.

Prise en charge d'IPv6 avec accès SMB et services CIFS

Si vous souhaitez utiliser IPv6 sur votre serveur CIFS, vous devez savoir comment ONTAP prend en charge IPv6 pour l'accès SMB et la communication réseau pour les services CIFS.

Prise en charge des serveurs et des clients Windows

ONTAP prend en charge les serveurs et clients Windows prenant en charge IPv6. La section suivante décrit la prise en charge du protocole IPv6 du serveur et du client Microsoft Windows :

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 et versions ultérieures prennent en charge IPv6 à la fois pour le partage de fichiers SMB et les services Active Directory, notamment les services DNS, LDAP, CLDAP et Kerberos.

Si les adresses IPv6 sont configurées, les versions Windows 7 et Windows Server 2008 et ultérieures utilisent IPv6 par défaut pour les services Active Directory. Les authentifications NTLM et Kerberos sur des connexions IPv6 sont prises en charge.

Tous les clients Windows pris en charge par ONTAP peuvent se connecter à des partages SMB à l'aide d'adresses IPv6.

Pour obtenir les informations les plus récentes sur les clients Windows pris en charge par ONTAP, reportez-vous au "[Matrice d'interopérabilité](#)".



Les domaines NT ne sont pas pris en charge pour IPv6.

Prise en charge supplémentaire de services CIFS

Outre la prise en charge IPv6 pour les partages de fichiers SMB et les services Active Directory, ONTAP prend en charge plusieurs protocoles :

- Services côté client, y compris les dossiers hors ligne, les profils itinérants, la redirection de dossiers et les versions précédentes
- Services côté serveur, y compris les répertoires locaux dynamiques (fonctionnalité Home Directory), les symlinks et les Widelinks, BranchCache, ODX, load des copies ODX, référencements automatiques des nœuds, Et versions précédentes
- Services de gestion de l'accès aux fichiers, y compris l'utilisation d'utilisateurs et de groupes Windows locaux pour le contrôle d'accès et la gestion des droits, la définition des autorisations de fichiers et des stratégies d'audit à l'aide de la CLI, le suivi de la sécurité, la gestion des verrous de fichiers et la surveillance de l'activité SMB
- Audit multiprotocole NAS
- FPolicy
- Partages disponibles en continu, protocole Witness et VSS distant (utilisés avec les configurations Hyper-V sur SMB)

Prise en charge du service d'authentification et du service de noms

La communication avec les services de noms suivants est prise en charge par IPv6 :

- Contrôleurs de domaine
- Serveurs DNS
- Serveurs LDAP
- Serveurs KDC
- Serveurs NIS

Pour créer une configuration qui répond à vos exigences, vous devez savoir comment les serveurs CIFS utilisent IPv6 lors de connexions à des serveurs externes.

- Sélection de l'adresse source

Si une tentative de connexion à un serveur externe est effectuée, l'adresse source sélectionnée doit être du même type que l'adresse de destination. Par exemple, si vous vous connectez à une adresse IPv6, la machine virtuelle de stockage (SVM) hébergeant le serveur CIFS doit disposer d'une LIF de données ou d'une LIF de gestion dont l'adresse IPv6 est à utiliser comme adresse source. De la même manière, en cas de connexion à une adresse IPv4, le SVM doit disposer d'une LIF de données ou d'une LIF de gestion qui possède une adresse IPv4 à utiliser comme adresse source.

- Pour les serveurs découverts dynamiquement à l'aide de DNS, la découverte de serveur s'effectue comme suit :

- Si IPv6 est désactivé sur le cluster, seules les adresses des serveurs IPv4 sont découvertes.
- Si IPv6 est activé sur le cluster, les adresses des serveurs IPv4 et IPv6 sont découvertes. L'un ou l'autre type peut être utilisé en fonction de l'adéquation du serveur auquel appartient l'adresse et de la disponibilité des LIF de gestion ou des données IPv6 ou IPv4.
La découverte de serveurs dynamiques est utilisée pour découvrir les contrôleurs de domaine et leurs services associés, tels que LSA, NETLOGON, Kerberos et LDAP.

- Connectivité du serveur DNS

Si le SVM utilise IPv6 lors de la connexion à un serveur DNS dépend de la configuration des services de noms DNS. Si les services DNS sont configurés pour utiliser des adresses IPv6, les connexions sont effectuées à l'aide d'IPv6. Si vous le souhaitez, la configuration des services de noms DNS peut utiliser des adresses IPv4 afin que les connexions aux serveurs DNS continuent d'utiliser des adresses IPv4. Des combinaisons d'adresses IPv4 et IPv6 peuvent être spécifiées lors de la configuration des services de noms DNS.

- Connectivité du serveur LDAP

Si le SVM utilise IPv6 lors de la connexion à un serveur LDAP dépend de la configuration du client LDAP. Si le client LDAP est configuré pour utiliser des adresses IPv6, les connexions sont effectuées à l'aide d'IPv6. Si vous le souhaitez, la configuration du client LDAP peut utiliser des adresses IPv4 pour que les connexions aux serveurs LDAP continuent d'utiliser des adresses IPv4. Des combinaisons d'adresses IPv4 et IPv6 peuvent être spécifiées lors de la configuration du client LDAP.



La configuration du client LDAP est utilisée lors de la configuration de LDAP pour les services d'utilisateur, de groupe et de nom de groupe de réseau UNIX.

- Connectivité serveur NIS

La question de savoir si le SVM utilise IPv6 lors de la connexion à un serveur NIS dépend de la configuration des services de nom NIS. Si les services NIS sont configurés pour utiliser des adresses IPv6, les connexions sont effectuées à l'aide d'IPv6. Si vous le souhaitez, la configuration des services de noms NIS peut utiliser des adresses IPv4 pour que les connexions aux serveurs NIS continuent d'utiliser des adresses IPv4. Des combinaisons d'adresses IPv4 et IPv6 peuvent être spécifiées lors de la configuration de services de noms NIS.



Les services de noms NIS sont utilisés pour stocker et gérer des objets de nom d'utilisateur, de groupe, de groupe et d'hôte UNIX.

Informations associées

[Activation d'IPv6 pour SMB \(administrateurs du cluster uniquement\)](#)

[Contrôle et affichage des informations relatives aux sessions SMB IPv6](#)

Activer IPv6 pour SMB (administrateurs du cluster uniquement)

Les réseaux IPv6 ne sont pas activés lors de la configuration du cluster. Un administrateur de cluster doit activer IPv6 une fois l'installation du cluster terminée pour utiliser IPv6 pour SMB. Lorsque l'administrateur de cluster active IPv6, il est activé pour l'ensemble du cluster.

Étape

1. Activer IPv6 : `network options ipv6 modify -enabled true`

Pour plus d'informations sur l'activation d'IPv6 sur le cluster et la configuration des LIF IPv6, reportez-vous au *Network Management Guide*.

IPv6 est activé. Les LIF de données IPv6 pour un accès SMB peuvent être configurées.

Informations associées

[Contrôle et affichage des informations relatives aux sessions SMB IPv6](#)

["Gestion du réseau"](#)

Désactivation de IPv6 pour SMB

Bien que IPv6 soit activé sur le cluster à l'aide d'une option réseau, vous ne pouvez pas désactiver IPv6 pour SMB en utilisant la même commande. En revanche, ONTAP désactive IPv6 lorsque l'administrateur de cluster désactive la dernière interface compatible IPv6 sur le cluster. Vous devez communiquer avec l'administrateur du cluster pour obtenir des informations sur la gestion de vos interfaces compatibles IPv6.

Pour plus d'informations sur la désactivation d'IPv6 sur le cluster, reportez-vous au *Network Management Guide*.

Informations associées

["Gestion du réseau"](#)

Contrôle et affichage des informations relatives aux sessions SMB IPv6

Vous pouvez contrôler et afficher des informations relatives aux sessions SMB connectées via les réseaux IPv6. Ces informations sont utiles pour déterminer quels clients se connectent à l'aide d'IPv6 ainsi que d'autres informations utiles sur les sessions SMB IPv6.

Étape

1. Effectuez l'action souhaitée :

Si vous voulez déterminer si...	Entrez la commande...
Les sessions SMB vers une machine virtuelle de stockage (SVM) sont connectées via IPv6	<pre>vserver cifs session show -vserver vserver_name -instance</pre>
IPv6 est utilisé pour les sessions SMB via une adresse LIF spécifiée	<pre>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance</pre> <p><i>LIF_IP_address</i> Est l'adresse IPv6 de la LIF de données.</p>

Configurez l'accès aux fichiers à l'aide de SMB

Configurer les styles de sécurité

Comment les styles de sécurité affectent l'accès aux données

Styles de sécurité et leurs effets

Il existe quatre styles de sécurité différents : UNIX, NTFS, mixte et unifié. Chaque style de sécurité a un effet différent sur la façon dont les autorisations sont traitées pour les données. Vous devez comprendre les différents effets pour vous assurer que vous sélectionnez le style de sécurité approprié à vos fins.

Il est important de comprendre que les styles de sécurité ne déterminent pas quels types de clients peuvent ou ne peuvent pas accéder aux données. Les styles de sécurité déterminent uniquement le type d'autorisations que ONTAP utilise pour contrôler l'accès aux données et le type de client pouvant modifier ces autorisations.

Par exemple, si un volume utilise le style de sécurité UNIX, les clients SMB peuvent toujours accéder aux données (à condition qu'ils s'authentifient et autorisent correctement) en raison de la nature multiprotocole de ONTAP. Toutefois, ONTAP utilise des autorisations UNIX que seuls les clients UNIX peuvent modifier à l'aide d'outils natifs.

Style de sécurité	Clients pouvant modifier des autorisations	Autorisations que les clients peuvent utiliser	Un style de sécurité efficace	Clients pouvant accéder aux fichiers
UNIX	NFS	Bits de mode NFSv3	UNIX	NFS et SMB
		Listes de contrôle d'accès NFSv4.x		
NTFS	PME	ALC NTFS	NTFS	
Mixte	NFS ou SMB	Bits de mode NFSv3	UNIX	
		ACL.NFSv4		
		ALC NTFS	NTFS	
Unifiée (Pour Infinite volumes uniquement, dans ONTAP 9.4 et les versions antérieures.)	NFS ou SMB	Bits de mode NFSv3	UNIX	
		ACL NFSv4.1		
		ALC NTFS	NTFS	

Les volumes FlexVol prennent en charge les styles de sécurité UNIX, NTFS et mixte. Lorsque le style de sécurité est mixte ou unifié, les autorisations effectives dépendent du type de client qui a modifié les autorisations pour la dernière fois, car les utilisateurs définissent le style de sécurité sur une base individuelle. Si le dernier client ayant modifié des autorisations était un client NFSv3, les autorisations sont des bits en mode UNIX NFSv3. Si le dernier client était un client NFSv4, les autorisations sont définies comme listes de contrôle d'accès NFSv4. Si le dernier client était un client SMB, les autorisations sont des listes de contrôle d'accès Windows NTFS.

La méthode de sécurité unifiée est uniquement disponible avec des volumes infinis, qui ne sont plus pris en charge dans ONTAP 9.5 et versions ultérieures. Pour plus d'informations, voir [Présentation de la gestion des volumes FlexGroup](#).

À partir de ONTAP 9.2, le `show-effective-permissions` paramètre au `vserver security file-directory` La commande vous permet d'afficher les autorisations effectives accordées à un utilisateur Windows ou UNIX sur le chemin d'accès au fichier ou au dossier spécifié. De plus, le paramètre facultatif `-share-name` vous permet d'afficher l'autorisation de partage effective.



ONTAP définit au départ certaines autorisations de fichier par défaut. Par défaut, le style de sécurité effectif sur toutes les données des volumes de style de sécurité UNIX, mixte et unifié est UNIX et le type d'autorisation effectif est bits de mode UNIX (0755 sauf indication contraire) jusqu'à ce qu'un client soit configuré comme autorisé par le style de sécurité par défaut. Par défaut, le style de sécurité effectif sur toutes les données des volumes de style de sécurité NTFS est NTFS et dispose d'une liste de contrôle d'accès permettant un contrôle total à tous.

Où et quand définir les styles de sécurité

Les styles de sécurité peuvent être définis sur les volumes FlexVol (volumes root ou de données) et les qtrees. Les styles de sécurité peuvent être définis manuellement au moment de la création, hérités automatiquement ou modifiés ultérieurement.

Choisissez le style de sécurité à utiliser sur les SVM

Pour vous aider à choisir le style de sécurité à utiliser sur un volume, vous devez tenir compte de deux facteurs. Le facteur principal est le type d'administrateur qui gère le système de fichiers. Le facteur secondaire désigne le type d'utilisateur ou de service qui accède aux données du volume.

Lorsque vous configurez le style de sécurité sur un volume, vous devez tenir compte des besoins de votre environnement pour vous assurer que vous sélectionnez le meilleur style de sécurité et éviter les problèmes liés à la gestion des autorisations. Vous pouvez décider des considérations suivantes :

Style de sécurité	Choisissez si...
UNIX	<ul style="list-style-type: none">• Le système de fichiers est géré par un administrateur UNIX.• La plupart des utilisateurs sont des clients NFS.• Une application accédant aux données utilise un utilisateur UNIX comme compte de service.
NTFS	<ul style="list-style-type: none">• Le système de fichiers est géré par un administrateur Windows.• La majorité des utilisateurs sont des clients SMB.• Une application accédant aux données utilise un utilisateur Windows comme compte de service.
Mixte	Le système de fichiers est géré à la fois par les administrateurs et utilisateurs d'UNIX et de Windows, et il se compose de clients NFS et SMB.

Fonctionnement de l'héritage du style de sécurité

Si vous ne spécifiez pas le style de sécurité lors de la création d'un nouveau volume FlexVol ou d'un qtree, il hérite de son style de sécurité de différentes manières.

Les styles de sécurité sont hérités de la manière suivante :

- Un volume FlexVol hérite du style de sécurité du volume root de son SVM contenant.
- Un qtree hérite du style de sécurité de son volume FlexVol.
- Un fichier ou un répertoire hérite du style de sécurité de son volume FlexVol ou qtree.

Comment ONTAP préserve les autorisations UNIX

Lorsque les fichiers d'un volume FlexVol qui disposent actuellement d'autorisations UNIX sont modifiés et enregistrés par des applications Windows, ONTAP peut préserver les autorisations UNIX.

Lorsque des applications sur des clients Windows modifient et enregistrent des fichiers, elles lisent les propriétés de sécurité du fichier, créent un nouveau fichier temporaire, appliquent ces propriétés au fichier

temporaire, puis donnent au fichier temporaire le nom du fichier d'origine.

Lorsque les clients Windows effectuent une requête pour les propriétés de sécurité, ils reçoivent une ACL construite qui représente exactement les autorisations UNIX. Le seul but de cette liste de contrôle d'accès construite est de préserver les autorisations UNIX du fichier lorsque les fichiers sont mis à jour par les applications Windows pour s'assurer que les fichiers résultants ont les mêmes autorisations UNIX. ONTAP ne définit pas d'ACL NTFS à l'aide de la liste de contrôle d'accès construite.

Gérez les autorisations UNIX à l'aide de l'onglet sécurité Windows

Si vous souhaitez manipuler les autorisations UNIX de fichiers ou de dossiers dans des volumes ou des qtree de style sécurité mixtes sur des SVM, vous pouvez utiliser l'onglet sécurité sur les clients Windows. Vous pouvez également utiliser des applications qui peuvent interroger et définir des listes de contrôle d'accès Windows.

- **Modification des autorisations UNIX**

Vous pouvez utiliser l'onglet sécurité Windows pour afficher et modifier les autorisations UNIX pour un volume ou qtree de style de sécurité mixte. Si vous utilisez l'onglet principal sécurité Windows pour modifier les autorisations UNIX, vous devez d'abord supprimer l'ACE que vous souhaitez modifier (ceci définit les bits de mode sur 0) avant d'effectuer vos modifications. Vous pouvez également utiliser l'éditeur avancé pour modifier les autorisations.

Si des autorisations de mode sont utilisées, vous pouvez modifier directement les autorisations de mode pour l'UID, le GID et d'autres (tous les autres utilisateurs disposant d'un compte sur l'ordinateur). Par exemple, si l'UID affiché possède des autorisations r-x, vous pouvez modifier les autorisations UID sur rwx.

- **Modification des autorisations UNIX en autorisations NTFS**

Vous pouvez utiliser l'onglet sécurité Windows pour remplacer les objets de sécurité UNIX par des objets de sécurité Windows sur un volume ou qtree de style de sécurité mixte, où les fichiers et les dossiers ont une méthode de sécurité efficace UNIX.

Vous devez d'abord supprimer toutes les entrées d'autorisation UNIX répertoriées pour pouvoir les remplacer par les objets utilisateur et groupe Windows souhaités. Vous pouvez ensuite configurer des listes de contrôle d'accès NTFS sur les objets utilisateur et groupe Windows. En supprimant tous les objets de sécurité UNIX et en ajoutant uniquement des utilisateurs et des groupes Windows à un fichier ou à un dossier dans un volume ou qtree de style de sécurité mixte, vous modifiez le style de sécurité effectif sur le fichier ou le dossier d'UNIX à NTFS.

Lors de la modification des autorisations sur un dossier, le comportement par défaut de Windows consiste à propager ces modifications à tous les sous-dossiers et fichiers. Par conséquent, vous devez modifier le choix de propagation sur le paramètre souhaité si vous ne souhaitez pas propager de modification du style de sécurité à tous les dossiers, sous-dossiers et fichiers enfants.

Configurer des styles de sécurité sur les volumes root SVM

Il configure la style de sécurité du volume root de la machine virtuelle de stockage (SVM) afin de déterminer le type d'autorisations utilisées pour les données sur le volume root de la SVM.

Étapes

1. Utilisez le `vserver create` commande avec `-rootvolume-security-style` paramètre pour définir

le style de sécurité.

Les options possibles pour le style de sécurité du volume racine sont `unix`, `ntfs`, ou `mixed`.

2. Afficher et vérifier la configuration, y compris le style de sécurité du volume root du SVM que vous avez créé : `vserver show -vserver vserver_name`

Configurer des styles de sécurité sur les volumes FlexVol

Configurez le style de sécurité des volumes FlexVol afin de déterminer le type d'autorisations utilisées pour les données sur des volumes FlexVol de la machine virtuelle de stockage (SVM).

Étapes

1. Effectuez l'une des opérations suivantes :

Si le volume FlexVol...	Utilisez la commande...
N'existe pas encore	<code>volume create</code> et inclure le <code>-security-style</code> paramètre pour spécifier le style de sécurité.
Existe déjà	<code>volume modify</code> et inclure le <code>-security-style</code> paramètre pour spécifier le style de sécurité.

Les options possibles pour le style de sécurité du volume FlexVol sont `unix`, `ntfs`, ou `mixed`.

Si vous ne spécifiez pas de style de sécurité lors de la création d'un volume FlexVol, le volume hérite du style de sécurité du volume racine.

Pour plus d'informations sur le `volume create` ou `volume modify` commandes, voir "[Gestion du stockage logique](#)".

2. Pour afficher la configuration, en incluant le style de sécurité du volume FlexVol que vous avez créé, entrez la commande suivante :

```
volume show -volume volume_name -instance
```

Configurer des styles de sécurité sur les qtrees

Vous configurez le style de sécurité du volume qtree afin de déterminer le type d'autorisations utilisées pour les données sur des qtrees.

Étapes

1. Effectuez l'une des opérations suivantes :

Si le qtree...	Utilisez la commande...
N'existe pas encore	<code>volume qtree create</code> et inclure le <code>-security-style</code> paramètre pour spécifier le style de sécurité.

Si le qtree...	Utilisez la commande...
Existe déjà	<code>volume qtree modify</code> et inclure le <code>-security -style</code> paramètre pour spécifier le style de sécurité.

Les options possibles pour la méthode de sécurité qtree sont `unix`, `ntfs`, ou `mixed`.

Si vous ne spécifiez pas de style de sécurité lors de la création d'un qtree, le style de sécurité par défaut est `mixed`.

Pour plus d'informations sur le `volume qtree create` ou `volume qtree modify` commandes, voir ["Gestion du stockage logique"](#).

2. Pour afficher la configuration, y compris le style de sécurité du qtree que vous avez créé, entrez la commande suivante : `volume qtree show -qtree qtree_name -instance`

Création et gestion des volumes de données dans les espaces de noms NAS

Créer et gérer des volumes de données dans les espaces de noms NAS

Pour gérer l'accès aux fichiers dans un environnement NAS, vous devez gérer les volumes et les points de jonction des données sur votre SVM (Storage Virtual machine). Cela inclut la planification de votre architecture d'espace de noms, la création de volumes avec ou sans points de jonction, le montage ou le démontage de volumes, et l'affichage des informations sur les volumes de données et les serveurs NFS ou les espaces de noms de serveurs CIFS.

Créez des volumes de données avec des points de jonction spécifiés

Vous pouvez spécifier le point de jonction lorsque vous créez un volume de données. Le volume ainsi obtenu est automatiquement monté au point de jonction et est immédiatement disponible pour la configuration pour l'accès NAS.

Avant de commencer

L'agrégat dans lequel vous souhaitez créer le volume doit déjà exister.



Les caractères suivants ne peuvent pas être utilisés dans le chemin de jonction : `* # " > < | ? \`

De plus, la longueur du chemin de jonction ne peut pas dépasser 255 caractères.

Étapes

1. Créer le volume avec un point de jonction : `volume create -vserver vservice_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path junction_path`

Le chemin de jonction doit commencer par la racine (`/`) et peut contenir à la fois des répertoires et des volumes reliés. Il n'est pas nécessaire que la Junction path contienne le nom du volume. Les Junction paths sont indépendants du nom du volume.

La spécification d'un style de sécurité de volume est facultative. Si vous ne spécifiez pas de style de sécurité, ONTAP crée le volume avec le même style de sécurité que celui appliqué au volume racine de la machine virtuelle de stockage (SVM). Cependant, le style de sécurité du volume racine n'est peut-être pas celui que vous souhaitez appliquer au volume de données que vous créez. Il est recommandé de spécifier le style de sécurité lors de la création du volume afin de minimiser les problèmes d'accès aux fichiers difficiles à résoudre.

Le chemin de jonction n'est pas sensible à la casse ; /ENG est identique à /eng. Si vous créez un partage CIFS, Windows traite le chemin de jonction comme s'il est sensible à la casse. Par exemple, si la jonction est de /ENG, Le chemin d'un partage CIFS doit commencer par /ENG`pas `/eng.

De nombreux paramètres facultatifs peuvent être utilisés pour personnaliser un volume de données. Pour en savoir plus, consultez les pages de manuel pour le `volume create` commande.

2. Vérifier que le volume a été créé avec le point de jonction souhaité : `volume show -vserver vs1 -volume volume_name -junction`

Exemple

L'exemple suivant crée un volume nommé « maison 4 » situé sur le SVM vs1 qui a une Junction path /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	home4	true	/eng/home	RW_volume

Créez des volumes de données sans spécifier de points de jonction

Vous pouvez créer un volume de données sans spécifier de point de jonction. Le volume résultant n'est pas monté automatiquement et n'est pas disponible pour configurer l'accès NAS. Vous devez monter le volume avant de configurer les partages SMB ou les exportations NFS pour ce volume.

Avant de commencer

L'agrégat dans lequel vous souhaitez créer le volume doit déjà exister.

Étapes

1. Créer le volume sans point de jonction en utilisant la commande suivante : `volume create -vserver vs1 -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

La spécification d'un style de sécurité de volume est facultative. Si vous ne spécifiez pas de style de sécurité, ONTAP crée le volume avec le même style de sécurité que celui appliqué au volume racine de la machine virtuelle de stockage (SVM). Toutefois, le style de sécurité du volume racine n'est peut-être pas

celui que vous souhaitez appliquer au volume de données. Il est recommandé de spécifier le style de sécurité lors de la création du volume afin de minimiser les problèmes d'accès aux fichiers difficiles à résoudre.

De nombreux paramètres facultatifs peuvent être utilisés pour personnaliser un volume de données. Pour en savoir plus, consultez les pages de manuel pour le `volume create` commande.

2. Vérifier que le volume a été créé sans point de jonction : `volume show -vserver vs1 -volume volume_name -junction`

Exemple

L'exemple suivant crée un volume nommé « sales » situé sur la SVM vs1 qui n'est pas monté à un point de jonction :

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

		Junction		Junction
Vserver	Volume	Active	Junction Path	Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	-	-	-

Montez ou démontez les volumes existants dans l'espace de noms NAS

Un volume doit être monté sur le namespace NAS avant de pouvoir configurer l'accès des clients NAS aux données contenues dans les volumes SVM (Storage Virtual machine). Vous pouvez monter un volume sur un point de jonction s'il n'est pas actuellement monté. Vous pouvez également démonter des volumes.

Description de la tâche

Si vous démontez et mettez un volume hors ligne, toutes les données du point de jonction, y compris les données des volumes dont les points de jonction se trouvent dans l'espace de noms du volume non monté, sont inaccessibles aux clients NAS.



Pour interrompre l'accès client NAS à un volume, il ne suffit pas de démonter le volume. Vous devez mettre le volume hors ligne ou prendre d'autres mesures pour vous assurer que les caches de descripteur de fichier côté client sont invalidés. Pour plus d'informations, consultez l'article suivant de la base de connaissances : ["Les clients NFSv3 ont toujours accès à un volume après avoir été supprimés du namespace dans ONTAP"](#)

Lorsque vous démontez et mettez un volume hors ligne, les données du volume ne sont pas perdues. En outre, les règles d'exportation de volume et les partages SMB créés sur le volume ou sur des répertoires et des points de jonction au sein du volume démonté sont conservés. Si vous remontez le volume démonté, les clients NAS peuvent accéder aux données contenues dans le volume à l'aide des règles d'exportation et des

partages SMB existants.

Étapes

1. Effectuez l'action souhaitée :

Les fonctions que vous recherchez...	Entrez les commandes...
Montez un volume	<code>volume mount -vserver svm_name -volume volume_name -junction-path junction_path</code>
Démonter un volume	<code>volume unmount -vserver svm_name -volume volume_name</code> <code>volume offline -vserver svm_name -volume volume_name</code>

2. Vérifiez que le volume est dans l'état de montage souhaité :

```
volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active
```

Exemples

L'exemple suivant monte un volume nommé « ventes » situé sur la SVM « vs1 » au point de jonction « /ventes » :

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver    volume    state    junction-path    junction-active
-----
vs1         data      online   /data            true
vs1         home4     online   /eng/home        true
vs1         sales     online   /sales           true
```

L'exemple suivant démonte et met hors ligne un volume nommé « data' » situé sur le SVM « vs1 » :

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active
```

vserver	volume	state	junction-path	junction-active
vs1	data	offline	-	-
vs1	home4	online	/eng/home	true
vs1	sales	online	/sales	true

Affiche les informations sur le montage du volume et le point de jonction

Vous pouvez afficher des informations sur les volumes montés pour les SVM et les points de jonction auxquels les volumes sont montés. Vous pouvez également déterminer quels volumes ne sont pas montés sur un point de jonction. Vous pouvez utiliser ces informations pour comprendre et gérer votre namespace SVM.

Étapes

1. Effectuez l'action souhaitée :

Si vous voulez afficher...	Entrez la commande...
Récapitulatif des informations sur les volumes montés et démontés sur le SVM	<code>volume show -vserver vs1 -junction</code>
Informations détaillées sur les volumes montés et démontés sur le SVM	<code>volume show -vserver vs1 -volume volume_name -instance</code>
Informations spécifiques sur les volumes montés et démontés sur le SVM	<p>a. Si nécessaire, vous pouvez afficher des champs valides pour l' <code>-fields</code> paramètre via la commande suivante : <code>volume show -fields ?</code></p> <p>b. Afficher les informations souhaitées à l'aide de l' <code>-fields</code> paramètre : <code>volume show -vserver vs1 -champs fieldname,...</code></p>

Exemples

L'exemple suivant affiche un récapitulatif des volumes montés et démontés sur le SVM vs1 :

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	true	/sales	RW_volume

L'exemple suivant affiche des informations sur les champs spécifiés pour les volumes situés sur le SVM vs2 :

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
```

vserver	volume	aggregate	size	state	type	security-style	junction-path	junction-parent	node
vs2	data1	aggr3	2GB	online	RW	unix	-	-	node3
vs2	data2	aggr3	1GB	online	RW	ntfs	/data2		
vs2	data2_1	aggr3	8GB	online	RW	ntfs	/data2/d2_1		
vs2	data2_2	aggr3	8GB	online	RW	ntfs	/data2/d2_2		
vs2	pubs	aggr1	1GB	online	RW	unix	/publications		
vs2	images	aggr3	2TB	online	RW	ntfs	/images		
vs2	logs	aggr1	1GB	online	RW	unix	/logs		
vs2	vs2_root	aggr3	1GB	online	RW	ntfs	/	-	node3

Configurez les mappages de noms

Présentation de la configuration des mappages de noms

ONTAP fait appel au mappage de noms pour mapper les identités CIFS aux identités UNIX, les identités Kerberos aux identités UNIX et les identités UNIX aux identités CIFS. Il a besoin de ces informations pour obtenir les informations d'identification des utilisateurs et fournir un accès approprié aux fichiers, qu'ils se connectent à partir d'un client NFS ou d'un client CIFS.

Il existe deux exceptions lorsque vous n'avez pas besoin d'utiliser le mappage de noms :

- Vous configurez un environnement UNIX pur et ne prévoyez pas d'utiliser l'accès CIFS ou le style de sécurité NTFS sur les volumes.
- Vous configurez l'utilisateur par défaut à utiliser à la place.

Dans ce scénario, le mappage de noms n'est pas nécessaire car au lieu de mapper chaque identifiant client individuel, toutes les informations d'identification client sont mappées au même utilisateur par défaut.

Notez que vous pouvez utiliser le mappage de noms uniquement pour les utilisateurs, pas pour les groupes.

Toutefois, vous pouvez mapper un groupe d'utilisateurs individuels à un utilisateur spécifique. Par exemple, vous pouvez mapper tous les utilisateurs AD qui commencent ou se terminent par le mot VENTES à un utilisateur UNIX spécifique et à l'UID de l'utilisateur.

Fonctionnement du mappage de noms

Lorsque ONTAP doit mapper les informations d'identification d'un utilisateur, il recherche tout d'abord un mappage existant dans la base de données de mappage de noms locaux et le serveur LDAP. Qu'elle vérifie un ou les deux et dans quel ordre est déterminé par la configuration du service de nom du SVM.

- Pour le mappage Windows à UNIX

Si aucun mappage n'est trouvé, ONTAP vérifie si le nom d'utilisateur Windows minuscule est un nom d'utilisateur valide dans le domaine UNIX. Si cela ne fonctionne pas, il utilise l'utilisateur UNIX par défaut à condition qu'il soit configuré. Si l'utilisateur UNIX par défaut n'est pas configuré et que ONTAP ne peut pas obtenir de mappage de cette façon, le mappage échoue et une erreur est renvoyée.

- Pour le mappage d'UNIX à Windows

Si aucun mappage n'est trouvé, ONTAP tente de trouver un compte Windows correspondant au nom UNIX dans le domaine SMB. Si cela ne fonctionne pas, il utilise l'utilisateur SMB par défaut, à condition qu'il soit configuré. Si l'utilisateur CIFS par défaut n'est pas configuré et que ONTAP ne peut pas obtenir de mappage de cette façon, le mappage échoue et une erreur est renvoyée.

Par défaut, les comptes machine sont mappés à l'utilisateur UNIX par défaut spécifié. Si aucun utilisateur UNIX par défaut n'est spécifié, les mappages de compte machine échouent.

- À partir de ONTAP 9.5, vous pouvez mapper des comptes machine à des utilisateurs autres que l'utilisateur UNIX par défaut.
- Dans ONTAP 9.4 et versions antérieures, vous ne pouvez pas mapper les comptes machine à d'autres utilisateurs.

Même si des mappages de noms pour des comptes machine sont définis, les mappages sont ignorés.

Multidomaine recherche les mappages de noms d'utilisateur UNIX vers Windows

ONTAP prend en charge les recherches multidomaine lors du mappage d'utilisateurs UNIX aux utilisateurs Windows. Tous les domaines de confiance découverts sont recherchés pour trouver des correspondances avec le modèle de remplacement jusqu'à

ce qu'un résultat correspondant soit renvoyé. Vous pouvez également configurer une liste de domaines de confiance préférés, qui est utilisée à la place de la liste de domaines de confiance découverts et est recherchée dans l'ordre jusqu'à ce qu'un résultat correspondant soit renvoyé.

La manière dont les approbations de domaine affectent les recherches de mappage de noms d'utilisateur UNIX à des noms d'utilisateur Windows

Pour comprendre le fonctionnement du mappage de noms d'utilisateur multidomaine, vous devez comprendre comment les approbations de domaine fonctionnent avec ONTAP. Les relations de confiance Active Directory avec le domaine personnel du serveur CIFS peuvent être une confiance bidirectionnelle ou l'un des deux types de fiducies unidirectionnelles, soit une confiance entrante, soit une confiance sortante. Le home domain est le domaine auquel le serveur CIFS du SVM appartient.

- *Confiance bidirectionnelle*

Avec des approbations bidirectionnelles, les deux domaines se font confiance. Si le domaine de base du serveur CIFS possède une confiance bidirectionnelle avec un autre domaine, le domaine de base peut authentifier et autoriser un utilisateur appartenant au domaine de confiance et vice versa.

Les recherches de mappage de noms d'utilisateur UNIX à Windows peuvent être effectuées uniquement sur les domaines avec des approbations bidirectionnelles entre le domaine principal et l'autre domaine.

- *Confiance sortante*

Avec une confiance sortante, le domaine d'origine approuve l'autre domaine. Dans ce cas, le domaine home peut authentifier et autoriser un utilisateur appartenant au domaine de confiance sortant.

Un domaine avec une confiance sortante avec le domaine d'origine est *NOT* recherché lors de l'exécution de recherches de mappage entre utilisateurs UNIX et noms d'utilisateur Windows.


- *Confiance entrante*

Avec une confiance entrante, l'autre domaine approuve le domaine personnel du serveur CIFS. Dans ce cas, le domaine personnel ne peut pas authentifier ni autoriser un utilisateur appartenant au domaine de confiance entrant.

Un domaine avec une confiance entrante avec le domaine d'origine est *NOT* recherché lors de l'exécution de recherches de mappage entre utilisateurs UNIX et noms d'utilisateur Windows.

Comment les caractères génériques (*) sont utilisés pour configurer les recherches multidomaines pour le mappage de noms

Les recherches de mappage de noms de domaines multiples sont facilitées par l'utilisation de caractères génériques dans la section domaine du nom d'utilisateur Windows. Le tableau suivant illustre comment utiliser des caractères génériques dans la partie domaine d'une entrée de mappage de nom pour activer les recherches multidomaine :

Motif	Remplacement	Résultat
racine	*\\administrateur	L'utilisateur UNIX « root » est mappé à l'utilisateur nommé « administrateur ». Tous les domaines approuvés sont recherchés dans l'ordre jusqu'à ce que le premier utilisateur correspondant nommé « administrateur » soit trouvé.
*	**	<p>Les utilisateurs UNIX valides sont mappés aux utilisateurs Windows correspondants. Tous les domaines approuvés sont recherchés dans l'ordre jusqu'à ce que le premier utilisateur correspondant à ce nom soit trouvé.</p> <div>  <p>Le schéma ** n'est valide que pour le mappage de noms d'UNIX à Windows, pas l'inverse.</p> </div>

Mode d'exécution des recherches sur plusieurs noms de domaine

Vous pouvez choisir l'une des deux méthodes pour déterminer la liste des domaines approuvés utilisés pour les recherches de noms multidomaines :

- Utilisez la liste d'approbation bidirectionnelle automatiquement découverte compilée par ONTAP
- Utilisez la liste de domaines approuvés que vous compilez

Si un utilisateur UNIX est mappé à un utilisateur Windows avec un caractère générique utilisé pour la section domaine du nom d'utilisateur, l'utilisateur Windows est recherché dans tous les domaines approuvés comme suit :

- Si une liste de domaines de confiance est configurée, l'utilisateur Windows mappé est uniquement recherché dans cette liste de recherche, dans l'ordre.
- Si une liste préférée de domaines approuvés n'est pas configurée, l'utilisateur Windows est alors recherché dans tous les domaines de confiance bidirectionnels du domaine de départ.
- S'il n'existe pas de domaines de confiance bidirectionnellement pour le domaine personnel, l'utilisateur est recherché dans le domaine personnel.

Si un utilisateur UNIX est mappé à un utilisateur Windows sans section de domaine dans le nom d'utilisateur, l'utilisateur Windows est recherché dans le domaine personnel.

Règles de conversion du mappage de noms

Un système ONTAP conserve un ensemble de règles de conversion pour chaque SVM. Chaque règle se compose de deux éléments : un *pattern* et un *remplacement*. Les

conversions commencent au début de la liste appropriée et effectuent une substitution basée sur la première règle correspondante. Le motif est une expression régulière de style UNIX. Le remplacement est une chaîne contenant des séquences d'échappement représentant des sous-expressions du motif, comme dans UNIX `sed` programme.

Créer un mappage de nom

Vous pouvez utiliser le `vserver name-mapping create` commande permettant de créer un mappage de noms. Vous utilisez les mappages de noms pour permettre aux utilisateurs Windows d'accéder aux volumes du style de sécurité UNIX et les inverser.

Description de la tâche

Par SVM, ONTAP prend en charge jusqu'à 12,500 mappages de noms dans chaque direction.

Étape

1. Créer un mappage de noms : `vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text`



Le `-pattern` et `-replacement` les énoncés peuvent être formulés comme des expressions régulières. Vous pouvez également utiliser le `-replacement` instruction pour refuser explicitement un mappage à l'utilisateur en utilisant la chaîne de remplacement nulle " " (le caractère d'espace). Voir la `vserver name-mapping create` page de manuel pour plus de détails.

Lorsque des mappages entre Windows et UNIX sont créés, tous les clients SMB disposant de connexions ouvertes au système ONTAP au moment de la création des nouveaux mappages doivent se déconnecter et se reconnecter pour voir les nouveaux mappages.

Exemples

La commande suivante crée un nom de mappage sur le SVM nommé `vs1`. Le mappage est un mappage d'UNIX à Windows à la position 1 dans la liste des priorités. Le mappage mappe l'utilisateur UNIX `johnd` à l'utilisateur Windows `ENG\johndoe`.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

La commande suivante crée un autre mappage de nom sur le SVM nommé `vs1`. Le mappage est un mappage de Windows à UNIX à la position 1 dans la liste des priorités. Dans ce cas, le motif et le remplacement incluent des expressions régulières. Le mapping mappe chaque utilisateur CIFS du domaine `ENG` aux utilisateurs du domaine LDAP associé avec la SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\\1"
```

La commande suivante crée un autre mappage de nom sur le SVM nommé vs1. Ici, le schéma inclut ""\$"" comme élément du nom d'utilisateur Windows qui doit être échappé. Le mappage mappe l'utilisateur Windows ENG\john\$OPS à l'utilisateur UNIX john_OPS.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configurez l'utilisateur par défaut

Vous pouvez configurer un utilisateur par défaut à utiliser si toutes les autres tentatives de mappage échouent pour un utilisateur, ou si vous ne souhaitez pas mapper des utilisateurs individuels entre UNIX et Windows. Si vous souhaitez que l'authentification des utilisateurs non mappés échoue, vous ne devez pas configurer un utilisateur par défaut.

Description de la tâche

Pour l'authentification CIFS, si vous ne souhaitez pas mapper chaque utilisateur Windows à un utilisateur UNIX individuel, vous pouvez spécifier un utilisateur UNIX par défaut.

Pour l'authentification NFS, si vous ne souhaitez pas mapper chaque utilisateur UNIX à un utilisateur Windows individuel, vous pouvez spécifier un utilisateur Windows par défaut.

Étapes


- 1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez...	Saisissez la commande suivante...
Configurez l'utilisateur UNIX par défaut	<code>vserver cifs options modify -default -unix-user <i>user_name</i></code>
Configurez l'utilisateur Windows par défaut	<code>vserver nfs modify -default-win-user <i>user_name</i></code>

Commandes permettant de gérer les mappages de noms

Il existe des commandes ONTAP spécifiques permettant de gérer les mappages de noms.

Les fonctions que vous recherchez...	Utilisez cette commande...
Créer un mappage de nom	<code>vserver name-mapping create</code>
Insérez un mappage de nom à une position spécifique	<code>vserver name-mapping insert</code>

Les fonctions que vous recherchez...	Utilisez cette commande...
Afficher les mappages de noms	<code>vserver name-mapping show</code>
<div>  <p>Un swap n'est pas autorisé lorsque le mappage-nom est configuré avec une entrée de qualificatif-ip.</p> </div> Échangez la position de deux mappages de noms	<code>vserver name-mapping swap</code>
Modifier un mappage de noms	<code>vserver name-mapping modify</code>
Supprime un mappage de noms	<code>vserver name-mapping delete</code>
Valider le mappage de nom correct	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win -user-name user1 -path / -share-name sh1</code>

Consultez la page man pour chaque commande pour plus d'informations.

Configurez les recherches de mappage de noms-domaines multiples

Activez ou désactivez les recherches de mappage de noms multidomaine

Avec les recherches de mappage de noms multidomaine, vous pouvez utiliser un caractère générique (*) dans la partie domaine d'un nom Windows lors de la configuration du mappage de noms d'utilisateurs UNIX vers Windows. L'utilisation d'un caractère générique (*) dans la partie domaine du nom permet à ONTAP de rechercher tous les domaines ayant une confiance bidirectionnelle avec le domaine qui contient le compte ordinateur du serveur CIFS.

Description de la tâche

Comme alternative à la recherche de tous les domaines de confiance bidirectionnels, vous pouvez configurer une liste de domaines de confiance préférés. Lorsqu'une liste de domaines de confiance privilégiés est configurée, ONTAP utilise la liste de domaines de confiance préférée au lieu des domaines de confiance bidirectionnels découverts pour effectuer des recherches de mappage de noms multiples domaines.

- Les recherches de mappage de noms de domaines multiples sont activées par défaut.
- Cette option est disponible au niveau de privilège avancé.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Pour effectuer des recherches sur le mappage de noms de domaines multiples...	Entrez la commande...
Activé	<code>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true</code>
Désactivé	<code>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false</code>

3. Retour au niveau de privilège admin : `set -privilege admin`

Informations associées

[Options de serveur SMB disponibles](#)

Réinitialiser et redécouvrir des domaines de confiance

Vous pouvez forcer la redécouverte de tous les domaines de confiance. Ceci peut être utile lorsque les serveurs de domaine approuvés ne répondent pas correctement ou que les relations de confiance ont changé. Seuls les domaines avec une confiance bidirectionnelle avec le domaine de base, qui est le domaine contenant le compte ordinateur du serveur CIFS, sont découverts.

Étape

1. Réinitialisez et redécouvrez des domaines de confiance à l'aide de `vserver cifs domain trusts rediscover` commande.

```
vserver cifs domain trusts rediscover -vserver vs1
```

Informations associées

[Affichage des informations sur les domaines de confiance découverts](#)

Affiche des informations sur les domaines de confiance découverts

Vous pouvez afficher des informations sur les domaines approuvés découverts pour le domaine personnel du serveur CIFS, qui est le domaine contenant le compte d'ordinateur du serveur CIFS. Cela peut être utile lorsque vous voulez savoir quels domaines de confiance sont découverts et comment ils sont ordonnés dans la liste domaine de confiance découvert.

Description de la tâche

Seuls les domaines avec des approbations bidirectionnelles avec le domaine de départ sont découverts. Étant donné que le contrôleur de domaine (DC) du domaine d'origine renvoie la liste des domaines de confiance dans un ordre déterminé par le DC, l'ordre des domaines dans la liste ne peut pas être prédit. En affichant la liste des domaines de confiance, vous pouvez déterminer l'ordre de recherche des recherches de mappage de noms de domaines multiples.

Les informations des domaines de confiance affichés sont regroupées par nœud et par SVM (Storage Virtual

machine).

Étape

1. Affiche des informations sur les domaines de confiance découverts à l'aide du `vserver cifs domain trusts show` commande.

```
vserver cifs domain trusts show -vserver vs1
```

```
Node: node1
Vserver: vs1

Home Domain          Trusted Domain
-----
EXAMPLE.COM          CIFS1.EXAMPLE.COM,
                     CIFS2.EXAMPLE.COM
                     EXAMPLE.COM

Node: node2
Vserver: vs1

Home Domain          Trusted Domain
-----
EXAMPLE.COM          CIFS1.EXAMPLE.COM,
                     CIFS2.EXAMPLE.COM
                     EXAMPLE.COM
```

Informations associées

[Réinitialisation et redécouverte des domaines de confiance](#)

Ajoutez, supprimez ou remplacez des domaines de confiance dans les listes de domaines de confiance préférées

Vous pouvez ajouter ou supprimer des domaines approuvés de la liste des domaines approuvés préférés pour le serveur SMB ou modifier la liste actuelle. Si vous configurez une liste de domaines de confiance privilégiés, cette liste est utilisée à la place des domaines de confiance bidirectionnels découverts lors de l'exécution de recherches sur le mappage de noms multidomaines.

Description de la tâche

- Si vous ajoutez des domaines approuvés à une liste existante, la nouvelle liste est fusionnée avec la liste existante et les nouvelles entrées sont placées à la fin. Les domaines de confiance sont recherchés dans l'ordre dans lequel ils apparaissent dans la liste des domaines de confiance.
- Si vous supprimez des domaines de confiance de la liste existante et ne spécifiez pas de liste, la liste de domaines de confiance complète pour la machine virtuelle de stockage (SVM) spécifiée est supprimée.
- Si vous modifiez la liste existante des domaines approuvés, la nouvelle liste remplace la liste existante.



Vous devez entrer uniquement les domaines de confiance bidirectionnels dans la liste des domaines de confiance préférés. Même si vous pouvez entrer des domaines de confiance sortants ou entrants dans la liste de domaines préférés, ils ne sont pas utilisés lors de recherches de mappage de noms de domaines multiples. ONTAP ignore l'entrée du domaine unidirectionnel et passe au domaine de confiance bidirectionnel suivant dans la liste.

Étape

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez effectuer les opérations suivantes avec la liste des domaines de confiance préférés...	Utilisez la commande...
Ajouter des domaines de confiance à la liste	<code>vserver cifs domain name-mapping-search add -vserver _vserver_name_-trusted-domains FQDN, ...</code>
Supprimer des domaines de confiance de la liste	<code>vserver cifs domain name-mapping-search remove -vserver _vserver_name_-trusted-domains FQDN, ...]</code>
Modifier la liste existante	<code>vserver cifs domain name-mapping-search modify -vserver _vserver_name_-trusted-domains FQDN, ...</code>

Exemples

La commande suivante ajoute deux domaines de confiance (cifs1.example.com et cifs2.example.com) à la liste de domaines de confiance privilégiée utilisée par le SVM vs1 :

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

La commande suivante supprime deux domaines de confiance de la liste utilisée par le SVM vs1 :

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

La commande suivante modifie la liste de domaines approuvés utilisée par le SVM vs1. La nouvelle liste remplace la liste d'origine :

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

Informations associées

[Affichage d'informations sur la liste de domaines de confiance préférée](#)

Affiche des informations sur la liste de domaines de confiance préférée

Vous pouvez afficher des informations sur les domaines de confiance dans la liste des domaines de confiance préférés et l'ordre dans lequel ils sont recherchés si les recherches de mappage de noms de domaines multiples sont activées. Vous pouvez configurer une liste de domaines de confiance préférée comme alternative à l'utilisation de la liste de domaines de confiance automatiquement découverts.

Étapes

- 1. Effectuez l'une des opérations suivantes :

Pour afficher des informations sur les éléments suivants...	Utilisez la commande...
Tous les domaines de confiance privilégiés dans le cluster regroupés par SVM (Storage Virtual machine)	<code>vserver cifs domain name-mapping-search show</code>
Tous les domaines fiables préférés pour un SVM spécifié	<code>vserver cifs domain name-mapping-search show -vserver vserver_name</code>

La commande suivante affiche des informations sur tous les domaines de confiance privilégiés sur le cluster :

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver          Trusted Domains
-----
vs1              CIFS1.EXAMPLE.COM
```

Informations associées

[Ajout, suppression ou remplacement de domaines de confiance dans les listes de domaines de confiance préférées](#)

Créez et configurez des partages SMB

Présentation de la création et de la configuration des partages SMB

Avant que les utilisateurs et les applications n'accèdent aux données sur le serveur CIFS via SMB, vous devez créer et configurer des partages SMB, qui est un point d'accès nommé dans un volume. Vous pouvez personnaliser les partages en spécifiant des paramètres de partage et des propriétés de partage. Vous pouvez modifier un partage existant à tout moment.

Lorsque vous créez un partage SMB, ONTAP crée une liste de contrôle d'accès par défaut pour le partage avec les autorisations de contrôle total pour tous.

Les partages SMB sont liés au serveur CIFS sur la machine virtuelle de stockage (SVM). Les partages SMB sont supprimés si le SVM est supprimé ou si le serveur CIFS auquel il est associé est supprimé de la SVM. Si

vous recréez le serveur CIFS sur le SVM, vous devez recréer les partages SMB.

Informations associées

[Gérer l'accès aux fichiers via SMB](#)

["Configuration SMB pour Microsoft Hyper-V et SQL Server"](#)

[Configurez le mappage de caractères pour la conversion de nom de fichier SMB sur des volumes](#)

Définition des partages administratifs par défaut

Lorsque vous créez un serveur CIFS sur votre SVM (Storage Virtual machine), les partages administratifs par défaut sont automatiquement créés. Vous devez comprendre ce que sont ces partages par défaut et comment ils sont utilisés.

Lors de la création du serveur CIFS, ONTAP crée les partages administratifs par défaut suivants :



Depuis ONTAP 9.8, le partage admin\$ n'est plus créé par défaut.

- ipc\$
- admin\$ (ONTAP 9.7 et versions antérieures uniquement)
- c\$

Les partages qui se terminent par le caractère \$ étant des partages masqués, les partages administratifs par défaut ne sont pas visibles depuis mon ordinateur, mais vous pouvez les afficher à l'aide de dossiers partagés.

Utilisation des partages IPC\$ et admin\$ par défaut

Les partages ipc\$ et admin\$ sont utilisés par ONTAP et ne peuvent pas être utilisés par les administrateurs Windows pour accéder aux données résidant sur la SVM.

- part ipc\$

La part ipc\$ est une ressource qui partage les canaux nommés qui sont essentiels à la communication entre les programmes. Le partage ipc\$ est utilisé lors de l'administration à distance d'un ordinateur et lors de l'affichage des ressources partagées d'un ordinateur. Vous ne pouvez pas modifier les paramètres de partage, les propriétés de partage ou les listes de contrôle d'accès du partage ipc\$. Vous ne pouvez pas non plus renommer ou supprimer le partage ipc\$.

- Partage admin\$ (ONTAP 9.7 et versions antérieures uniquement)



Depuis ONTAP 9.8, le partage admin\$ n'est plus créé par défaut.

Le partage admin\$ est utilisé pendant l'administration à distance du SVM. Le chemin de cette ressource est toujours le chemin vers la racine SVM. Vous ne pouvez pas modifier les paramètres de partage, les propriétés de partage ou les listes de contrôle d'accès pour le partage admin\$. Vous ne pouvez pas non plus renommer ou supprimer le partage admin\$.

Utilisation du partage par défaut c\$

Le partage c\$ est un partage administratif que l'administrateur du cluster ou du SVM peut utiliser pour accéder au volume root du SVM et le gérer.

Voici les caractéristiques de la part c\$:

- Le chemin pour ce partage est toujours le chemin vers le volume root du SVM et ne peut pas être modifié.
- La liste de contrôle d'accès par défaut pour le partage c\$ est Administrator / Full Control.

Cet utilisateur est le BUILTIN\Administrator. Par défaut, BUILTIN\Administrator peut mapper sur le partage et l'affichage, créer, modifier ou supprimer des fichiers et dossiers dans le répertoire racine mappé. Soyez prudent lorsque vous gérez des fichiers et des dossiers dans ce répertoire.

- Vous pouvez modifier l'ACL du partage c\$.
- Vous pouvez modifier les paramètres de partage c\$ et les propriétés de partage.
- Vous ne pouvez pas supprimer le partage c\$.
- L'administrateur du SVM peut accéder au reste de l'espace de noms du SVM à partir du partage c\$ mappé en croisant les jonctions de l'espace de noms.
- Le partage c\$ est accessible à l'aide de la console de gestion Microsoft.

Informations associées

[Configuration des autorisations de fichier NTFS avancées à l'aide de l'onglet sécurité de Windows](#)

Exigences de nommage des partages SMB

Lors de la création de partages SMB sur votre serveur SMB, veuillez à respecter les exigences de dénomination des partages ONTAP.

Les conventions de nom des partages pour ONTAP sont identiques à celles de Windows et doivent être respectées dans ce cas :

- Le nom de chaque partage doit être unique pour le serveur SMB.
- Les noms de partage ne sont pas sensibles à la casse.
- La longueur maximale du nom de partage est de 80 caractères.
- Les noms de partage Unicode sont pris en charge.
- Les noms de partage se terminant par le caractère \$ sont des partages masqués.
- Pour ONTAP 9.7 et les versions antérieures, les partages administratifs admin\$, ipc\$ et c\$ sont automatiquement créés sur chaque serveur CIFS et sont des noms de partage réservés. Depuis ONTAP 9.8, le partage admin\$ n'est plus créé automatiquement.
- Lors de la création d'un partage, vous ne pouvez pas utiliser le nom de partage ONTAP_ADMIN\$.
- Les noms de partage contenant des espaces sont pris en charge :
 - Vous ne pouvez pas utiliser un espace comme premier caractère ou comme dernier caractère dans un nom de partage.
 - Vous devez inclure des noms de partage contenant un espace entre guillemets.



Les guillemets simples sont considérés comme faisant partie du nom du partage et ne peuvent pas être utilisés à la place des guillemets.

- Les caractères spéciaux suivants sont pris en charge lorsque vous nommez des partages SMB :

! @ # \$ % et ' _ - . ~ () { }

- Les caractères spéciaux suivants ne sont pas pris en charge lorsque vous nommez des partages SMB :
 - " / \ : ; | < > , ? * =

Exigences de sensibilité aux cas de répertoire lors de la création de partages dans un environnement multiprotocole

Si vous créez des partages dans un SVM où le schéma de nommage 8.3 est utilisé pour faire la distinction entre les noms de répertoire où il n'y a que des différences de cas entre les noms, vous devez utiliser le nom 8.3 du chemin de partage pour s'assurer que le client se connecte au chemin de répertoire souhaité.

Dans l'exemple suivant, deux répertoires nommés « testdir » et « TESTDIR » ont été créés sur un client Linux. La Junction path du volume contenant les répertoires est /home. La première sortie provient d'un client Linux et la seconde sortie provient d'un client SMB.

```
ls -l
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:24 TESTDIR
```

```
dir
```

```
Directory of Z:\
```

```
04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

Lorsque vous créez un partage dans le second répertoire, vous devez utiliser le nom 8.3 dans le chemin du partage. Dans cet exemple, le chemin du partage vers le premier répertoire est /home/testdir et le chemin du partage vers le second répertoire est /home/TESTDI~1.

Utilisez les propriétés du partage SMB

Utiliser la présentation des propriétés de partage SMB

Vous pouvez personnaliser les propriétés des partages SMB.

Les propriétés de partage disponibles sont les suivantes :

Propriétés du partage	Description
oplocks	Cette propriété indique que le partage utilise des verrous opportunistes, également appelés mise en cache côté client.
browsable	Cette propriété permet aux clients Windows de parcourir le partage.

Propriétés du partage	Description
showsnapshot	Cette propriété spécifie que les copies Snapshot peuvent être visualisées et traversées par les clients.
changenotify	Cette propriété indique que le partage prend en charge les demandes de notification des modifications. Pour les partages sur un SVM, il s'agit d'une propriété initiale par défaut.
attributecache	Cette propriété permet la mise en cache des attributs de fichier sur le partage SMB afin d'accélérer l'accès aux attributs. La valeur par défaut est de désactiver la mise en cache des attributs. Cette propriété ne doit être activée que si des clients se connectent à des partages sur SMB 1.0. Cette propriété de partage n'est pas applicable si les clients se connectent à des partages via SMB 2.x ou SMB 3.0.
continuously-available	Cette propriété permet aux clients SMB qui la prennent en charge d'ouvrir des fichiers de façon persistante. Les fichiers ouverts de cette façon sont protégés contre les événements perturbateurs, tels que le basculement et le rétablissement.
branchcache	Cette propriété spécifie que le partage permet aux clients de demander des hachages de BranchCache sur les fichiers de ce partage. Cette option n'est utile que si vous spécifiez « par partage » en mode de fonctionnement dans la configuration de BranchCache CIFS.
access-based-enumeration	Cette propriété spécifie que <i>accès basé sur Enumeration</i> (ABE) est activé sur ce partage. Les dossiers partagés filtrés PAR ABE sont visibles par un utilisateur en fonction des droits d'accès de cet utilisateur, empêchant l'affichage des dossiers ou d'autres ressources partagées que l'utilisateur ne dispose pas des droits d'accès.

Propriétés du partage	Description
namespace-caching	Cette propriété spécifie que les clients SMB qui se connectent à ce partage peuvent mettre en cache les résultats d'énumération de répertoire renvoyés par les serveurs CIFS, ce qui peut fournir de meilleures performances. Par défaut, les clients SMB 1 ne mettent pas en cache les résultats d'énumération des répertoires. Étant donné que les clients SMB 2 et SMB 3 mettent en cache les résultats d'énumération de répertoires par défaut, la spécification de cette propriété de partage n'offre des avantages en termes de performances que pour les connexions clients SMB 1.
encrypt-data	Cette propriété spécifie que le chiffrement SMB doit être utilisé lors de l'accès à ce partage. Les clients SMB qui ne prennent pas en charge le chiffrement lors de l'accès aux données SMB ne pourront pas accéder à ce partage.

Ajouter ou supprimer des propriétés de partage sur un partage SMB existant

Vous pouvez personnaliser un partage SMB existant en ajoutant ou en supprimant des propriétés de partage. Cela peut être utile si vous voulez modifier la configuration du partage pour répondre aux exigences changeantes de votre environnement.

Avant de commencer

Le partage dont vous souhaitez modifier les propriétés doit exister.

Description de la tâche

Instructions pour l'ajout de propriétés de partage :

- Vous pouvez ajouter une ou plusieurs propriétés de partage à l'aide d'une liste délimitée par des virgules.
- Toutes les propriétés de partage que vous avez précédemment spécifiées restent en vigueur.

Les nouvelles propriétés ajoutées sont ajoutées à la liste existante des propriétés de partage.

- Si vous spécifiez une nouvelle valeur pour les propriétés de partage qui sont déjà appliquées au partage, la nouvelle valeur spécifiée remplace la valeur d'origine.
- Vous ne pouvez pas supprimer les propriétés de partage à l'aide de `vserver cifs share properties add` commande.

Vous pouvez utiliser le `vserver cifs share properties remove` commande permettant de supprimer les propriétés de partage.

Consignes de suppression des propriétés de partage :

- Vous pouvez supprimer une ou plusieurs propriétés de partage à l'aide d'une liste délimitée par des virgules.

- Toutes les propriétés de partage que vous avez précédemment spécifiées mais que vous ne les supprimez pas restent en vigueur.

Étapes

1. Saisissez la commande appropriée :

Les fonctions que vous recherchez...	Entrez la commande...
Ajouter des propriétés de partage	<code>vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</code>
Supprimer les propriétés de partage	<code>vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</code>

2. Vérifiez les paramètres de propriété de partage : `vserver cifs share show -vserver vserver_name -share-name share_name`

Exemples

La commande suivante ajoute la `showsnapshot` Partagez la propriété avec une part nommée « `khare1' » sur la SVM vs1 :

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver      Share    Path      Properties    Comment    ACL
-----
vs1          share1   /share1   oplocks       -          Everyone / Full
Control
                browsable
                changenotify
                showsnapshot
```

La commande suivante supprime le `browsable` Partagez des biens d'une part nommée « sune2 » sur la SVM vs1 :

```
cluster1::> vservers cifs share properties remove -vservers vs1 -share-name
share2 -share-properties browsable

cluster1::> vservers cifs share show -vservers vs1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1	share2	/share2	oplocks	-	Everyone / Full
Control			changenotify		

Informations associées

Commandes de gestion des partages SMB

Optimisez l'accès des utilisateurs SMB à l'aide du paramètre de partage force-groupe

Lorsque vous créez un partage à partir de la ligne de commande ONTAP vers des données avec sécurité efficace UNIX, vous pouvez spécifier que tous les fichiers créés par les utilisateurs SMB de ce partage appartiennent au même groupe, appelé *force-group*, qui doit être un groupe prédéfini dans la base de données du groupe UNIX. L'utilisation d'un groupe de force facilite l'accès aux fichiers par les utilisateurs SMB appartenant à différents groupes.

La spécification d'un groupe de force n'est pertinente que si le partage est dans un qtree UNIX ou mixte. Il n'est pas nécessaire de définir un groupe de force pour les partages d'un volume NTFS ou d'un qtree, car l'accès aux fichiers de ces partages est déterminé par les autorisations Windows, et non par des GIDS UNIX.

Si un groupe de force a été spécifié pour un partage, les valeurs suivantes deviennent vraies pour le partage :

- Les moyennes entreprises qui accèdent à ce partage sont temporairement modifiées en GID du groupe force.

Ce GID leur permet d'accéder aux fichiers de ce partage qui ne sont pas accessibles normalement avec leur GID ou leur UID principal.

- Tous les fichiers de ce partage créés par les utilisateurs SMB appartiennent au même groupe de force, quel que soit le GID principal du propriétaire du fichier.

Lorsque les utilisateurs SMB essaient d'accéder à un fichier créé par NFS, les principaux GID des utilisateurs SMB déterminent les droits d'accès.

La force-group n'affecte pas la façon dont les utilisateurs NFS accèdent aux fichiers dans ce partage. Un fichier créé par NFS acquiert le GID du propriétaire du fichier. La détermination des autorisations d'accès est basée sur l'UID et le GID principal de l'utilisateur NFS qui tente d'accéder au fichier.

L'utilisation d'un groupe de force facilite l'accès aux fichiers par les utilisateurs SMB appartenant à différents groupes. Par exemple, si vous souhaitez créer un partage pour stocker les pages Web de l'entreprise et donner un accès en écriture aux utilisateurs des départements Ingénierie et Marketing, vous pouvez créer un partage et donner accès en écriture à un groupe de force nommé « webgroupe1 ». En raison du groupe de force, tous les fichiers créés par les utilisateurs SMB de ce partage appartiennent au groupe « webgroupe1 ». En outre, les utilisateurs se voient automatiquement attribuer le GID du groupe « webgroupe1 » lorsqu'ils

accèdent au partage. Par conséquent, tous les utilisateurs peuvent écrire sur ce partage sans avoir à gérer les droits d'accès des utilisateurs dans les services Ingénierie et Marketing.

Informations associées

[Création d'un partage SMB avec le paramètre de partage force-group](#)

Créez un partage SMB avec le paramètre de partage force-group

Vous pouvez créer un partage SMB avec le paramètre de partage force-group si vous souhaitez que les utilisateurs SMB qui accèdent aux données sur des volumes ou des qtrees avec la sécurité de fichier UNIX soient considérés par ONTAP comme appartenant au même groupe UNIX.

Étape

1. Créez le partage SMB : `vserver cifs share create -vserver vserver_name -share-name share_name -path path -force-group-for-create UNIX_group_name`

Si le chemin UNC (\\servername\sharename\filepath) du partage contient plus de 256 caractères (à l'exclusion de la première « \\ » Dans le chemin UNC), l'onglet **sécurité** de la boîte Propriétés de Windows n'est pas disponible. Il s'agit d'un problème de client Windows plutôt que d'un problème ONTAP. Pour éviter ce problème, ne créez pas de partages avec des chemins UNC de plus de 256 caractères.

Si vous souhaitez supprimer le groupe de force après la création du partage, vous pouvez modifier le partage à tout moment et spécifier une chaîne vide ("") comme valeur pour le `-force-group-for-create` paramètre. Si vous supprimez le groupe de force en modifiant le partage, toutes les connexions existantes à ce partage continuent d'avoir le groupe de force précédemment défini comme GID principal.

Exemple

La commande suivante crée un partage « pages Web » accessible sur le Web dans le /corp/companyinfo Répertoire dans lequel tous les fichiers créés par les utilisateurs SMB sont affectés au groupe webgroupe1 :

```
vserver cifs share create -vserver vs1 -share-name webpages -path /corp/companyinfo -force-group-for-create webgroup1
```

Informations associées

[Optimisez l'accès des utilisateurs SMB à l'aide du paramètre de partage force-groupe](#)

Afficher les informations sur les partages SMB à l'aide de la console MMC

Vous pouvez afficher les informations relatives aux partages SMB sur votre SVM et effectuer certaines tâches de gestion à l'aide de la console de gestion Microsoft (MMC). Avant de pouvoir afficher les partages, vous devez connecter la MMC au SVM.

Description de la tâche

Vous pouvez effectuer les tâches suivantes sur les partages contenus dans les SVM à l'aide de MMC :

- Afficher les partages
- Afficher les sessions actives
- Afficher les fichiers ouverts
- Énumérer la liste des sessions, des fichiers et des connexions d'arborescence dans le système

- Fermez les fichiers ouverts dans le système
- Fermer les sessions ouvertes
- Création/gestion de partages



Les vues affichées par les fonctionnalités précédentes sont propres à chaque nœud et non à chaque cluster. Par conséquent, lorsque vous utilisez le MMC pour vous connecter au nom d'hôte du serveur SMB (à savoir, cifs01.domain.local), vous êtes routé, selon la façon dont vous avez configuré DNS, vers une seule LIF au sein de votre cluster.

Les fonctions suivantes ne sont pas prises en charge dans MMC pour ONTAP :

- Création de nouveaux utilisateurs/groupe locaux
- Gestion/affichage des utilisateurs/groupe locaux existants
- Affichage des événements ou des journaux de performances
- Stockage
- Services et applications

Dans les cas où l'opération n'est pas prise en charge, vous pouvez être confrontés à une situation `remote procedure call failed` erreurs.

"FAQ : utilisation de Windows MMC avec ONTAP"

Étapes

1. Pour ouvrir Computer Management MMC sur n'importe quel serveur Windows, dans le **panneau de configuration**, sélectionnez **Outils d'administration > gestion de l'ordinateur**.
2. Sélectionnez **action > connexion à un autre ordinateur**.

La boîte de dialogue Sélectionner un ordinateur s'affiche.

3. Tapez le nom du système de stockage ou cliquez sur **Parcourir** pour localiser le système de stockage.
4. Cliquez sur **OK**.

La MMC se connecte à la SVM.

5. Dans le volet de navigation, cliquez sur **dossiers partagés > partages**.

Une liste des partages sur le SVM est affichée dans le volet d'affichage droit.

6. Pour afficher les propriétés de partage d'un partage, double-cliquez sur le partage pour ouvrir la boîte de dialogue **Propriétés**.
7. Si vous ne pouvez pas vous connecter au système de stockage à l'aide de MMC, vous pouvez ajouter l'utilisateur au groupe BULTIN\Administrators ou BULTIN\Power Users en utilisant l'une des commandes suivantes sur le système de stockage :


```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

Commandes de gestion des partages SMB

Vous utilisez le `vserver cifs share` et `vserver cifs share properties` Commandes pour gérer les partages SMB.

Les fonctions que vous recherchez...	Utilisez cette commande...
Créez un partage SMB	<code>vserver cifs share create</code>
Affiche les partages SMB	<code>vserver cifs share show</code>
Modifiez un partage SMB	<code>vserver cifs share modify</code>
Supprime un partage SMB	<code>vserver cifs share delete</code>
Ajouter des propriétés de partage à un partage existant	<code>vserver cifs share properties add</code>
Supprimer les propriétés de partage d'un partage existant	<code>vserver cifs share properties remove</code>
Affiche des informations sur les propriétés de partage	<code>vserver cifs share properties show</code>

Consultez la page man pour chaque commande pour plus d'informations.

Sécurisez l'accès aux fichiers à l'aide des ACL de partage SMB

Directives pour la gestion des ACL de niveau partage SMB

Vous pouvez modifier les listes de contrôle d'accès au niveau du partage pour accorder aux utilisateurs plus ou moins de droits d'accès au partage. Vous pouvez configurer les listes de contrôle d'accès au niveau du partage en utilisant soit des utilisateurs et des groupes Windows, soit des utilisateurs et des groupes UNIX.

Après avoir créé un partage, par défaut, la liste de contrôle d'accès au niveau du partage donne un accès en lecture au groupe standard nommé Everyone. L'accès en lecture dans la liste de contrôle d'accès signifie que tous les utilisateurs du domaine et tous les domaines approuvés ont un accès en lecture seule au partage.

Vous pouvez modifier une liste de contrôle d'accès au niveau du partage en utilisant la console MMC (Microsoft Management Console) sur un client Windows ou la ligne de commande ONTAP.

Les directives suivantes s'appliquent lorsque vous utilisez la console MMC :

- Les noms d'utilisateur et de groupe spécifiés doivent être des noms Windows.
- Vous ne pouvez spécifier que des autorisations Windows.

Les consignes suivantes s'appliquent lorsque vous utilisez la ligne de commande ONTAP :

- Les noms d'utilisateur et de groupe spécifiés peuvent être des noms Windows ou UNIX.

Si un type d'utilisateur et de groupe n'est pas spécifié lors de la création ou de la modification des listes de contrôle d'accès, le type par défaut est utilisateurs et groupes Windows.

- Vous ne pouvez spécifier que des autorisations Windows.

Créer des listes de contrôle d'accès pour le partage SMB

La configuration des autorisations de partage en créant des listes de contrôle d'accès (ACL) pour les partages SMB vous permet de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes.

Description de la tâche

Vous pouvez configurer les listes de contrôle d'accès au niveau du partage à l'aide des noms d'utilisateur ou de groupe Windows locaux ou de domaine ou des noms d'utilisateur ou de groupe UNIX.

Avant de créer une nouvelle liste de contrôle d'accès, vous devez supprimer la liste de contrôle d'accès de partage par défaut `Everyone / Full Control`, qui pose un risque pour la sécurité.

En mode Workgroup, le nom de domaine local est le nom du serveur SMB.

Étapes

1. Supprimez la liste de contrôle d'accès du partage par défaut : « `vserver cifs share Access-control delete -vserver vserver_name -share share_name -user-or-group everyone` »
2. Configurer la nouvelle liste de contrôle d'accès :

Si vous souhaitez configurer des listes de contrôle d'accès à l'aide d'un...	Entrez la commande...
Utilisateur Windows	<code>vserver cifs share access-control create -vserver <i>vserver_name</i> -share <i>share_name</i> -user-group-type windows -user-or-group <i>Windows_domain_name\user_name</i> -permission <i>access_right</i></code>
Groupe Windows	<code>vserver cifs share access-control create -vserver <i>vserver_name</i> -share <i>share_name</i> -user-group-type windows -user-or-group <i>Windows_domain_name\group_name</i> -permission <i>access_right</i></code>

Si vous souhaitez configurer des listes de contrôle d'accès à l'aide d'un...	Entrez la commande...
Utilisateur UNIX	<code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-user -user-or-group UNIX_user_name -permission access_right</code>
Groupe UNIX	<code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-group -user-or-group UNIX_group_name -permission access_right</code>

3. Vérifiez que la liste de contrôle d'accès appliquée au partage est correcte à l'aide de la `vserver cifs share access-control show` commande.

Exemple

La commande suivante donne Change Autorisations au groupe Windows "sales Team" pour la part "sales" sur le SVM "vs1.example.com":

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs1.example.com	sales	DOMAIN\Sales Team	windows	Change

La commande suivante donne Read Autorisation au groupe UNIX « ingénierie » pour la part « eng » sur le SVM « vs2.example.com » :

```
cluster1::> vsriver cifs share access-control create -vsriver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vsriver cifs share access-control show -vsriver
vs2.example.com
```

Vsriver	Share	User/Group	User/Group	Access
Permission	Name	Name	Type	
-----	-----	-----	-----	

vs2.example.com	c\$	BUILTIN\Administrators	windows	
Full_Control				
vs2.example.com	eng	engineering	unix-group	Read

Les commandes suivantes fournissent Change L'autorisation au groupe Windows local nommé « Tiger Team » et Full_Control Autorisation à l'utilisateur Windows local nommé "rue Chang" pour le partage "vatavol5" sur le "SVM" "vs1":

```
cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vsriver cifs share access-control show -vsriver vs1
```

Vsriver	Share	User/Group	User/Group	Access
Permission	Name	Name	Type	
-----	-----	-----	-----	

vs1	c\$	BUILTIN\Administrators	windows	
Full_Control				
vs1	datavol5	Tiger Team	windows	Change
vs1	datavol5	Sue Chang	windows	Full_Control

Commandes de gestion des listes de contrôle d'accès au partage SMB

Vous devez connaître les commandes de gestion des listes de contrôle d'accès (ACL) SMB, notamment leur création, leur affichage, leur modification et leur suppression.

Les fonctions que vous recherchez...	Utilisez cette commande...
Créer une nouvelle liste de contrôle d'accès	<code>vserver cifs share access-control create</code>
Afficher les ACL	<code>vserver cifs share access-control show</code>
Modifier une ACL	<code>vserver cifs share access-control modify</code>
Supprimer une ACL	<code>vserver cifs share access-control delete</code>

Sécurisez l'accès aux fichiers grâce aux autorisations liées aux fichiers

Configurez les autorisations de fichier NTFS avancées à l'aide de l'onglet sécurité de Windows

Vous pouvez configurer les autorisations de fichier NTFS standard sur les fichiers et les dossiers en utilisant l'onglet **sécurité Windows** de la fenêtre Propriétés Windows.

Avant de commencer

L'administrateur effectuant cette tâche doit disposer d'autorisations NTFS suffisantes pour modifier les autorisations sur les objets sélectionnés.

Description de la tâche

La configuration des autorisations de fichiers NTFS se fait sur un hôte Windows en ajoutant des entrées aux listes de contrôle d'accès discrétionnaire NTFS (DACL) associées à un descripteur de sécurité NTFS. Le descripteur de sécurité est ensuite appliqué aux fichiers et répertoires NTFS. Ces tâches sont traitées automatiquement par l'interface graphique de Windows.

Étapes

1. Dans le menu **Tools** de l'Explorateur Windows, sélectionnez **Map network drive**.
2. Renseignez la boîte de dialogue **Map Network Drive** :
 - a. Sélectionnez une lettre **lecteur**.
 - b. Dans la zone **Folder**, saisissez le nom du serveur CIFS contenant le partage contenant les données auxquelles vous souhaitez appliquer les autorisations et le nom du partage.

Si le nom de votre serveur CIFS est ""CIFS_SERVER"" et que votre partage est nommé ""hare1"", vous devez taper \\CIFS_SERVER\share1.



Vous pouvez spécifier l'adresse IP de l'interface de données du serveur CIFS au lieu du nom du serveur CIFS.

- c. Cliquez sur **Terminer**.

Le lecteur sélectionné est monté et prêt avec la fenêtre de l'Explorateur Windows affichant les fichiers et dossiers contenus dans le partage.

3. Sélectionnez le fichier ou le répertoire pour lequel vous souhaitez définir les autorisations de fichier NTFS.
4. Cliquez avec le bouton droit de la souris sur le fichier ou le répertoire, puis sélectionnez **Propriétés**.
5. Sélectionnez l'onglet **sécurité**.

L'onglet **sécurité** affiche la liste des utilisateurs et des groupes pour lesquels les autorisations NTFS sont définies. La zone **autorisations pour** affiche une liste des autorisations Autoriser et refuser en vigueur pour chaque utilisateur ou groupe sélectionné.

6. Cliquez sur **Avancé**.

La fenêtre Propriétés de Windows affiche des informations sur les autorisations de fichier existantes attribuées aux utilisateurs et aux groupes.

7. Cliquez sur **Modifier les autorisations**.

La fenêtre autorisations s'ouvre.

8. Effectuez les opérations souhaitées :

Les fonctions que vous recherchez...	Procédez comme suit...
Configurez des autorisations NTFS avancées pour un nouvel utilisateur ou un nouveau groupe	<ol style="list-style-type: none"> a. Cliquez sur Ajouter. b. Dans la zone Entrez le nom de l'objet à sélectionner, saisissez le nom de l'utilisateur ou du groupe que vous souhaitez ajouter. c. Cliquez sur OK.
Modifiez les autorisations NTFS avancées d'un utilisateur ou d'un groupe	<ol style="list-style-type: none"> a. Dans la zone permissions Entrées:, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier les autorisations avancées. b. Cliquez sur Modifier.
Supprimez les autorisations NTFS avancées pour un utilisateur ou un groupe	<ol style="list-style-type: none"> a. Dans la zone permissions Entrées:, sélectionnez l'utilisateur ou le groupe à supprimer. b. Cliquez sur Supprimer. c. Passez à l'étape 13.

Si vous ajoutez des autorisations NTFS avancées sur un nouvel utilisateur ou un nouveau groupe ou si vous modifiez les autorisations avancées NTFS sur un utilisateur ou un groupe existant, la zone entrée d'autorisation de <objet> s'ouvre.

9. Dans la zone **appliquer à**, sélectionnez la façon dont vous souhaitez appliquer cette entrée d'autorisation de fichier NTFS.

Si vous configurez des autorisations de fichier NTFS sur un seul fichier, la case **appliquer à** n'est pas active. Le paramètre **appliquer à** est défini par défaut sur **cet objet uniquement**.

10. Dans la zone **permissions**, sélectionnez les cases **Autoriser** ou **refuser** pour les autorisations avancées que vous souhaitez définir sur cet objet.

- Pour autoriser l'accès spécifié, cochez la case **Autoriser**.
- Pour ne pas autoriser l'accès spécifié, cochez la case **Deny**.
Vous pouvez définir des autorisations sur les droits avancés suivants :

- **Contrôle total**

Si vous choisissez ce droit avancé, tous les autres droits avancés sont automatiquement choisis (autoriser ou refuser des droits).

- **Dossier traverse / fichier d'exécution**
- **Liste de dossiers / lecture de données**
- **Lire les attributs**
- **Lire les attributs étendus**
- **Créer des fichiers / écrire des données**
- **Créer des dossiers / ajouter des données**
- **Ecrire des attributs**
- **Ecrire des attributs étendus**
- **Supprimer des sous-dossiers et des fichiers**
- **Supprimer**
- **Autorisations de lecture**
- **Modifier les autorisations**
- * Prendre possession*



Si l'une des zones d'autorisation avancée n'est pas sélectionnable, c'est parce que les autorisations sont héritées de l'objet parent.

11. Si vous souhaitez que les sous-dossiers et les fichiers de cet objet héritent de ces autorisations, cochez la case **appliquer ces autorisations aux objets et/ou aux conteneurs dans ce conteneur uniquement**.
12. Cliquez sur **OK**.
13. Une fois que vous avez terminé d'ajouter, de supprimer ou de modifier des autorisations NTFS, spécifiez le paramètre d'héritage de cet objet :

- Sélectionnez la case **inclure les autorisations hérissables dans la boîte parent** de cet objet.

Il s'agit de la valeur par défaut.

- Sélectionnez la case **remplacer toutes les autorisations d'objet enfant par des autorisations hérissables de cet objet**.

Ce paramètre n'est pas présent dans la zone autorisations si vous définissez des autorisations de fichier NTFS sur un seul fichier.



Soyez prudent lorsque vous sélectionnez ce paramètre. Ce paramètre supprime toutes les autorisations existantes sur tous les objets enfants et les remplace par les paramètres d'autorisation de cet objet. Vous pourriez supprimer par inadvertance les autorisations que vous ne souhaitez pas supprimer. Il est particulièrement important lorsque vous définissez des autorisations dans un volume mixte de style de sécurité ou qtree. Si les objets enfant ont un style de sécurité UNIX effectif, la propagation des autorisations NTFS à ces objets enfant entraîne le ONTAP changement de style de sécurité UNIX au style de sécurité NTFS, et toutes les autorisations UNIX sur ces objets enfants sont remplacées par des autorisations NTFS.

- Sélectionnez les deux cases.
- Sélectionnez aucune case.

14. Cliquez sur **OK** pour fermer la case **permissions**.

15. Cliquez sur **OK** pour fermer la case **Paramètres de sécurité avancés pour <objet>**.

Pour plus d'informations sur la définition des autorisations NTFS avancées, consultez votre documentation Windows.

Informations associées

[Configurez et appliquez la sécurité des fichiers sur les fichiers et dossiers NTFS à l'aide de l'interface de ligne de commande](#)

[Affichage d'informations sur la sécurité des fichiers sur les volumes de style de sécurité NTFS](#)

[Affichage d'informations sur la sécurité des fichiers sur des volumes de style de sécurité mixtes](#)

[Affichage d'informations sur la sécurité des fichiers sur des volumes de style de sécurité UNIX](#)

Configurez les autorisations d'accès aux fichiers NTFS à l'aide de l'interface de ligne de commande ONTAP

Vous pouvez configurer les autorisations d'accès aux fichiers NTFS sur les fichiers et les répertoires à l'aide de l'interface de ligne de commande ONTAP. Cela vous permet de configurer les autorisations d'accès aux fichiers NTFS sans avoir à vous connecter aux données à l'aide d'un partage SMB sur un client Windows.

Vous pouvez configurer les autorisations d'accès aux fichiers NTFS en ajoutant des entrées aux listes de contrôle d'accès discrétionnaire NTFS (DACL) associées à un descripteur de sécurité NTFS. Le descripteur de sécurité est ensuite appliqué aux fichiers et répertoires NTFS.

Vous ne pouvez configurer les autorisations de fichier NTFS qu'à l'aide de la ligne de commande. Vous ne pouvez pas configurer les listes de contrôle d'accès NFSv4 en utilisant l'interface de ligne de commandes.

Étapes

1. Créez un descripteur de sécurité NTFS.

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -owner owner_name -group primary_group_name  
-control-flags-raw raw_control_flags
```

2. Ajoutez des listes de contrôle d'accès discrétionnaire au descripteur de sécurité NTFS.


```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name  
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to  
{this-folder|sub-folders|files}
```

3. Créez une stratégie de sécurité de fichiers/répertoires.

```
vserver security file-directory policy create -vserver svm_name -policy-name  
policy_name
```

Comment les autorisations d'accès aux fichiers UNIX permettent de contrôler l'accès aux fichiers sur SMB

Un volume FlexVol peut avoir l'un des trois types de style de sécurité suivants : NTFS, UNIX ou mixte. Vous pouvez accéder aux données via SMB quel que soit le style de sécurité. Cependant, des autorisations appropriées sur les fichiers UNIX sont nécessaires pour accéder aux données à l'aide de la sécurité effective d'UNIX.

Lorsque vous accédez aux données via SMB, plusieurs contrôles d'accès sont utilisés pour déterminer si un utilisateur est autorisé à effectuer une action demandée :

- Droits d'exportation

La configuration des autorisations d'exportation pour l'accès SMB est facultative.

- Partager les autorisations
- Autorisations liées aux fichiers

Les types d'autorisations de fichier suivants peuvent être appliqués aux données sur lesquelles l'utilisateur souhaite effectuer une action :

- NTFS
- ACL UNIX NFSv4
- Bits mode UNIX

Pour les données avec des ACL NFSv4 ou des bits de mode UNIX définis, les autorisations de style UNIX sont utilisées afin de déterminer les droits d'accès aux fichiers aux données. L'administrateur du SVM doit définir l'autorisation appropriée pour garantir que les utilisateurs disposent des droits nécessaires pour effectuer l'action souhaitée.



Les données d'un volume de type sécurité mixte peuvent avoir un style de sécurité NTFS ou UNIX. Si les données ont un style de sécurité UNIX effectif, les autorisations NFSv4 ou les bits du mode UNIX sont utilisés pour déterminer les droits d'accès aux fichiers aux données.

Accès sécurisé aux fichiers à l'aide du contrôle d'accès dynamique (DAC)

Sécuriser l'accès aux fichiers à l'aide de la présentation du contrôle d'accès dynamique (DAC)

Vous pouvez sécuriser l'accès à l'aide du contrôle d'accès dynamique et en créant des stratégies d'accès centrales dans Active Directory et en les appliquant aux fichiers et dossiers sur les SVM via des objets de stratégie de groupe appliqués (GPO, Applied Group Policy Objects). Vous pouvez configurer l'audit de manière à utiliser les

événements d'activation de stratégie d'accès central pour voir les effets des modifications apportées aux stratégies d'accès central avant de les appliquer.

Ajouts aux informations d'identification CIFS

Avant le contrôle d'accès dynamique, un identifiant CIFS incluait une identité de sécurité (de l'utilisateur) et une appartenance au groupe Windows. Avec le contrôle d'accès dynamique, trois autres types d'informations sont ajoutés à l'identité du périphérique, aux réclamations du périphérique et aux réclamations de l'utilisateur :

- Identité du périphérique

Analogique des informations d'identité de l'utilisateur, à l'exception de l'identité et de l'appartenance au groupe de l'appareil à partir de lequel l'utilisateur se connecte.

- Réclamations de l'appareil

Assertions sur un principal de sécurité de périphérique. Par exemple, un sinistre de périphérique peut être qu'il est membre d'une UO spécifique.

- Réclamations de l'utilisateur

Assertions sur un principal de sécurité utilisateur. Par exemple, une réclamation d'utilisateur peut être que son compte AD est membre d'une unité d'organisation spécifique.

Politiques d'accès centralisé

Les stratégies d'accès centrales aux fichiers permettent aux organisations de déployer et de gérer de manière centralisée des stratégies d'autorisation qui incluent des expressions conditionnelles à l'aide de groupes d'utilisateurs, de revendications d'utilisateurs, de revendications de périphériques et de propriétés de ressources.

Par exemple, pour accéder aux données à fort impact sur l'entreprise, un utilisateur doit être un employé à plein temps et n'a accès qu'aux données à partir d'un périphérique géré. Les stratégies d'accès central sont définies dans Active Directory et distribuées aux serveurs de fichiers via le mécanisme GPO.

Mise en place centralisée des stratégies d'accès avec audit avancé

Les politiques d'accès central peuvent être « mises en service », auquel cas elles sont évaluées de manière « par quoi » lors des contrôles d'accès aux fichiers. Les résultats de ce qui se serait passé si la stratégie était en vigueur et la différence par rapport à ce qui est actuellement configuré sont consignés en tant qu'événement d'audit. De cette façon, les administrateurs peuvent utiliser les journaux d'événements d'audit pour étudier l'impact d'une modification de stratégie d'accès avant de mettre la stratégie en jeu. Après avoir évalué l'impact d'une modification de règle d'accès, la règle peut être déployée via des GPO sur les SVM souhaités.

Informations associées

[Stratégies de groupe prises en charge](#)

[Application d'objets de stratégie de groupe aux serveurs CIFS](#)

[Activation ou désactivation de la prise en charge de GPO sur un serveur CIFS](#)

[Affichage des informations sur les configurations GPO](#)

[Affichage d'informations sur les règles d'accès central](#)

[Affichage d'informations sur les règles de stratégie d'accès central](#)

[Configuration des règles d'accès centrales pour sécuriser les données sur les serveurs CIFS](#)

[Affichage d'informations sur la sécurité du contrôle d'accès dynamique](#)

["Audit et suivi de sécurité SMB et NFS"](#)

Prise en charge de la fonctionnalité de contrôle dynamique d'accès

Si vous souhaitez utiliser le contrôle d'accès dynamique (DAC) sur votre serveur CIFS, vous devez comprendre comment ONTAP prend en charge la fonctionnalité de contrôle d'accès dynamique dans les environnements Active Directory.

Pris en charge pour le contrôle d'accès dynamique

ONTAP prend en charge la fonctionnalité suivante lorsque le contrôle d'accès dynamique est activé sur le serveur CIFS :

Fonctionnalité	Commentaires
Réclamations dans le système de fichiers	Les revendications sont des paires de nom et de valeur simples qui indiquent une certaine vérité sur un utilisateur. Les informations d'identification utilisateur contiennent des informations sur les sinistres, et les descripteurs de sécurité sur les fichiers peuvent effectuer des vérifications d'accès qui incluent des vérifications de sinistres. Les administrateurs peuvent ainsi mieux contrôler qui peut accéder aux fichiers.
Expressions conditionnelles pour les vérifications d'accès aux fichiers	Lors de la modification des paramètres de sécurité d'un fichier, les utilisateurs peuvent ajouter des expressions conditionnelles arbitrairement complexes au descripteur de sécurité du fichier. L'expression conditionnelle peut inclure des vérifications pour les sinistres.
Contrôle centralisé de l'accès aux fichiers via des règles d'accès centrales	Les stratégies d'accès central sont des types de listes de contrôle d'accès stockées dans Active Directory et peuvent être balisées vers un fichier. L'accès au fichier n'est accordé que si les contrôles d'accès du Security Descriptor sur disque et de la stratégie d'accès centrale balisée permettent l'accès. cela permet aux administrateurs de contrôler l'accès aux fichiers à partir d'un emplacement central (AD) sans avoir à modifier le Security Descriptor sur disque.
Mise en place de stratégies d'accès centrales	Ajoute la capacité d'essayer des changements de sécurité sans affecter l'accès réel aux fichiers, en "mettant en place" un changement aux politiques d'accès central, et en voyant l'effet de la modification dans un rapport d'audit.

Fonctionnalité	Commentaires
Affichage d'informations sur la sécurité des règles d'accès centrales à l'aide de l'interface de ligne de commande de ONTAP	Étend le <code>vserver security file-directory show</code> commande pour afficher les informations sur les règles d'accès central appliquées.
Suivi de la sécurité qui inclut les stratégies d'accès centralisé	Étend le <code>vserver security trace</code> famille de commandes permettant d'afficher les résultats qui incluent des informations sur les stratégies d'accès central appliquées.

Non pris en charge pour le contrôle d'accès dynamique

ONTAP ne prend pas en charge la fonctionnalité suivante lorsque le contrôle d'accès dynamique est activé sur le serveur CIFS :

Fonctionnalité	Commentaires
Classification automatique des objets du système de fichiers NTFS	Il s'agit d'une extension de l'infrastructure de classification de fichiers Windows qui n'est pas prise en charge dans ONTAP.
Audit avancé autre que la mise en place de stratégies d'accès centrales	Seul le staging de stratégie d'accès central est pris en charge pour l'audit avancé.

Considérations relatives à l'utilisation du contrôle d'accès dynamique et des règles d'accès central avec des serveurs CIFS

Vous devez garder à l'esprit certaines considérations lorsque vous utilisez le contrôle d'accès dynamique (DAC) et les règles d'accès central pour sécuriser les fichiers et dossiers sur les serveurs CIFS.

L'accès NFS peut être refusé à la racine si la règle de stratégie s'applique à l'utilisateur de domaine\administrateur

Dans certaines circonstances, l'accès NFS à la racine peut être refusé lorsque la sécurité de la stratégie d'accès centrale est appliquée aux données auxquelles l'utilisateur root tente d'accéder. Le problème se produit lorsque la stratégie d'accès central contient une règle appliquée au domaine\administrateur et que le compte racine est mappé au compte domaine\administrateur.

Au lieu d'appliquer une règle à l'utilisateur domaine/administrateur, vous devez appliquer la règle à un groupe avec des privilèges d'administration, tels que le groupe domaine/administrateurs. De cette façon, vous pouvez mapper root sur le compte domaine\administrateur sans que ce problème n'ait d'impact sur la racine.

Le groupe BUILTIN\Administrators du serveur CIFS a accès aux ressources lorsque la stratégie d'accès central appliquée n'est pas trouvée dans Active Directory

Il est possible que les ressources contenues dans le serveur CIFS aient des règles d'accès centrales qui leur sont appliquées, mais lorsque le serveur CIFS utilise le SID de la stratégie d'accès centrale pour tenter de récupérer des informations à partir d'Active Directory, le SID ne correspond à aucun SID de stratégie d'accès centrale existant dans Active Directory. Dans ces circonstances, le serveur CIFS applique la stratégie de

restauration par défaut locale pour cette ressource.

La stratégie de récupération par défaut locale permet au groupe BUILTIN\Administrators du serveur CIFS d'accéder à cette ressource.

Activer ou désactiver la présentation du contrôle d'accès dynamique

L'option qui vous permet d'utiliser le contrôle d'accès dynamique (DAC) pour sécuriser les objets sur votre serveur CIFS est désactivée par défaut. Vous devez activer cette option si vous souhaitez utiliser le contrôle d'accès dynamique sur votre serveur CIFS. Si vous décidez par la suite de ne pas utiliser le contrôle d'accès dynamique pour sécuriser les objets stockés sur le serveur CIFS, vous pouvez désactiver cette option.

Description de la tâche

Une fois le contrôle d'accès dynamique activé, le système de fichiers peut contenir des listes de contrôle d'accès avec des entrées liées au contrôle d'accès dynamique. Si le contrôle d'accès dynamique est désactivé, les entrées de contrôle d'accès dynamique actuelles seront ignorées et les nouvelles ne seront pas autorisées.

Cette option n'est disponible qu'au niveau de privilège avancé.

Étape

- 1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
- 2. Effectuez l'une des opérations suivantes :

Si vous voulez que le contrôle d'accès dynamique soit...	Entrez la commande...
Activé	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled true</code>
Désactivé	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled false</code>

- 3. Revenir au niveau de privilège administrateur : `set -privilege admin`

Informations associées

[Configuration des règles d'accès centrales pour sécuriser les données sur les serveurs CIFS](#)

Gérer les listes de contrôle d'accès qui contiennent des ACE de contrôle d'accès dynamique lorsque le contrôle d'accès dynamique est désactivé

Si vous disposez de ressources dont les listes de contrôle d'accès sont appliquées avec les ACE de contrôle d'accès dynamique et que vous désactivez le contrôle d'accès dynamique sur la machine virtuelle de stockage (SVM), vous devez supprimer les ACE de contrôle d'accès dynamique avant de pouvoir gérer les ACE de contrôle d'accès non dynamique sur cette ressource.

Description de la tâche

Une fois le contrôle d'accès dynamique désactivé, vous ne pouvez pas supprimer les ACE existants de

contrôle d'accès non dynamique ou ajouter de nouveaux ACE de contrôle d'accès non dynamique tant que vous n'avez pas supprimé les ACE de contrôle d'accès dynamique existants.

Vous pouvez utiliser n'importe quel outil que vous utilisez normalement pour gérer les listes de contrôle d'accès pour effectuer ces étapes.

Étapes

1. Déterminez quels ACE de contrôle d'accès dynamique sont appliqués à la ressource.
2. Supprimez les ACE de contrôle d'accès dynamique de la ressource.
3. Ajoutez ou supprimez des ACE de contrôle d'accès non dynamiques comme vous le souhaitez de la ressource.

Configurez les règles d'accès centrales pour sécuriser les données sur les serveurs CIFS

Il existe plusieurs étapes à suivre pour sécuriser l'accès aux données sur le serveur CIFS à l'aide de stratégies d'accès centrales, notamment l'activation du contrôle d'accès dynamique (DAC) sur le serveur CIFS, la configuration de stratégies d'accès central dans Active Directory, l'application des règles d'accès central aux conteneurs Active Directory avec des GPO, Et activation des stratégies de groupe sur le serveur CIFS.

Avant de commencer

- L'Active Directory doit être configuré pour utiliser les stratégies d'accès central.
- Vous devez disposer d'un accès suffisant sur les contrôleurs de domaine Active Directory pour créer des stratégies d'accès centrales et pour créer et appliquer des GPO aux conteneurs contenant les serveurs CIFS.
- Vous devez disposer d'un accès administratif suffisant sur le SVM (Storage Virtual machine) pour exécuter les commandes nécessaires.

Description de la tâche

Les stratégies d'accès central sont définies et appliquées aux objets de stratégie de groupe (GPO, Group Policy Objects) d'Active Directory. Vous pouvez consulter la bibliothèque Microsoft TechNet pour obtenir des instructions sur la configuration des stratégies d'accès centralisé et des GPO.

["Bibliothèque Microsoft TechNet"](#)

Étapes

1. Activer le contrôle dynamique d'accès sur le SVM si celui-ci n'est pas déjà activé à l'aide de `vserver cifs options modify` commande.


```
vserver cifs options modify -vserver vs1 -is-dac-enabled true
```
2. Activez les objets de stratégie de groupe (GPO, Group policy objects) sur le serveur CIFS s'ils ne sont pas déjà activés à l'aide de `vserver cifs group-policy modify` commande.


```
vserver cifs group-policy modify -vserver vs1 -status enabled
```
3. Créez des règles d'accès centrales et des stratégies d'accès central sur Active Directory.
4. Créez un objet de stratégie de groupe (GPO) pour déployer les stratégies d'accès central sur Active Directory.

5. Appliquez l'objet GPO au conteneur où se trouve le compte d'ordinateur du serveur CIFS.
6. Mettre à jour manuellement les GPO appliqués au serveur CIFS à l'aide de `vserver cifs group-policy update` commande.

```
vserver cifs group-policy update -vserver vs1
```

7. Vérifiez que la stratégie d'accès central GPO est appliquée aux ressources du serveur CIFS à l'aide de `vserver cifs group-policy show-applied` commande.

L'exemple suivant montre que la stratégie de domaine par défaut comporte deux stratégies d'accès central appliquées au serveur CIFS :

```
vserver cifs group-policy show-applied
```

```
Vserver: vs1
-----
GPO Name: Default Domain Policy
  Level: Domain
  Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
```

```
No enumeration of SAM accounts: true
No enumeration of SAM accounts and shares: false
Restrict anonymous access to shares and named pipes: true
Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
             cap2

GPO Name: Resultant Set of Policy
Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age: 7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
```



```
gpr1
gpr2
Central Access Policy Settings:
  Policies: cap1
            cap2
2 entries were displayed.
```

Informations associées

[Affichage des informations sur les configurations GPO](#)

[Affichage d'informations sur les règles d'accès central](#)

[Affichage d'informations sur les règles de stratégie d'accès central](#)

[Activation ou désactivation du contrôle d'accès dynamique](#)

Afficher des informations sur la sécurité du contrôle d'accès dynamique

Vous pouvez afficher des informations sur la sécurité DAC (Dynamic Access Control) sur des volumes NTFS et sur des données avec la sécurité efficace NTFS sur des volumes de type sécurité mixtes. Cela comprend de l'information sur les ACE conditionnels, les ACE de ressources et les ACE de politique d'accès central. Les résultats vous permettent de valider votre configuration de sécurité ou de résoudre les problèmes d'accès aux fichiers.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux données dont vous souhaitez afficher les informations de sécurité des fichiers ou des dossiers. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

Étape

1. Afficher les paramètres de sécurité des fichiers et des répertoires avec le niveau de détail souhaité :

Pour afficher les informations...	Saisissez la commande suivante...
Sous forme récapitulative	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
Avec détails étendus	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>
Où la sortie est affichée avec les SID de groupe et d'utilisateur	<pre>vserver security file-directory show -vserver vserver_name -path path -lookup-names false</pre>

Pour afficher les informations...	Saisissez la commande suivante...
A propos de la sécurité des fichiers et des répertoires pour les fichiers et les répertoires où le masque binaire hexadécimal est traduit en format texte	<code>vserver security file-directory show -vserver vserver_name -path path -textual-mask true</code>

Exemples

L'exemple suivant affiche les informations de sécurité du contrôle d'accès dynamique sur le chemin /vol1 Au SVM vs1 :

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
      Vserver: vs1
      File Path: /vol1
      File Inode Number: 112
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attribute: -
      Unix User Id: 0
      Unix Group Id: 1
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
      Control:0xbf14
      Owner:CIFS1\Administrator
      Group:CIFS1\Domain Admins
      SACL - ACEs
      ALL-Everyone-0xf01ff-OI|CI|SA|FA
      RESOURCE ATTRIBUTE-Everyone-0x0

      ("Department_MS",TS,0x10020,"Finance")
      POLICY ID-All resources - No Write-
      0x0-OI|CI
      DACL - ACEs
      ALLOW-CIFS1\Administrator-0x1f01ff-
      OI|CI
      ALLOW-Everyone-0x1f01ff-OI|CI
      ALLOW CALLBACK-DAC\user1-0x1200a9-
      OI|CI

      ((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@Device.department==@Resource.Department_MS)
```

Informations associées

[Affichage des informations sur les configurations GPO](#)

[Affichage d'informations sur les règles d'accès central](#)

[Affichage d'informations sur les règles de stratégie d'accès central](#)

Considérations relatives au contrôle d'accès dynamique

Vous devez savoir ce qui se passe lors du retour à une version de ONTAP qui ne prend pas en charge le contrôle d'accès dynamique (DAC) et ce que vous devez faire avant et après le rétablissement.

Si vous souhaitez restaurer le cluster vers une version de ONTAP qui ne prend pas en charge le contrôle d'accès dynamique et que le contrôle d'accès dynamique est activé sur une ou plusieurs machines virtuelles de stockage (SVM), vous devez effectuer les opérations suivantes avant le rétablissement :

- Vous devez désactiver le contrôle d'accès dynamique sur tous les SVM sur lesquels il est activé sur le cluster.
- Vous devez modifier toutes les configurations d'audit sur le cluster contenant le `cap-staging` type d'événement pour utiliser uniquement le `file-op` type d'événement.

Vous devez comprendre et agir sur certaines considérations importantes concernant la restauration des fichiers et dossiers avec les ACE Dynamic Access Control :

- Si le cluster est rétabli, les ACE de contrôle d'accès dynamique existants ne sont pas supprimés ; cependant, ils seront ignorés lors des vérifications d'accès aux fichiers.
- Comme les ACE de contrôle d'accès dynamique sont ignorés après réversion, l'accès aux fichiers change sur les fichiers avec les ACE de contrôle d'accès dynamique.

Cela pourrait permettre aux utilisateurs d'accéder aux fichiers qu'ils ne pouvaient pas accéder ou ne pouvaient pas accéder aux fichiers qu'ils pouvaient auparavant.

- Vous devez appliquer des ACE de contrôle d'accès non dynamique aux fichiers concernés pour restaurer leur niveau de sécurité précédent.

Cette opération peut être effectuée avant le rétablissement ou immédiatement après la fin de la nouvelle version.



Les ACE de contrôle d'accès dynamique étant ignorés après la réversion, il n'est pas nécessaire de les supprimer lors de l'application d'ACE de contrôle d'accès non dynamique aux fichiers affectés. Toutefois, si vous le souhaitez, vous pouvez les supprimer manuellement.

Où trouver des informations supplémentaires sur la configuration et l'utilisation du contrôle d'accès dynamique et des stratégies d'accès central

Des ressources supplémentaires sont disponibles pour vous aider à configurer et utiliser le contrôle d'accès dynamique et les stratégies d'accès central.

Vous trouverez des informations sur la configuration des stratégies de contrôle d'accès dynamique et d'accès central dans Active Directory dans la bibliothèque Microsoft TechNet.

["Microsoft TechNet : présentation des scénarios de contrôle d'accès dynamique"](#)

["Microsoft TechNet : scénario de stratégie d'accès centralisé"](#)

Les références suivantes peuvent vous aider à configurer le serveur SMB afin qu'il utilise et prend en charge les stratégies de contrôle d'accès dynamique et d'accès central :

- **Utilisation de stratégies de groupe sur le serveur SMB**

[Application d'objets de stratégie de groupe aux serveurs SMB](#)

- **Configuration de l'audit NAS sur le serveur SMB**

["Audit et suivi de sécurité SMB et NFS"](#)

Sécurisez l'accès SMB à l'aide de règles d'exportation

Mode d'utilisation des export-policy avec les accès SMB

Si les export policy pour accès SMB sont activées sur le serveur SMB, les export policies sont utilisées lors du contrôle de l'accès aux volumes du SVM par les clients SMB. Pour accéder aux données, vous pouvez créer une export policy qui autorise l'accès SMB, puis associer la policy aux volumes contenant des partages SMB.

Une export policy applique une ou plusieurs règles qui lui permettent de spécifier les clients autorisés à accéder aux données et les protocoles d'authentification pris en charge pour l'accès en lecture seule et en lecture/écriture. Vous pouvez configurer des stratégies d'exportation afin d'autoriser l'accès via SMB à tous les clients, à un sous-réseau de clients ou à un client spécifique et autoriser l'authentification à l'aide de l'authentification Kerberos, de l'authentification NTLM ou des deux authentifications Kerberos et NTLM lors de la détermination de l'accès en lecture seule et en lecture/écriture aux données.

Après le traitement de toutes les règles d'exportation appliquées à l'export policy, ONTAP peut déterminer si le client dispose d'un accès et quel niveau d'accès. Les règles d'exportation s'appliquent aux ordinateurs clients et non aux utilisateurs et groupes Windows. Les règles d'exportation ne remplacent pas l'authentification et l'autorisation basées sur les utilisateurs et les groupes Windows. Les règles d'exportation offrent une autre couche de sécurité d'accès en plus des autorisations de partage et d'accès aux fichiers.

Vous associez exactement une export policy à chaque volume pour configurer l'accès client au volume. Chaque SVM peut contenir plusieurs export policy. Vous pouvez ainsi effectuer les opérations suivantes pour les SVM avec plusieurs volumes :

- Assigner différentes export policy à chaque volume du SVM pour le contrôle d'accès client individuel à chaque volume du SVM.
- Assigner la même export policy à plusieurs volumes du SVM pour un contrôle d'accès client identique sans avoir à créer de nouvelles export policy pour chaque volume.

Chaque SVM possède au moins une export policy appelée « default », qui ne contient aucune règle. Vous ne pouvez pas supprimer cette export-policy, mais vous pouvez la renommer ou la modifier. Par défaut, chaque volume du SVM est associé aux export policy par défaut. Si les export policy pour accès SMB sont désactivées sur le SVM, la « default » export policy n'a aucun impact sur l'accès SMB.

Vous pouvez configurer les règles fournissant l'accès aux hôtes NFS et SMB et associer cette règle à une export policy, qui peut ensuite être associée au volume qui contient des données auxquelles les hôtes NFS et SMB ont besoin d'accéder. Alternativement, s'il existe des volumes dans lesquels seuls les clients SMB ont

besoin d'accéder, vous pouvez configurer une export policy avec des règles qui autorisent uniquement l'accès à l'aide du protocole SMB et qui utilisent uniquement Kerberos ou NTLM (ou les deux) pour l'authentification en lecture seule et l'accès en écriture. L'export policy est ensuite associée aux volumes pour lesquels seul l'accès SMB est souhaité.

Si les export policy pour SMB sont activées et qu'un client effectue une demande d'accès qui n'est pas autorisée par les export policy applicables, la requête échoue et un message d'autorisation refusée. Si un client ne correspond à aucune règle de l'export policy du volume, l'accès est refusé. Si une export policy est vide, alors tous les accès sont implicitement refusés. Ceci est vrai même si les autorisations de partage et de fichier autorisent autrement l'accès. Cela signifie que vous devez configurer votre export policy de manière à limiter les possibilités suivantes sur les volumes contenant des partages SMB :

- Autoriser l'accès à tous les clients ou au sous-ensemble de clients approprié
- Autoriser l'accès via SMB
- Autoriser un accès en lecture seule et en écriture approprié via l'authentification Kerberos ou NTLM (ou les deux)

Découvrez ["configuration et gestion des export-policies"](#).

Fonctionnement des règles d'exportation

Les règles d'exportation sont les éléments fonctionnels d'une export-policy. Les règles d'exportation correspondent aux demandes d'accès client à un volume par rapport à des paramètres spécifiques que vous configurez pour déterminer comment traiter les demandes d'accès client.

Une export-policy doit contenir au moins une règle d'exportation pour permettre l'accès aux clients. Si une export-policy contient plusieurs règles, celles-ci sont traitées dans l'ordre dans lequel elles apparaissent dans l'export-policy. L'ordre des règles est dicté par le numéro d'index des règles. Si une règle correspond à un client, les autorisations de cette règle sont utilisées et aucune autre règle n'est traitée. Si aucune règle ne correspond, l'accès au client est refusé.

Vous pouvez configurer des règles d'exportation pour déterminer les autorisations d'accès client à l'aide des critères suivants :

- Protocole d'accès aux fichiers utilisé par le client envoyant la requête, par exemple, NFSv4 ou SMB.
- Identifiant client, par exemple, nom d'hôte ou adresse IP.

La taille maximale du `-clientmatch` le champ est composé de 4096 caractères.

- Type de sécurité utilisé par le client pour l'authentification, par exemple Kerberos v5, NTLM ou AUTH_SYS.

Si une règle spécifie plusieurs critères, le client doit tous les correspondre pour que la règle s'applique.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`

- `-rwrule any`

La requête d'accès client est envoyée à l'aide du protocole NFSv3 et le client a l'adresse IP 10.1.17.37.

Bien que le protocole d'accès client corresponde, l'adresse IP du client se trouve dans un sous-réseau différent de celui spécifié dans la règle d'exportation. Par conséquent, la correspondance des clients échoue et cette règle ne s'applique pas à ce client.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La requête d'accès client est envoyée via le protocole NFSv4 et le client a l'adresse IP 10.1.16.54.

Le protocole d'accès client correspond et l'adresse IP du client se trouve dans le sous-réseau spécifié. Par conséquent, la correspondance du client a réussi et cette règle s'applique à ce client. Le client obtient un accès en lecture-écriture quel que soit son type de sécurité.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Le client #1 a l'adresse IP 10.1.16.207, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec AUTH_SYS.

Le protocole d'accès client et l'adresse IP correspondent pour les deux clients. Le paramètre en lecture seule permet l'accès en lecture seule à tous les clients, quel que soit le type de sécurité auquel ils sont authentifiés. Par conséquent, les deux clients bénéficient d'un accès en lecture seule. Cependant, seul le client #1 obtient l'accès en lecture-écriture car il a utilisé le type de sécurité approuvé Kerberos v5 pour s'authentifier. Le client n° 2 ne dispose pas d'un accès en lecture/écriture.

Exemples de règles d'export-policy qui limitent ou autorisent l'accès à SMB

Les exemples montrent comment créer des règles d'export policy qui limitent ou autorisent l'accès via SMB sur un SVM dont les export policy pour l'accès SMB sont activées.

Les export policy pour accès SMB sont désactivées par défaut. Vous devez configurer des règles d'export policy qui limitent ou autorisent l'accès sur SMB uniquement si vous avez activé les export policy pour l'accès

SMB.

Règle d'exportation pour l'accès SMB uniquement

La commande suivante crée une règle d'exportation sur le SVM nommé « vs1 » qui dispose de la configuration suivante :

- Nom de la politique: Cifs1
- Numéro d'index : 1
- Correspondance client : correspond uniquement aux clients sur le réseau 192.168.1.0/24
- Protocole : autorise uniquement l'accès SMB
- Accès en lecture seule : aux clients utilisant l'authentification NTLM ou Kerberos
- Accès en lecture/écriture : aux clients utilisant l'authentification Kerberos

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname  
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0  
-rorule krb5,ntlm -rwrule krb5
```

Règle d'exportation pour les accès SMB et NFS

La commande suivante crée une règle d'exportation sur le SVM nommé « vs1 », qui dispose de la configuration suivante :

- Nom de la politique: Cifs1
- Numéro d'index : 2
- Correspondance client : correspond à tous les clients
- Protocole : accès SMB et NFS
- Accès en lecture seule : pour tous les clients
- Accès en lecture/écriture : aux clients utilisant l'authentification Kerberos (NFS et SMB) ou NTLM (SMB)
- Mappage de l'ID utilisateur UNIX 0 (zéro) : mappé à l'ID utilisateur 65534 (qui correspond généralement au nom utilisateur personne)
- L'accès SUID et sgID permet

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname  
cifs nfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any  
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Règle d'exportation pour accès SMB uniquement à l'aide de NTLM

La commande suivante crée une règle d'exportation sur le SVM nommé « vs1 » qui dispose de la configuration suivante :

- Nom de la stratégie : ntlm1
- Numéro d'index : 1

- Correspondance client : correspond à tous les clients
- Protocole : autorise uniquement l'accès SMB
- Accès en lecture seule : uniquement aux clients utilisant NTLM
- Accès en lecture/écriture : uniquement aux clients utilisant NTLM



Si vous configurez l'option lecture seule ou l'option lecture/écriture pour l'accès NTLM uniquement, vous devez utiliser des entrées basées sur l'adresse IP dans l'option de correspondance client. Autrement, vous recevez `access denied` erreurs. En effet, ONTAP utilise les noms de service Kerberos (SPN) lors de l'utilisation d'un nom d'hôte pour vérifier les droits d'accès du client. L'authentification NTLM ne prend pas en charge les noms SPN.

```
cluster1::> vservers export-policy rule create -vservers vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Activez ou désactivez les export policy pour l'accès SMB

Vous pouvez activer ou désactiver les export policy pour l'accès SMB sur les SVM (Storage Virtual machines). L'utilisation des règles d'exportation pour contrôler l'accès SMB aux ressources est facultative.

Avant de commencer

Les conditions suivantes sont requises pour l'activation des export policy pour SMB :

- Le client doit avoir un enregistrement « PTR » dans DNS avant de créer les règles d'exportation pour ce client.
- Un ensemble supplémentaire d'enregistrements « A » et « PTR » pour les noms d'hôte est nécessaire si la SVM fournit l'accès aux clients NFS et que le nom d'hôte que vous souhaitez utiliser pour l'accès NFS est différent du nom du serveur CIFS.

Description de la tâche

Lors de la configuration d'un nouveau serveur CIFS sur votre SVM, l'utilisation des export policies pour l'accès SMB est désactivée par défaut. Vous pouvez activer des export policy pour l'accès SMB si vous souhaitez contrôler l'accès en fonction du protocole d'authentification, des adresses IP clientes ou des noms d'hôte. Vous pouvez activer ou désactiver des export policy pour l'accès SMB à tout moment.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Activer ou désactiver les export-policies :
 - Activer les export-policies : `vservers cifs options modify -vservers vservers_name -is -exportpolicy-enabled true`
 - Désactiver les export-policies : `vservers cifs options modify -vservers vservers_name -is -exportpolicy-enabled false`
3. Retour au niveau de privilège admin : `set -privilege admin`

Exemple

L'exemple suivant permet d'utiliser les export policy pour contrôler l'accès des clients SMB aux ressources sur le SVM vs1 :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

Sécurisez l'accès aux fichiers à l'aide de Storage-Level Access Guard

Sécurisez l'accès aux fichiers à l'aide de Storage-Level Access Guard

Outre la sécurisation de l'accès à l'aide de la sécurité native au niveau des fichiers et de l'exportation et du partage, vous pouvez configurer Storage-Level Access Guard, une troisième couche de sécurité appliquée par ONTAP au niveau du volume. Storage-Level Access Guard s'applique à l'accès à partir de tous les protocoles NAS vers l'objet de stockage auquel il est appliqué.

Seules les autorisations d'accès NTFS sont prises en charge. Pour que ONTAP puisse effectuer des vérifications de sécurité sur les utilisateurs UNIX afin d'accéder aux données sur les volumes pour lesquels Storage-Level Access Guard a été appliqué, l'utilisateur UNIX doit mapper un utilisateur Windows sur le SVM propriétaire du volume.

Comportement de la protection d'accès au niveau du stockage

- Storage-Level Access Guard s'applique à tous les fichiers ou tous les répertoires d'un objet de stockage.

Comme tous les fichiers ou répertoires d'un volume sont soumis aux paramètres Storage-Level Access Guard, l'héritage par propagation n'est pas requis.

- Vous pouvez configurer Storage-Level Access Guard pour qu'il s'applique aux fichiers uniquement, aux répertoires uniquement ou aux fichiers et répertoires d'un volume.

- Sécurité des fichiers et des répertoires

S'applique à chaque répertoire et fichier de l'objet de stockage. Il s'agit du paramètre par défaut.

- Sécurité des fichiers

S'applique à chaque fichier de l'objet de stockage. L'application de cette sécurité n'affecte pas l'accès aux répertoires ou leur audit.

- Sécurité de l'annuaire

S'applique à chaque répertoire de l'objet de stockage. L'application de cette sécurité n'affecte pas l'accès aux fichiers ou leur audit.

- Storage-Level Access Guard est utilisé pour restreindre les autorisations.

Il ne vous donnera jamais d'autorisations d'accès supplémentaires.

- Si vous affichez les paramètres de sécurité d'un fichier ou d'un répertoire à partir d'un client NFS ou SMB, vous ne voyez pas la sécurité Storage-Level Access Guard.

Elle est appliquée au niveau de l'objet de stockage et stockée dans les métadonnées utilisées afin de déterminer les autorisations efficaces.

- La sécurité au niveau du stockage ne peut pas être révoquée d'un client, même par un administrateur système (Windows ou UNIX).

Il est conçu pour être modifié par les administrateurs de stockage uniquement.

- Vous pouvez appliquer Storage-Level Access Guard aux volumes dotés de NTFS ou d'un style de sécurité mixte.
- Vous pouvez appliquer Storage-Level Access Guard aux volumes de style de sécurité UNIX, tant que le SVM contenant le volume a un serveur CIFS configuré.
- Lorsque les volumes sont montés sous un chemin de jonction de volume et que Storage-Level Access Guard est présent sur ce chemin, il ne sera pas propagé aux volumes montés sous celui-ci.
- Le descripteur de sécurité Storage-Level Access Guard est répliqué avec la réplication des données SnapMirror et avec la réplication SVM.
- Il existe une dispensation spéciale pour les scanners de virus.

Un accès exceptionnel est autorisé à ces serveurs pour afficher des fichiers et des répertoires, même si Storage-Level Access Guard refuse l'accès à l'objet.

- Les notifications FPolicy ne sont pas envoyées si l'accès est refusé car la protection d'accès du niveau de stockage est disponible.

Ordre des contrôles d'accès

L'accès à un fichier ou à un répertoire est déterminé par l'effet combiné des autorisations d'exportation ou de partage, des autorisations Storage-Level Access Guard définies sur les volumes et des autorisations de fichier natif appliquées aux fichiers et/ou répertoires. Tous les niveaux de sécurité sont évalués pour déterminer les autorisations efficaces qu'un fichier ou un répertoire possède. Les contrôles d'accès de sécurité sont effectués dans l'ordre suivant :

1. Partage SMB ou autorisations au niveau des exportations NFS
2. Protection d'accès au niveau du stockage
3. Listes de contrôle d'accès aux fichiers/dossiers NTFS (ACL), listes de contrôle d'accès NFSv4 ou bits en mode UNIX

Cas d'utilisation de Storage-Level Access Guard

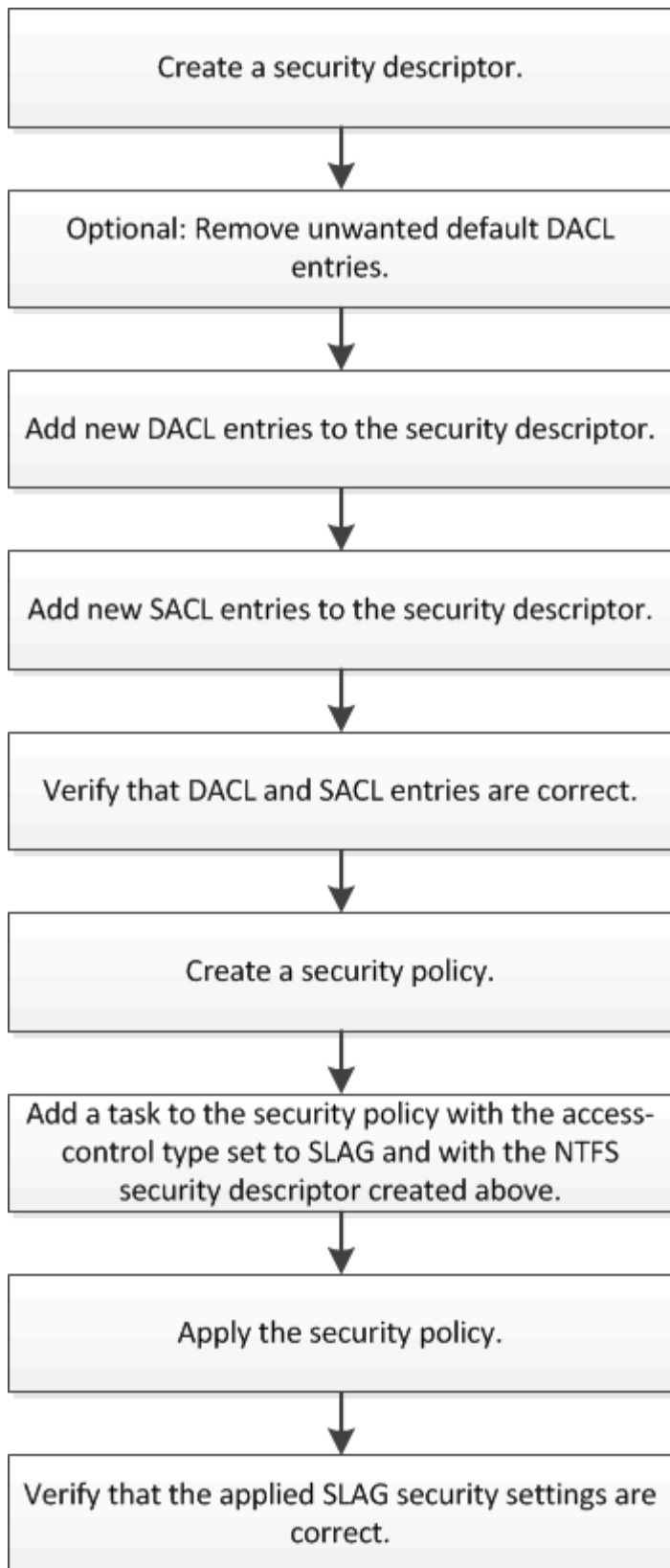
Storage-Level Access Guard fournit une sécurité supplémentaire au niveau du stockage, qui n'est pas visible du côté client. Par conséquent, il ne peut être révoqué par aucun des utilisateurs ou administrateurs de leur poste de travail. Dans certains cas, il est préférable de pouvoir contrôler l'accès au niveau de stockage.

Les cas d'utilisation typiques de cette fonctionnalité sont les suivants :

- Protection de la propriété intellectuelle par l'audit et le contrôle de l'accès de tous les utilisateurs au niveau du stockage
- Stockage pour les entreprises de services financiers, y compris les services bancaires et les groupes de transactions
- Services publics avec stockage de fichiers distinct dans les différents départements
- Universités protégeant tous les fichiers des étudiants

Workflow de configuration de Storage-Level Access Guard

Le workflow de configuration de Storage-Level Access Guard (SLAG) utilise les mêmes commandes CLI de ONTAP que celles que vous utilisez pour configurer les autorisations d'accès aux fichiers NTFS et les stratégies d'audit. Au lieu de configurer l'accès aux fichiers et aux répertoires sur une cible désignée, vous configurez LE SLAG sur le volume SVM (Storage Virtual machine) désigné.



Informations associées

[Configuration de Storage-Level Access Guard](#)

Plusieurs étapes sont nécessaires pour configurer Storage-Level Access Guard sur un volume ou un qtree. Storage-Level Access Guard fournit un niveau de sécurité d'accès défini au niveau du stockage. Elle fournit une sécurité qui s'applique à tous les accès à partir de tous les protocoles NAS vers l'objet de stockage auquel il a été appliqué.

Étapes

- 1. Créez un descripteur de sécurité à l'aide du `vserver security file-directory ntfs create` commande.

`vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sdl vserver security file-directory ntfs show -vserver vs1`

```
Vserver: vs1

NTFS Security      Owner Name
Descriptor Name
-----
sdl                -
```

Un descripteur de sécurité est créé avec les quatre entrées de contrôle d'accès DACL (ACE) suivantes :

```
Vserver: vs1
NTFS Security Descriptor Name: sdl

Account Name      Access  Access  Apply To
                  Type    Rights
-----
BUILTIN\Administrators
allow    full-control  this-folder, sub-folders,
files
BUILTIN\Users
allow    full-control  this-folder, sub-folders,
files
CREATOR OWNER
allow    full-control  this-folder, sub-folders,
files
NT AUTHORITY\SYSTEM
allow    full-control  this-folder, sub-folders,
files
```

Si vous ne souhaitez pas utiliser les entrées par défaut lors de la configuration de Storage-Level Access Guard, vous pouvez les supprimer avant de créer et d'ajouter vos propres ACE au descripteur de sécurité.

- 2. Supprimez l'un des ACE DACL par défaut du descripteur de sécurité que vous ne souhaitez pas configurer avec la sécurité Storage-Level Access Guard :

- a. Supprimez les ACE DACL indésirables à l'aide du `vserver security file-directory ntfs dacl remove` commande.

Dans cet exemple, trois ACE DACL par défaut sont supprimés du descripteur de sécurité : BUILTIN\Administrators, BULTIN\Users et CRÉATEUR OWNER.

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
-access-type allow -account builtin\users vserver security file-directory
ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
builtin\administrators vserver security file-directory ntfs dacl remove
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

- b. Vérifiez que les ACE DACL que vous ne souhaitez pas utiliser pour la sécurité Storage-Level Access Guard sont supprimés du descripteur de sécurité à l'aide de `vserver security file-directory ntfs dacl show` commande.

Dans cet exemple, la sortie de la commande vérifie que trois ACE DACL par défaut ont été supprimés du descripteur de sécurité, ne laissant que l'entrée ACE DACL par défaut du SYSTÈME/AUTORITÉ NT :

```
vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access      Access      Apply To
Type              Rights
-----
NT AUTHORITY\SYSTEM
                  allow      full-control  this-folder, sub-folders,
files
```

3. Ajoutez une ou plusieurs entrées DACL à un descripteur de sécurité en utilisant le `vserver security file-directory ntfs dacl add` commande.

Dans cet exemple, deux ACE DACL sont ajoutés au descripteur de sécurité :

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account example\engineering -rights full-control -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs dacl add
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
-rights read -apply-to this-folder,sub-folders,files
```

4. Ajoutez une ou plusieurs entrées SACL à un descripteur de sécurité à l'aide du `vserver security file-directory ntfs sacl add` commande.

Dans cet exemple, deux ACE SACL sont ajoutés au descripteur de sécurité :

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
```

```
this-folder,sub-folders,files vserver security file-directory ntfs sac1 add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Vérifier que les ACE DACL et SACL sont correctement configurés à l'aide du `vserver security file-directory ntfs dacl show` et `vserver security file-directory ntfs sac1 show` respectivement.

Dans cet exemple, la commande suivante affiche des informations sur les entrées DACL pour le descripteur de sécurité "sd1":

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
EXAMPLE\Domain Users	allow	read	this-folder, sub-folders, files
EXAMPLE\engineering	allow	full-control	this-folder, sub-folders, files
NT AUTHORITY\SYSTEM	allow	full-control	this-folder, sub-folders, files

Dans cet exemple, la commande suivante affiche des informations sur les entrées SACL pour le descripteur de sécurité « `sd1' » :

```
vserver security file-directory ntfs sac1 show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
EXAMPLE\Domain Users	failure	read	this-folder, sub-folders, files
EXAMPLE\engineering	success	full-control	this-folder, sub-folders, files

6. Créez une stratégie de sécurité à l'aide de `vserver security file-directory policy create` commande.

L'exemple suivant crée une politique nommée « politique 1 » :

```
vserver security file-directory policy create -vserver vs1 -policy-name policy1
```

7. Vérifiez que la stratégie est correctement configurée à l'aide du `vserver security file-directory policy show` commande.

```
vserver security file-directory policy show
```

Vserver	Policy Name
-----	-----
vs1	policy1

8. Ajoutez une tâche avec un descripteur de sécurité associé à la stratégie de sécurité en utilisant le `vserver security file-directory policy task add` commande avec `-access-control` paramètre défini sur `slag`.

Même si une stratégie peut contenir plusieurs tâches Storage-Level Access Guard, vous ne pouvez pas configurer une stratégie pour contenir à la fois des tâches file-Directory et Storage-Level Access Guard. Une stratégie doit contenir soit toutes les tâches Storage-Level Access Guard, soit toutes les tâches du répertoire de fichiers.

Dans cet exemple, une tâche est ajoutée à la politique nommée "politie1", qui est affectée au descripteur de sécurité "s1". Il est affecté à l' `/datavol1` chemin avec le type de contrôle d'accès défini sur "stable".

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode propagate -ntfs-sd sd1
```

9. Vérifiez que la tâche est correctement configurée à l'aide de l' `vserver security file-directory policy task show` commande.

```
vserver security file-directory policy task show -vserver vs1 -policy-name policy1
```



```
Vserver: vs1
Policy: policy1
```

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	Descriptor
Name					
-----	-----	-----	-----	-----	

1	/datavol1	slag	ntfs	propagate	sd1

10. Appliquez la stratégie de sécurité de Storage-Level Access Guard à l'aide du `vserver security file-directory apply` commande.

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

La tâche d'application de la stratégie de sécurité est planifiée.

11. Vérifiez que les paramètres de sécurité de Storage-Level Access Guard sont corrects à l'aide de l'`vserver security file-directory show` commande.

Dans cet exemple, le résultat de la commande indique que la sécurité Storage-Level Access Guard a été appliquée au volume NTFS `/datavol1`. Bien que la DACL par défaut permettant un contrôle total à tout le monde reste, la sécurité de Storage-Level Access Guard limite (et vérifie) l'accès aux groupes définis dans les paramètres Storage-Level Access Guard.

```
vserver security file-directory show -vserver vs1 -path /datavol1
```

```

        Vserver: vs1
        File Path: /datavol1
File Inode Number: 77
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
              Control:0x8004
              Owner:BUILTIN\Administrators
              Group:BUILTIN\Administrators
              DACL - ACEs
                  ALLOW-Everyone-0x1f01ff
                  ALLOW-Everyone-0x10000000-OI|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
    AUDIT-EXAMPLE\Domain Users-0x120089-FA
    AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
    ALLOW-EXAMPLE\Domain Users-0x120089
    ALLOW-EXAMPLE\engineering-0x1f01ff
    ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
    AUDIT-EXAMPLE\Domain Users-0x120089-FA
    AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
    ALLOW-EXAMPLE\Domain Users-0x120089
    ALLOW-EXAMPLE\engineering-0x1f01ff
    ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

Informations associées

[Gestion de la sécurité des fichiers NTFS, des règles d'audit NTFS et Storage-Level Access Guard sur les SVM via l'interface de ligne de commande](#)

[Workflow de configuration de Storage-Level Access Guard](#)

[Affichage d'informations sur Storage-Level Access Guard](#)

[Retrait de Storage-Level Access Guard](#)

Matrice de SCORIES efficace

Vous pouvez configurer LE SCORIES sur un volume, un qtree ou les deux. La matrice DE SCORIES définit le volume ou qtree en tant que configuration SLAG applicable dans les différents scénarios répertoriés dans le tableau.

	SCORIES de volume dans un système AFS	FIGURE de volume dans une copie Snapshot	Qtree SCORIES dans un système AFS	Qtree LAG dans une copie Snapshot
Accès au volume dans un système de fichiers d'accès (AFS)	OUI	NON	S/O	S/O
Accès de volume dans une copie Snapshot	OUI	NON	S/O	S/O
Accès au qtree dans un AFS (lorsque LE SCORIES est présent dans le qtree)	NON	NON	OUI	NON
Accès au qtree dans un AFS (lorsque LE SCORIES n'est pas présente dans le qtree)	OUI	NON	NON	NON
Accès qtree dans la copie Snapshot (lorsque LE SCORIES est présente dans le qtree AFS)	NON	NON	OUI	NON
Accès qtree dans la copie Snapshot (si SLAG n'est pas présent dans le qtree AFS)	OUI	NON	NON	NON

Afficher des informations sur Storage-Level Access Guard

La protection d'accès au niveau du stockage est une troisième couche de sécurité appliquée à un volume ou à un qtree. Les paramètres de Storage-Level Access Guard ne peuvent pas être affichés à l'aide de la fenêtre Propriétés de Windows. Vous devez utiliser l'interface de ligne de commande ONTAP pour afficher des informations sur la

sécurité de Storage-Level Access Guard, que vous pouvez utiliser pour valider votre configuration ou pour résoudre les problèmes d'accès aux fichiers.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès au volume ou qtree dont vous souhaitez afficher les informations de sécurité Storage-Level Access Guard. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

Étape

- 1. Afficher les paramètres de sécurité de Access Guard au niveau du stockage avec le niveau de détail souhaité :

Pour afficher les informations...	Saisissez la commande suivante...
Sous forme récapitulative	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Avec détails étendus	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Exemples

L'exemple suivant présente les informations de sécurité Storage-Level Access Guard pour le volume de style de sécurité NTFS avec le chemin d'accès /datavol1 Au SVM vs1 :

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1
```

```

    Vserver: vs1
    File Path: /datavol1
    File Inode Number: 77
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
          Control:0x8004
          Owner: BUILTIN\Administrators
          Group: BUILTIN\Administrators
          DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-OI|CI|IO

    Storage-Level Access Guard security
    SACL (Applies to Directories):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Directories):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
    SACL (Applies to Files):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Files):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

L'exemple suivant affiche les informations Storage-Level Access Guard sur le volume de style de sécurité mixte au niveau du chemin /datavol15 Au SVM vs1. Le niveau supérieur de ce volume dispose d'une sécurité effective UNIX. Le volume est doté de la sécurité Storage-Level Access Guard.

```

cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
      Vserver: vs1
      File Path: /datavol5
      File Inode Number: 3374
      Security Style: mixed
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 755
      Unix Mode Bits in Text: rwxr-xr-x
      ACLs: Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

Retirez la protection d'accès au niveau du stockage

Vous pouvez supprimer Storage-Level Access Guard sur un volume ou qtree si vous ne souhaitez plus définir de sécurité d'accès au niveau du stockage. La suppression de Storage-Level Access Guard ne modifie pas ou ne supprime pas la sécurité des fichiers et répertoires NTFS standard.

Étapes

1. Vérifier que la protection d'accès au niveau du stockage est configurée à l'aide du volume ou qtree
vserver security file-directory show commande.

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```

Vserver: vs1
File Path: /datavol2
File Inode Number: 99
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0xbf14
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
SACL - ACEs
AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

Storage-Level Access Guard security
DACL (Applies to Directories):
ALLOW-BUILTIN\Administrators-0x1f01ff
ALLOW-CREATOR OWNER-0x1f01ff
ALLOW-EXAMPLE\Domain Admins-0x1f01ff
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
DACL (Applies to Files):
ALLOW-BUILTIN\Administrators-0x1f01ff
ALLOW-CREATOR OWNER-0x1f01ff
ALLOW-EXAMPLE\Domain Admins-0x1f01ff
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

2. Retirez le protecteur d'accès au niveau du stockage à l'aide du `vserver security file-directory remove-slag` commande.

```
vserver security file-directory remove-slag -vserver vs1 -path /datavol2
```

3. Vérifiez que Storage-Level Access Guard a été supprimé du volume ou qtree en utilisant le `vserver security file-directory show` commande.

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```
Vserver: vs1
File Path: /datavol2
File Inode Number: 99
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0xbf14
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
SACL - ACEs
AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

Gérer l'accès aux fichiers via SMB

Utilisez des utilisateurs et des groupes locaux pour l'authentification et l'autorisation

Utilisation des utilisateurs et des groupes locaux par ONTAP

Concepts d'utilisateurs et de groupes locaux

Vous devez connaître les utilisateurs et les groupes locaux, ainsi que quelques informations de base à leur sujet, avant de déterminer si vous devez configurer et utiliser des utilisateurs et des groupes locaux dans votre environnement.

- **Utilisateur local**

Un compte utilisateur avec un identifiant de sécurité unique (SID) qui n'a de visibilité que sur la machine virtuelle de stockage (SVM) sur laquelle elle est créée. Les comptes d'utilisateur locaux ont un ensemble d'attributs, y compris le nom d'utilisateur et le SID. Un compte utilisateur local s'authentifie localement sur le serveur CIFS à l'aide de l'authentification NTLM.

Les comptes d'utilisateur ont plusieurs utilisations :

- Permet d'accorder des privilèges *User Rights Management* à un utilisateur.
- Permet de contrôler l'accès au niveau du partage et du fichier aux ressources de fichiers et de dossiers détenues par la SVM.

- **Groupe local**

Un groupe avec un SID unique n'a de visibilité que sur le SVM sur lequel il est créé. Les groupes contiennent un ensemble de membres. Les membres peuvent être des utilisateurs locaux, des utilisateurs de domaine, des groupes de domaines et des comptes de machine de domaine. Les groupes peuvent être créés, modifiés ou supprimés.

Les groupes ont plusieurs utilisations :

- Utilisé pour accorder des privilèges *User Rights Management* à ses membres.
- Permet de contrôler l'accès au niveau du partage et du fichier aux ressources de fichiers et de dossiers détenues par la SVM.

- **Domaine local**

Domaine qui dispose de son étendue locale, limitée par le SVM. Le nom du domaine local est le nom du serveur CIFS. Les utilisateurs et groupes locaux sont contenus dans le domaine local.

- **Identificateur de sécurité (SID)**

Un SID est une valeur numérique de longueur variable qui identifie les entités de sécurité de type Windows. Par exemple, un SID type prend le format suivant : s-1-5-21-3139654847-1303905135-2517279418-123456.

- **Authentification NTLM**

Méthode de sécurité Microsoft Windows utilisée pour authentifier les utilisateurs sur un serveur CIFS.

- **Cluster Replicated database (RDB)**

Base de données répliquée avec une instance sur chaque nœud d'un cluster. Les objets utilisateur et groupe locaux sont stockés dans le RDB.

Raisons de la création d'utilisateurs et de groupes locaux

Il existe plusieurs raisons de créer des utilisateurs et des groupes locaux sur votre SVM (Storage Virtual machine). Par exemple, vous pouvez accéder à un serveur SMB à l'aide d'un compte d'utilisateur local si les contrôleurs de domaine (DCS) ne sont pas disponibles, vous pouvez utiliser des groupes locaux pour attribuer des privilèges ou si votre serveur SMB se trouve dans un groupe de travail.

Vous pouvez créer un ou plusieurs comptes utilisateur locaux pour les raisons suivantes :

- Votre serveur SMB se trouve dans un groupe de travail et les utilisateurs de domaine ne sont pas disponibles.

Les utilisateurs locaux sont requis dans les configurations de groupe de travail.

- Vous souhaitez pouvoir vous authentifier et vous connecter au serveur SMB si les contrôleurs de domaine ne sont pas disponibles.

Les utilisateurs locaux peuvent s'authentifier auprès du serveur SMB en utilisant l'authentification NTLM lorsque le contrôleur de domaine est en panne, ou en cas de problèmes réseau empêchant votre serveur SMB de contacter le contrôleur de domaine.

- Vous souhaitez attribuer des privilèges *User Rights Management* à un utilisateur local.

User Rights Management permet à un administrateur de serveurs SMB de contrôler les droits des utilisateurs et des groupes sur le SVM. Vous pouvez attribuer des privilèges à un utilisateur en lui attribuant des privilèges ou en faisant de l'utilisateur un membre d'un groupe local disposant de ces privilèges.

Vous pouvez créer un ou plusieurs groupes locaux pour les raisons suivantes :

- Votre serveur SMB se trouve dans un groupe de travail et les groupes de domaines ne sont pas disponibles.

Les groupes locaux ne sont pas requis dans les configurations de groupes de travail, mais ils peuvent être utiles pour gérer les privilèges d'accès pour les utilisateurs de groupes de travail locaux.

- Vous souhaitez contrôler l'accès aux ressources de fichiers et de dossiers à l'aide des groupes locaux pour le contrôle du partage et de l'accès aux fichiers.
- Vous souhaitez créer des groupes locaux avec des privilèges *User Rights Management* personnalisés.

Certains groupes d'utilisateurs intégrés ont des privilèges prédéfinis. Pour attribuer un ensemble personnalisé de privilèges, vous pouvez créer un groupe local et attribuer les privilèges nécessaires à ce groupe. Vous pouvez ensuite ajouter des utilisateurs locaux, des utilisateurs de domaine et des groupes de domaines au groupe local.

Informations associées

[Fonctionnement de l'authentification des utilisateurs locaux](#)

[Liste des privilèges pris en charge](#)

Fonctionnement de l'authentification des utilisateurs locaux

Avant qu'un utilisateur local puisse accéder aux données sur un serveur CIFS, il doit créer une session authentifiée.

SMB étant basé sur une session, l'identité de l'utilisateur peut être déterminée une seule fois, lors de la première configuration de la session. Le serveur CIFS utilise l'authentification NTLM lors de l'authentification des utilisateurs locaux. Les fournisseurs de NTLMv1 et NTLMv2 sont tous deux pris en charge.

ONTAP utilise l'authentification locale dans trois cas d'utilisation. Chaque cas d'utilisation dépend du fait que la partie du domaine du nom d'utilisateur (au format DOMAINE\utilisateur) correspond au nom de domaine local du serveur CIFS (le nom du serveur CIFS) :

- La partie domaine correspond

Les utilisateurs qui fournissent des informations d'identification d'utilisateur local lors de la demande d'accès aux données sont authentifiés localement sur le serveur CIFS.

- La partie du domaine ne correspond pas

ONTAP tente d'utiliser l'authentification NTLM avec un contrôleur de domaine dans le domaine auquel le serveur CIFS appartient. Si l'authentification réussit, la connexion est terminée. Si cela ne fonctionne pas, ce qui se passe ensuite dépend de la raison pour laquelle l'authentification n'a pas réussi.

Par exemple, si l'utilisateur existe dans Active Directory mais que le mot de passe est incorrect ou expiré,

ONTAP ne tente pas d'utiliser le compte d'utilisateur local correspondant sur le serveur CIFS. Au lieu de cela, l'authentification échoue. Dans d'autres cas, ONTAP utilise le compte local correspondant sur le serveur CIFS, s'il existe, pour l'authentification, même si les noms de domaine NetBIOS ne correspondent pas. Par exemple, si un compte de domaine correspondant existe mais est désactivé, ONTAP utilise le compte local correspondant sur le serveur CIFS pour l'authentification.

- La partie domaine n'est pas spécifiée

ONTAP tente d'abord l'authentification en tant qu'utilisateur local. Si l'authentification en tant qu'utilisateur local échoue, ONTAP authentifie l'utilisateur avec un contrôleur de domaine dans le domaine auquel le serveur CIFS appartient.

Une fois l'authentification des utilisateurs locaux ou de domaine terminée, ONTAP crée un jeton d'accès complet, qui tient compte de l'appartenance et des privilèges des groupes locaux.

Pour plus d'informations sur l'authentification NTLM pour les utilisateurs locaux, consultez la documentation Microsoft Windows.

Informations associées

[Activation ou désactivation de l'authentification des utilisateurs locaux](#)

Comment les jetons d'accès utilisateur sont construits

Lorsqu'un utilisateur mappe un partage, une session SMB authentifiée est établie et un jeton d'accès utilisateur est construit qui contient des informations sur l'utilisateur, l'appartenance au groupe de l'utilisateur et les privilèges cumulatifs, ainsi que l'utilisateur UNIX mappé.

À moins que la fonctionnalité ne soit désactivée, les informations d'utilisateur et de groupe locaux sont également ajoutées au jeton d'accès utilisateur. La manière dont les jetons d'accès sont créés dépend de la manière dont la connexion est destinée à un utilisateur local ou à un utilisateur de domaine Active Directory :

- Connexion de l'utilisateur local

Bien que les utilisateurs locaux puissent être membres de groupes locaux différents, les groupes locaux ne peuvent pas être membres d'autres groupes locaux. Le jeton d'accès utilisateur local se compose d'une Union de tous les privilèges attribués aux groupes auxquels un utilisateur local particulier est membre.

- Connexion utilisateur du domaine

Lorsqu'un utilisateur de domaine se connecte, ONTAP obtient un jeton d'accès utilisateur contenant le SID de l'utilisateur et les SID pour tous les groupes de domaine auxquels l'utilisateur est membre. ONTAP utilise l'Union du jeton d'accès d'utilisateur du domaine avec le jeton d'accès fourni par les membres locaux des groupes de domaine de l'utilisateur (le cas échéant), ainsi que tout privilège direct attribué à l'utilisateur du domaine ou à l'un de ses membres de groupe de domaine.

Pour les connexions utilisateur locales et de domaine, le GROUPE principal RID est également défini pour le jeton d'accès utilisateur. Le RID par défaut est `Domain Users` (RID 513). Vous ne pouvez pas modifier la valeur par défaut.

Le processus de mappage de noms Windows-to-UNIX et UNIX-to-Windows suit les mêmes règles pour les comptes locaux et de domaine.



Il n'y a pas de mappage automatique implicite d'un utilisateur UNIX vers un compte local. Si cela est nécessaire, une règle de mappage explicite doit être spécifiée à l'aide des commandes de mappage de noms existantes.

Consignes relatives à l'utilisation de SnapMirror sur des SVM contenant des groupes locaux

Notez les instructions lorsque vous configurez SnapMirror sur des volumes appartenant aux SVM contenant des groupes locaux.

Vous ne pouvez pas utiliser des groupes locaux dans des ACE appliqués à des fichiers, des répertoires ou des partages qui sont répliqués par SnapMirror vers une autre SVM. Si vous utilisez la fonctionnalité SnapMirror pour créer un miroir de reprise sur incident sur un volume situé sur un autre SVM et que le volume dispose d'une version ACE pour un groupe local, l'ACE n'est pas valide pour le miroir. Si les données sont répliquées sur un autre SVM, celles-ci se croisent efficacement et un autre domaine local. Les autorisations accordées aux utilisateurs et groupes locaux ne sont valides qu'au sein du périmètre de la SVM sur lequel ils ont été créés.

Ce qui arrive aux utilisateurs et aux groupes locaux lors de la suppression des serveurs CIFS

L'ensemble par défaut des utilisateurs et groupes locaux est créé lors de la création d'un serveur CIFS et ils sont associés au serveur virtuel de stockage (SVM) qui héberge le serveur CIFS. Les administrateurs SVM peuvent créer à tout moment des utilisateurs et groupes locaux. Lorsque vous supprimez le serveur CIFS, vous devez connaître ce qui arrive aux utilisateurs et aux groupes locaux.

Les utilisateurs et groupes locaux sont associés à des SVM ; ils ne sont donc pas supprimés lorsque des serveurs CIFS sont supprimés pour des raisons de sécurité. Bien que les utilisateurs et groupes locaux ne soient pas supprimés lors de la suppression du serveur CIFS, ils sont masqués. Vous ne pouvez ni afficher ni gérer des utilisateurs et groupes locaux tant que vous n'avez pas recréés un serveur CIFS sur la SVM.



L'état d'administration du serveur CIFS n'affecte pas la visibilité des utilisateurs ou des groupes locaux.

Utilisation de la console de gestion Microsoft avec des utilisateurs et des groupes locaux

Vous pouvez afficher des informations sur les utilisateurs et groupes locaux à partir de la console de gestion Microsoft. Avec cette version de ONTAP, vous ne pouvez pas effectuer d'autres tâches de gestion pour les utilisateurs et groupes locaux à partir de la console de gestion Microsoft.

Instructions pour le rétablissement

Si vous prévoyez de restaurer le cluster à une version de ONTAP qui ne prend pas en charge les utilisateurs et groupes locaux, ainsi que les utilisateurs et groupes locaux utilisés pour gérer l'accès aux fichiers ou les droits des utilisateurs, vous devez tenir compte de certaines considérations.

- Pour des raisons de sécurité, les informations concernant les utilisateurs, groupes et privilèges locaux configurés ne sont pas supprimées lorsque ONTAP est rétabli sur une version qui ne prend pas en charge les fonctionnalités des utilisateurs et des groupes locaux.

- Lors de la restauration d'une version majeure antérieure de ONTAP, ONTAP n'utilise pas d'utilisateurs et de groupes locaux pendant l'authentification et la création des informations d'identification.
- Les utilisateurs et groupes locaux ne sont pas supprimés des listes de contrôle d'accès aux fichiers et aux dossiers.
- Les demandes d'accès aux fichiers qui dépendent de l'accès sont refusées en raison des autorisations accordées aux utilisateurs ou groupes locaux.

Pour autoriser l'accès, vous devez reconfigurer les autorisations d'accès aux fichiers afin d'autoriser l'accès en fonction des objets de domaine au lieu d'objets d'utilisateur et de groupe locaux.

Quels sont les privilèges locaux

Liste des privilèges pris en charge

ONTAP dispose d'un ensemble prédéfini de privilèges pris en charge. Certains groupes locaux prédéfinis ont certains de ces privilèges ajoutés par défaut. Vous pouvez également ajouter ou supprimer des privilèges des groupes prédéfinis ou créer de nouveaux utilisateurs ou groupes locaux et ajouter des privilèges aux groupes que vous avez créés ou aux utilisateurs et groupes de domaine existants.

Le tableau ci-dessous répertorie les privilèges pris en charge sur la machine virtuelle de stockage (SVM) et fournit la liste des groupes BUILTIN avec des privilèges attribués :

Nom de privilège	Paramètre de sécurité par défaut	Description
SeTcbPrivilege	Aucune	Faire partie du système d'exploitation
SeBackupPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Sauvegardez des fichiers et des répertoires, en remplaçant les listes de contrôle d'accès
SeRestorePrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Restaurez les fichiers et les répertoires, en remplaçant les listes de contrôle d'accès, définissez tout ID utilisateur ou groupe valide comme propriétaire du fichier
SeTakeOwnershipPrivilege	BUILTIN\Administrators	Prendre possession de fichiers ou d'autres objets
SeSecurityPrivilege	BUILTIN\Administrators	Gérer les audits Cela inclut l'affichage, le vidage et l'effacement du journal de sécurité.

Nom de privilège	Paramètre de sécurité par défaut	Description
SeChangeNotifyPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators, BUILTIN\Power Users, BUILTIN\Users, Everyone	Vérification de la traverse de dérivation Les utilisateurs disposant de ce privilège ne sont pas tenus d'avoir des autorisations traverse (x) pour traverser des dossiers, des liens symboliques ou des jonctions.

Informations associées

- [Attribuez des privilèges locaux](#)
- [Configuration de la vérification de la traverse de dérivation](#)

Attribuer des privilèges

Vous pouvez attribuer des privilèges directement aux utilisateurs locaux ou aux utilisateurs du domaine. Vous pouvez également affecter des utilisateurs à des groupes locaux dont les privilèges attribués correspondent aux fonctions que vous souhaitez que ces utilisateurs disposent.

- Vous pouvez attribuer un ensemble de privilèges à un groupe que vous créez.

Vous ajoutez ensuite un utilisateur au groupe disposant des privilèges que vous souhaitez que cet utilisateur dispose.

- Vous pouvez également attribuer des utilisateurs locaux et des utilisateurs de domaine à des groupes prédéfinis dont les privilèges par défaut correspondent aux privilèges que vous souhaitez accorder à ces utilisateurs.

Informations associées

- [Ajout de privilèges aux utilisateurs ou groupes locaux ou de domaine](#)
- [Suppression des privilèges des utilisateurs ou groupes locaux ou de domaine](#)
- [Réinitialisation des privilèges pour les utilisateurs et groupes locaux ou de domaine](#)
- [Configuration de la vérification de la traverse de dérivation](#)

Instructions d'utilisation des groupes BULILTIN et du compte administrateur local

Il y a certaines directives que vous devez garder à l'esprit lorsque vous utilisez les groupes BULTIN et le compte d'administrateur local. Par exemple, vous pouvez renommer le compte d'administrateur local, mais vous ne pouvez pas supprimer ce compte.

- Le compte Administrateur peut être renommé mais ne peut pas être supprimé.
- Le compte Administrateur ne peut pas être supprimé du groupe BULTIN\Administrators.
- Les groupes INTÉGRÉS peuvent être renommés mais ne peuvent pas être supprimés.

Une fois le groupe BUILTIN renommé, un autre objet local peut être créé avec le nom connu ; cependant,

l'objet est affecté à un nouveau RID.

- Il n'y a pas de compte invité local.

Informations associées

[Groupes et privilèges par défaut prédéfinis BUILTIN](#)

Conditions requises pour les mots de passe des utilisateurs locaux

Par défaut, les mots de passe des utilisateurs locaux doivent répondre aux exigences de complexité. Les exigences de complexité des mots de passe sont similaires aux exigences définies dans la stratégie de sécurité Microsoft Windows *local*.

Le mot de passe doit répondre aux critères suivants :

- Doit comporter au moins six caractères
- Ne doit pas contenir le nom du compte d'utilisateur
- Doit contenir des caractères d'au moins trois des quatre catégories suivantes :
 - Caractères majuscules anglais (A à Z)
 - Caractères anglais minuscules (a à z)
 - Chiffres de base 10 (0 à 9)
 - Caractères spéciaux :

~ ! @ # \$ % ^ et * _ - + = ` \ | () [] : ; " < > , . ? /

Informations associées

[Activation ou désactivation de la complexité requise des mots de passe pour les utilisateurs SMB locaux](#)

[Affichage d'informations sur les paramètres de sécurité du serveur CIFS](#)

[Modification des mots de passe des comptes utilisateur locaux](#)

Groupes et privilèges par défaut prédéfinis BUILTIN

Vous pouvez affecter l'appartenance d'un utilisateur local ou d'un utilisateur de domaine à un ensemble prédéfini de groupes BUILTIN fourni par ONTAP. Les groupes prédéfinis ont des privilèges prédéfinis attribués.

Le tableau suivant décrit les groupes prédéfinis :

Groupe prédéfini BUILTIN	Privilèges par défaut
<p>BUILTIN\AdministratorsRID 544</p> <p>Lors de sa création initiale, le local Administrator Compte, avec UN RID de 500, est automatiquement fait membre de ce groupe. Lorsque l'ordinateur virtuel de stockage (SVM) est rejoint un domaine, le domain\Domain Admins le groupe est ajouté au groupe. Si le SVM laisse le domaine, le domain\Domain Admins le groupe est supprimé du groupe.</p>	<ul style="list-style-type: none"> • SeBackupPrivilege • SeRestorePrivilege • SeSecurityPrivilege • SeTakeOwnershipPrivilege • SeChangeNotifyPrivilege
<p>BUILTIN\Power UsersRID 547</p> <p>Lors de sa création initiale, ce groupe n'a aucun membre. Les membres de ce groupe ont les caractéristiques suivantes :</p> <ul style="list-style-type: none"> • Peut créer et gérer des utilisateurs et des groupes locaux. • Impossible d'ajouter eux-mêmes ou tout autre objet au BUILTIN\Administrators groupe. 	SeChangeNotifyPrivilege
<p>BUILTIN\Backup OperatorsRID 551</p> <p>Lors de sa création initiale, ce groupe n'a aucun membre. Les membres de ce groupe peuvent remplacer les autorisations de lecture et d'écriture sur des fichiers ou des dossiers s'ils sont ouverts avec l'intention de sauvegarde.</p>	<ul style="list-style-type: none"> • SeBackupPrivilege • SeRestorePrivilege • SeChangeNotifyPrivilege
<p>BUILTIN\UsersRID 545</p> <p>Lors de sa création initiale, ce groupe n'a pas de membres (autre que les membres implicites) Authenticated Users groupe spécial). Lorsque le SVM est joint à un domaine, le domain\Domain Users le groupe est ajouté à ce groupe. Si le SVM laisse le domaine, le domain\Domain Users le groupe est supprimé de ce groupe.</p>	SeChangeNotifyPrivilege
<p>EveryoneSID S-1-1-0</p> <p>Ce groupe inclut tous les utilisateurs, y compris les invités (mais pas les utilisateurs anonymes). Il s'agit d'un groupe implicite avec une adhésion implicite.</p>	SeChangeNotifyPrivilege

Informations associées

[Instructions d'utilisation des groupes BUILTIN et du compte administrateur local](#)

[Liste des privilèges pris en charge](#)

[Configuration de la vérification de la traverse de dérivation](#)

Activez ou désactivez la fonctionnalité utilisateurs et groupes locaux

Activer ou désactiver la présentation des fonctionnalités des utilisateurs et groupes locaux

Avant de pouvoir utiliser des utilisateurs et des groupes locaux pour contrôler l'accès aux données de style de sécurité NTFS, les fonctionnalités d'utilisateur et de groupe locaux doivent être activées. En outre, si vous souhaitez utiliser des utilisateurs locaux pour l'authentification SMB, la fonctionnalité d'authentification des utilisateurs locaux doit être activée.

Les fonctionnalités des utilisateurs et groupes locaux et l'authentification des utilisateurs locaux sont activées par défaut. Si elles ne sont pas activées, vous devez les activer avant de pouvoir configurer et utiliser des utilisateurs et des groupes locaux. Vous pouvez désactiver les fonctionnalités des utilisateurs et groupes locaux à tout moment.

En plus de désactiver explicitement la fonctionnalité des utilisateurs et groupes locaux, ONTAP désactive les fonctionnalités utilisateur et groupe locaux si un nœud du cluster est rétabli sur une version de ONTAP qui ne prend pas en charge cette fonctionnalité. Les fonctionnalités des utilisateurs et groupes locaux ne sont pas activées tant que tous les nœuds du cluster n'exécutent pas une version de ONTAP qui le prend en charge.

Informations associées

[Modifier les comptes utilisateur locaux](#)

[Modifier les groupes locaux](#)

[Ajoutez des privilèges aux utilisateurs ou groupes locaux ou de domaine](#)

Activez ou désactivez les utilisateurs et groupes locaux

Vous pouvez activer ou désactiver les utilisateurs et groupes locaux pour l'accès SMB sur des SVM (Storage Virtual machines). La fonctionnalité utilisateurs et groupes locaux est activée par défaut.

Description de la tâche

Vous pouvez utiliser des utilisateurs et des groupes locaux lors de la configuration des autorisations de partage SMB et de fichiers NTFS et, éventuellement, utiliser des utilisateurs locaux pour l'authentification lors de la création d'une connexion SMB. Pour utiliser les utilisateurs locaux pour l'authentification, vous devez également activer l'option d'authentification des utilisateurs et groupes locaux.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Si vous voulez que les utilisateurs et les groupes locaux soient...	Entrez la commande...
Activé	<code>vserver cifs options modify -vserver vserver_name -is-local-users-and-groups-enabled true</code>
Désactivé	<code>vserver cifs options modify -vserver vserver_name -is-local-users-and-groups-enabled false</code>

3. Retour au niveau de privilège admin : `set -privilege admin`

Exemple

L'exemple suivant permet aux utilisateurs et groupes locaux de la fonctionnalité sur le SVM vs1 :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Informations associées

[Activez ou désactivez l'authentification des utilisateurs locaux](#)

[Activez ou désactivez les comptes utilisateur locaux](#)

Activez ou désactivez l'authentification des utilisateurs locaux

Vous pouvez activer ou désactiver l'authentification des utilisateurs locaux pour l'accès SMB sur des SVM (Storage Virtual machines). La valeur par défaut est d'autoriser l'authentification des utilisateurs locaux, ce qui est utile lorsque la SVM ne peut pas contacter un contrôleur de domaine ou si vous choisissez de ne pas utiliser de contrôles d'accès au niveau des domaines.

Avant de commencer

La fonctionnalité utilisateurs et groupes locaux doit être activée sur le serveur CIFS.

Description de la tâche

Vous pouvez activer ou désactiver l'authentification des utilisateurs locaux à tout moment. Si vous souhaitez utiliser des utilisateurs locaux pour l'authentification lors de la création d'une connexion SMB, vous devez également activer l'option utilisateurs et groupes locaux du serveur CIFS.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Si vous voulez que l'authentification locale soit...	Entrez la commande...
Activé	<code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled true</code>
Désactivé	<code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled false</code>

3. Retour au niveau de privilège admin : `set -privilege admin`

Exemple

L'exemple suivant active l'authentification utilisateur local sur le SVM vs1 :

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Informations associées

[Fonctionnement de l'authentification des utilisateurs locaux](#)

[Activation ou désactivation des utilisateurs et groupes locaux](#)

Gérez les comptes utilisateurs locaux

Modifier les comptes utilisateur locaux

Vous pouvez modifier un compte d'utilisateur local si vous souhaitez modifier le nom complet ou la description d'un utilisateur existant et si vous souhaitez activer ou désactiver le compte d'utilisateur. Vous pouvez également renommer un compte d'utilisateur local si le nom de l'utilisateur est compromis ou si un changement de nom est nécessaire à des fins administratives.

Les fonctions que vous recherchez...	Entrez la commande...
Modifier le nom complet de l'utilisateur local	<code>vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user -name <i>user_name</i> -full-name text</code> Si le nom complet contient un espace, il doit être placé entre guillemets.
Modifier la description de l'utilisateur local	<code>vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user -name <i>user_name</i> -description text</code> Si la description contient un espace, elle doit être placée entre guillemets.
Activez ou désactivez le compte utilisateur local	<code>`vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user-name <i>user_name</i> -is -account-disabled {true</code>
<code>false}`</code>	Renommez le compte d'utilisateur local

Exemple

L'exemple suivant renomme l'utilisateur local « CIFS_SERVER\sue » en « CIFS_SERVER\sue_New » sur la machine virtuelle de stockage (SVM, précédemment appelé vServer) vs1 :

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Activez ou désactivez les comptes utilisateur locaux

Vous activez un compte utilisateur local si vous souhaitez que l'utilisateur puisse accéder aux données contenues dans la machine virtuelle de stockage (SVM) via une connexion SMB. Vous pouvez également désactiver un compte utilisateur local si vous ne souhaitez pas que cet utilisateur accède aux données des SVM via SMB.

Description de la tâche

Vous activez un utilisateur local en modifiant le compte utilisateur.

Étape

1. Effectuez l'action appropriée :

Les fonctions que vous recherchez...	Entrez la commande...
Activez le compte utilisateur	<code>vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user-name <i>user_name</i> -is-account -disabled false</code>

Les fonctions que vous recherchez...	Entrez la commande...
Désactivez le compte utilisateur	<code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account-disabled true</code>

Modifier les mots de passe des comptes utilisateur locaux

Vous pouvez modifier le mot de passe du compte d'un utilisateur local. Cela peut être utile si le mot de passe de l'utilisateur est compromis ou si l'utilisateur a oublié le mot de passe.

Étape

1. Modifiez le mot de passe en effectuant l'action appropriée : `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

Exemple

L'exemple suivant définit le mot de passe pour l'utilisateur local « CIFS_SERVER\sue » associé à une machine virtuelle de stockage (SVM, anciennement Vserver) vs1 :

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1
```

Enter the new password:

Confirm the new password:

Informations associées

[Activation ou désactivation de la complexité requise des mots de passe pour les utilisateurs SMB locaux](#)

[Affichage d'informations sur les paramètres de sécurité du serveur CIFS](#)

Affiche des informations sur les utilisateurs locaux

Vous pouvez afficher une liste de tous les utilisateurs locaux sous forme de résumé. Si vous souhaitez déterminer les paramètres de compte configurés pour un utilisateur spécifique, vous pouvez afficher des informations détaillées sur le compte de cet utilisateur ainsi que les informations sur le compte de plusieurs utilisateurs. Ces informations peuvent vous aider à déterminer si vous devez modifier les paramètres d'un utilisateur et à résoudre les problèmes d'authentification ou d'accès aux fichiers.

Description de la tâche

Les informations relatives au mot de passe d'un utilisateur ne s'affichent jamais.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez...	Entrez la commande...
Affichage des informations relatives à tous les utilisateurs sur la machine virtuelle de stockage (SVM)	<code>vserver cifs users-and-groups local-user show -vserver <i>vserver_name</i></code>
Affiche des informations détaillées sur le compte d'un utilisateur	<code>vserver cifs users-and-groups local-user show -instance -vserver <i>vserver_name</i> -user-name <i>user_name</i></code>

D'autres paramètres facultatifs peuvent être choisis lors de l'exécution de la commande. Consultez la page man pour plus d'informations

Exemple

L'exemple suivant affiche les informations relatives à tous les utilisateurs locaux sur le SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                               Full Name      Description
-----  -
vs1      CIFS_SERVER\Administrator      James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue                Sue   Jones
```

Affiche des informations sur les membres de groupe pour les utilisateurs locaux

Vous pouvez afficher des informations sur les groupes locaux auxquels un utilisateur local appartient. Vous pouvez utiliser ces informations pour déterminer l'accès que l'utilisateur doit avoir aux fichiers et dossiers. Ces informations peuvent être utiles pour déterminer les droits d'accès que l'utilisateur doit posséder aux fichiers et dossiers ou pour résoudre les problèmes d'accès aux fichiers.

Description de la tâche

Vous pouvez personnaliser la commande pour afficher uniquement les informations que vous souhaitez afficher.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez...	Entrez la commande...
Afficher les informations d'appartenance des utilisateurs locaux pour un utilisateur local spécifié	<code>vserver cifs users-and-groups local-user show-membership -user-name <i>user_name</i></code>

Les fonctions que vous recherchez...	Entrez la commande...
Affiche les informations d'appartenance de l'utilisateur local pour le groupe local dont cet utilisateur local est membre	<code>vserver cifs users-and-groups local-user show-membership -membership group_name</code>
Afficher les informations d'appartenance des utilisateurs aux utilisateurs locaux associés à une machine virtuelle de stockage (SVM) spécifiée	<code>vserver cifs users-and-groups local-user show-membership -vserver vserver_name</code>
Affiche des informations détaillées pour tous les utilisateurs locaux sur un SVM spécifié	<code>vserver cifs users-and-groups local-user show-membership -instance -vserver vserver_name</code>

Exemple

L'exemple suivant affiche les informations d'appartenance de tous les utilisateurs locaux sur le SVM vs1 ; l'utilisateur « CIFS_SERVER\Administrator » est membre du groupe « BUILTIN\Administrators » et « CIFS_SERVER\sue » est membre du groupe « CIFS_SERVER\g1 » :

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
```

Vserver	User Name	Membership
vs1	CIFS_SERVER\Administrator	BUILTIN\Administrators
	CIFS_SERVER\sue	CIFS_SERVER\g1

Supprimer les comptes utilisateur locaux

Vous pouvez supprimer des comptes utilisateurs locaux de votre machine virtuelle de stockage (SVM) s'ils ne sont plus nécessaires pour l'authentification SMB locale sur le serveur CIFS ou pour déterminer les droits d'accès aux données contenues dans votre SVM.

Description de la tâche

Tenez compte des points suivants lors de la suppression d'utilisateurs locaux :

- Le système de fichiers n'est pas modifié.

Les descripteurs de sécurité Windows sur les fichiers et les répertoires qui font référence à cet utilisateur ne sont pas ajustés.

- Toutes les références aux utilisateurs locaux sont supprimées des bases de données d'appartenance et de privilèges.
- Les utilisateurs standard bien connus tels que Administrateur ne peuvent pas être supprimés.

Étapes

1. Déterminez le nom du compte d'utilisateur local que vous souhaitez supprimer : `vserver cifs users-`

```
and-groups local-user show -vserver vs1
```

2. Supprimez l'utilisateur local : `vserver cifs users-and-groups local-user delete -vserver vs1 -user-name username_name`
3. Vérifiez que le compte utilisateur est supprimé : `vserver cifs users-and-groups local-user show -vserver vs1`

Exemple

L'exemple suivant supprime l'utilisateur local « CIFS_SERVER\sue » associé à la SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                Full Name                Description
-----  -
vs1      CIFS_SERVER\Administrator  James Smith              Built-in administrator
account
vs1      CIFS_SERVER\sue           Sue    Jones

cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                Full Name                Description
-----  -
vs1      CIFS_SERVER\Administrator  James Smith              Built-in administrator
account
```

Gérez des groupes locaux

Modifier les groupes locaux

Vous pouvez modifier les groupes locaux existants en modifiant la description d'un groupe local existant ou en renommant ce groupe.

Les fonctions que vous recherchez...	Utilisez la commande...
Modifier la description du groupe local	<code>vserver cifs users-and-groups local-group modify -vserver vs1 -group-name group_name -description text</code> Si la description contient un espace, elle doit être placée entre guillemets.
Renommer le groupe local	<code>vserver cifs users-and-groups local-group rename -vserver vs1 -group-name group_name -new-group-name new_group_name</code>

Exemples

L'exemple suivant renomme le groupe local « CIFS_SERVER\engineering » en « CIFS_SERVER\engineering_New » :

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

L'exemple suivant modifie la description du groupe local « CIFS_SERVER\engineering » :

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Affiche des informations sur les groupes locaux

Vous pouvez afficher la liste de tous les groupes locaux configurés sur le cluster ou sur une machine virtuelle de stockage (SVM) spécifiée. Ces informations peuvent être utiles pour résoudre les problèmes d'accès aux fichiers aux données contenues dans la SVM ou sur les problèmes liés aux droits d'utilisateur (privilège) sur la SVM.

Étape

- 1. Effectuez l'une des opérations suivantes :

Pour obtenir des informations sur...	Entrez la commande...
Tous les groupes locaux du cluster	vserver cifs users-and-groups local-group show
Tous les groupes locaux sur le SVM	vserver cifs users-and-groups local-group show -vserver vserver_name

D'autres paramètres facultatifs peuvent être choisis lors de l'exécution de cette commande. Consultez la page man pour plus d'informations

Exemple

L'exemple suivant affiche les informations sur tous les groupes locaux sur le SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
```

Vserver	Group Name	Description
vs1	BUILTIN\Administrators	Built-in Administrators group
vs1	BUILTIN\Backup Operators	Backup Operators group
vs1	BUILTIN\Power Users	Restricted administrative privileges
vs1	BUILTIN\Users	All users
vs1	CIFS_SERVER\engineering	
vs1	CIFS_SERVER\sales	

Gérer l'appartenance à un groupe local

Vous pouvez gérer l'appartenance à un groupe local en ajoutant et en supprimant des utilisateurs locaux ou de domaine, ou en ajoutant et supprimant des groupes de domaines. Ceci est utile si vous souhaitez contrôler l'accès aux données en fonction des contrôles d'accès placés sur le groupe ou si vous souhaitez que les utilisateurs disposent de privilèges associés à ce groupe.

Description de la tâche

Directives pour l'ajout de membres à un groupe local :

- Vous ne pouvez pas ajouter d'utilisateurs au groupe spécial *Everyone*.
- Le groupe local doit exister avant de pouvoir y ajouter un utilisateur.
- L'utilisateur doit exister avant de pouvoir ajouter l'utilisateur à un groupe local.
- Vous ne pouvez pas ajouter un groupe local à un autre groupe local.
- Pour ajouter un utilisateur ou un groupe de domaine à un groupe local, Data ONTAP doit pouvoir résoudre le nom en SID.

Directives pour le retrait de membres d'un groupe local :

- Vous ne pouvez pas supprimer des membres du groupe spécial *Everyone*.
- Le groupe dont vous souhaitez supprimer un membre doit exister.
- ONTAP doit pouvoir résoudre les noms des membres que vous souhaitez supprimer du groupe vers un SID correspondant.

Étape

1. Ajouter ou supprimer un membre d'un groupe.

Les fonctions que vous recherchez...	Utilisez ensuite la commande...
Ajouter un membre à un groupe	<pre>vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> <p>Vous pouvez spécifier une liste délimitée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaine à ajouter au groupe local spécifié.</p>
Supprimer un membre d'un groupe	<pre>vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> <p>Vous pouvez spécifier une liste délimitée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaine à supprimer du groupe local spécifié.</p>

L'exemple suivant ajoute un utilisateur local « SMB_SERVER\sue » et un groupe de domaine « AD_DOM\dom_eng » au groupe local « 'SMB_SERVER\engineering' » sur la SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

L'exemple suivant supprime les utilisateurs locaux « SMB_SERVER\sue » et « SMB_SERVER\james » du groupe local « 'SMB_SERVER\engineering' » sur la SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Informations associées

[Affichage des informations relatives aux membres des groupes locaux](#)

Affiche des informations sur les membres des groupes locaux

Vous pouvez afficher la liste de tous les membres des groupes locaux configurés sur le cluster ou sur une machine virtuelle de stockage (SVM) spécifiée. Ces informations peuvent être utiles pour résoudre les problèmes d'accès aux fichiers ou de droits d'utilisateur (privileges).

Étape

1. Effectuez l'une des opérations suivantes :

Pour afficher des informations sur...	Entrez la commande...
Membres de tous les groupes locaux du cluster	<code>vserver cifs users-and-groups local-group show-members</code>
Membres de tous les groupes locaux sur le SVM	<code>vserver cifs users-and-groups local-group show-members -vserver <i>vserver_name</i></code>

Exemple

L'exemple suivant affiche les informations sur les membres de tous les groupes locaux sur le SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver      Group Name                Members
-----
vs1          BUILTIN\Administrators    CIFS_SERVER\Administrator
                                     AD_DOMAIN\Domain Admins
                                     AD_DOMAIN\dom_grp1
                                     AD_DOMAIN\Domain Users
                                     AD_DOMAIN\dom_usr1
                                     CIFS_SERVER\james
          BUILTIN\Users
          CIFS_SERVER\engineering
```

Supprimer un groupe local

Vous pouvez supprimer un groupe local de la machine virtuelle de stockage (SVM) s'il n'est plus nécessaire pour déterminer les droits d'accès aux données associées à ce SVM ou s'il n'est plus nécessaire d'attribuer des droits d'utilisateur de SVM (privilèges) aux membres du groupe.

Description de la tâche

Lors de la suppression de groupes locaux, tenez compte des points suivants :

- Le système de fichiers n'est pas modifié.

Les descripteurs de sécurité Windows sur les fichiers et les répertoires faisant référence à ce groupe ne sont pas ajustés.

- Si le groupe n'existe pas, une erreur est renvoyée.
- Le groupe *Everyone* spécial ne peut pas être supprimé.
- Les groupes intégrés tels que *BUILTIN\Administrators* *BUILTIN\Users* ne peuvent pas être supprimés.

Étapes

1. Déterminer le nom du groupe local que vous souhaitez supprimer en affichant la liste des groupes locaux sur la SVM : `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Supprimez le groupe local : `vserver cifs users-and-groups local-group delete -vserver`

```
vserver_name -group-name group_name
```

3. Vérifiez que le groupe est supprimé : `vserver cifs users-and-groups local-user show -vserver vserver_name`

Exemple

L'exemple suivant supprime le groupe local « CIFS_SERVER\sales » associé à la SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
```

Vserver	Group Name	Description
vs1	BUILTIN\Administrators	Built-in Administrators group
vs1	BUILTIN\Backup Operators	Backup Operators group
vs1	BUILTIN\Power Users	Restricted administrative
privileges		
vs1	BUILTIN\Users	All users
vs1	CIFS_SERVER\engineering	
vs1	CIFS_SERVER\sales	

```
cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1 -group-name CIFS_SERVER\sales
```

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
```

Vserver	Group Name	Description
vs1	BUILTIN\Administrators	Built-in Administrators group
vs1	BUILTIN\Backup Operators	Backup Operators group
vs1	BUILTIN\Power Users	Restricted administrative
privileges		
vs1	BUILTIN\Users	All users
vs1	CIFS_SERVER\engineering	

Mettre à jour les noms d'utilisateur et de groupe du domaine dans les bases de données locales

Vous pouvez ajouter des utilisateurs et des groupes de domaine aux groupes locaux d'un serveur CIFS. Ces objets de domaine sont enregistrés dans des bases de données locales sur le cluster. Si un objet domaine est renommé, les bases de données locales doivent être mises à jour manuellement.

Description de la tâche

On doit préciser le nom de la machine virtuelle de stockage (SVM) sur laquelle vous souhaitez mettre à jour les noms de domaine.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'action appropriée :

Si vous souhaitez mettre à jour les utilisateurs et les groupes du domaine et...	Utilisez cette commande...
Affiche les utilisateurs et groupes du domaine mis à jour avec succès et dont la mise à jour a échoué	<code>vserver cifs users-and-groups update-names -vserver vserver_name</code>
Afficher les utilisateurs et groupes du domaine mis à jour avec succès	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false</code>
Afficher uniquement les utilisateurs et les groupes du domaine qui n'ont pas été mis à jour	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true</code>
Supprimez toutes les informations d'état concernant les mises à jour	<code>vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true</code>

3. Retour au niveau de privilège admin : `set -privilege admin`

Exemple

L'exemple suivant met à jour les noms des utilisateurs et groupes de domaine associés à la machine virtuelle de stockage (SVM, anciennement Vserver) vs1. Pour la dernière mise à jour, une chaîne de noms dépendante doit être mise à jour :

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs users-and-groups update-names -vsserver vs1

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-12345
Domain:           EXAMPLE1
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:           Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654322-23456
Domain:           EXAMPLE2
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:           Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-123456
Domain:           EXAMPLE1
Out-of-date Name: dom_user3
Updated Name:     dom_user4
Status:           Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                  to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                  to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                  to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                  to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin

```

Gérer les privilèges locaux

Ajoutez des privilèges aux utilisateurs ou groupes locaux ou de domaine

Vous pouvez gérer les droits d'utilisateur pour les utilisateurs ou groupes locaux ou de domaine en ajoutant des privilèges. Les privilèges ajoutés remplacent les privilèges par défaut attribués à l'un de ces objets. Cela vous permet de renforcer la sécurité en vous permettant de personnaliser les privilèges d'un utilisateur ou d'un groupe.

Avant de commencer

L'utilisateur ou le groupe local ou de domaine auquel les privilèges seront ajoutés doit déjà exister.

Description de la tâche

L'ajout d'un privilège à un objet remplace les privilèges par défaut pour cet utilisateur ou ce groupe. L'ajout d'un privilège ne supprime pas les privilèges précédemment ajoutés.

Lorsque vous ajoutez des privilèges aux utilisateurs ou groupes locaux ou de domaine, vous devez garder à l'esprit les éléments suivants :

- Vous pouvez ajouter un ou plusieurs privilèges.
- Lors de l'ajout de privilèges à un utilisateur ou à un groupe de domaine, ONTAP peut valider l'utilisateur ou le groupe du domaine en contactant le contrôleur de domaine.

La commande peut échouer si ONTAP n'est pas en mesure de contacter le contrôleur de domaine.

Étapes

1. Ajoutez un ou plusieurs privilèges à un utilisateur ou groupe local ou de domaine : `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Vérifiez que les privilèges souhaités sont appliqués à l'objet : `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Exemple

L'exemple suivant ajoute les privilèges « `Enregistrer TcbPrivilege` » et « `Enregistrer OwnershipPrivilege` » à l'utilisateur « CIFS_SERVER\sue » sur la machine virtuelle de stockage (SVM, précédemment connue sous le nom de Vserver) vs1 :

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

Supprimez les privilèges des utilisateurs ou groupes locaux ou de domaine

Vous pouvez gérer les droits d'utilisateur pour les utilisateurs ou groupes locaux ou de

domaine en supprimant les privilèges. Cela vous permet de renforcer la sécurité en vous permettant de personnaliser le nombre maximal de privilèges dont disposent les utilisateurs et les groupes.

Avant de commencer

L'utilisateur ou le groupe local ou de domaine dont les privilèges seront supprimés doit déjà exister.

Description de la tâche

Vous devez garder à l'esprit les éléments suivants lorsque vous supprimez des privilèges des utilisateurs ou groupes locaux ou de domaine :

- Vous pouvez supprimer un ou plusieurs privilèges.
- Lors de la suppression de privilèges d'un utilisateur ou d'un groupe de domaines, ONTAP peut valider l'utilisateur ou le groupe de domaines en contactant le contrôleur de domaine.

La commande peut échouer si ONTAP n'est pas en mesure de contacter le contrôleur de domaine.

Étapes

1. Supprimer un ou plusieurs privilèges d'un utilisateur ou groupe local ou de domaine : `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Vérifiez que les privilèges souhaités ont été supprimés de l'objet : `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Exemple

L'exemple suivant supprime les privilèges « `Enregistrer TcbPrivilege` » et « `Saba OwnershipPrivilege` » de l'utilisateur « CIFS_SERVER\sue » sur la machine virtuelle de stockage (SVM, précédemment connue sous le nom de Vserver) vs1 :

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
-----
vs1        CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
-----
vs1        CIFS_SERVER\sue      -
```

Réinitialisez les privilèges pour les utilisateurs et les groupes locaux ou de domaine

Vous pouvez réinitialiser les privilèges des utilisateurs et groupes locaux ou de domaine.

Cela peut s'avérer utile lorsque vous avez apporté des modifications aux privilèges d'un utilisateur ou d'un groupe local ou de domaine et que ces modifications ne sont plus nécessaires ou souhaitées.

Description de la tâche

La réinitialisation des privilèges d'un utilisateur ou groupe local ou de domaine supprime toutes les entrées de privilèges de cet objet.

Étapes

1. Réinitialisez les privilèges sur un utilisateur ou groupe local ou de domaine : `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Vérifiez que les privilèges sont réinitialisés sur l'objet : `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Exemples

L'exemple suivant réinitialise les privilèges de l'utilisateur « CIFS_SERVER\sue » sur la machine virtuelle de stockage (SVM, anciennement appelée Vserver) vs1. Par défaut, les utilisateurs normaux ne disposent pas de privilèges associés à leurs comptes :

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        SeTcbPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

L'exemple suivant réinitialise les privilèges du groupe « BUILTIN\Administrators », supprimant ainsi l'entrée de privilège :

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver      User or Group Name      Privileges
-----
vs1          BUILTIN\Administrators  SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Affiche des informations sur les remplacements de privilèges

Vous pouvez afficher des informations sur les privilèges personnalisés attribués à des comptes ou groupes d'utilisateurs locaux ou de domaine. Ces informations vous aident à déterminer si les droits d'utilisateur souhaités sont appliqués.

Étape

1. Effectuez l'une des opérations suivantes :

Pour afficher des informations sur...	Entrez cette commande...
Privilèges personnalisés pour tous les utilisateurs et groupes locaux et du domaine sur la machine virtuelle de stockage (SVM)	<code>vserver cifs users-and-groups privilege show -vserver vserver_name</code>
Privilèges personnalisés pour un domaine spécifique ou un utilisateur et groupe local sur le SVM	<code>vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name</code>

D'autres paramètres facultatifs peuvent être choisis lors de l'exécution de cette commande. Consultez la page man pour plus d'informations

Exemple

La commande suivante affiche tous les privilèges explicitement associés aux utilisateurs et groupes locaux ou de domaine pour le SVM vs1 :

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
```

Vserver	User or Group Name	Privileges
vs1	BUILTIN\Administrators	SeTakeOwnershipPrivilege SeRestorePrivilege
vs1	CIFS_SERVER\sue	SeTcbPrivilege SeTakeOwnershipPrivilege

Configurer la vérification de la traverse de dérivation

Configurer la vue d'ensemble de vérification de la traverse de dérivation

La vérification du contournement de la traverse est un droit utilisateur (également appelé *Privilege*) qui détermine si un utilisateur peut traverser tous les répertoires du chemin d'accès à un fichier, même si l'utilisateur ne dispose pas des autorisations sur le répertoire de parcours. Vous devez comprendre ce qui se passe lors de l'autorisation ou de la désautorisation de la vérification transversale et comment configurer la vérification de dérivation pour les utilisateurs sur les machines virtuelles de stockage (SVM).

Que se passe-t-il lors de l'autorisation ou de la désautorisation du contrôle de la traverse de dérivation

- Si l'accès est autorisé, lorsqu'un utilisateur tente d'accéder à un fichier, ONTAP ne vérifie pas l'autorisation traverse pour les répertoires intermédiaires lorsqu'il détermine s'il faut accorder ou refuser l'accès au fichier.
- S'il n'est pas autorisé, ONTAP vérifie l'autorisation traverse (exécution) pour tous les répertoires du chemin d'accès au fichier.

Si l'un des répertoires intermédiaires ne dispose pas de l'autorisation « X » (traverse), ONTAP refuse l'accès au fichier.

Configurer la vérification de la traverse de dérivation

Vous pouvez configurer la vérification de contournement via l'interface de ligne de commande ONTAP ou en configurant des règles de groupe Active Directory avec ce droit d'utilisateur.

Le `SeChangeNotifyPrivilege` privilège contrôle si les utilisateurs sont autorisés à contourner la vérification transversale.

- L'ajout aux utilisateurs ou groupes SMB locaux sur le SVM, ou aux utilisateurs ou groupes de domaine permet de contourner la vérification transversale.
- L'élimination de ce groupe ou des utilisateurs SMB locaux sur le SVM, ou des utilisateurs ou groupes de domaine permet de contourner la vérification des traversent.

Par défaut, les groupes BUILTIN suivants sur le SVM ont le droit de contourner le contrôle de la traverse :

- BUILTIN\Administrators
- BUILTIN\Power Users

- BUILTIN\Backup Operators
- BUILTIN\Users
- Everyone

Si vous ne souhaitez pas autoriser les membres de l'un de ces groupes à contourner la vérification de la traverse, vous devez supprimer ce privilège du groupe.

Lors de la configuration de la vérification de dérivation des utilisateurs et groupes SMB locaux sur le SVM, il faut garder ce qui suit à l'aide de l'interface de ligne de commande :

- Si vous souhaitez autoriser les membres d'un groupe local ou de domaine personnalisé à contourner la vérification transversale, vous devez ajouter le `SeChangeNotifyPrivilege` privilège de ce groupe.
- Si vous souhaitez autoriser un utilisateur local ou de domaine individuel à contourner la vérification de la traverse et que cet utilisateur n'est pas membre d'un groupe avec ce privilège, vous pouvez ajouter `SeChangeNotifyPrivilege` privilège de ce compte utilisateur.
- Vous pouvez désactiver la vérification de contournement pour les utilisateurs ou groupes locaux ou de domaine en supprimant le `SeChangeNotifyPrivilege` privilège à tout moment.



Pour désactiver la vérification des trvers de contournement pour les utilisateurs ou groupes locaux ou de domaine spécifiés, vous devez également supprimer le `SeChangeNotifyPrivilege` privilège du `Everyone` groupe.

Informations associées

[Permet aux utilisateurs ou aux groupes de contourner la vérification de la traverse du répertoire](#)

[Interdire aux utilisateurs ou aux groupes de contourner la vérification de la traverse de répertoire](#)

[Configurez le mappage de caractères pour la conversion de nom de fichier SMB sur des volumes](#)

[Créer des listes de contrôle d'accès pour le partage SMB](#)

[Sécurisez l'accès aux fichiers à l'aide de Storage-Level Access Guard](#)

[Liste des privilèges pris en charge](#)

[Ajoutez des privilèges aux utilisateurs ou groupes locaux ou de domaine](#)

Permet aux utilisateurs ou aux groupes de contourner la vérification de la traverse du répertoire

Si vous souhaitez qu'un utilisateur puisse parcourir tous les répertoires du chemin d'accès à un fichier, même si l'utilisateur ne dispose pas des autorisations sur un répertoire de parcours, vous pouvez ajouter le `SeChangeNotifyPrivilege` Privilège pour les utilisateurs ou groupes SMB locaux sur des SVM (Storage Virtual machine). Par défaut, les utilisateurs peuvent contourner la vérification par passage de répertoire.

Avant de commencer

- Un serveur SMB doit être existant sur le SVM.
- L'option serveur SMB des utilisateurs et groupes locaux doit être activée.

- Utilisateur ou groupe local ou de domaine auquel SeChangeNotifyPrivilege le privilège sera ajouté doit déjà exister.

Description de la tâche

Lors de l'ajout de privilèges à un utilisateur ou à un groupe de domaine, ONTAP peut valider l'utilisateur ou le groupe du domaine en contactant le contrôleur de domaine. La commande peut échouer si ONTAP ne parvient pas à contacter le contrôleur de domaine.

Étapes

1. Activer la vérification de la traverse de dérivation en ajoutant le SeChangeNotifyPrivilege privilège d'un utilisateur ou groupe local ou de domaine :

```
vserver cifs users-and-groups privilege add-privilege -vserver vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege
```

La valeur pour le -user-or-group-name il s'agit d'un utilisateur ou d'un groupe local, ou d'un utilisateur ou d'un groupe de domaines.

2. Vérifiez que la vérification de la dérivation transversale est activée pour l'utilisateur ou le groupe spécifié :

```
vserver cifs users-and-groups privilege show -vserver vs1 -user-or-group-name EXAMPLE\eng
```

Exemple

La commande suivante permet aux utilisateurs qui appartiennent au groupe « EXAMPLE\eng » de contourner la vérification de la traverse de répertoire en ajoutant le SeChangeNotifyPrivilege privilège du groupe :

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege
```



```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
```

Vserver	User or Group Name	Privileges
vs1	EXAMPLE\eng	SeChangeNotifyPrivilege

Informations associées

[Interdire aux utilisateurs ou aux groupes de contourner la vérification de la traverse de répertoire](#)

Interdire aux utilisateurs ou aux groupes de contourner la vérification de la traverse de répertoire

Si vous ne souhaitez pas qu'un utilisateur traverse tous les répertoires du chemin d'accès à un fichier car l'utilisateur ne dispose pas des autorisations sur le répertoire de parcours, vous pouvez supprimer le SeChangeNotifyPrivilege Privilège des utilisateurs ou groupes SMB locaux sur des SVM (Storage Virtual machine).

Avant de commencer

L'utilisateur ou le groupe local ou de domaine dont les privilèges seront supprimés doit déjà exister.

Description de la tâche

Lors de la suppression de privilèges d'un utilisateur ou d'un groupe de domaines, ONTAP peut valider l'utilisateur ou le groupe de domaines en contactant le contrôleur de domaine. La commande peut échouer si

ONTAP ne parvient pas à contacter le contrôleur de domaine.

Étapes

1. Interdire la vérification de la traverse de dérivation :
`vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

La commande supprime le `SeChangeNotifyPrivilege` privilège de l'utilisateur ou groupe local ou de domaine que vous spécifiez avec la valeur pour le `-user-or-group-name name` paramètre.

2. Vérifiez que le contrôle de la traverse de dérivation de l'utilisateur ou du groupe spécifié est désactivé :
`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Exemple

La commande suivante empêche les utilisateurs appartenant au groupe « `EXEMPLE\eng` » de contourner la vérification de la traverse de répertoire :

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
-----
vs1        EXEMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXEMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
-----
vs1        EXEMPLE\eng        -
```

Informations associées

[Possibilité pour les utilisateurs ou les groupes de contourner la vérification de la traverse du répertoire](#)

Affiche des informations sur la sécurité des fichiers et les stratégies d'audit

Affiche des informations sur la sécurité des fichiers et l'aperçu des stratégies d'audit

Vous pouvez afficher des informations sur la sécurité des fichiers dans les fichiers et les répertoires contenus dans les volumes des SVM (Storage Virtual machine). Vous pouvez afficher des informations sur les règles d'audit sur les volumes FlexVol. Si configuré, vous pouvez afficher des informations sur les paramètres de sécurité Storage-Level Access Guard et Dynamic Access Control sur les volumes FlexVol.

Affichage des informations relatives à la sécurité des fichiers

Vous pouvez afficher les informations relatives à la sécurité des fichiers appliquées aux données contenues

dans des volumes et des qtrees (pour les volumes FlexVol) avec les styles de sécurité suivants :

- NTFS
- UNIX
- Mixte

Affichage des informations relatives aux stratégies d'audit

Vous pouvez afficher des informations sur les règles d'audit pour l'audit des événements d'accès sur les volumes FlexVol sur les protocoles NAS suivants :

- SMB (toutes les versions)
- NFSv4.x

Affichage d'informations sur la sécurité de Storage-Level Access Guard (SLAG)

La sécurité de la protection d'accès au niveau du stockage peut être appliquée sur des volumes FlexVol et des objets qtree avec les styles de sécurité suivants :

- NTFS
- Mixte
- UNIX (si un serveur CIFS est configuré sur le SVM qui contient le volume)

Affichage d'informations sur la sécurité du contrôle d'accès dynamique (DAC)

La sécurité du contrôle d'accès dynamique peut être appliquée à un objet au sein d'un volume FlexVol avec les styles de sécurité suivants :

- NTFS
- Mixte (si l'objet dispose d'une sécurité NTFS effective)

Informations associées

[Sécurisation de l'accès aux fichiers à l'aide de Storage-Level Access Guard](#)

[Affichage d'informations sur Storage-Level Access Guard](#)

Affiche des informations sur la sécurité des fichiers sur les volumes de style de sécurité NTFS

Vous pouvez afficher des informations sur la sécurité des fichiers et des répertoires sur les volumes de style de sécurité NTFS, notamment le style de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les attributs DOS. Les résultats vous permettent de valider votre configuration de sécurité ou de résoudre les problèmes d'accès aux fichiers.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux données dont vous souhaitez afficher les informations de sécurité des fichiers ou des dossiers. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Étant donné que les volumes et les qtrees de style de sécurité NTFS utilisent uniquement les autorisations de fichier NTFS et les utilisateurs et groupes Windows lors de la détermination des droits d'accès aux

fichiers, les champs de sortie liés à UNIX contiennent des informations d'autorisation de fichier UNIX en affichage uniquement.

- Les valeurs de sortie ACL sont affichées pour les fichiers et les dossiers avec la sécurité NTFS.
- Étant donné que la sécurité Storage-Level Access Guard peut être configurée sur le volume racine ou qtree, le résultat d'un chemin de volume ou qtree dans lequel Storage-Level Access Guard est configuré peut afficher à la fois les listes de contrôle d'accès standard des fichiers et les listes de contrôle d'accès Storage-Level Access Guard.
- La sortie affiche également des informations sur les ACE de contrôle d'accès dynamique si le contrôle d'accès dynamique est configuré pour le chemin de fichier ou de répertoire donné.

Étape

1. Afficher les paramètres de sécurité des fichiers et des répertoires avec le niveau de détail souhaité :

Pour afficher les informations...	Saisissez la commande suivante...
Sous forme récapitulative	<pre>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i></pre>
Avec détails étendus	<pre>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i> -expand-mask true</pre>

Exemples

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès /vol4 Au SVM vs1 :

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4
```

```

        Vserver: vs1
        File Path: /vol4
    File Inode Number: 64
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
            Control:0x8004
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff
            ALLOW-Everyone-0x10000000-
```

OI|CI|IO

L'exemple suivant affiche les informations de sécurité avec des masques étendus sur le chemin /data/engineering Au SVM vs1 :

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true
```

```

        Vserver: vs1
        File Path: /data/engineering
    File Inode Number: 5544
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
```

```

    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
    Control:0x8004

```

```

1... .. = Self Relative
.0.. .. = RM Control Valid
..0. .. = SACL Protected
...0 .. = DACL Protected
.... 0... .. = SACL Inherited
.... .0.. .. = DACL Inherited
.... ..0. .. = SACL Inherit Required
.... ...0 .. = DACL Inherit Required
.... ....0. .. = SACL Defaulted
.... ....0 .. = SACL Present
.... .... 0... = DACL Defaulted
.... .... .1.. = DACL Present
.... .... ..0. = Group Defaulted
.... .... ...0 = Owner Defaulted

```

```

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs

```

```

ALLOW-Everyone-0x1f01ff

```

	0... .. =
Generic Read	
	.0.. .. =
Generic Write	
	..0. =
Generic Execute	
	...0 =
Generic All	
0 =
System Security	
1 =
Synchronize	
 1... .. =
Write Owner	
1.. =
Write DAC	
1. =
Read Control	
1 =
Delete	

1..... =
Write Attributes	
1.... =
Read Attributes	
1... =
Delete Child	
1. =
Execute	
1 =
Write EA	
1... =
Read EA	
1... =
Append	
1. =
Write	
1 =
Read	
	ALLOW-Everyone-0x10000000-OI CI IO
	0..... =
Generic Read	
	.0..... =
Generic Write	
	..0..... =
Generic Execute	
	...1..... =
Generic All	
0..... =
System Security	
0..... =
Synchronize	
0..... =
Write Owner	
0..... =
Write DAC	
0..... =
Read Control	
0..... =
Delete	
0..... =
Write Attributes	
0..... =
Read Attributes	
0..... =
Delete Child	

Execute0..... =
Write EA0..... =
Read EA0..... =
Append0..... =
Write0..... =
Read0..... =

L'exemple suivant affiche des informations de sécurité, y compris des informations de sécurité Storage-Level Access Guard, pour le volume avec le chemin d'accès /datavol1 Au SVM vs1 :

```
cluster::> vserver security file-directory show -vserver vs1 -path /datavol1
```

```

    Vserver: vs1
    File Path: /datavol1
    File Inode Number: 77
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
          Control:0x8004
          Owner: BUILTIN\Administrators
          Group: BUILTIN\Administrators
          DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-OI|CI|IO

    Storage-Level Access Guard security
    SACL (Applies to Directories):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Directories):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
    SACL (Applies to Files):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Files):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Informations associées

[Affichage d'informations sur la sécurité des fichiers sur des volumes de style de sécurité mixtes](#)

[Affichage d'informations sur la sécurité des fichiers sur des volumes de style de sécurité UNIX](#)

Vous pouvez afficher des informations sur la sécurité des fichiers et des répertoires sur des volumes de style de sécurité mixtes, y compris le style de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les propriétaires et groupes UNIX. Les résultats vous permettent de valider votre configuration de sécurité ou de résoudre les problèmes d'accès aux fichiers.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux données dont vous souhaitez afficher les informations de sécurité des fichiers ou des dossiers. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Les qtrees et volumes de style de sécurité mixtes peuvent contenir certains fichiers et dossiers qui utilisent des autorisations de fichier UNIX, soit les bits de mode ou les ACL NFSv4, ainsi que certains fichiers et répertoires utilisant les autorisations de fichier NTFS.
- Le niveau supérieur d'un volume de type sécurité mixte peut avoir une sécurité efficace UNIX ou NTFS.
- Les valeurs de sortie ACL s'affichent uniquement pour les fichiers et les dossiers avec sécurité NTFS ou NFSv4.

Ce champ est vide pour les fichiers et les répertoires utilisant la sécurité UNIX qui n'ont que des autorisations de bit de mode appliquées (pas de listes de contrôle d'accès NFSv4).

- Les champs de sortie propriétaire et groupe de la sortie ACL ne s'appliquent que dans le cas des descripteurs de sécurité NTFS.
- Étant donné que la sécurité de Storage-Level Access Guard peut être configurée sur un volume mixte de style de sécurité, même si le style de sécurité efficace de la racine du volume ou de qtree est UNIX, La sortie d'un chemin de volume ou qtree dans lequel Storage-Level Access Guard est configuré peut afficher à la fois les autorisations de fichiers UNIX et les listes de contrôle d'accès Storage-Level Access Guard.
- Si le chemin entré dans la commande est de données avec la sécurité effective NTFS, la sortie affiche également des informations sur les ACE de contrôle d'accès dynamique si le contrôle d'accès dynamique est configuré pour le chemin de fichier ou de répertoire donné.

Étape

1. Afficher les paramètres de sécurité des fichiers et des répertoires avec le niveau de détail souhaité :

Pour afficher les informations...	Saisissez la commande suivante...
Sous forme récapitulative	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Avec détails étendus	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Exemples

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès /projects Dans le SVM vs1 sous forme de masque étendu. Ce chemin de sécurité mixte possède une sécurité efficace UNIX.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true
```

```

        Vserver: vs1
        File Path: /projects
    File Inode Number: 78
        Security Style: mixed
    Effective Style: unix
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
    Unix Mode Bits in Text: rwx-----
        ACLs: -
```

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès /data Au SVM vs1. Ce chemin de sécurité mixte dispose d'une sécurité NTFS efficace.


```
cluster1::> vserver security file-directory show -vserver vs1 -path /data
```

```

        Vserver: vs1
        File Path: /data
    File Inode Number: 544
        Security Style: mixed
        Effective Style: ntfs
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
            Control:0x8004
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-
```

OI|CI|IO

L'exemple suivant affiche les informations de sécurité relatives au volume sur le chemin d'accès /datavol5 Au SVM vs1. Le niveau supérieur de ce volume de type sécurité mixte dispose d'une sécurité effective UNIX. Le volume est doté de la sécurité Storage-Level Access Guard.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /datavol5
```

```
      Vserver: vs1
      File Path: /datavol5
      File Inode Number: 3374
      Security Style: mixed
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 755
      Unix Mode Bits in Text: rwxr-xr-x
      ACLs: Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-EXAMPLE\market-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-EXAMPLE\market-0x1f01ff
```

Informations associées

[Affichage d'informations sur la sécurité des fichiers sur les volumes de style de sécurité NTFS](#)

[Affichage d'informations sur la sécurité des fichiers sur des volumes de style de sécurité UNIX](#)

Affiche des informations sur la sécurité des fichiers sur des volumes de type sécurité UNIX

Vous pouvez afficher des informations sur la sécurité des fichiers et des répertoires sur les volumes de style de sécurité UNIX, notamment les styles de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les propriétaires et

groupes UNIX. Les résultats vous permettent de valider votre configuration de sécurité ou de résoudre les problèmes d'accès aux fichiers.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux données dont vous souhaitez afficher les informations de sécurité de fichier ou de répertoire. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Les volumes et les qtrees de style de sécurité UNIX n'utilisent que les autorisations de fichier UNIX, soit les bits de mode, soit les listes de contrôle d'accès NFSv4 lors de la détermination des droits d'accès aux fichiers.
- Les valeurs de sortie ACL s'affichent uniquement pour les fichiers et les dossiers avec la sécurité NFSv4.

Ce champ est vide pour les fichiers et les répertoires utilisant la sécurité UNIX qui n'ont que des autorisations de bit de mode appliquées (pas de listes de contrôle d'accès NFSv4).

- Les champs de sortie propriétaire et groupe de la sortie ACL ne s'appliquent pas dans le cas des descripteurs de sécurité NFSv4.

Ils ne sont utiles que pour les descripteurs de sécurité NTFS.

- Étant donné que la sécurité Storage-Level Access Guard est prise en charge sur un volume UNIX ou qtree si un serveur CIFS est configuré sur le SVM, le résultat peut contenir des informations relatives à la sécurité Storage-Level Access Guard appliquée au volume ou au qtree spécifié dans le `-path` paramètre.

Étape

1. Afficher les paramètres de sécurité des fichiers et des répertoires avec le niveau de détail souhaité :

Pour afficher les informations...	Saisissez la commande suivante...
Sous forme récapitulative	<code>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i></code>
Avec détails étendus	<code>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i> -expand-mask true</code>

Exemples

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès `/home` Au SVM `vs1` :

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
```

```

        Vserver: vs1
        File Path: /home
    File Inode Number: 9590
        Security Style: unix
        Effective Style: unix
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
    Unix Mode Bits in Text: rwx-----
        ACLs: -
```

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès /home Au SVM vs1 sous forme de masque étendu :

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true
```

```

        Vserver: vs1
        File Path: /home
    File Inode Number: 9590
        Security Style: unix
        Effective Style: unix
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... = Normal
    .... .... ..0. = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
    Unix Mode Bits in Text: rwx-----
        ACLs: -
```

Informations associées

[Affichage d'informations sur la sécurité des fichiers sur les volumes de style de sécurité NTFS](#)

[Affichage d'informations sur la sécurité des fichiers sur des volumes de style de sécurité mixtes](#)

Affiche des informations sur les règles d'audit NTFS sur les volumes FlexVol à l'aide de l'interface de ligne de commande

Vous pouvez afficher des informations sur les stratégies d'audit NTFS sur les volumes FlexVol, notamment les styles de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les listes de contrôle d'accès système. Vous pouvez utiliser les résultats pour valider votre configuration de sécurité ou pour résoudre les problèmes d'audit.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux fichiers ou dossiers dont vous souhaitez afficher les informations d'audit. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Les volumes et les qtrees de style de sécurité NTFS utilisent uniquement des listes de contrôle d'accès au système NTFS pour les stratégies d'audit.
- Les règles d'audit NTFS peuvent être appliquées aux fichiers et dossiers d'un volume de style de sécurité mixte avec la sécurité efficace NTFS.

Les volumes et qtrees de style de sécurité mixtes peuvent contenir certains fichiers et répertoires qui utilisent des autorisations de fichier UNIX, soit les bits de mode, soit les ACL NFSv4, ainsi que certains fichiers et répertoires utilisant les autorisations de fichier NTFS.

- Le niveau supérieur d'un volume de style de sécurité mixte peut avoir une sécurité efficace sous UNIX ou NTFS et peut-être ne pas contenir des CLS NTFS.
- Étant donné que la sécurité de Storage-Level Access Guard peut être configurée sur un volume mixte de style de sécurité, même si le style de sécurité efficace de la racine du volume ou de qtree est UNIX, La sortie d'un chemin de volume ou qtree dans lequel Storage-Level Access Guard est configuré peut afficher à la fois le fichier régulier et le dossier SACLs NFSv4 et les SACLs NTFS Storage-Level Access Guard.
- Si le chemin entré dans la commande est celui des données avec la sécurité effective NTFS, la sortie affiche également des informations sur les ACE de contrôle d'accès dynamique si le contrôle d'accès dynamique est configuré pour le chemin d'accès au fichier ou au répertoire donné.
- Lorsque vous affichez des informations de sécurité sur les fichiers et les dossiers avec la sécurité efficace NTFS, les champs de sortie liés à UNIX contiennent des informations d'autorisation de fichier UNIX en affichage uniquement.

Les fichiers et dossiers de style de sécurité NTFS utilisent uniquement les autorisations de fichier NTFS et les utilisateurs et groupes Windows lors de la détermination des droits d'accès aux fichiers.

- Les valeurs de sortie ACL s'affichent uniquement pour les fichiers et les dossiers disposant de la sécurité NTFS ou NFSv4.

Ce champ est vide pour les fichiers et les dossiers utilisant la sécurité UNIX qui n'ont que des autorisations de bit de mode appliquées (pas de listes de contrôle d'accès NFSv4).

- Les champs de sortie propriétaire et groupe de la sortie ACL ne s'appliquent que dans le cas des descripteurs de sécurité NTFS.

Étape

1. Afficher les paramètres de stratégie d'audit de fichier et de répertoire avec le niveau de détail souhaité :

Pour afficher les informations...	Saisissez la commande suivante...
Sous forme récapitulative	<code>vserver security file-directory show -vserver vserver_name -path path</code>
En tant que liste détaillée	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Exemples

L'exemple suivant affiche les informations de la stratégie d'audit pour le chemin /corp Au SVM vs1. Le chemin dispose d'une sécurité NTFS efficace. Le descripteur de sécurité NTFS contient à la fois une entrée RACL RÉUSSIE/ÉCHEC.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
      Vserver: vs1
      File Path: /corp
      File Inode Number: 357
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8014
            Owner:DOMAIN\Administrator
            Group:BUILTIN\Administrators
            SACL - ACEs
                  ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                  SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
            DACL - ACEs
                  ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                  ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                  ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

L'exemple suivant affiche les informations de la stratégie d'audit pour le chemin /datavol1 Au SVM vs1. Le chemin contient à la fois des fichiers standard et des SACL de dossier et des SALC de Storage-Level Access Guard.

```

cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

      Vserver: vs1
      File Path: /datavol1
      File Inode Number: 77
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xaa14
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            SACL - ACEs
                  AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
            DACL - ACEs
                  ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                  ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

      Storage-Level Access Guard security
      SACL (Applies to Directories):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

Affiche des informations sur les règles d'audit NFSv4 sur les volumes FlexVol à l'aide de l'interface de ligne de commandes

Vous pouvez afficher des informations sur les stratégies d'audit NFSv4 sur les volumes FlexVol à l'aide de l'interface de ligne de commande ONTAP, notamment les styles de

sécurité et les styles de sécurité efficaces, les autorisations appliquées, ainsi que les informations sur les listes de contrôle d'accès système (SACL). Vous pouvez utiliser les résultats pour valider votre configuration de sécurité ou pour résoudre les problèmes d'audit.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux fichiers ou aux répertoires dont vous souhaitez afficher les informations d'audit. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Les volumes et les qtrees de style de sécurité UNIX n'utilisent que les règles d'audit NFSv4.
 - Les fichiers et les répertoires d'un volume mixte de style de sécurité UNIX peuvent appliquer des règles d'audit NFSv4.
- Les volumes et qtrees de style de sécurité mixtes peuvent contenir certains fichiers et répertoires qui utilisent des autorisations de fichier UNIX, soit les bits de mode, soit les ACL NFSv4, ainsi que certains fichiers et répertoires utilisant les autorisations de fichier NTFS.
- Le niveau supérieur d'un volume de type sécurité mixte peut présenter une sécurité efficace sous UNIX ou NTFS et peut-être ne pas contenir des CLS NFSv4.
 - Les valeurs de sortie ACL s'affichent uniquement pour les fichiers et les dossiers avec sécurité NTFS ou NFSv4.

Ce champ est vide pour les fichiers et les dossiers utilisant la sécurité UNIX qui n'ont que des autorisations de bit de mode appliquées (pas de listes de contrôle d'accès NFSv4).

- Les champs de sortie propriétaire et groupe de la sortie ACL ne s'appliquent que dans le cas des descripteurs de sécurité NTFS.
- Étant donné que la sécurité de Storage-Level Access Guard peut être configurée sur un volume mixte de style de sécurité, même si le style de sécurité efficace de la racine du volume ou de qtree est UNIX, La sortie d'un chemin de volume ou qtree dans lequel Storage-Level Access Guard est configuré peut afficher à la fois le fichier NFSv4 régulier et le répertoire SACLs et les SACLs NTFS Storage-Level Access Guard.
- Étant donné que la sécurité Storage-Level Access Guard est prise en charge sur un volume UNIX ou qtree si un serveur CIFS est configuré sur le SVM, le résultat peut contenir des informations relatives à la sécurité Storage-Level Access Guard appliquée au volume ou au qtree spécifié dans le `-path` paramètre.

Étapes

1. Afficher les paramètres de sécurité des fichiers et des répertoires avec le niveau de détail souhaité :

Pour afficher les informations...	Saisissez la commande suivante...
Sous forme récapitulative	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Avec détails étendus	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Exemples

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès /lab Au SVM vs1. Ce chemin de style de sécurité UNIX dispose d'un SACL NFSv4.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

      Vserver: vs1
      File Path: /lab
      File Inode Number: 288
      Security Style: unix
      Effective Style: unix
      DOS Attributes: 11
      DOS Attributes in Text: ----D--R
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 0
      Unix Mode Bits in Text: -----
      ACLs: NFSV4 Security Descriptor
            Control:0x8014
            SACL - ACEs
                  SUCCESSFUL-S-1-520-0-0xf01ff-SA
                  FAILED-S-1-520-0-0xf01ff-FA
            DACL - ACEs
                  ALLOW-S-1-520-1-0xf01ff
```

Moyens d'afficher des informations sur la sécurité des fichiers et les stratégies d'audit

Vous pouvez utiliser le caractère générique (*) pour afficher des informations sur la sécurité des fichiers et les stratégies d'audit de tous les fichiers et répertoires sous un chemin donné ou un volume racine.

Le caractère générique () **peut être utilisé comme dernier sous-composant d'un chemin d'accès de répertoire donné, sous lequel vous souhaitez afficher les informations de tous les fichiers et répertoires. Si vous souhaitez afficher les informations d'un fichier ou d'un répertoire donné nommé "",** vous devez alors indiquer le chemin complet à l'intérieur de guillemets doubles ("").

Exemple

La commande suivante avec le caractère générique affiche les informations relatives à tous les fichiers et répertoires sous le chemin d'accès /1/ Du SVM vs1 :

```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*

      Vserver: vs1
      File Path: /1/1
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8514
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

      Vserver: vs1
      File Path: /1/1/abc
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8404
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

La commande suivante affiche les informations d'un fichier nommé "" sous le chemin d'accès /vol1/a Du SVM vs1. Le chemin est entouré de guillemets doubles (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path  
"/vol1/a/*"
```

```
        Vserver: vs1  
        File Path: "/vol1/a/*"  
        Security Style: mixed  
        Effective Style: unix  
        DOS Attributes: 10  
        DOS Attributes in Text: ----D---  
        Expanded Dos Attributes: -  
            Unix User Id: 1002  
            Unix Group Id: 65533  
            Unix Mode Bits: 755  
        Unix Mode Bits in Text: rwxr-xr-x  
        ACLs: NFSV4 Security Descriptor  
            Control:0x8014  
            SACL - ACEs  
                AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA  
            DACL - ACEs  
                ALLOW-EVERYONE@-0x1f00a9-FI|DI  
                ALLOW-OWNER@-0x1f01ff-FI|DI  
                ALLOW-GROUP@-0x1200a9-IG
```

Gérez la sécurité des fichiers NTFS, les règles d'audit NTFS et Storage-Level Access Guard sur les SVM à l'aide de l'interface de ligne de commande

Gérez la sécurité des fichiers NTFS, les règles d'audit NTFS et Storage-Level Access Guard sur les SVM à l'aide de la présentation de l'interface de ligne de commande

Vous pouvez gérer la sécurité des fichiers NTFS, les règles d'audit NTFS et Storage-Level Access Guard sur les SVM de stockage virtuels à l'aide de l'interface de ligne de commande.

Vous pouvez gérer les règles de sécurité et d'audit des fichiers NTFS des clients SMB ou à l'aide de l'interface de ligne de commande. Toutefois, l'utilisation de la CLI pour configurer les stratégies de sécurité des fichiers et d'audit supprime la nécessité d'utiliser un client distant pour gérer la sécurité des fichiers. L'utilisation de l'interface de ligne de commande permet de réduire considérablement le temps nécessaire à l'application de la sécurité sur de nombreux fichiers et dossiers à l'aide d'une seule commande.

Vous pouvez configurer Storage-Level Access Guard, qui est une autre couche de sécurité appliquée par ONTAP aux volumes de SVM. Storage-Level Access Guard s'applique aux accès de tous les protocoles NAS à l'objet de stockage auquel Storage-Level Access Guard est appliqué.

Storage-Level Access Guard peut être configuré et géré uniquement à partir de l'interface de ligne de commande ONTAP. Vous ne pouvez pas gérer les paramètres Storage-Level Access Guard à partir des clients SMB. De plus, si vous affichez les paramètres de sécurité d'un fichier ou d'un répertoire à partir d'un client NFS ou SMB, vous ne verrez pas la sécurité Storage-Level Access Guard. La sécurité Access Guard au niveau du stockage ne peut pas être révoquée d'un client, même par un administrateur système (Windows ou UNIX). Par conséquent, Storage-Level Access Guard offre une couche supplémentaire de sécurité pour

l'accès aux données, qui est défini et géré de façon indépendante par l'administrateur du stockage.



Bien que seules les autorisations d'accès NTFS soient prises en charge pour Storage-Level Access Guard, ONTAP peut effectuer des vérifications de sécurité pour l'accès via NFS aux données sur les volumes où Storage-Level Access Guard est appliqué si l'utilisateur UNIX mappe avec un utilisateur Windows sur le SVM propriétaire du volume.

Volumes de sécurité NTFS

Tous les fichiers et dossiers contenus dans des volumes et qtrees de style de sécurité NTFS bénéficient d'une sécurité efficace. Vous pouvez utiliser le `vserver security file-directory` Famille de commandes permettant d'implémenter les types de sécurité suivants sur les volumes de style de sécurité NTFS :

- Autorisations liées aux fichiers et stratégies d'audit pour les fichiers et les dossiers contenus dans le volume
- Sécurité Access Guard du niveau de stockage sur les volumes

Volumes de sécurité mixtes

Les qtrees et volumes de style de sécurité mixtes peuvent contenir certains fichiers et dossiers disposant d'une sécurité effective UNIX et utiliser des autorisations de fichiers UNIX, soit les bits de mode, soit les listes de contrôle d'accès NFSv4.x et les règles d'audit NFSv4.x, ainsi que certains fichiers et dossiers disposant d'une sécurité efficace NTFS, et utilisant les autorisations d'accès aux fichiers NTFS et les règles d'audit. Vous pouvez utiliser le `vserver security file-directory` famille de commandes pour appliquer les types de sécurité suivants aux données de style de sécurité mixte :

- Autorisations liées aux fichiers et règles d'audit sur les fichiers et les dossiers avec le style de sécurité effectif NTFS dans le volume mixte ou le qtree
- Access Guard au niveau du stockage pour les volumes NTFS et UNIX

Volumes de style de sécurité UNIX

Les volumes et les qtrees de style de sécurité UNIX contiennent des fichiers et des dossiers qui disposent d'une sécurité effective UNIX (soit les bits de mode, soit les ACL NFSv4.x). Si vous souhaitez utiliser le, vous devez garder à l'esprit les éléments suivants `vserver security file-directory` Famille de commandes pour implémenter la sécurité sur des volumes de type sécurité UNIX :

- Le `vserver security file-directory` Les familles de commandes ne peuvent pas être utilisées pour gérer la sécurité des fichiers UNIX et les règles d'audit sur les volumes et les qtrees de style de sécurité UNIX.
- Vous pouvez utiliser le `vserver security file-directory` Gamme de commandes permettant de configurer Storage-Level Access Guard sur des volumes de style de sécurité UNIX, à condition que le SVM avec le volume cible contienne un serveur CIFS.

Informations associées

[Affiche des informations sur la sécurité des fichiers et les stratégies d'audit](#)

[Configurez et appliquez la sécurité des fichiers sur les fichiers et dossiers NTFS à l'aide de l'interface de ligne de commande](#)

[Configurez et appliquez des règles d'audit aux fichiers et dossiers NTFS à l'aide de l'interface de ligne de commande](#)

Utilisez les cas d'utilisation de l'interface de ligne de commande pour définir la sécurité des fichiers et des dossiers

Puisque vous pouvez appliquer et gérer la sécurité des fichiers et des dossiers localement sans l'intervention d'un client distant, vous pouvez réduire considérablement le temps nécessaire pour définir la sécurité en bloc sur un grand nombre de fichiers ou de dossiers.

Vous pouvez utiliser l'interface de ligne de commande pour définir la sécurité des fichiers et des dossiers dans les cas d'utilisation suivants :

- Stockage de fichiers dans les grands environnements d'entreprise, tels que le stockage de fichiers dans les répertoires locaux
- Migration des données
- Changement de domaine Windows
- Standardisation des règles de sécurité des fichiers et d'audit sur l'ensemble des systèmes de fichiers NTFS

Limites lors de l'utilisation de l'interface de ligne de commande pour définir la sécurité des fichiers et des dossiers

Vous devez connaître certaines limites lorsque vous utilisez l'interface de ligne de commande pour définir la sécurité des fichiers et des dossiers.

- Le `vserver security file-directory` La famille de commandes ne prend pas en charge la configuration des listes de contrôle d'accès NFSv4.

Vous pouvez uniquement appliquer des descripteurs de sécurité NTFS aux fichiers et dossiers NTFS.

Comment les descripteurs de sécurité sont utilisés pour appliquer la sécurité des fichiers et des dossiers

Les descripteurs de sécurité contiennent les listes de contrôle d'accès qui déterminent les actions qu'un utilisateur peut effectuer sur les fichiers et les dossiers, et ce qui est vérifié lorsqu'un utilisateur accède à des fichiers et à des dossiers.

• Autorisations

Les autorisations sont autorisées ou refusées par le propriétaire d'un objet et déterminent les actions qu'un objet (utilisateurs, groupes ou objets informatiques) peut exécuter sur des fichiers ou dossiers spécifiés.

• Descripteurs de sécurité

Les descripteurs de sécurité sont des structures de données contenant des informations de sécurité qui définissent les autorisations associées à un fichier ou à un dossier.

• Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès sont les listes contenues dans un descripteur de sécurité qui contiennent des informations sur les actions que les utilisateurs, les groupes ou les objets informatiques peuvent exécuter sur le fichier ou le dossier auquel le descripteur de sécurité est appliqué. Le Security Descriptor peut contenir les deux types de listes de contrôle d'accès suivants :

- Listes de contrôle d'accès discrétionnaire (DACL)
- Listes de contrôle d'accès au système (SACL)
- * Listes de contrôle d'accès discrétionnaire (listes DACL)*

Les DACL contiennent la liste des SID pour les utilisateurs, les groupes et les objets d'ordinateur qui sont autorisés ou refusés à effectuer des actions sur des fichiers ou des dossiers. Les listes DACL contiennent au moins zéro entrée de contrôle d'accès (ACE).

- **Listes de contrôle d'accès au système (SACL)**

Les SACL contiennent la liste des PEID pour les utilisateurs, les groupes et les objets d'ordinateur pour lesquels des événements d'audit réussis ou échoués sont consignés. Les SACL contiennent au moins zéro entrée de contrôle d'accès (ACE).

- **Entrées de contrôle d'accès (ACE)**

Ces sont des entrées individuelles dans DACL ou SACL :

- Une entrée de contrôle d'accès DACL spécifie les droits d'accès autorisés ou refusés pour certains utilisateurs, groupes ou objets d'ordinateur.
- Une entrée de contrôle d'accès SACL spécifie les événements succès ou échec à consigner lors de l'audit des actions spécifiées effectuées par des utilisateurs, des groupes ou des objets d'ordinateur particuliers.

- **Héritage des autorisations**

L'héritage des autorisations décrit comment les autorisations définies dans les descripteurs de sécurité sont propagées à un objet à partir d'un objet parent. Seules les autorisations héréditaires sont héritées par des objets enfants. Lorsque vous définissez des autorisations sur l'objet parent, vous pouvez décider si les dossiers, sous-dossiers et fichiers peuvent les hériter avec "appliquer à this-folder, sub-folders, et `fichiers`".

Informations associées

["Audit et suivi de sécurité SMB et NFS"](#)

[Configuration et application de règles d'audit aux fichiers et dossiers NTFS à l'aide de l'interface de ligne de commande](#)

Consignes d'application des stratégies de répertoires de fichiers utilisant des utilisateurs ou des groupes locaux sur la destination de reprise après incident du SVM

Si la configuration de votre politique de répertoire de fichiers utilise des utilisateurs ou des groupes locaux dans le Security Descriptor ou les entrées DACL ou SACL, vous devez garder à l'esprit avant d'appliquer les stratégies de répertoires de fichiers sur la destination de reprise après incident SVM (Storage Virtual machine) en configuration de suppression d'ID.

Il est possible de configurer une configuration de reprise sur incident pour un SVM où le SVM source sur le cluster source réplique les données et la configuration depuis le SVM source vers un SVM destination sur un cluster de destination.

Vous pouvez configurer l'un des deux types de reprise après incident des SVM :

- Identité préservée

Avec cette configuration, l'identité du SVM et du serveur CIFS est préservée.

- Identité rejetée

Avec cette configuration, l'identité du SVM et du serveur CIFS n'est pas conservée. Dans ce scénario, le nom du SVM et du serveur CIFS sur le SVM de destination est différent de celui du SVM et du nom du serveur CIFS sur le SVM source.

Instructions pour les configurations éliminées par identité

Dans une configuration définie par l'identité, pour une source SVM qui contient des configurations utilisateur, groupe et privilège local, le nom du domaine local (nom du serveur CIFS local) doit être modifié afin de correspondre au nom du serveur CIFS sur la destination du SVM. Par exemple, si le nom du SVM source est « vs1 » et que le nom du serveur CIFS est « CIFS1 », et que le nom du SVM de destination est « vs1_dst » et que le nom du serveur CIFS est « CIFS1_DST », le nom de domaine local d'un utilisateur local nommé « DST C1\user1 » est automatiquement modifié sur la SVM « destination » :

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

Vserver	User Name	Full Name	Description
vs1	CIFS1\Administrator		Built-in
administrator	account		
vs1	CIFS1\user1	-	-

```
cluster1dst::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

Vserver	User Name	Full Name	Description
vs1_dst	CIFS1_DST\Administrator		Built-in
administrator	account		
vs1_dst	CIFS1_DST\user1	-	-

Même si les noms d'utilisateur et de groupe locaux sont automatiquement modifiés dans les bases de données des utilisateurs et des groupes locaux, les noms d'utilisateurs ou de groupes locaux ne sont pas automatiquement modifiés dans les configurations des stratégies de répertoires de fichiers (règles configurées sur la CLI à l'aide de l'`vserver security file-directory` famille de commande).

Par exemple, pour « vs1 », si vous avez configuré une entrée DACL où le `-account` Le paramètre est défini sur « CIFS1\user1 », le paramètre n'est pas automatiquement modifié sur le SVM de destination pour refléter le nom du serveur CIFS de destination.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
CIFS1\user1	allow	full-control	this-folder

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1_dst
```

```
Vserver: vs1_dst
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
CIFS1\user1	allow	full-control	this-folder

Vous devez utiliser le `vserver security file-directory modify` Commandes permettant de modifier manuellement le nom du serveur CIFS sur le nom du serveur CIFS de destination.

Composants de configuration de la stratégie de répertoire de fichiers contenant des paramètres de compte

Il existe trois composants de configuration de stratégie de répertoire de fichiers qui peuvent utiliser des paramètres pouvant contenir des utilisateurs ou des groupes locaux :

- Descripteur de sécurité

Vous pouvez éventuellement spécifier le propriétaire du descripteur de sécurité et le groupe principal du propriétaire du descripteur de sécurité. Si le Security Descriptor utilise un utilisateur ou groupe local pour les entrées propriétaire et groupe principal, vous devez modifier le Security Descriptor afin d'utiliser le SVM destination dans le nom du compte. Vous pouvez utiliser le `vserver security file-directory ntfs modify` commande permettant de modifier les noms de compte si nécessaire.

- Entrées DACL

Chaque entrée DACL doit être associée à un compte. Vous devez modifier tout DACL qui utilisent des comptes utilisateur ou groupe locaux pour utiliser le nom de SVM de destination. Étant donné que vous ne pouvez pas modifier le nom du compte pour les entrées DACL existantes, vous devez supprimer toutes les entrées DACL avec des utilisateurs ou des groupes locaux des descripteurs de sécurité, créer de nouvelles entrées DACL avec les noms de compte de destination corrigés et associer ces nouvelles entrées DACL aux descripteurs de sécurité appropriés.

- Entrées SACL

Chaque entrée SACL doit être associée à un compte. Vous devez modifier les CLS qui utilisent des

comptes utilisateur ou groupe locaux pour utiliser le nom de SVM de destination. Comme vous ne pouvez pas modifier le nom du compte pour les entrées SACL existantes, vous devez supprimer les entrées SACL avec des utilisateurs ou des groupes locaux des descripteurs de sécurité, créer de nouvelles entrées SACL avec les noms de compte de destination corrigés et associer ces nouvelles entrées SACL aux descripteurs de sécurité appropriés.

Vous devez apporter les modifications nécessaires aux utilisateurs ou groupes locaux utilisés dans la configuration de la stratégie de répertoire de fichiers avant d'appliquer la stratégie. Sinon, la tâche d'application échoue.

Configurez et appliquez la sécurité des fichiers sur les fichiers et dossiers NTFS à l'aide de l'interface de ligne de commande

Créez un descripteur de sécurité NTFS

La création d'un Security Descriptor (politique de sécurité des fichiers) NTFS constitue la première étape de configuration et d'application des listes de contrôle d'accès (ACL) NTFS aux fichiers et dossiers résidant sur les SVM (Storage Virtual machines). Vous pouvez associer le descripteur de sécurité au chemin du fichier ou du dossier dans une tâche de stratégie.

Description de la tâche

Vous pouvez créer des descripteurs de sécurité NTFS pour les fichiers et les dossiers résidant dans des volumes de style de sécurité NTFS ou pour les fichiers et dossiers résidant sur des volumes de type sécurité mixtes.

Par défaut, lorsqu'un descripteur de sécurité est créé, quatre entrées de contrôle d'accès (ACE) de liste de contrôle d'accès discrétionnaire (DACL) sont ajoutées à ce descripteur de sécurité. Les quatre ACE par défaut sont les suivants :

Objet	Type d'accès	Droits d'accès	Où appliquer les autorisations
INTÉGRÉ\administrateurs	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers
INTÉGRÉ\utilisateurs	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers
PROPRIÉTAIRE DU CRÉATEUR	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers
AUTORITÉ NT\SYSTÈME	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers

Vous pouvez personnaliser la configuration du descripteur de sécurité à l'aide des paramètres facultatifs suivants :

- Propriétaire du Security Descriptor
- Groupe principal du propriétaire

- Indicateurs de contrôle bruts

La valeur de n'importe quel paramètre facultatif est ignorée pour Storage-Level Access Guard. Consultez les pages de manuels pour plus d'informations.

Ajoutez des entrées de contrôle d'accès NTFS DACL au descripteur de sécurité NTFS

L'ajout d'entrées de contrôle d'accès (ACE) DACL (liste de contrôle d'accès discrétionnaire) au descripteur de sécurité NTFS est la deuxième étape de la configuration et de l'application des listes de contrôle d'accès NTFS à un fichier ou à un dossier. Chaque entrée identifie quel objet est autorisé ou refusé à accéder et définit ce que l'objet peut ou ne peut pas faire pour les fichiers ou dossiers définis dans ACE.

Description de la tâche

Vous pouvez ajouter un ou plusieurs ACE au DACL du Security Descriptor.

Si le descripteur de sécurité contient un DACL contenant des ACE existants, la commande ajoute le nouveau ACE au DACL. Si le descripteur de sécurité ne contient pas de DACL, la commande crée le DACL et y ajoute le nouveau ACE.

Vous pouvez éventuellement personnaliser les entrées DACL en spécifiant les droits que vous souhaitez autoriser ou refuser pour le compte spécifié dans `-account` paramètre. Il existe trois méthodes mutuellement exclusives de définition des droits :

- Droits
- Droits avancés
- Droits bruts (privilège avancé)



Si vous ne spécifiez pas de droits pour l'entrée DACL, la valeur par défaut est de définir les droits sur `Full Control`.

Vous pouvez personnaliser les entrées DACL en spécifiant la manière d'appliquer l'héritage.

La valeur de n'importe quel paramètre facultatif est ignorée pour Storage-Level Access Guard. Consultez les pages de manuels pour plus d'informations.

Étapes

1. Ajouter une entrée DACL à un descripteur de sécurité : `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

```
vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
-account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. Vérifier que l'entrée DACL est correcte : `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```

Vserver: vs1
Security Descriptor Name: sd1
  Allow or Deny: deny
    Account Name or SID: DOMAIN\joe
      Access Rights: full-control
Advanced Access Rights: -
  Apply To: this-folder
    Access Rights: full-control

```

Créer des stratégies de sécurité

La création d'une politique de sécurité des fichiers pour les SVM représente la troisième étape de la configuration et de l'application de ces ACL à un fichier ou dossier. Une règle agit comme un conteneur pour différentes tâches, où chaque tâche est une entrée unique qui peut être appliquée à des fichiers ou des dossiers. Vous pouvez ajouter des tâches à la stratégie de sécurité ultérieurement.

Description de la tâche

Les tâches que vous ajoutez à une stratégie de sécurité contiennent des associations entre le descripteur de sécurité NTFS et les chemins de fichier ou de dossier. Vous devez donc associer la politique de sécurité à chaque SVM (qui contient des volumes de style de sécurité NTFS ou des volumes de type sécurité mixtes).

Étapes

1. Création d'une stratégie de sécurité : `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver vs1
```

2. Vérifiez la stratégie de sécurité : `vserver security file-directory policy show`

```

vserver security file-directory policy show
      Vserver              Policy Name
      -----              -
      vs1                  policy1

```

Ajoutez une tâche à la stratégie de sécurité

La création et l'ajout d'une tâche policy à une policy de sécurité constitue la quatrième étape de la configuration et de l'application de ACL à des fichiers ou dossiers des SVM. Lorsque vous créez la tâche de stratégie, vous associez la tâche à une stratégie de sécurité. Vous pouvez ajouter une ou plusieurs entrées de tâche à une stratégie de sécurité.

Description de la tâche

La stratégie de sécurité est un conteneur pour une tâche. Une tâche fait référence à une opération unique qui peut être effectuée par une stratégie de sécurité pour les fichiers ou dossiers avec NTFS ou la sécurité mixte (ou à un objet de volume si vous configurez Storage-Level Access Guard).

Il existe deux types de tâches :

- Tâches de fichier et de répertoire

Permet de spécifier les tâches qui appliquent des descripteurs de sécurité aux fichiers et dossiers spécifiés. Les ACL appliquées via les tâches de fichier et de répertoire peuvent être gérées avec les clients SMB ou l'interface de ligne de commande ONTAP.

- Tâches de Storage-Level Access Guard

Permet de spécifier les tâches qui appliquent des descripteurs de sécurité Storage-Level Access Guard à un volume spécifié. Les listes de contrôle d'accès appliquées via les tâches Storage-Level Access Guard peuvent être gérées uniquement via l'interface de ligne de commande ONTAP.

Une tâche contient des définitions pour la configuration de sécurité d'un fichier (ou d'un dossier) ou d'un ensemble de fichiers (ou de dossiers). Chaque tâche d'une stratégie est identifiée de manière unique par le chemin. Il ne peut y avoir qu'une seule tâche par chemin au sein d'une même stratégie. Une stratégie ne peut pas avoir d'entrées de tâche en double.

Instructions pour l'ajout d'une tâche à une stratégie :

- Il peut y avoir un maximum de 10,000 entrées de tâches par stratégie.
- Une stratégie peut contenir une ou plusieurs tâches.

Même si une stratégie peut contenir plusieurs tâches, vous ne pouvez pas configurer une stratégie pour contenir à la fois des tâches de répertoire de fichiers et de Storage-Level Access Guard. Une stratégie doit contenir soit toutes les tâches Storage-Level Access Guard, soit toutes les tâches du répertoire de fichiers.

- Storage-Level Access Guard est utilisé pour restreindre les autorisations.

Il ne vous donnera jamais d'autorisations d'accès supplémentaires.

Lorsque vous ajoutez des tâches aux stratégies de sécurité, vous devez spécifier les quatre paramètres requis suivants :

- Nom du SVM
- Nom de la règle
- Chemin
- Descripteur de sécurité à associer au chemin d'accès

Vous pouvez personnaliser la configuration du descripteur de sécurité à l'aide des paramètres facultatifs suivants :

- Type de sécurité
- Mode de propagation
- Position de l'index
- Type de contrôle d'accès

La valeur de n'importe quel paramètre facultatif est ignorée pour Storage-Level Access Guard. Consultez les pages de manuels pour plus d'informations.

Étapes

1. Ajoutez une tâche avec un descripteur de sécurité associé à la stratégie de sécurité :
`vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

file-directory est la valeur par défaut de l' -access-control paramètre. La définition du type de contrôle d'accès lors de la configuration des tâches d'accès aux fichiers et aux répertoires est facultative.

`vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory`
2. Vérifiez la configuration de la tâche de stratégie :
`vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

`vserver security file-directory policy task show`

Vserver: vs1
Policy: policy1

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	
Descriptor	Name				
-----	-----	-----	-----	-----	

1	/home/dir1	file-directory	ntfs	propagate	sd2

Appliquez des règles de sécurité

L'application d'une politique de sécurité des fichiers aux SVM est la dernière étape de la création et de l'application de ces ACL NTFS aux fichiers ou aux dossiers.

Description de la tâche

Vous pouvez appliquer les paramètres de sécurité définis dans la stratégie de sécurité aux fichiers et dossiers NTFS résidant au sein de volumes FlexVol (NTFS ou style de sécurité mixte).



Lorsqu'une stratégie d'audit et des CLS associées sont appliquées, les CLS existantes sont écrasées. Lorsqu'une stratégie de sécurité et les listes de contrôle d'accès discrétionnaire associées sont appliquées, toutes les listes de contrôle d'accès discrétionnaire existantes sont écrasées. Il est recommandé de passer en revue les stratégies de sécurité existantes avant d'en créer et d'en appliquer de nouvelles.

Étape

1. Appliquer une politique de sécurité :
`vserver security file-directory apply -vserver`

```
vserver_name -policy-name policy_name
```

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

La tâche d'application de la politique est planifiée et l'ID de la tâche est renvoyé.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

Surveillez la tâche de stratégie de sécurité

Lorsque vous appliquez la stratégie de sécurité aux serveurs virtuels de stockage (SVM), vous pouvez surveiller la progression de la tâche en surveillant la tâche de stratégie de sécurité. Ceci est utile si vous voulez vérifier que l'application de la politique de sécurité a réussi. Ceci est également utile si vous avez un travail de longue durée où vous appliquez la sécurité en bloc à un grand nombre de fichiers et de dossiers.

Description de la tâche

Pour afficher des informations détaillées sur une tâche de stratégie de sécurité, vous devez utiliser le `-instance` paramètre.

Étape

1. Surveillez la tâche de stratégie de sécurité : `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

Job ID	Name	Vserver	Node	State
53322	Fsecurity Apply	vs1	node1	Success
Description: File Directory Security Apply Job				

Vérifiez la sécurité appliquée des fichiers

Vous pouvez vérifier les paramètres de sécurité des fichiers pour confirmer que les fichiers ou les dossiers de la machine virtuelle de stockage (SVM) à laquelle vous avez appliqué la stratégie de sécurité disposent des paramètres souhaités.

Description de la tâche

Vous devez fournir le nom de la SVM qui contient les données et le chemin d'accès au fichier et aux dossiers sur lesquels vous souhaitez vérifier les paramètres de sécurité. Vous pouvez utiliser l'option `-expand-mask` paramètre pour afficher des informations détaillées sur les paramètres de sécurité.

Étape

1. Afficher les paramètres de sécurité des fichiers et dossiers : `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

```
vserver security file-directory show -vserver vs1 -path /data/engineering
-expand-mask true
```

```
Vserver: vs1
      File Path: /data/engineering
File Inode Number: 5544
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8004

            1... .... = Self Relative
            .0.. .... = RM Control Valid
            ..0. .... = SACL Protected
            ...0 .... = DACL Protected
            .... 0... .... = SACL Inherited
            .... .0.. .... = DACL Inherited
            .... ..0. .... = SACL Inherit Required
            .... ...0 .... = DACL Inherit Required
            .... .... ..0. .... = SACL Defaulted
            .... .... ...0 .... = SACL Present
            .... .... .... 0... = DACL Defaulted
            .... .... .... .1.. = DACL Present
            .... .... .... ..0. = Group Defaulted
            .... .... .... ...0 = Owner Defaulted

Owner: BUILTIN\Administrators
Group: BUILTIN\Administrators
DACL - ACEs
      ALLOW-Everyone-0x1f01ff
      0... .... =
```

Generic Read	.0..	=
Generic Write	..0.	=
Generic Execute	...0	=
Generic All0	=
System Security1	=
Synchronize1...	=
Write Owner1..	=
Write DAC1.	=
Read Control1.	=
Delete1	=
Write Attributes1	=
Read Attributes1...	=
Delete Child1.	=
Execute1	=
Write EA1...	=
Read EA1.. =	
Append1. =	
Write1 =	
Read1 =	
ALLOW-Everyone-0x10000000-OI CI IO		
Generic Read	0...	=
Generic Write	.0..	=
Generic Execute	..0.	=
	...1	=

Generic All0..... =
System Security0..... =
Synchronize0..... =
Write Owner0..... =
Write DAC0..... =
Read Control0..... =
Delete0..... =
Write Attributes0..... =
Read Attributes0..... =
Delete Child0..... =
Execute0..... =
Write EA0..... =
Read EA0..... =
Append0..... =
Write0..... =
Read0..... =

Configurez et appliquez des règles d’audit aux fichiers et dossiers NTFS à l’aide de la vue d’ensemble de l’interface de ligne de commande

Lorsque vous utilisez l’interface de ligne de commande ONTAP, vous devez effectuer plusieurs étapes pour appliquer des règles d’audit aux fichiers et dossiers NTFS. Tout d’abord, vous créez un descripteur de sécurité NTFS et ajoutez des CLS au descripteur de sécurité. Ensuite, vous créez une stratégie de sécurité et ajoutez des tâches de stratégie. Vous appliquez ensuite la politique de sécurité sur une machine virtuelle de stockage (SVM).

Description de la tâche

Après avoir appliqué la stratégie de sécurité, vous pouvez surveiller la tâche de stratégie de sécurité, puis vérifier les paramètres de la stratégie d’audit appliquée.



Lorsqu'une stratégie d'audit et des CLS associées sont appliquées, les CLS existantes sont écrasées. Il est recommandé de passer en revue les stratégies de sécurité existantes avant d'en créer et d'en appliquer de nouvelles.

Informations associées

[Sécurisation de l'accès aux fichiers à l'aide de Storage-Level Access Guard](#)

[Limites lors de l'utilisation de l'interface de ligne de commande pour définir la sécurité des fichiers et des dossiers](#)

[Comment les descripteurs de sécurité sont utilisés pour appliquer la sécurité des fichiers et des dossiers](#)

["Audit et suivi de sécurité SMB et NFS"](#)

[Configurez et appliquez la sécurité des fichiers sur les fichiers et dossiers NTFS à l'aide de l'interface de ligne de commande](#)

Créez un descripteur de sécurité NTFS

La création d'une règle d'audit NTFS est la première étape de la configuration et de l'application des listes de contrôle d'accès (ACL) NTFS aux fichiers et dossiers qui résident au sein des SVM. Vous associez le descripteur de sécurité au chemin du fichier ou du dossier dans une tâche de stratégie.

Description de la tâche

Vous pouvez créer des descripteurs de sécurité NTFS pour les fichiers et les dossiers résidant dans des volumes de style de sécurité NTFS ou pour les fichiers et dossiers résidant sur des volumes de type sécurité mixtes.

Par défaut, lorsqu'un descripteur de sécurité est créé, quatre entrées de contrôle d'accès (ACE) de liste de contrôle d'accès discrétionnaire (DACL) sont ajoutées à ce descripteur de sécurité. Les quatre ACE par défaut sont les suivants :

Objet	Type d'accès	Droits d'accès	Où appliquer les autorisations
INTÉGRÉ\administrateurs	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers
INTÉGRÉ\utilisateurs	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers
PROPRIÉTAIRE DU CRÉATEUR	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers
AUTORITÉ NT\SYSTEME	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers

Vous pouvez personnaliser la configuration du descripteur de sécurité à l'aide des paramètres facultatifs suivants :

- Propriétaire du Security Descriptor
- Groupe principal du propriétaire
- Indicateurs de contrôle bruts

La valeur de n'importe quel paramètre facultatif est ignorée pour Storage-Level Access Guard. Consultez les pages de manuels pour plus d'informations.

Étapes

1. Si vous souhaitez utiliser les paramètres avancés, définissez le niveau de privilège sur avancé : `set -privilege advanced`

2. Créez un Security Descriptor: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_name optional_parameters`

```
vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe
```

3. Vérifiez que la configuration du descripteur de sécurité est correcte : `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

```
vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
Security Descriptor Name: sd1
Owner of the Security Descriptor: DOMAIN\joe
```

4. Si vous êtes au niveau de privilège avancé, revenez au niveau de privilège admin : `set -privilege admin`

Ajoutez des entrées de contrôle d'accès NTFS SACL au descripteur de sécurité NTFS

L'ajout d'entrées de contrôle d'accès (ACE) SACL (System Access Control list) au descripteur de sécurité NTFS est la deuxième étape de création des politiques d'audit NTFS pour les fichiers ou les dossiers des SVM. Chaque entrée identifie l'utilisateur ou le groupe que vous souhaitez auditer. L'entrée SACL définit si vous souhaitez auditer les tentatives d'accès réussies ou échouées.

Description de la tâche

Vous pouvez ajouter un ou plusieurs ACE au SACL du descripteur de sécurité.

Si le descripteur de sécurité contient une SACL comportant des ACE existants, la commande ajoute la nouvelle ACE à la SACL. Si le descripteur de sécurité ne contient pas de SACL, la commande crée la SACL et y ajoute la nouvelle ACE.

Vous pouvez configurer les entrées SACL en spécifiant les droits que vous souhaitez auditer pour les événements de réussite ou d'échec du compte spécifié dans `-account` paramètre. Il existe trois méthodes mutuellement exclusives de définition des droits :

- Droits
- Droits avancés
- Droits bruts (privilège avancé)



Si vous ne spécifiez pas de droits pour l'entrée SACL, le paramètre par défaut est `Full Control`.

Vous pouvez personnaliser des entrées SACL en spécifiant la façon d'appliquer l'héritage à l' `apply to` paramètre. Si vous ne spécifiez pas ce paramètre, la valeur par défaut est d'appliquer cette entrée SACL à ce dossier, sous-dossiers et fichiers.

Étapes

1. Ajoutez une entrée SACL à un descripteur de sécurité : `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID optional_parameters`

```
vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
failure -account domain\joe -rights full-control -apply-to this-folder
-vserver vs1
```

2. Vérifiez que l'entrée SACL est correcte : `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
Account Name or SID: DOMAIN\joe
Access Rights: full-control
Advanced Access Rights: -
Apply To: this-folder
Access Rights: full-control
```

Créer des stratégies de sécurité

La création d'une policy d'audit pour les SVM (Storage Virtual machines) constitue la troisième étape de la configuration et de l'application de ces ACL à un fichier ou à un dossier. Une règle agit comme un conteneur pour différentes tâches, où chaque tâche est une entrée unique qui peut être appliquée à des fichiers ou des dossiers. Vous pouvez ajouter des tâches à la stratégie de sécurité ultérieurement.

Description de la tâche

Les tâches que vous ajoutez à une stratégie de sécurité contiennent des associations entre le descripteur de sécurité NTFS et les chemins de fichier ou de dossier. Par conséquent, vous devez associer la stratégie de

sécurité à chaque SVM (Storage Virtual machine) (contenant des volumes de style de sécurité NTFS ou des volumes de type sécurité mixtes).

Étapes

1. Création d'une stratégie de sécurité : `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver vs1
```

2. Vérifiez la stratégie de sécurité : `vserver security file-directory policy show`

```
vserver security file-directory policy show
Vserver      Policy Name
-----
vs1          policy1
```

Ajoutez une tâche à la stratégie de sécurité

La création et l'ajout d'une tâche policy à une policy de sécurité constitue la quatrième étape de la configuration et de l'application de ACL à des fichiers ou dossiers des SVM. Lorsque vous créez la tâche de stratégie, vous associez la tâche à une stratégie de sécurité. Vous pouvez ajouter une ou plusieurs entrées de tâche à une stratégie de sécurité.

Description de la tâche

La stratégie de sécurité est un conteneur pour une tâche. Une tâche fait référence à une opération unique qui peut être effectuée par une stratégie de sécurité pour les fichiers ou dossiers avec NTFS ou la sécurité mixte (ou à un objet de volume si vous configurez Storage-Level Access Guard).

Il existe deux types de tâches :

- Tâches de fichier et de répertoire

Permet de spécifier les tâches qui appliquent des descripteurs de sécurité aux fichiers et dossiers spécifiés. Les ACL appliquées via les tâches de fichier et de répertoire peuvent être gérées avec les clients SMB ou l'interface de ligne de commande ONTAP.

- Tâches de Storage-Level Access Guard

Permet de spécifier les tâches qui appliquent des descripteurs de sécurité Storage-Level Access Guard à un volume spécifié. Les listes de contrôle d'accès appliquées via les tâches Storage-Level Access Guard peuvent être gérées uniquement via l'interface de ligne de commande ONTAP.

Une tâche contient des définitions pour la configuration de sécurité d'un fichier (ou d'un dossier) ou d'un ensemble de fichiers (ou de dossiers). Chaque tâche d'une stratégie est identifiée de manière unique par le chemin. Il ne peut y avoir qu'une seule tâche par chemin au sein d'une même stratégie. Une stratégie ne peut pas avoir d'entrées de tâche en double.

Instructions pour l'ajout d'une tâche à une stratégie :

- Il peut y avoir un maximum de 10,000 entrées de tâches par stratégie.
- Une stratégie peut contenir une ou plusieurs tâches.

Même si une stratégie peut contenir plusieurs tâches, vous ne pouvez pas configurer une stratégie pour contenir à la fois des tâches de répertoire de fichiers et de Storage-Level Access Guard. Une stratégie doit contenir soit toutes les tâches Storage-Level Access Guard, soit toutes les tâches du répertoire de fichiers.

- Storage-Level Access Guard est utilisé pour restreindre les autorisations.

Il ne vous donnera jamais d'autorisations d'accès supplémentaires.

Vous pouvez personnaliser la configuration du descripteur de sécurité à l'aide des paramètres facultatifs suivants :

- Type de sécurité
- Mode de propagation
- Position de l'index
- Type de contrôle d'accès

La valeur de n'importe quel paramètre facultatif est ignorée pour Storage-Level Access Guard. Consultez les pages de manuels pour plus d'informations.

Étapes

1. Ajoutez une tâche avec un descripteur de sécurité associé à la stratégie de sécurité : `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` est la valeur par défaut de l' `-access-control` paramètre. La définition du type de contrôle d'accès lors de la configuration des tâches d'accès aux fichiers et aux répertoires est facultative.

```
vserver security file-directory policy task add -vserver vs1 -policy-name
policy1 -path /home/dirl1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
-index-num 1 -access-control file-directory
```

2. Vérifiez la configuration de la tâche de stratégie : `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

```
Vserver: vs1
Policy: policy1
```

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	
Descriptor	Name				
-----	-----	-----	-----	-----	

1	/home/dir1	file-directory	ntfs	propagate	sd2

Appliquez des règles de sécurité

L'application d'une règle d'audit aux SVM constitue la dernière étape de création et d'application des listes de contrôle d'accès NTFS aux fichiers ou dossiers.

Description de la tâche

Vous pouvez appliquer les paramètres de sécurité définis dans la stratégie de sécurité aux fichiers et dossiers NTFS résidant au sein de volumes FlexVol (NTFS ou style de sécurité mixte).



Lorsqu'une stratégie d'audit et des CLS associées sont appliquées, les CLS existantes sont écrasées. Lorsqu'une stratégie de sécurité et les listes de contrôle d'accès discrétionnaire associées sont appliquées, toutes les listes de contrôle d'accès discrétionnaire existantes sont écrasées. Il est recommandé de passer en revue les stratégies de sécurité existantes avant d'en créer et d'en appliquer de nouvelles.

Étape

1. Appliquer une politique de sécurité : `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

La tâche d'application de la politique est planifiée et l'ID de la tâche est renvoyé.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

Surveillez la tâche de stratégie de sécurité

Lorsque vous appliquez la stratégie de sécurité aux serveurs virtuels de stockage (SVM), vous pouvez surveiller la progression de la tâche en surveillant la tâche de stratégie de sécurité. Ceci est utile si vous voulez vérifier que l'application de la politique de sécurité a réussi. Ceci est également utile si vous avez un travail de longue durée où vous appliquez la sécurité en bloc à un grand nombre de fichiers et de dossiers.

Description de la tâche

Pour afficher des informations détaillées sur une tâche de stratégie de sécurité, vous devez utiliser le `-instance` paramètre.

Étape

1. Surveillez la tâche de stratégie de sécurité : `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

Job ID	Name	Vserver	Node	State
53322	Fsecurity Apply	vs1	node1	Success
Description: File Directory Security Apply Job				

Vérifiez la règle d'audit appliquée

Vous pouvez vérifier la stratégie d'audit pour confirmer que les fichiers ou les dossiers de la machine virtuelle de stockage (SVM) à laquelle vous avez appliqué la stratégie de sécurité disposent des paramètres de sécurité d'audit souhaités.

Description de la tâche

Vous utilisez le `vserver security file-directory show` commande permettant d'afficher les informations relatives aux règles d'audit. Vous devez fournir le nom de la SVM qui contient les données et le chemin d'accès aux données dont vous souhaitez afficher les informations de la politique d'audit de fichier ou de dossier.

Étape

1. Afficher les paramètres de stratégie d'audit : `vserver security file-directory show -vserver vserver_name -path path`

Exemple

La commande suivante affiche les informations de la politique d'audit appliquées au chemin `"/corp"` du SVM `vs1`. Le chemin a à la fois UN SUCCÈS et une entrée SACL SUCCÈS/ÉCHEC qui lui est appliquée :


```

cluster::> vserver security file-directory show -vserver vs1 -path /corp

      Vserver: vs1
      File Path: /corp
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8014
            Owner:DOMAIN\Administrator
            Group:BUILTIN\Administrators
            SACL - ACEs
                  ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                  SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
            DACL - ACEs
                  ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                  ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                  ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI

```

Considérations relatives à la gestion des tâches de stratégie de sécurité

Si une tâche de stratégie de sécurité existe, dans certaines circonstances, vous ne pouvez pas modifier cette stratégie de sécurité ou les tâches affectées à cette stratégie. Vous devez comprendre dans quelles conditions vous pouvez ou ne pouvez pas modifier les stratégies de sécurité pour que toute tentative de modification de la stratégie soit réussie. Les modifications apportées à la stratégie comprennent l'ajout, la suppression ou la modification de tâches affectées à la stratégie et la suppression ou la modification de celle-ci.

Vous ne pouvez pas modifier une stratégie de sécurité ou une tâche affectée à cette stratégie si un travail existe pour cette stratégie et que ce travail se trouve dans les États suivants :

- Le travail est en cours d'exécution ou en cours d'exécution.
- Le travail est suspendu.
- Le travail reprend et est en cours d'exécution.
- Si le travail attend le basculement vers un autre nœud.

Dans les circonstances suivantes, si une tâche existe pour une stratégie de sécurité, vous pouvez modifier avec succès cette stratégie de sécurité ou une tâche affectée à cette stratégie :

- La tâche de stratégie est arrêtée.
- La tâche de stratégie s'est terminée avec succès.

Commandes de gestion des descripteurs de sécurité NTFS

Il existe des commandes ONTAP spécifiques pour gérer les descripteurs de sécurité. Vous pouvez créer, modifier, supprimer et afficher des informations sur les descripteurs de sécurité.

Les fonctions que vous recherchez...	Utilisez cette commande...
Créer des descripteurs de sécurité NTFS	<code>vserver security file-directory ntfs create</code>
Modifiez les descripteurs de sécurité NTFS existants	<code>vserver security file-directory ntfs modify</code>
Affiche des informations sur les descripteurs de sécurité NTFS existants	<code>vserver security file-directory ntfs show</code>
Supprimez les descripteurs de sécurité NTFS	<code>vserver security file-directory ntfs delete</code>

Consultez les pages de manuel pour le `vserver security file-directory ntfs` commandes pour plus d'informations.

Commandes de gestion des entrées de contrôle d'accès NTFS DACL

Il existe des commandes ONTAP spécifiques pour la gestion des entrées de contrôle d'accès DACL (ACE). Vous pouvez ajouter des ACE aux listes de contrôle d'accès NTFS à tout moment. Vous pouvez également gérer les listes de contrôle d'accès NTFS existantes en modifiant, supprimant et affichant des informations sur les ACE dans les listes de contrôle d'accès.

Les fonctions que vous recherchez...	Utilisez cette commande...
Créez des ACE et ajoutez-les dans les listes de contrôle d'accès NTFS	<code>vserver security file-directory ntfs dacl add</code>
Modifier les ACE existants dans les listes de contrôle d'accès NTFS	<code>vserver security file-directory ntfs dacl modify</code>
Affiche des informations sur les ACE existants dans les DACL NTFS	<code>vserver security file-directory ntfs dacl show</code>

Les fonctions que vous recherchez...	Utilisez cette commande...
Supprimez les ACE existants des listes de contrôle d'accès NTFS	<code>vserver security file-directory ntfs dacl remove</code>

Consultez les pages de manuel pour le `vserver security file-directory ntfs dacl` commandes pour plus d'informations.

Commandes de gestion des entrées de contrôle d'accès NTFS SACL

Il existe des commandes ONTAP spécifiques pour gérer les entrées de contrôle d'accès SACL (ACE). Vous pouvez ajouter des ACE aux CLS NTFS à tout moment. Vous pouvez également gérer les SACL NTFS existants en modifiant, supprimant et affichant des informations sur les ACE dans les SACL.

Les fonctions que vous recherchez...	Utilisez cette commande...
Créez des ACE et ajoutez-les aux CLS NTFS	<code>vserver security file-directory ntfs sacl add</code>
Modifier les ACE existants dans les SACL NTFS	<code>vserver security file-directory ntfs sacl modify</code>
Affiche des informations sur les ACE existants dans les CLS NTFS	<code>vserver security file-directory ntfs sacl show</code>
Supprimez les ACE existants des SACL NTFS	<code>vserver security file-directory ntfs sacl remove</code>

Consultez les pages de manuel pour le `vserver security file-directory ntfs sacl` commandes pour plus d'informations.

Commandes permettant de gérer les stratégies de sécurité

Il existe des commandes ONTAP spécifiques pour gérer les stratégies de sécurité. Vous pouvez afficher des informations sur les règles et supprimer les règles. Vous ne pouvez pas modifier une stratégie de sécurité.

Les fonctions que vous recherchez...	Utilisez cette commande...
Créer des stratégies de sécurité	<code>vserver security file-directory policy create</code>
Affiche des informations sur les stratégies de sécurité	<code>vserver security file-directory policy show</code>

Les fonctions que vous recherchez...	Utilisez cette commande...
Supprimer des stratégies de sécurité	<code>vserver security file-directory policy delete</code>

Consultez les pages de manuel pour le `vserver security file-directory policy` commandes pour plus d'informations.

Commandes permettant de gérer les tâches de stratégie de sécurité

Il existe des commandes ONTAP permettant d'ajouter, de modifier, de supprimer et d'afficher des informations relatives aux tâches de la stratégie de sécurité.

Les fonctions que vous recherchez...	Utilisez cette commande...
Ajouter des tâches de stratégie de sécurité	<code>vserver security file-directory policy task add</code>
Modifier les tâches de stratégie de sécurité	<code>vserver security file-directory policy task modify</code>
Afficher des informations sur les tâches de stratégie de sécurité	<code>vserver security file-directory policy task show</code>
Supprimer les tâches de stratégie de sécurité	<code>vserver security file-directory policy task remove</code>

Consultez les pages de manuel pour le `vserver security file-directory policy task` commandes pour plus d'informations.

Commandes permettant de gérer les tâches de stratégie de sécurité

Des commandes ONTAP permettent d'interrompre, de reprendre, d'arrêter et d'afficher des informations sur les tâches de stratégie de sécurité.

Les fonctions que vous recherchez...	Utilisez cette commande...
Interrompre les tâches de stratégie de sécurité	<code>vserver security file-directory job pause -vserver vserver_name -id integer</code>
Reprendre les tâches de stratégie de sécurité	<code>vserver security file-directory job resume -vserver vserver_name -id integer</code>
Affiche des informations sur les tâches de stratégie de sécurité	<code>vserver security file-directory job show -vserver vserver_name</code> Vous pouvez déterminer l'ID d'un travail à l'aide de cette commande.

Les fonctions que vous recherchez...	Utilisez cette commande...
Arrêtez les tâches de stratégie de sécurité	<code>vserver security file-directory job stop -vserver vserver_name -id integer</code>

Consultez les pages de manuel pour le `vserver security file-directory job` commandes pour plus d'informations.

Configurez le cache des métadonnées pour les partages SMB

Fonctionnement de la mise en cache des métadonnées SMB

La mise en cache des métadonnées permet la mise en cache des attributs de fichier sur les clients SMB 1.0 pour un accès plus rapide aux attributs des fichiers et des dossiers. Vous pouvez activer ou désactiver la mise en cache des attributs par partage. Vous pouvez également configurer le temps de mise en service des entrées mises en cache si la mise en cache des métadonnées est activée. La configuration de la mise en cache des métadonnées n'est pas nécessaire si les clients se connectent aux partages SMB 2.x ou SMB 3.0.

Lorsqu'il est activé, le cache de métadonnées SMB stocke les données d'attribut de chemin et de fichier pendant un temps limité. Ceci peut améliorer les performances SMB des clients SMB 1.0 avec des charges de travail communes.

Pour certaines tâches, SMB crée un trafic important, pouvant inclure plusieurs requêtes identiques pour les métadonnées des chemins d'accès et des fichiers. Vous pouvez réduire le nombre de requêtes redondantes et améliorer les performances des clients SMB 1.0 en utilisant la mise en cache de métadonnées SMB pour récupérer les informations du cache.



Même si cela est peu probable, il est possible que le cache de métadonnées transmette des informations obsolètes aux clients SMB 1.0. Si votre environnement ne peut pas se permettre ce risque, vous ne devez pas activer cette fonctionnalité.

Activez le cache de métadonnées SMB

Vous pouvez améliorer les performances SMB des clients SMB 1.0 en activant le cache de métadonnées SMB. Par défaut, la mise en cache des métadonnées SMB est désactivée.

Étape

1. Effectuez l'action souhaitée :

Les fonctions que vous recherchez...	Entrez la commande...
Activez la mise en cache des métadonnées SMB lorsque vous créez un partage	<code>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties attributecache</code>

Les fonctions que vous recherchez...	Entrez la commande...
Activez la mise en cache des métadonnées SMB sur un partage existant	<code>vserver cifs share properties add -vserver <i>vserver_name</i> -share-name <i>share_name</i> -share-properties attributecache</code>

Informations associées

[Configuration de la durée de vie des entrées du cache de métadonnées SMB](#)

[Ajout ou suppression de propriétés de partage sur un partage SMB existant](#)

Configurez la durée de vie des entrées du cache de métadonnées SMB

Vous pouvez configurer la durée de vie des entrées du cache de métadonnées SMB afin d'optimiser les performances du cache de métadonnées SMB dans votre environnement. La valeur par défaut est 10 secondes.

Avant de commencer

Vous devez avoir activé la fonctionnalité de cache de métadonnées SMB. Si le cache des métadonnées SMB n'est pas activé, le paramètre TTL du cache SMB n'est pas utilisé.

Étape

1. Effectuez l'action souhaitée :

Si vous souhaitez configurer la durée de vie des entrées du cache de métadonnées SMB lorsque vous...	Entrez la commande...
Créer un partage	<code>vserver cifs share -create -vserver <i>vserver_name</i> -share-name <i>share_name</i> -path <i>path</i> -attribute-cache-ttl [<i>integerh</i>][<i>integerm</i>][<i>integers</i>]</code>
Modifier un partage existant	<code>vserver cifs share -modify -vserver <i>vserver_name</i> -share-name <i>share_name</i> -attribute-cache-ttl [<i>integerh</i>][<i>integerm</i>][<i>integers</i>]</code>

Vous pouvez spécifier d'autres options et propriétés de configuration de partage lorsque vous créez ou modifiez des partages. Consultez les pages de manuels pour plus d'informations.

Gérer les verrous de fichier

A propos du verrouillage de fichier entre les protocoles

Le verrouillage de fichier est une méthode utilisée par les applications client pour empêcher un utilisateur d'accéder à un fichier précédemment ouvert par un autre utilisateur. Le mode de verrouillage des fichiers par ONTAP dépend du protocole du

client.

Si le client est un client NFS, les verrouillages sont consultatifs ; si le client est un client SMB, les verrous sont obligatoires.

En raison des différences entre les verrouillages de fichiers NFS et SMB, un client NFS peut ne pas accéder à un fichier précédemment ouvert par une application SMB.

Ce qui suit se produit lorsqu'un client NFS tente d'accéder à un fichier verrouillé par une application SMB :

- Dans les volumes mixtes ou NTFS, les opérations de manipulation de fichiers telles que `rm`, `rmdir`, et `mv` peut entraîner l'échec de l'application NFS.
- Les opérations de lecture et d'écriture NFS sont refusées par les modes SMB Deny-read et deny-write open, respectivement.
- Les opérations d'écriture NFS échouent lorsque la plage d'écriture du fichier est verrouillée par un bytelock SMB exclusif.
- Dissocier
 - Pour les systèmes de fichiers NTFS, les opérations de suppression SMB et CIFS sont prises en charge.

Le fichier sera supprimé après la dernière fermeture.

- Les opérations de liaison NFS ne sont pas prises en charge.

Elle n'est pas prise en charge car les sémantiques NTFS et SMB sont requises et l'opération dernière suppression-fermeture n'est pas prise en charge pour NFS.

- Pour les systèmes de fichiers UNIX, l'opération de liaison est prise en charge.

Il est pris en charge car la sémantique NFS et UNIX est requise.

- Renommer
 - Pour les systèmes de fichiers NTFS, si le fichier de destination est ouvert depuis SMB ou CIFS, le fichier de destination peut être renommé.
 - Le renommage NFS n'est pas pris en charge.

Elle n'est pas prise en charge car NTFS et la sémantique SMB sont requises.

Dans les volumes de style de sécurité UNIX, les opérations de dissociation NFS et de renommage ignorent l'état du verrouillage SMB et permettent l'accès au fichier. Toutes les autres opérations NFS sur des volumes de type sécurité UNIX respectent l'état de verrouillage SMB.

Comment ONTAP traite les bits en lecture seule

Le bit de lecture seule est défini fichier par fichier pour indiquer si un fichier est inscriptible (désactivé) ou en lecture seule (activé).

Les clients SMB qui utilisent Windows peuvent définir un bit en lecture seule par fichier. Les clients NFS ne définissent pas de bit en lecture seule par fichier, car les clients NFS ne disposent d'aucune opération de protocole utilisant un bit en lecture seule par fichier.

ONTAP peut définir un bit en lecture seule sur un fichier lorsqu'un client SMB utilisant Windows crée ce fichier.

ONTAP peut également définir un bit en lecture seule lorsqu'un fichier est partagé entre les clients NFS et les clients SMB. Certains logiciels, lorsqu'ils sont utilisés par des clients NFS et SMB, nécessitent l'activation du bit en lecture seule.

Pour que ONTAP garde les autorisations appropriées en lecture et écriture sur un fichier partagé entre les clients NFS et les clients SMB, il traite le bit en lecture seule conformément aux règles suivantes :

- NFS traite tous les fichiers dont le bit de lecture seule est activé comme s'il n'a pas de bits d'autorisation d'écriture activés.
- Si un client NFS désactive tous les bits d'autorisation d'écriture et qu'au moins un de ces bits avait été précédemment activé, ONTAP active le bit en lecture seule pour ce fichier.
- Si un client NFS active un bit d'autorisation d'écriture, ONTAP désactive le bit en lecture seule pour ce fichier.
- Si le bit de lecture seule d'un fichier est activé et qu'un client NFS tente de détecter les autorisations pour le fichier, les bits d'autorisation du fichier ne sont pas envoyés au client NFS. ONTAP envoie les bits d'autorisation au client NFS avec les bits d'autorisation d'écriture masqués.
- Si le bit de lecture seule d'un fichier est activé et qu'un client SMB désactive le bit de lecture seule, ONTAP active le bit d'autorisation d'écriture du propriétaire pour le fichier.
- Les fichiers dont le bit de lecture seule est activé sont accessibles en écriture uniquement par root.



Les modifications des autorisations liées aux fichiers sont immédiatement appliquées aux clients SMB, mais elles peuvent ne pas être immédiatement appliquées aux clients NFS si le client NFS active la mise en cache des attributs.

La différence entre ONTAP et Windows en ce qui concerne la gestion des verrous sur les composants de chemin de partage

Contrairement à Windows, ONTAP ne verrouille pas chaque composant du chemin d'accès à un fichier ouvert lorsque le fichier est ouvert. Ce comportement affecte également les chemins de partage SMB.

Étant donné que ONTAP ne verrouille pas chaque composant du chemin d'accès, il est possible de renommer un composant de chemin au-dessus du fichier ou du partage ouvert, ce qui peut causer des problèmes pour certaines applications ou peut rendre le chemin de partage dans la configuration SMB invalide. Cela peut rendre le partage inaccessible.

Pour éviter les problèmes causés par la modification du nom des composants du chemin d'accès, vous pouvez appliquer des paramètres de sécurité qui empêchent les utilisateurs ou les applications de renommer les répertoires critiques.

Affiche des informations sur les verrous

Vous pouvez afficher des informations sur les verrous de fichier en cours, y compris les types de verrous qui sont conservés et l'état de verrouillage, les détails sur les verrous de plage d'octets, les modes de verrouillage de sharelock, les verrous de délégation et les verrous opportunistes, et si les verrous sont ouverts avec des poignées durables ou persistantes.

Description de la tâche

L'adresse IP du client ne peut pas être affichée pour les verrouillages établis via NFS V4 ou NFS v4.1.

Par défaut, la commande affiche des informations relatives à tous les verrouillages. Vous pouvez utiliser les paramètres de la commande pour afficher des informations sur les verrous d'une machine virtuelle de stockage (SVM) spécifique ou pour filtrer les résultats de la commande par d'autres critères.

Le `vserver locks show` la commande affiche des informations sur quatre types de verrous :

- Les verrous de plage d'octets, qui verrouillent uniquement une partie d'un fichier.
- Verrous de partage, qui verrouillent les fichiers ouverts.
- Verrouillages opportunistes, qui contrôlent la mise en cache côté client sur SMB.
- Des délégations qui contrôlent la mise en cache côté client sur NFSv4.x.

En spécifiant des paramètres facultatifs, vous pouvez déterminer des informations importantes sur chaque type de verrou. Consultez la page man pour la commande pour plus d'informations.

Étape

1. Affiche des informations sur les verrous à l'aide de `vserver locks show` commande.

Exemples

L'exemple suivant présente un récapitulatif des informations relatives à un verrouillage NFSv4 sur un fichier avec le chemin d'accès `/vol1/file1`. Le mode d'accès de sharelock est `Write-deny_none` et le verrou a été accordé avec la délégation d'écriture :

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF          Protocol  Lock Type  Client
-----
-----
vol1    /vol1/file1                    lif1         nfsv4     share-level -
                                     Sharelock Mode: write-deny_none
                                     delegation  -
                                     Delegation Type: write
```

L'exemple suivant affiche des informations détaillées sur le verrou SMB d'un fichier avec le chemin d'accès `/data2/data2_2/intro.pptx`. Un descripteur durable est accordé sur le fichier avec un mode d'accès à verrouillage de partage `Write-Deny_none` à un client dont l'adresse IP est 10.3.1.3. Un oplock de location est accordé avec un niveau de oplock de lot :

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/intro.pptx
Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
Lock Protocol: cifs
Lock Type: share-level
```

```
Node Holding Lock State: node3
    Lock State: granted
Bytelock Starting Offset: -
    Number of Bytes Locked: -
    Bytelock is Mandatory: -
    Bytelock is Exclusive: -
    Bytelock is Superlock: -
    Bytelock is Soft: -
    Oplock Level: -
Shared Lock Access Mode: write-deny_none
    Shared Lock is Soft: false
    Delegation Type: -
    Client Address: 10.3.1.3
    SMB Open Type: durable
    SMB Connect State: connected
SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

    Vserver: vs1
    Volume: data2_2
    Logical Interface: lif2
    Object Path: /data2/data2_2/test.pptx
    Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
    Lock Protocol: cifs
    Lock Type: op-lock
Node Holding Lock State: node3
    Lock State: granted
Bytelock Starting Offset: -
    Number of Bytes Locked: -
    Bytelock is Mandatory: -
    Bytelock is Exclusive: -
    Bytelock is Superlock: -
    Bytelock is Soft: -
    Oplock Level: batch
Shared Lock Access Mode: -
    Shared Lock is Soft: -
    Delegation Type: -
    Client Address: 10.3.1.3
    SMB Open Type: -
    SMB Connect State: connected
SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Verrous de rupture

Lorsque des verrous de fichier empêchent l'accès client aux fichiers, vous pouvez afficher des informations sur les verrous actuellement mis en attente, puis interrompre des verrous spécifiques. Les applications de débogage sont des exemples de scénarios dans lesquels vous devrez peut-être interrompre les verrous.

Description de la tâche

Le `vserver locks break` la commande n'est disponible que au niveau de privilège avancé et supérieur. La page man de la commande contient des informations détaillées.

Étapes

1. Pour trouver les informations dont vous avez besoin pour interrompre un verrouillage, utilisez le `vserver locks show` commande.

La page man de la commande contient des informations détaillées.

2. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
3. Effectuez l'une des opérations suivantes :

Si vous voulez rompre un verrou en spécifiant...	Entrez la commande...
Le nom du SVM, le nom du volume, le nom de la LIF et le chemin de fichier	<code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code>
L'ID de verrouillage	<code>vserver locks break -lockid UUID</code>

4. Retour au niveau de privilège admin : `set -privilege admin`

Surveiller l'activité des PME

Affiche les informations relatives aux sessions SMB

Vous pouvez afficher des informations sur les sessions SMB établies, notamment la connexion SMB et l'ID de session ainsi que l'adresse IP du poste de travail à l'aide de la session. Vous pouvez afficher des informations sur la version du protocole SMB de la session et le niveau de protection disponible en continu, ce qui vous aide à déterminer si cette session prend en charge la continuité de l'activité.

Description de la tâche

Vous pouvez afficher les informations de toutes les sessions de votre SVM sous forme récapitulative. Cependant, dans de nombreux cas, la quantité de sortie renvoyée est importante. Vous pouvez personnaliser les informations affichées dans la sortie en spécifiant des paramètres facultatifs :

- Vous pouvez utiliser l'option `-fields` paramètre pour afficher la sortie des champs que vous choisissez.

Vous pouvez entrer `-fields ?` pour déterminer les champs que vous pouvez utiliser.

- Vous pouvez utiliser le `-instance` Paramètre pour afficher des informations détaillées sur les sessions SMB établies.
- Vous pouvez utiliser le `-fields` ou le `-instance` paramètre seul ou associé à d'autres paramètres facultatifs.

Étape

1. Effectuez l'une des opérations suivantes :

Pour afficher les informations de session SMB...	Saisissez la commande suivante...
Pour toutes les sessions sur le SVM sous forme résumée	<code>vserver cifs session show -vserver vserver_name</code>
Sur un ID de connexion spécifié	<code>vserver cifs session show -vserver vserver_name -connection-id integer</code>
À partir d'une adresse IP de poste de travail spécifiée	<code>vserver cifs session show -vserver vserver_name -address workstation_IP_address</code>
Sur une adresse IP LIF spécifiée	<code>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address</code>
Sur un nœud spécifié	<code>`vserver cifs session show -vserver vserver_name -node {node_name</code>
<code>local}`</code>	D'un utilisateur Windows spécifié
<code>vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name</code>	Avec un mécanisme d'authentification spécifié
<code>`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1</code>	NTLMv2
Kerberos	Anonymous}`
Avec une version de protocole spécifiée	<code>`vserver cifs session show -vserver vserver_name -protocol-version {SMB1</code>
SMB2	SMB2_1

Pour afficher les informations de session SMB...	Saisissez la commande suivante...
SMB3	<p>SMB3_1}</p> <p>[NOTE]</p> <p>====</p> <p>La protection et SMB Multichannel sont disponibles en continu uniquement pour les sessions SMB 3.0 et ultérieures. Pour afficher leur statut sur toutes les sessions de qualification, vous devez spécifier ce paramètre avec la valeur définie sur SMB3 ou ultérieure.</p> <p>====</p>
Avec un niveau spécifié de protection disponible en continu	`vserver cifs session show -vserver vs1_name -continuously-available {No
Yes	<p>Partial}</p> <p>[NOTE]</p> <p>====</p> <p>Si l'état disponible en continu est de Partial, cela signifie que la session contient au moins un fichier ouvert en continu disponible, mais que la session contient certains fichiers qui ne sont pas ouverts avec une protection disponible en continu. Vous pouvez utiliser le <code>vserver cifs sessions file show</code> commande permettant de déterminer quels fichiers de la session établie ne sont pas ouverts avec une protection disponible en continu.</p> <p>====</p>
Avec un état de session de signature SMB spécifié	`vserver cifs session show -vserver vs1_name -is-session-signed {true

Exemples

La commande suivante affiche les informations relatives aux sessions sur le SVM vs1 établies à partir d'un poste de travail avec l'adresse IP 10.1.1.1 :

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session
ID        ID        Workstation      Windows User      Open      Idle
-----  -
3151272279,
3151272280,
3151272281  1        10.1.1.1        DOMAIN\joe        2        23s
```

La commande suivante affiche des informations détaillées pour les sessions avec protection disponible en continu sur le SVM vs1. La connexion a été établie à l'aide du compte de domaine.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation IP address: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\SERVER1$
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: Yes
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

La commande suivante affiche les informations relatives aux sessions sur une session utilisant SMB 3.0 et SMB Multichannel sur le SVM vs1. Dans l'exemple, l'utilisateur connecté à ce partage à un client SMB 3.0 en utilisant l'adresse IP du LIF ; par conséquent, le mécanisme d'authentification par défaut est NTLMv2. La connexion doit se faire à l'aide de l'authentification Kerberos pour se connecter à une protection disponible en continu.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3
```

```

    Node: node1
    Vserver: vs1
    Session ID: 1
    **Connection IDs: 3151272607,31512726078,3151272609
    Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
    Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
        Windows User: DOMAIN\administrator
        UNIX User: pcuser
    Open Shares: 1
        Open Files: 0
        Open Other: 0
    Connected Time: 6m 22s
        Idle Time: 5m 42s
    Protocol Version: SMB3
    Continuously Available: No
        Is Session Signed: false
    User Authenticated as: domain-user
        NetBIOS Name: -
    SMB Encryption Status: Unencrypted
```

Informations associées

[Affichage des informations relatives aux fichiers SMB ouverts](#)

Affiche des informations sur les fichiers SMB ouverts

Vous pouvez afficher des informations sur les fichiers SMB ouverts, notamment la connexion SMB et l'ID de session, le volume hôte, le nom du partage et le chemin du partage. Vous pouvez afficher des informations sur le niveau de protection disponible en continu d'un fichier, ce qui permet de déterminer si un fichier ouvert est dans un état qui prend en charge la continuité de l'activité.

Description de la tâche

Vous pouvez afficher des informations sur les fichiers ouverts dans une session SMB établie. Les informations affichées sont utiles lorsque vous devez déterminer les informations de session SMB pour des fichiers particuliers dans une session SMB.

Par exemple, si vous disposez d'une session SMB où certains fichiers ouverts sont ouverts avec une protection disponible en continu et certains ne sont pas ouverts avec une protection disponible en continu (valeur pour le `-continuously-available` champ dans `vserver cifs session show` la sortie de la commande est `Partial`), vous pouvez déterminer quels fichiers ne sont pas disponibles en continu à l'aide de cette commande.

Vous pouvez afficher les informations de tous les fichiers ouverts sur des sessions SMB établies sur des SVM

(Storage Virtual machines) sous forme de récapitulatif à l'aide de `vserver cifs session file show` commande sans paramètres facultatifs.

Cependant, dans de nombreux cas, la quantité de production renvoyée est importante. Vous pouvez personnaliser les informations affichées dans la sortie en spécifiant des paramètres facultatifs. Cela peut être utile lorsque vous souhaitez afficher des informations pour un petit sous-ensemble de fichiers ouverts uniquement.

- Vous pouvez utiliser l'option `-fields` paramètre pour afficher la sortie sur les champs de votre choix.

Vous pouvez utiliser ce paramètre seul ou en combinaison avec d'autres paramètres facultatifs.

- Vous pouvez utiliser le `-instance` Paramètre pour afficher des informations détaillées sur les fichiers SMB ouverts.

Vous pouvez utiliser ce paramètre seul ou en combinaison avec d'autres paramètres facultatifs.

Étape

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez afficher des fichiers SMB ouverts...	Saisissez la commande suivante...
Sur le SVM sous forme résumée	<code>vserver cifs session file show -vserver vserver_name</code>
Sur un nœud spécifié	<code>`vserver cifs session file show -vserver vserver_name -node {node_name</code>
<code>local}`</code>	Sur un ID de fichier spécifié
<code>vserver cifs session file show -vserver vserver_name -file-id integer</code>	Sur un ID de connexion SMB spécifié
<code>vserver cifs session file show -vserver vserver_name -connection-id integer</code>	Sur un ID de session SMB spécifié
<code>vserver cifs session file show -vserver vserver_name -session-id integer</code>	Sur l'agrégat d'hébergement spécifié
<code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code>	Sur le volume spécifié
<code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code>	Sur le partage SMB spécifié

Si vous souhaitez afficher des fichiers SMB ouverts...	Saisissez la commande suivante...
<code>vserver cifs session file show -vserver vserver_name -share share_name</code>	Sur le chemin SMB spécifié
<code>vserver cifs session file show -vserver vserver_name -path path</code>	Avec le niveau spécifié de protection disponible en continu
<code>`vserver cifs session file show -vserver vserver_name -continuously-available {No</code>	Yes}` [NOTE] ==== Si l'état disponible en continu est de No, cela signifie que ces fichiers ouverts ne peuvent pas être rétablis sans interruption à partir du basculement et du rétablissement. Ils ne peuvent pas non plus récupérer d'une relocalisation générale entre les partenaires dans une relation de haute disponibilité. ====
Avec l'état reconnecté spécifié	<code>`vserver cifs session file show -vserver vserver_name -reconnected {No</code>

D'autres paramètres facultatifs peuvent être utilisés pour affiner les résultats de sortie. Consultez la page man pour plus d'informations

Exemples

L'exemple suivant affiche les informations sur les fichiers ouverts sur le SVM vs1 :

```
cluster1::> vserver cifs session file show -vserver vs1
Node:      node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File        File      Open Hosting      Continuously
ID          Type       Mode Volume      Share      Available
-----
41          Regular    r    data      data      Yes
Path: \mytest.rtf
```

L'exemple suivant affiche des informations détaillées sur les fichiers SMB ouverts avec l'ID de fichier 82 sur le SVM vs1 :

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance
```

```
Node: node1
Vserver: vs1
File ID: 82
Connection ID: 104617
Session ID: 1
File Type: Regular
Open Mode: rw
Aggregate Hosting File: aggr1
Volume Hosting File: data1
CIFS Share: data1
Path from CIFS Share: windows\win8\test\test.txt
Share Mode: rw
Range Locks: 1
Continuously Available: Yes
Reconnected: No
```

Informations associées

[Affichage des informations sur les sessions SMB](#)

Déterminez les objets statistiques et les compteurs disponibles

Avant d'obtenir des informations sur les statistiques de hachage CIFS, SMB, d'audit et de BranchCache, ainsi que sur les performances, vous devez connaître les objets et compteurs disponibles, à partir desquels vous pouvez obtenir des données.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Si vous voulez déterminer...	Entrer...
Les objets disponibles	<code>statistics catalog object show</code>
Objets spécifiques disponibles	<code>statistics catalog object show object object_name</code>
Quels compteurs sont disponibles	<code>statistics catalog counter show object object_name</code>

Pour plus d'informations sur les objets et les compteurs disponibles, consultez les pages de manuels.

3. Retour au niveau de privilège admin : `set -privilege admin`

Exemples

La commande suivante affiche la description des objets statistiques sélectionnés relatifs à l'accès CIFS et SMB au cluster, comme s'il s'affiche au niveau de privilège avancé :

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog object show -object audit
      audit_ng                      CM object for exporting audit_ng
performance counters
```

```
cluster1::*> statistics catalog object show -object cifs
      cifs                          The CIFS object reports activity of the
                                   Common Internet File System protocol
                                   ...
```

```
cluster1::*> statistics catalog object show -object nblade_cifs
      nblade_cifs                   The Common Internet File System (CIFS)
                                   protocol is an implementation of the
Server
                                   ...
```

```
cluster1::*> statistics catalog object show -object smb1
      smb1                          These counters report activity from the
SMB
                                   revision of the protocol. For information
                                   ...
```

```
cluster1::*> statistics catalog object show -object smb2
      smb2                          These counters report activity from the
                                   SMB2/SMB3 revision of the protocol. For
                                   ...
```

```
cluster1::*> statistics catalog object show -object hashd
      hashd                         The hashd object provides counters to
measure
                                   the performance of the BranchCache hash
daemon.
```

```
cluster1::*> set -privilege admin
```

La commande suivante affiche des informations sur certains compteurs de `cifs` objet tel qu'il apparaît au niveau de privilège avancé :



Cet exemple n'affiche pas tous les compteurs disponibles pour le `cifs` objet ; la sortie est tronquée.

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

Counter	Description
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
...	...

```
cluster2::> statistics start -object client -sample-id
```

Object: client

Counter	Value
cifs_ops	0
cifs_read_ops	0
cifs_read_recv_ops	0
cifs_read_recv_size	0B
cifs_read_size	0B
cifs_write_ops	0
cifs_write_recv_ops	0
cifs_write_recv_size	0B
cifs_write_size	0B
instance_name	vserver_1:10.72.205.179
instance_uuid	2:10.72.205.179
local_ops	0
mount_ops	0

[...]

Informations associées

[Affichage des statistiques](#)

Affiche les statistiques

Vous pouvez afficher plusieurs statistiques, notamment des statistiques sur CIFS et SMB, l'audit et des hachages de BranchCache, pour surveiller les performances et diagnostiquer les problèmes.

Avant de commencer

Vous devez avoir collecté des échantillons de données à l'aide du `statistics start` et `statistics stop` commandes avant de pouvoir afficher les informations relatives aux objets.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Pour afficher les statistiques de...	Entrer...
Toutes les versions de SMB	<code>statistics show -object cifs</code>
SMB 1.0	<code>statistics show -object smb1</code>
SMB 2.x et SMB 3.0	<code>statistics show -object smb2</code>
Sous-système CIFS du nœud	<code>statistics show -object nblade_cifs</code>
Audit multiprotocole	<code>statistics show -object audit_ng</code>
Service de hachage BranchCache	<code>statistics show -object hashd</code>
DNS dynamique	<code>statistics show -object ddns_update</code>

Consultez la page man pour chaque commande pour plus d'informations.

3. Retour au niveau de privilège admin : `set -privilege admin`

Informations associées

[Détermination des objets statistiques et des compteurs disponibles](#)

[Contrôle des statistiques de session signées SMB](#)

[Affichage des statistiques de BranchCache](#)

[Utilisation des statistiques pour surveiller l'activité de renvoi automatique de nœud](#)

["Configuration SMB pour Microsoft Hyper-V et SQL Server"](#)

Déploiement des services basés sur les clients SMB

Utilisez les fichiers hors ligne pour permettre la mise en cache des fichiers pour une utilisation hors ligne

Utilisez les fichiers hors ligne pour permettre la mise en cache des fichiers pour une utilisation hors ligne

ONTAP prend en charge la fonctionnalité de fichiers hors ligne Microsoft, ou *mise en cache côté client*, qui permet de mettre les fichiers en cache sur l'hôte local pour une utilisation hors ligne. Les utilisateurs peuvent utiliser la fonctionnalité fichiers hors ligne pour continuer à travailler sur des fichiers même lorsqu'ils sont déconnectés du réseau.

Vous pouvez spécifier si les documents et programmes utilisateur Windows sont automatiquement mis en cache sur un partage ou si les fichiers doivent être sélectionnés manuellement pour la mise en cache. La mise en cache manuelle est activée par défaut pour les nouveaux partages. Les fichiers mis hors ligne sont synchronisés avec le disque local du client Windows. La synchronisation a lieu lorsque la connectivité réseau à un partage de système de stockage spécifique est restaurée.

Étant donné que les fichiers et dossiers hors ligne conservent les mêmes autorisations d'accès que la version des fichiers et dossiers enregistrés sur le serveur CIFS, l'utilisateur doit disposer des autorisations suffisantes sur les fichiers et dossiers enregistrés sur le serveur CIFS pour effectuer des actions sur les fichiers et dossiers hors ligne.

Lorsque l'utilisateur et une autre personne du réseau modifient le même fichier, l'utilisateur peut enregistrer la version locale du fichier sur le réseau, conserver l'autre version ou enregistrer les deux. Si l'utilisateur conserve les deux versions, un nouveau fichier avec les modifications de l'utilisateur local est enregistré localement et le fichier mis en cache est écrasé par des modifications de la version du fichier enregistré sur le serveur CIFS.

Vous pouvez configurer des fichiers hors ligne par partage à l'aide des paramètres de configuration du partage. Vous pouvez choisir l'une des quatre configurations de dossiers hors ligne lorsque vous créez ou modifiez des partages :

- Pas de mise en cache

Désactive la mise en cache côté client pour le partage. Les fichiers et les dossiers ne sont pas automatiquement mis en cache localement sur les clients et les utilisateurs ne peuvent pas choisir de mettre en cache des fichiers ou des dossiers localement.

- Mise en cache manuelle

Permet la sélection manuelle des fichiers à mettre en cache sur le partage. Il s'agit du paramètre par défaut. Par défaut, aucun fichier ni dossier n'est mis en cache sur le client local. Les utilisateurs peuvent choisir les fichiers et dossiers qu'ils souhaitent mettre en cache localement pour une utilisation hors ligne.

- Mise en cache automatique des documents

Permet de mettre automatiquement en cache les documents utilisateur sur le partage. Seuls les fichiers et les dossiers accessibles sont mis en cache localement.

- Mise en cache automatique des programmes

Permet de mettre automatiquement en cache les programmes et les documents utilisateur sur le partage. Seuls les fichiers, les dossiers et les programmes accessibles sont mis en cache localement. De plus, ce paramètre permet au client d'exécuter des exécutables mis en cache localement, même lorsqu'il est connecté au réseau.

Pour plus d'informations sur la configuration des fichiers hors ligne sur les serveurs et les clients Windows, consultez la bibliothèque Microsoft TechNet.

Informations associées

[Utilisation de profils itinérants pour stocker les profils utilisateurs de façon centralisée sur un serveur CIFS associé à la SVM](#)

[Utilisation de la redirection de dossiers pour stocker des données sur un serveur CIFS](#)

[Utilisation de BranchCache pour mettre en cache le contenu de partage SMB dans une succursale](#)

["Bibliothèque Microsoft TechNet : \[technet.microsoft.com/en-us/library/\]\(http://technet.microsoft.com/en-us/library/\)"](#)

Conditions d'utilisation des fichiers hors ligne

Avant de pouvoir utiliser la fonctionnalité Microsoft Offline Files avec votre serveur CIFS, vous devez savoir quelles versions de ONTAP et SMB et quels clients Windows prennent en charge cette fonctionnalité.

Configuration requise pour la version ONTAP

Les versions d'ONTAP prennent en charge les fichiers hors ligne.

Version requise du protocole SMB

Pour le SVM (Storage Virtual machine), ONTAP prend en charge les fichiers hors ligne dans toutes les versions de SMB.

Configuration requise pour le client Windows

Le client Windows doit prendre en charge les fichiers hors ligne.

Pour obtenir les informations les plus récentes sur les clients Windows prenant en charge la fonctionnalité fichiers hors ligne, reportez-vous à la matrice d'interopérabilité.

["mysupport.netapp.com/matrix"](http://mysupport.netapp.com/matrix)

Instructions pour le déploiement de fichiers hors ligne

Il existe certaines directives importantes que vous devez comprendre lorsque vous déployez des fichiers hors ligne sur des partages de répertoire personnel qui possèdent le `showsnapshot` propriété de partage définie sur les répertoires d'accueil.

Si la propriété `showsnapshot` La propriété `Share` est définie sur un partage de répertoire personnel sur lequel les fichiers hors ligne sont configurés. Les clients Windows mettent en cache toutes les copies Snapshot sous `~snapshot` dans le répertoire de base de l'utilisateur.

Les clients Windows mettent en cache toutes les copies Snapshot sous le `home` Directory si l'un des

nombreux éléments suivants est vrai :

- L'utilisateur rend le répertoire personnel disponible hors ligne à partir du client.

Le contenu du `~snapshot` le dossier du répertoire personnel est inclus et rendu disponible hors ligne.

- L'utilisateur configure la redirection de dossier pour rediriger un dossier tel que `My Documents` À la racine d'un répertoire local résidant sur le partage CIFS Server.

Certains clients Windows peuvent rendre automatiquement le dossier redirigé hors ligne. Si le dossier est redirigé vers la racine du répertoire de base, le `~snapshot` le dossier est inclus dans le contenu hors ligne mis en cache.



Déploiement de fichiers hors ligne où `~snapshot` le dossier est inclus dans les fichiers hors ligne doit être évité. Copies Snapshot dans le `~snapshot` Le dossier contient toutes les données du volume au point où ONTAP a créé la copie Snapshot. Par conséquent, la création d'une copie hors ligne du `~snapshot` la consommation d'un stockage local important dans le dossier du client consomme de la bande passante réseau lors de la synchronisation des fichiers hors ligne, et augmente le temps nécessaire à la synchronisation des fichiers hors ligne.

Configurer la prise en charge des fichiers hors ligne sur les partages SMB à l'aide de l'interface de ligne de commande

Vous pouvez configurer la prise en charge des fichiers hors ligne à l'aide de l'interface de ligne de commandes ONTAP en spécifiant l'un des quatre paramètres de fichier hors ligne lorsque vous créez des partages SMB ou en modifiant à tout moment des partages SMB existants. La prise en charge des fichiers manuels hors ligne est le paramètre par défaut.

Description de la tâche

Lors de la configuration de la prise en charge des fichiers hors ligne, vous pouvez choisir l'un des quatre paramètres de fichiers hors ligne suivants :

Réglage	Description
<code>none</code>	Interdire aux clients Windows de mettre en cache les fichiers sur ce partage.
<code>manual</code>	Permet aux utilisateurs des clients Windows de sélectionner manuellement les fichiers à mettre en cache.
<code>documents</code>	Permet aux clients Windows de mettre en cache les documents utilisateur qui sont utilisés par l'utilisateur pour l'accès hors ligne.
<code>programs</code>	Permet aux clients Windows de mettre en cache les programmes utilisés par l'utilisateur pour l'accès hors ligne. Les clients peuvent utiliser les fichiers de programme mis en cache en mode hors ligne, même si le partage est disponible.

Vous ne pouvez choisir qu'un seul paramètre de fichier hors ligne. Si vous modifiez un paramètre de fichiers hors ligne sur un partage SMB existant, le nouveau paramètre de fichiers hors ligne remplace le paramètre d'origine. Les autres paramètres de configuration et propriétés de partage SMB existants ne sont ni supprimés ni remplacés. Ils restent en vigueur jusqu'à ce qu'ils soient explicitement supprimés ou modifiés.

Étapes

- 1. Effectuez l'action appropriée :

Si vous souhaitez configurer des fichiers hors ligne sur...	Entrez la commande...
Un nouveau partage SMB	<code>`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none</code>
manual	documents
programs}`	Un partage SMB existant
<code>`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none</code>	manual
documents	programs}`

- 2. Vérifiez que la configuration du partage SMB est correcte : `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Exemple

La commande suivante crée un partage SMB nommé "data1" avec des fichiers hors ligne définis sur documents:

```
cluster1::> vsserver cifs share create -vsriver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vsserver cifs share show -vsriver vs1 -share-name data1
-instance

                Vserver: vs1
                Share: data1
CIFS Server NetBIOS Name: VS1
                Path: /data1
                Share Properties: oplocks
                                browsable
                                changenotify
                Symlink Properties: enable
                File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                Share Comment: Offline files
                Share ACL: Everyone / Full Control
                File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: documents
                Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
                UNIX Group for File Create: -
```

La commande suivante modifie un partage SMB existant nommé "data1" en changeant le paramètre fichiers hors ligne sur manual et ajout de valeurs pour le masque de création de mode fichier et répertoire :

```
cluster1::> vsserver cifs share modify -vsserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777
```

```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name data1
-instance
```

```

                Vserver: vs1
                Share: data1
    CIFS Server NetBIOS Name: VS1
                Path: /data1
    Share Properties: oplocks
                    browsable
                    changenotify
    Symlink Properties: enable
    File Mode Creation Mask: 644
    Directory Mode Creation Mask: 777
    Share Comment: Offline files
    Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                Volume Name: -
    Offline Files: manual
    Vscan File-Operations Profile: standard
    Maximum Tree Connections on Share: 4294967295
    UNIX Group for File Create: -
```

Informations associées

[Ajout ou suppression de propriétés de partage sur un partage SMB existant](#)

Configurez la prise en charge des fichiers hors ligne sur les partages SMB à l'aide de la console MMC gestion de l'ordinateur

Si vous souhaitez autoriser les utilisateurs à mettre en cache des fichiers localement pour une utilisation hors ligne, vous pouvez configurer la prise en charge des fichiers hors ligne à l'aide de la console MMC gestion de l'ordinateur (Microsoft Management Console).

Étapes

1. Pour ouvrir la console MMC sur votre serveur Windows, dans l'Explorateur Windows, cliquez avec le bouton droit de la souris sur l'icône de l'ordinateur local, puis sélectionnez **gérer**.
2. Dans le panneau de gauche, sélectionnez **Computer Management**.
3. Sélectionnez **action > connexion à un autre ordinateur**.

La boîte de dialogue Sélectionner un ordinateur s'affiche.

4. Tapez le nom du serveur CIFS ou cliquez sur **Browse** pour localiser le serveur CIFS.

Si le nom du serveur CIFS est identique au nom d'hôte SVM (Storage Virtual machine), tapez le nom du

SVM. Si le nom du serveur CIFS est différent du nom d'hôte du SVM, tapez le nom du serveur CIFS.

5. Cliquez sur **OK**.
6. Dans l'arborescence de la console, cliquez sur **Outils système > dossiers partagés**.
7. Cliquez sur **partages**.
8. Dans le volet des résultats, cliquez avec le bouton droit de la souris sur le partage.
9. Cliquez sur **Propriétés**.

Les propriétés du partage sélectionné s'affichent.

10. Dans l'onglet **général**, cliquez sur **Paramètres hors ligne**.

La boîte de dialogue Paramètres hors ligne s'affiche.

11. Configurez les options de disponibilité hors ligne selon les besoins.
12. Cliquez sur **OK**.

Utilisez les profils itinérants pour stocker les profils utilisateurs de façon centralisée sur un serveur SMB associé à la SVM

Utilisez les profils itinérants pour stocker les profils utilisateurs de façon centralisée sur un serveur SMB associé à la présentation de la SVM

ONTAP prend en charge le stockage des profils itinérants Windows sur un serveur CIFS associé à la machine virtuelle de stockage (SVM). La configuration des profils itinérants d'utilisateurs offre des avantages à l'utilisateur, tels que la disponibilité automatique des ressources, quel que soit l'endroit où l'utilisateur se connecte. Les profils itinérants simplifient également l'administration et la gestion des profils utilisateur.

Les profils utilisateur itinérants présentent les avantages suivants :

- Disponibilité automatique des ressources

Le profil unique d'un utilisateur est automatiquement disponible lorsque cet utilisateur se connecte à n'importe quel ordinateur du réseau exécutant Windows 8, Windows 7, Windows 2000 ou Windows XP. Les utilisateurs n'ont pas besoin de créer de profil sur chaque ordinateur qu'ils utilisent sur un réseau.

- Remplacement simplifié de l'ordinateur

Étant donné que toutes les informations de profil de l'utilisateur sont conservées séparément sur le réseau, le profil de l'utilisateur peut être facilement téléchargé sur un nouvel ordinateur de remplacement. Lorsque l'utilisateur se connecte au nouvel ordinateur pour la première fois, la copie du profil de l'utilisateur est copiée sur le nouvel ordinateur.

Informations associées

[Utilisation de fichiers hors ligne pour permettre la mise en cache de fichiers pour une utilisation hors ligne](#)

[Utilisation de la redirection de dossiers pour stocker des données sur un serveur CIFS](#)

Conditions requises pour l'utilisation des profils itinérants

Avant de pouvoir utiliser les profils itinérants de Microsoft avec votre serveur CIFS, vous devez savoir quelles versions de ONTAP et SMB et quels clients Windows prennent en charge cette fonctionnalité.

Configuration requise pour la version ONTAP

ONTAP prend en charge les profils itinérants.

Version requise du protocole SMB

Pour le serveur virtuel de stockage (SVM), ONTAP prend en charge les profils itinérants sur toutes les versions de SMB.

Configuration requise pour le client Windows

Avant qu'un utilisateur puisse utiliser les profils itinérants, le client Windows doit prendre en charge cette fonctionnalité.

Pour obtenir les dernières informations sur les clients Windows qui prennent en charge les profils itinérants, consultez la matrice d'interopérabilité.

["Matrice d'interopérabilité NetApp"](#)

Configurez les profils itinérants

Si vous souhaitez rendre automatiquement le profil d'un utilisateur disponible lorsque cet utilisateur se connecte à n'importe quel ordinateur du réseau, vous pouvez configurer des profils itinérants via le composant logiciel enfichable MMC utilisateurs et ordinateurs Active Directory. Si vous configurez des profils itinérants sur Windows Server, vous pouvez utiliser le Centre d'administration Active Directory.

Étapes

1. Sur le serveur Windows, ouvrez la MMC utilisateurs et ordinateurs Active Directory (ou le Centre d'administration Active Directory sur les serveurs Windows).
2. Recherchez l'utilisateur pour lequel vous souhaitez configurer un profil d'itinérance.
3. Cliquez avec le bouton droit de la souris sur l'utilisateur et cliquez sur **Propriétés**.
4. Dans l'onglet **profil**, entrez le chemin du profil vers le partage où vous souhaitez stocker le profil d'itinérance de l'utilisateur, suivi de %username%.

Par exemple, un chemin de profil peut être le suivant : \\vs1.example.com\profiles\%username%. La première fois qu'un utilisateur se connecte, %username% est remplacé par le nom de l'utilisateur.



Dans le chemin \\vs1.example.com\profiles\%username%, profiles Est le nom de partage d'un partage sur SVM (Storage Virtual machine) vs1 qui dispose de droits de contrôle total pour tous.

5. Cliquez sur **OK**.

Utiliser la redirection de dossiers pour stocker des données sur un serveur SMB

Utiliser la redirection de dossiers pour stocker des données sur une présentation du serveur SMB

ONTAP prend en charge la redirection de dossiers Microsoft, qui permet aux utilisateurs ou aux administrateurs de rediriger le chemin d'un dossier local vers un emplacement sur le serveur CIFS. Il apparaît comme si les dossiers redirigés sont stockés sur le client Windows local, même si ces données sont stockées dans un partage SMB.

La redirection de dossiers s'adresse principalement aux entreprises qui ont déjà déployé des répertoires locaux et qui souhaitent maintenir la compatibilité avec leur environnement de home Directory existant.

- Documents, Desktop, et Start Menu sont des exemples de dossiers que vous pouvez rediriger.
- Les utilisateurs peuvent rediriger les dossiers à partir de leur client Windows.
- Les administrateurs peuvent configurer et gérer de façon centralisée la redirection de dossiers en configurant des GPO dans Active Directory.
- Si les administrateurs ont configuré des profils itinérants, la redirection de dossiers permet aux administrateurs de diviser les données utilisateur à partir des données de profil.
- Les administrateurs peuvent utiliser la redirection de dossiers et les fichiers hors ligne ensemble pour rediriger le stockage des données des dossiers locaux vers le serveur CIFS, tout en permettant aux utilisateurs de mettre le contenu en cache localement.

Informations associées

[Utilisation de fichiers hors ligne pour permettre la mise en cache de fichiers pour une utilisation hors ligne](#)

[Utilisation de profils itinérants pour stocker les profils utilisateurs de façon centralisée sur un serveur CIFS associé à la SVM](#)

Conditions requises pour l'utilisation de la redirection de dossiers

Avant de pouvoir utiliser la redirection de dossiers de Microsoft avec votre serveur CIFS, vous devez connaître les versions de ONTAP et SMB et les clients Windows qui prennent en charge cette fonctionnalité.

Configuration requise pour la version ONTAP

ONTAP prend en charge la redirection de dossiers Microsoft.

Version requise du protocole SMB

Pour le serveur virtuel de stockage (SVM), ONTAP prend en charge la redirection de dossiers de Microsoft sur toutes les versions de SMB.

Configuration requise pour le client Windows

Avant qu'un utilisateur puisse utiliser la redirection de dossier de Microsoft, le client Windows doit prendre en charge cette fonctionnalité.

Pour obtenir les dernières informations sur les clients Windows prenant en charge la redirection de dossiers, consultez la matrice d'interopérabilité.

Configurer la redirection de dossier

Vous pouvez configurer la redirection de dossiers à l'aide de la fenêtre Propriétés de Windows. L'avantage de cette méthode est que l'utilisateur Windows peut configurer la redirection de dossiers sans l'aide de l'administrateur SVM.

Étapes

1. Dans l'Explorateur Windows, cliquez avec le bouton droit de la souris sur le dossier que vous souhaitez rediriger vers un partage réseau.
2. Cliquez sur **Propriétés**.

Les propriétés du partage sélectionné s'affichent.

3. Dans l'onglet **raccourci**, cliquez sur **cible** et spécifiez le chemin d'accès à l'emplacement réseau où vous souhaitez rediriger le dossier sélectionné.

Par exemple, si vous souhaitez rediriger un dossier vers le data dossier dans un répertoire personnel mappé sur Q : \, spécifiez Q : \data comme cible.

4. Cliquez sur **OK**.

Pour plus d'informations sur la configuration des dossiers hors ligne, consultez la bibliothèque Microsoft TechNet.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Accéder au répertoire ~snapshot à partir de clients Windows à l'aide de SMB 2.x

La méthode que vous utilisez pour accéder à l' ~snapshot Le répertoire des clients Windows utilisant SMB 2.x diffère de la méthode utilisée pour SMB 1.0. Vous devez comprendre comment accéder à l' ~snapshot Répertoire lors de l'utilisation de connexions SMB 2.x pour accéder correctement aux données stockées dans des copies Snapshot.

L'administrateur du SVM contrôle si les utilisateurs des clients Windows peuvent afficher et accéder à l' ~snapshot répertoire sur un partage en activant ou désactivant le showsnapshot partager la propriété en utilisant les commandes du vserver cifs share properties familles.

Lorsque le showsnapshot La propriété partager est désactivée, un utilisateur d'un client Windows utilisant SMB 2.x ne peut pas afficher ~snapshot Et ne peut pas accéder aux copies Snapshot dans le ~snapshot répertoire, même lors de la saisie manuelle du chemin d'accès au ~snapshot Ou à des copies Snapshot spécifiques dans le répertoire.

Lorsque le showsnapshot La propriété partager est activée, un utilisateur sur un client Windows utilisant SMB 2.x ne peut toujours pas afficher ~snapshot répertoire soit à la racine du partage, soit dans une jonction ou un répertoire sous la racine du partage. Toutefois, après la connexion à un partage, l'utilisateur peut accéder au système masqué ~snapshot en ajoutant manuellement le répertoire \~snapshot à la fin du chemin de partage. Le masqué ~snapshot le répertoire est accessible à partir de deux points d'entrée :

- À la racine du partage
- À chaque point de jonction de l'espace de partage

Le masqué ~snapshot le répertoire n'est pas accessible à partir de sous-répertoires non-jonctions dans le partage.

Exemple

Avec la configuration indiquée dans l'exemple suivant, un utilisateur d'un client Windows avec une connexion SMB 2.x au partage « eng » peut accéder à l' ~snapshot en ajoutant manuellement le répertoire \~snapshot au chemin de partage à la racine du partage et à chaque point de jonction du chemin. Le masqué ~snapshot le répertoire est accessible à partir des trois chemins suivants :

- \\vs1\eng\~snapshot
- \\vs1\eng\projects1\~snapshot
- \\vs1\eng\projects2\~snapshot

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume      junction-path
-----
vs1      vs1_root      /
vs1      vs1_vol1     /eng
vs1      vs1_vol2     /eng/projects1
vs1      vs1_vol3     /eng/projects2

cluster1::> vsserver cifs share show
Vserver  Share  Path  Properties  Comment  ACL
-----
vs1      eng    /eng  oplocks     -        Everyone / Full Control
        changenotify
        browsable
        showsnapshot
```

Restaurez des fichiers et des dossiers à l'aide des versions précédentes

Restaurer des fichiers et des dossiers à l'aide de la présentation des versions précédentes

La possibilité d'utiliser les versions précédentes de Microsoft s'applique aux systèmes de fichiers prenant en charge les copies Snapshot sous une forme ou une autre et les permettant de les activer. La technologie Snapshot fait partie intégrante de ONTAP. Les utilisateurs peuvent restaurer des fichiers et des dossiers à partir de copies Snapshot à partir de leur client Windows à l'aide de la fonction versions précédentes de Microsoft.

Avec les versions précédentes, les utilisateurs peuvent parcourir les copies Snapshot ou restaurer des données à partir d'une copie Snapshot sans l'intervention d'un administrateur de stockage. Les versions précédentes ne peuvent pas être configurées. Elle est toujours activée. Si l'administrateur du stockage a mis des copies Snapshot disponibles sur un partage, l'utilisateur peut utiliser les versions précédentes pour effectuer les tâches suivantes :

- Restaurer les fichiers supprimés par inadvertance.
- Récupération après écrasement accidentel d'un fichier.
- Comparer les versions du fichier pendant le fonctionnement.

Les données stockées dans les copies Snapshot sont en lecture seule. Les utilisateurs doivent enregistrer une copie d'un fichier à un autre emplacement pour apporter des modifications au fichier. Les copies Snapshot sont régulièrement supprimées. Les utilisateurs doivent donc créer des copies des fichiers contenus dans les versions précédentes s'ils souhaitent conserver indéfiniment une version précédente d'un fichier.

Conditions requises pour l'utilisation des versions précédentes de Microsoft

Avant de pouvoir utiliser les versions précédentes avec votre serveur CIFS, vous devez savoir quelles versions de ONTAP et SMB et quels clients Windows le prennent en charge. Vous devez également connaître les exigences relatives au paramètre de copie Snapshot.

Configuration requise pour la version ONTAP

Prend en charge les versions précédentes.

Version requise du protocole SMB

Pour les machines virtuelles de stockage (SVM), ONTAP prend en charge les versions précédentes sur toutes les versions de SMB.

Configuration requise pour le client Windows

Avant qu'un utilisateur puisse utiliser les versions précédentes pour accéder aux données de copies Snapshot, le client Windows doit prendre en charge cette fonction.

Pour obtenir les dernières informations sur les clients Windows prenant en charge les versions précédentes, consultez la matrice d'interopérabilité.

["Matrice d'interopérabilité NetApp"](#)

Configuration requise pour les paramètres de copie Snapshot

Pour accéder aux données de copies Snapshot, une règle Snapshot activée doit être associée au volume contenant les données, les clients doivent pouvoir accéder aux données Snapshot et des copies Snapshot doivent exister.

Utilisez l'onglet versions précédentes pour afficher et gérer les données de copie Snapshot

Les utilisateurs des ordinateurs clients Windows peuvent utiliser l'onglet versions précédentes de la fenêtre Propriétés de Windows pour restaurer les données stockées dans des copies Snapshot sans avoir à faire appel à l'administrateur de la machine virtuelle de stockage (SVM).

Description de la tâche

Si l'administrateur a activé les copies Snapshot sur le volume contenant le partage, l'onglet versions précédentes permet uniquement d'afficher et de gérer les données des copies Snapshot des données stockées sur la SVM et si l'administrateur configure le partage pour afficher les copies Snapshot.

Étapes

1. Dans l'Explorateur Windows, affichez le contenu du lecteur mappé des données stockées sur le serveur CIFS.
2. Cliquez avec le bouton droit de la souris sur le fichier ou le dossier dans le lecteur réseau mappé dont vous souhaitez afficher ou gérer les copies Snapshot.
3. Cliquez sur **Propriétés**.

Les propriétés du fichier ou dossier sélectionné s'affichent.

4. Cliquez sur l'onglet **versions précédentes**.

La liste des copies Snapshot disponibles du fichier ou dossier sélectionné s'affiche dans la case versions de dossier. Les copies Snapshot répertoriées sont identifiées par le préfixe du nom de la copie Snapshot et par l'horodatage de création.

5. Dans la zone **versions de dossier**, cliquez avec le bouton droit de la souris sur la copie du fichier ou du dossier que vous souhaitez gérer.
6. Effectuez l'action appropriée :

Les fonctions que vous recherchez...	Procédez comme suit...
Affichez les données de cette copie Snapshot	Cliquez sur Ouvrir .
Créer une copie des données à partir de cette copie Snapshot	Cliquez sur Copier .

Les données des copies Snapshot sont en lecture seule. Si vous souhaitez apporter des modifications aux fichiers et dossiers répertoriés dans l'onglet versions précédentes, vous devez enregistrer une copie des fichiers et dossiers que vous souhaitez modifier à un emplacement inscriptible et apporter des modifications aux copies.

7. Une fois que vous avez terminé de gérer les données de snapshot, fermez la boîte de dialogue **Propriétés** en cliquant sur **OK**.

Pour plus d'informations sur l'utilisation de l'onglet versions précédentes pour afficher et gérer les données de snapshot, consultez la bibliothèque Microsoft TechNet.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Déterminez si des copies Snapshot sont disponibles pour les versions précédentes

Vous pouvez afficher les copies Snapshot depuis l'onglet versions précédentes uniquement si une règle Snapshot activée est appliquée au volume contenant le partage et si la configuration de volume permet d'accéder aux copies Snapshot. Il est utile de déterminer la disponibilité des copies Snapshot pour aider un utilisateur à accéder aux versions précédentes.

Étapes

1. Déterminez si le volume sur lequel résident les données du partage est activé pour les copies Snapshot

automatiques et si les clients ont accès aux répertoires Snapshot : `volume show -vserver vservers -name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

Le résultat de cette commande affiche la règle Snapshot associée au volume, l'activation ou non de l'accès au répertoire Snapshot client et le nombre de copies Snapshot disponibles.

2. Déterminez si la règle Snapshot associée est activée : `volume snapshot policy show -policy policy-name`
3. Lister les copies Snapshot disponibles : `volume snapshot show -volume volume_name`

Pour plus d'informations sur la configuration et la gestion des règles Snapshot et des planifications Snapshot, reportez-vous à la section "[La protection des données](#)".

Exemple

L'exemple suivant présente des informations sur les politiques Snapshot associées au volume nommé « data1 » qui contient les données partagées et les copies Snapshot disponibles sur « data1 ».

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-----
vs1      data1  true                default                10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1

                Number of Is
Policy Name      Schedules Enabled Comment
-----
default          3 true      Default policy with hourly, daily &
weekly schedules.
    Schedule      Count      Prefix      SnapMirror Label
    -----
    hourly        6        hourly      -
    daily          2        daily        daily
    weekly         2        weekly        weekly

cluster1::> volume snapshot show -volume data1

                ---Blocks---
Vserver  Volume  Snapshot                State      Size  Total%  Used%
-----
vs1      data1
        weekly.2012-12-16_0015  valid      408KB    0%    1%
        daily.2012-12-22_0010  valid      420KB    0%    1%
        daily.2012-12-23_0010  valid      192KB    0%    0%
        weekly.2012-12-23_0015  valid      360KB    0%    1%
        hourly.2012-12-23_1405  valid      196KB    0%    0%
        hourly.2012-12-23_1505  valid      196KB    0%    0%
        hourly.2012-12-23_1605  valid      212KB    0%    0%
        hourly.2012-12-23_1705  valid      136KB    0%    0%
        hourly.2012-12-23_1805  valid      200KB    0%    0%
        hourly.2012-12-23_1905  valid      184KB    0%    0%
```

Informations associées

[Création d'une configuration de snapshot pour activer l'accès aux versions précédentes](#)

"Protection des données"

Créez une configuration de snapshot pour activer l'accès aux versions précédentes

Les versions précédentes sont toujours disponibles dans la mesure où l'accès du client aux copies Snapshot est activé et à condition que des copies Snapshot existent. Si votre configuration de copie Snapshot ne répond pas à ces exigences, vous pouvez créer une configuration de copie Snapshot qui le fait.

Étapes

1. Si le volume contenant le partage auquel vous souhaitez autoriser l'accès aux versions précédentes n'est pas associé à une stratégie Snapshot, associez une politique Snapshot au volume et activez-la à l'aide du `volume modify` commande.

Pour plus d'informations sur l'utilisation du `volume modify` commandes, consultez les pages de manuels.

2. Accès aux copies Snapshot à l'aide du `volume modify` pour définir le `-snap-dir` option à `true`.

Pour plus d'informations sur l'utilisation du `volume modify` commandes, consultez les pages de manuels.

3. Vérifiez que les règles Snapshot sont activées et que l'accès aux répertoires Snapshot est activé à l'aide du `volume show` et `volume snapshot policy show` commandes.

Pour plus d'informations sur l'utilisation du `volume show` et `volume snapshot policy show` commandes, consultez les pages de manuels.

Pour plus d'informations sur la configuration et la gestion des règles Snapshot et des planifications Snapshot, reportez-vous à la section "[La protection des données](#)".

Informations associées

["Protection des données"](#)

Instructions pour la restauration de répertoires contenant des jonctions

Vous devez garder à l'esprit certaines consignes lorsque vous utilisez les versions précédentes pour restaurer des dossiers contenant des points de jonction.

Lorsque vous utilisez les versions précédentes pour restaurer des dossiers comportant des dossiers enfants qui sont des points de jonction, la restauration peut échouer avec un `Access Denied` erreur.

Vous pouvez déterminer si le dossier que vous essayez de restaurer contient une jonction à l'aide de l' `vol show` commande avec `-parent` option. Vous pouvez également utiliser le `vserver security trace` commandes permettant de créer des journaux détaillés sur les problèmes d'accès aux fichiers et aux dossiers.

Informations associées

[Création et gestion des volumes de données dans les espaces de noms NAS](#)

Déployez les services basés sur serveur SMB

Gérer les répertoires locaux

Comment ONTAP rend possible les répertoires locaux dynamiques

Les home directories ONTAP vous permettent de configurer un partage SMB qui correspond à différents répertoires en fonction de l'utilisateur qui se connecte à celui-ci et d'un ensemble de variables. Au lieu de créer des partages distincts pour chaque utilisateur, vous pouvez configurer un partage avec quelques paramètres de home Directory afin de définir la relation d'un utilisateur entre un point d'entrée (le partage) et le

home Directory (un répertoire sur la SVM).

Un utilisateur connecté en tant qu'utilisateur invité ne dispose pas d'un répertoire personnel et ne peut pas accéder aux répertoires d'accueil d'autres utilisateurs. Il existe quatre variables qui déterminent la manière dont un utilisateur est mappé à un répertoire :

- **Nom de partage**

Il s'agit du nom du partage que vous créez et auquel l'utilisateur se connecte. Vous devez définir la propriété du répertoire personnel pour ce partage.

Le nom du partage peut utiliser les noms dynamiques suivants :

- %w (Nom d'utilisateur Windows de l'utilisateur)
- %d (Nom de domaine Windows de l'utilisateur)
- %u (Nom d'utilisateur UNIX mappé de l'utilisateur)
Pour que le nom du partage soit unique dans tous les répertoires d'accueil, le nom du partage doit contenir soit %w ou le %u variable. Le nom du partage peut contenir les deux %d et le %w variable (par exemple, %d/%w), ou le nom du partage peut contenir une partie statique et une partie variable (par exemple, home_/%w).

- **Chemin de partage**

Il s'agit du chemin relatif, défini par le partage, et donc associé à l'un des noms de partage, qui est ajouté à chaque chemin de recherche pour générer le chemin d'accès complet du home Directory de l'utilisateur, à partir de la racine de la SVM. Il peut être statique (par exemple, home), dynamique (par exemple, %w), ou une combinaison des deux (par exemple, eng/%w).

- **Chemins de recherche**

Il s'agit de l'ensemble des chemins absolus depuis la racine du SVM que vous spécifiez qui dirigent la recherche ONTAP pour les répertoires locaux. Vous pouvez spécifier un ou plusieurs chemins de recherche à l'aide du `vserver cifs home-directory search-path add` commande. Si vous spécifiez plusieurs chemins de recherche, ONTAP les essaie dans l'ordre spécifié jusqu'à ce qu'il trouve un chemin valide.

- **Répertoire**

Il s'agit du répertoire de base de l'utilisateur que vous créez pour l'utilisateur. Le nom du répertoire est généralement le nom de l'utilisateur. Vous devez créer le répertoire personnel dans l'un des répertoires définis par les chemins de recherche.

Prenons l'exemple de la configuration suivante :

- Utilisateur : John Smith
- Domaine utilisateur : acme
- Nom d'utilisateur: Jsmith
- Nom du SVM : vs1
- Nom de partage du répertoire de base n°1 : Home_ %w - chemin de partage : %w
- Nom de partage du répertoire racine #2 : %w - chemin de partage : %d/%w

- Chemin de recherche n°1 : /vol0home/home
- Chemin de recherche n°2 : /vol1home/home
- Chemin de recherche n°3 : /vol2home/home
- Home Directory : /vol1home/home/jsmith

Scénario 1 : l'utilisateur se connecte à \\vs1\home_jsmith. Ceci correspond au premier nom de partage du répertoire racine et génère le chemin relatif jsmith. ONTAP recherche désormais un répertoire nommé jsmith en vérifiant chaque chemin de recherche dans l'ordre suivant :

- /vol0home/home/jsmith n'existe pas ; passer au chemin de recherche n°2.
- /vol1home/home/jsmith existe ; par conséquent, le chemin de recherche #3 n'est pas coché ; l'utilisateur est maintenant connecté à son répertoire de base.

Scénario 2 : l'utilisateur se connecte à \\vs1\jsmith. Ceci correspond au deuxième nom de partage du répertoire de base et génère le chemin relatif acme/jsmith. ONTAP recherche désormais un répertoire nommé acme/jsmith en vérifiant chaque chemin de recherche dans l'ordre suivant :

- /vol0home/home/acme/jsmith n'existe pas ; passer au chemin de recherche n°2.
- /vol1home/home/acme/jsmith n'existe pas ; passer au chemin de recherche #3.
- /vol2home/home/acme/jsmith n'existe pas ; le répertoire personnel n'existe pas ; la connexion échoue donc.

Partages de répertoires locaux

Ajouter un partage de répertoire de base

Si vous souhaitez utiliser la fonction de répertoire de base SMB, vous devez ajouter au moins un partage avec la propriété de répertoire de base incluse dans les propriétés de partage.

Description de la tâche

Vous pouvez créer un partage de répertoire personnel au moment de la création du partage en utilisant le `vserver cifs share create` vous pouvez également modifier un partage existant en un partage de répertoire personnel à tout moment à l'aide de l'`vserver cifs share modify` commande.

Pour créer un partage de répertoire personnel, vous devez inclure le `homedirectory` valeur dans le `-share-properties` lorsque vous créez ou modifiez un partage. Vous pouvez spécifier le nom du partage et le chemin du partage à l'aide de variables développées dynamiquement lorsque les utilisateurs se connectent à leurs répertoires locaux. Les variables disponibles que vous pouvez utiliser dans le chemin sont `%w`, `%d`, et `%u`, Correspondant respectivement au nom d'utilisateur Windows, au domaine et au nom d'utilisateur UNIX mappé.

Étapes

1. Ajouter un partage de répertoire de base :

```
vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties homedirectory[,...]
```

`-vserver vserver` Spécifie la machine virtuelle de stockage (SVM) compatible CIFS sur laquelle ajouter le chemin de recherche.

`-share-name share-name` spécifie le nom de partage du répertoire racine.

En plus de contenir l'une des variables requises, si le nom du partage contient l'une des chaînes littérales %w, %u, ou %d, Vous devez faire précéder la chaîne littérale d'un caractère % (pourcentage) pour empêcher ONTAP de traiter la chaîne littérale comme une variable (par exemple, %%w).

- Le nom du partage doit contenir soit le %w ou le %u variable.
- Le nom du partage peut également contenir le %d variable (par exemple, %d/%w) ou une partie statique dans le nom du partage (par exemple, home1_/%w).
- Si le partage est utilisé par les administrateurs pour se connecter aux répertoires d'accueil d'autres utilisateurs ou pour permettre aux utilisateurs de se connecter aux répertoires d'accueil d'autres utilisateurs, le modèle de nom de partage dynamique doit être précédé d'un tilde (~).

Le `vserver cifs home-directory modify` est utilisé pour activer cet accès en configurant le `-is-home-dirs-access-for-admin-enabled` option à `true`) ou en définissant l'option avancée `-is-home-dirs-access-for-public-enabled` à `true`.

`-path path` spécifie le chemin relatif vers le répertoire de base.

`-share-properties homedirectory[,...]` spécifie les propriétés de partage pour ce partage. Vous devez spécifier le `homedirectory` valeur. Vous pouvez spécifier d'autres propriétés de partage à l'aide d'une liste délimitée par des virgules.

1. Vérifiez que vous avez correctement ajouté le partage du répertoire personnel à l'aide de l' `vserver cifs share show` commande.

Exemple

La commande suivante crée un partage de répertoire personnel nommé %w. Le `oplocks`, `browsable`, et `changenotify` les propriétés de partage sont définies en plus de la configuration du `homedirectory` propriété de partage.



Cet exemple n'affiche pas les valeurs de sortie de tous les partages du SVM. La sortie est tronquée.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1	%w	%w	oplocks	-	Everyone / Full
Control			browsable		
			changenotify		
			homedirectory		

Informations associées

[Ajout d'un chemin de recherche de répertoire personnel](#)

Les partages de répertoires locaux requièrent des noms d'utilisateur uniques

Veillez à attribuer des noms d'utilisateur uniques lors de la création de partages de répertoires locaux à l'aide de l' `%w` (Nom d'utilisateur Windows) ou `%u` (Nom d'utilisateur UNIX) variables permettant de générer des partages de façon dynamique. Le nom du partage est mappé sur votre nom d'utilisateur.

Deux problèmes peuvent survenir lorsqu'un nom de partage statique et un nom d'utilisateur sont identiques :

- Lorsque l'utilisateur répertorie les partages sur un cluster utilisant le `net view` commande : deux partages portant le même nom d'utilisateur sont affichés.
- Lorsque l'utilisateur se connecte à ce nom de partage, l'utilisateur est toujours connecté au partage statique et ne peut pas accéder au partage de répertoire personnel portant le même nom.

Par exemple, il y a un partage nommé « administrateur » et vous avez un nom d'utilisateur Windows « administrateur ». Si vous créez un partage de répertoire personnel et vous connectez à ce partage, vous êtes connecté au partage statique « administrateur » et non à votre partage de répertoire personnel « administrateur ».

Vous pouvez résoudre le problème avec les noms de partage en double en suivant l'une des étapes suivantes :

- Renommer le partage statique de sorte qu'il n'entre plus en conflit avec le partage du répertoire personnel de l'utilisateur.
- Donner à l'utilisateur un nouveau nom d'utilisateur pour qu'il n'entre plus en conflit avec le nom du partage statique.
- Création d'un partage CIFS home Directory avec un nom statique tel que « home » au lieu d'utiliser le `%w` paramètre pour éviter les conflits avec les noms des partages.

Ce qui arrive aux noms de partage de répertoire personnel statique après la mise à niveau

Les noms de partage de répertoire racine doivent contenir soit le `%w` ou le `%u` variable dynamique. Vous devez savoir ce qui arrive aux noms de partage de répertoire personnel statiques après la mise à niveau vers une version de ONTAP avec la nouvelle exigence.

Si votre configuration de répertoire personnel contient des noms de partage statiques et que vous effectuez une mise à niveau vers ONTAP, les noms de partage de répertoire personnel statique ne sont pas modifiés et sont toujours valides. Cependant, vous ne pouvez pas créer de nouveaux partages de répertoire personnel qui ne contiennent ni `%w` ou `%u` variable.

Le fait de demander que l'une de ces variables soit incluse dans le nom de partage du répertoire de base de l'utilisateur garantit que chaque nom de partage est unique dans la configuration du répertoire de base. Si vous le souhaitez, vous pouvez modifier les noms de partage des répertoires d'accueil statiques en noms contenant l'un ou l'autre `%w` ou `%u` variable.

Ajouter un chemin de recherche de répertoire de base

Si vous souhaitez utiliser les home directories ONTAP SMB, vous devez ajouter au moins un chemin de recherche de répertoire personnel.

Description de la tâche

Vous pouvez ajouter un chemin de recherche de répertoire personnel à l'aide de la `vserver cifs home-directory search-path add` commande.

Le `vserver cifs home-directory search-path add` la commande vérifie le chemin d'accès spécifié dans `-path` option pendant l'exécution de la commande. Si le chemin spécifié n'existe pas, la commande génère un message vous invitant à continuer. Votre choix `y` ou `n`. Si vous le souhaitez `y` Pour continuer, ONTAP crée le chemin de recherche. Toutefois, vous devez créer la structure du répertoire avant de pouvoir utiliser le chemin de recherche dans la configuration du répertoire racine. Si vous choisissez de ne pas continuer, la commande échoue ; le chemin de recherche n'est pas créé. Vous pouvez ensuite créer la structure du répertoire de chemins d'accès et réexécuter le `vserver cifs home-directory search-path add` commande.

Étapes

1. Ajouter un chemin de recherche de répertoire de base : `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Vérifiez que vous avez correctement ajouté le chemin de recherche à l'aide de l' `vserver cifs home-directory search-path show` commande.

Exemple

L'exemple suivant ajoute le chemin `/home1` Vers la configuration home Directory sur le SVM `vs1`.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path /home1

vs1::> vserver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1      /home1
```

L'exemple suivant tente d'ajouter le chemin d'accès `/home2` Vers la configuration home Directory sur le SVM `vs1`. Le chemin d'accès n'existe pas. Le choix est de ne pas continuer.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path /home2
Warning: The specified path "/home2" does not exist in the namespace
        belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

Informations associées

[Ajout d'un partage de répertoire personnel](#)

Vous pouvez créer une configuration de répertoire personnel à l'aide de l' %w et %d variables. Les utilisateurs peuvent ensuite se connecter à leur partage personnel à l'aide de partages créés de manière dynamique.

Étapes

1. Créer un qtree pour contenir les home directories de l'utilisateur : `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Vérifier que le qtree utilise le style de sécurité approprié : `volume qtree show`
3. Si le qtree n'utilise pas le style de sécurité souhaité, modifiez le style de sécurité à l'aide de `volume qtree security` commande.
4. Ajouter un partage de répertoire de base : `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

`-vserver vserver` Spécifie la machine virtuelle de stockage (SVM) compatible CIFS sur laquelle ajouter le chemin de recherche.

`-share-name %w` spécifie le nom de partage du répertoire racine. ONTAP crée dynamiquement le nom du partage lorsque chaque utilisateur se connecte à son répertoire de base. Le nom du partage sera sous la forme *Windows_user_name*.

`-path %d/%w` spécifie le chemin relatif vers le répertoire de base. Le chemin relatif est créé de façon dynamique au fur et à mesure que chaque utilisateur se connecte à son répertoire de départ et sera sous la forme *domain/Windows_user_name*.

`-share-properties homedirectory\[,...\]` spécifie les propriétés de partage pour ce partage. Vous devez spécifier le `homedirectory` valeur. Vous pouvez spécifier d'autres propriétés de partage à l'aide d'une liste délimitée par des virgules.

5. Vérifiez que le partage dispose de la configuration souhaitée à l'aide du `vserver cifs share show` commande.
6. Ajouter un chemin de recherche de répertoire de base : `vserver cifs home-directory search-path add -vserver vserver -path path`

`-vserver vserver-name` Spécifie le SVM activé sur CIFS sur lequel ajouter le chemin de recherche.

`-path path` spécifie le chemin absolu du répertoire vers le chemin de recherche.

7. Vérifiez que vous avez correctement ajouté le chemin de recherche à l'aide de l' `vserver cifs home-directory search-path show` commande.
8. Pour les utilisateurs disposant d'un home Directory, créez un répertoire correspondant dans le qtree ou le volume désigné pour contenir des home directories.

Par exemple, si vous avez créé un qtree avec le chemin d'accès du groupe `/vol/vol1/users` et le nom d'utilisateur dont vous souhaitez créer le répertoire est `mydomain\user1`, vous devez créer un répertoire avec le chemin suivant : `/vol/vol1/users/mydomain/user1`.

Si vous avez créé un volume nommé « `home1` » monté à `/home1`, vous créeriez un répertoire avec le chemin suivant : `/home1/mydomain/user1`.

9. Vérifiez qu'un utilisateur peut se connecter avec succès au partage d'accueil en mappant un lecteur ou en vous connectant à l'aide du chemin UNC.

Par exemple, si l'utilisateur mydomain\user1 souhaite se connecter au répertoire créé à l'étape 8 situé sur le SVM vs1, l'utilisateur 1 se connecte à l'aide du chemin UNC \\vs1\user1.

Exemple

Dans l'exemple suivant, les commandes permettent de créer une configuration de home Directory avec les paramètres suivants :

- Le nom du partage est %w.
- Le chemin relatif du répertoire d'accueil est %d/%w.
- Le chemin de recherche utilisé pour contenir les répertoires locaux, /home1, Est un volume configuré avec le style de sécurité NTFS.
- La configuration est créée sur le SVM vs1.

Vous pouvez utiliser ce type de configuration de répertoire personnel lorsque les utilisateurs accèdent à leurs répertoires personnels à partir d'hôtes Windows. Vous pouvez également utiliser ce type de configuration lorsque les utilisateurs accèdent à leurs répertoires personnels à partir d'hôtes Windows et UNIX et que l'administrateur du système de fichiers utilise des utilisateurs et des groupes Windows pour contrôler l'accès au système de fichiers.

```

cluster::> vsriver cifs share create -vsriver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vsriver cifs share show -vsriver vs1 -share-name %w

                Vserver: vs1
                Share: %w
CIFS Server NetBIOS Name: VS1
                Path: %d/%w
                Share Properties: oplocks
                                browsable
                                changenotify
                                homedirectory
                Symlink Properties: enable
                File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vsriver cifs home-directory search-path add -vsriver vs1 -path
/home1

cluster::> vsriver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1        /home1

```

Informations associées

[Configuration des répertoires d'accueil à l'aide de la variable %u](#)

[Configurations supplémentaires des home Directory](#)

[Affichage des informations sur le chemin du répertoire local d'un utilisateur SMB](#)

Configurez les répertoires d'accueil à l'aide de la variable %u

Vous pouvez créer une configuration de répertoire personnel dans laquelle vous désignez le nom du partage à l'aide de l' %w variable mais vous utilisez %u variable pour désigner le chemin relatif vers le partage du répertoire racine. Les utilisateurs peuvent ensuite se connecter à leur partage d'origine à l'aide de partages dynamiques créés à l'aide de leur nom d'utilisateur Windows sans connaître le nom ou le chemin réel du répertoire d'accueil.

Étapes

1. Créer un qtree pour contenir les home directories de l'utilisateur : `volume qtree create -vserver vsver_name -qtree-path qtree_path`
2. Vérifier que le qtree utilise le style de sécurité approprié : `volume qtree show`
3. Si le qtree n'utilise pas le style de sécurité souhaité, modifiez le style de sécurité à l'aide de `volume qtree security` commande.
4. Ajouter un partage de répertoire de base : `vserver cifs share create -vserver vsver_name -share-name %w -path %u -share-properties homedirectory ,...]`

`-vserver vsver_name` Spécifie la machine virtuelle de stockage (SVM) compatible CIFS sur laquelle ajouter le chemin de recherche.

`-share-name %w` spécifie le nom de partage du répertoire racine. Le nom du partage est créé dynamiquement lorsque chaque utilisateur se connecte à son répertoire de départ et se présente sous la forme *Windows_user_name*.



Vous pouvez également utiliser le `%u` variable pour le `-share-name` option. Cela crée un chemin de partage relatif qui utilise le nom d'utilisateur UNIX mappé.

`-path %u` spécifie le chemin relatif vers le répertoire de base. Le chemin relatif est créé dynamiquement au fur et à mesure que chaque utilisateur se connecte à son répertoire de départ et se présente sous la forme *mappé_UNIX_user_name*.



La valeur de cette option peut également contenir des éléments statiques. Par exemple : `eng/%u`.

`-share-properties homedirectory\[,... \]` spécifie les propriétés de partage pour ce partage. Vous devez spécifier le `homedirectory` valeur. Vous pouvez spécifier d'autres propriétés de partage à l'aide d'une liste délimitée par des virgules.

5. Vérifiez que le partage dispose de la configuration souhaitée à l'aide du `vserver cifs share show` commande.
6. Ajouter un chemin de recherche de répertoire de base : `vserver cifs home-directory search-path add -vserver vsver_name -path path`

`-vserver vsver_name` Spécifie le SVM activé sur CIFS sur lequel ajouter le chemin de recherche.

`-path path` spécifie le chemin absolu du répertoire vers le chemin de recherche.
7. Vérifiez que vous avez correctement ajouté le chemin de recherche à l'aide de `vserver cifs home-directory search-path show` commande.
8. Si l'utilisateur UNIX n'existe pas, créez l'utilisateur UNIX à l'aide de `vserver services unix-user create` commande.



Le nom d'utilisateur UNIX auquel vous associez le nom d'utilisateur Windows doit exister avant le mappage de l'utilisateur.

9. Créer un mappage de nom pour l'utilisateur Windows auprès de l'utilisateur UNIX à l'aide de la commande

suivante : `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`



Si des mappages de noms existent déjà et mappent des utilisateurs Windows aux utilisateurs UNIX, vous n'avez pas besoin d'effectuer l'étape de mappage.

Le nom d'utilisateur Windows est mappé sur le nom d'utilisateur UNIX correspondant. Lorsque l'utilisateur Windows se connecte à son partage de répertoire personnel, il se connecte à un répertoire personnel créé dynamiquement avec un nom de partage qui correspond à son nom d'utilisateur Windows sans avoir à savoir que le nom de répertoire correspond au nom d'utilisateur UNIX.

10. Pour les utilisateurs disposant d'un home Directory, créez un répertoire correspondant dans le qtree ou le volume désigné pour contenir des home directories.

Par exemple, si vous avez créé un qtree avec le chemin d'accès du groupe `/vol/vol1/users` Et le nom d'utilisateur UNIX mappé de l'utilisateur dont vous souhaitez créer le répertoire est « `unixuser1` », vous devez créer un répertoire avec le chemin suivant : `/vol/vol1/users/unixuser1`.

Si vous avez créé un volume nommé « `home1` » monté à `/home1`, vous créeriez un répertoire avec le chemin suivant : `/home1/unixuser1`.

11. Vérifiez qu'un utilisateur peut se connecter avec succès au partage d'accueil en mappant un lecteur ou en vous connectant à l'aide du chemin UNC.

Par exemple, si l'utilisateur `mydomain\user1` est mappé sur l'utilisateur UNIX `unixuser1` et souhaite se connecter au répertoire créé à l'étape 10 situé sur le SVM `vs1`, l'utilisateur 1 se connecte à l'aide du chemin UNC `\\vs1\user1`.

Exemple

Dans l'exemple suivant, les commandes permettent de créer une configuration de home Directory avec les paramètres suivants :

- Le nom du partage est `%w`.
- Le chemin relatif du répertoire d'accueil est `%U`.
- Le chemin de recherche utilisé pour contenir les répertoires locaux, `/home1`, Est un volume configuré avec le style de sécurité UNIX.
- La configuration est créée sur le SVM `vs1`.

Vous pouvez utiliser ce type de configuration de répertoire personnel lorsque les utilisateurs accèdent à leurs répertoires personnels à partir des hôtes Windows ou Windows et UNIX et que l'administrateur de système de fichiers utilise des utilisateurs et des groupes UNIX pour contrôler l'accès au système de fichiers.

```
cluster::> vsriver cifs share create -vsriver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
cluster::> vsriver cifs share show -vsriver vs1 -share-name %u
```

```

                Vserver: vs1
                Share: %w
CIFS Server NetBIOS Name: VS1
                Path: %u
        Share Properties: oplocks
                        browsable
                        changenotify
                        homedirectory
        Symlink Properties: enable
        File Mode Creation Mask: -
        Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster::> vsriver cifs home-directory search-path add -vsriver vs1 -path
/home1
```

```
cluster::> vsriver cifs home-directory search-path show -vsriver vs1
```

Vserver	Position	Path

vs1	1	/home1

```
cluster::> vsriver name-mapping create -vsriver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1
```

```
cluster::> vsriver name-mapping show -pattern user1
```

Vserver	Direction	Position

vs1	win-unix	5
		Pattern: user1
		Replacement: unixuser1

Informations associées

[Création d'une configuration de répertoire personnel à l'aide des variables %w et %d](#)

[Configurations supplémentaires des home Directory](#)

[Affichage des informations sur le chemin du répertoire local d'un utilisateur SMB](#)

Configurations supplémentaires des home Directory

Vous pouvez créer d'autres configurations de home Directory à l'aide du %w, %d, et %u variables, qui vous permettent de personnaliser la configuration du répertoire personnel pour répondre à vos besoins.

Vous pouvez créer un certain nombre de configurations de répertoire personnel en utilisant une combinaison de variables et de chaînes statiques dans les noms de partage et les chemins de recherche. Le tableau suivant fournit des exemples illustrant la création de différentes configurations de répertoires locaux :

Chemins d'accès créés lors de /vol1/user contient les répertoires locaux...	Partager, commande...
Pour créer un chemin de partage \\vs1\~win_username qui dirige l'utilisateur vers /vol1/user/win_username	<code>vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory</code>
Pour créer un chemin de partage \\vs1\win_username qui dirige l'utilisateur vers /vol1/user/domain/win_username	<code>vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory</code>
Pour créer un chemin de partage \\vs1\win_username qui dirige l'utilisateur vers /vol1/user/unix_username	<code>vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory</code>
Pour créer un chemin de partage \\vs1\unix_username qui dirige l'utilisateur vers /vol1/user/unix_username	<code>vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory</code>

Commandes de gestion des chemins de recherche

Il existe des commandes ONTAP spécifiques permettant de gérer les chemins de recherche pour les configurations du home Directory SMB. Par exemple, il existe des commandes permettant d'ajouter, de supprimer et d'afficher les informations relatives aux chemins de recherche. Il existe également une commande permettant de modifier l'ordre du chemin de recherche.

Les fonctions que vous recherchez...	Utilisez cette commande...
Ajouter un chemin de recherche	<code>vserver cifs home-directory search-path add</code>
Afficher les chemins de recherche	<code>vserver cifs home-directory search-path show</code>

Les fonctions que vous recherchez...	Utilisez cette commande...
Modifier l'ordre du chemin de recherche	<code>vserver cifs home-directory search-path reorder</code>
Supprimer un chemin de recherche	<code>vserver cifs home-directory search-path remove</code>

Consultez la page man pour chaque commande pour plus d'informations.

Affiche des informations sur le chemin du répertoire personnel d'un utilisateur SMB

Vous pouvez afficher le chemin d'accès au home Directory d'un utilisateur SMB sur la machine virtuelle de stockage (SVM), que vous pouvez utiliser si plusieurs chemins de home Directory CIFS sont configurés et que vous souhaitez voir quel chemin contient le home Directory de l'utilisateur.

Étape

1. Afficher le chemin du répertoire racine à l'aide de la `vserver cifs home-directory show-user` commande.

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

Vserver	User	Home Dir Path
-----	-----	-----
vs1	user1	/home/user1

Informations associées

[Gestion de l'accessibilité aux répertoires locaux des utilisateurs](#)

Gérer l'accessibilité aux répertoires locaux des utilisateurs

Par défaut, le répertoire personnel d'un utilisateur est accessible uniquement par cet utilisateur. Pour les partages dont le nom dynamique du partage est précédé d'un tilde (~), vous pouvez activer ou désactiver l'accès aux répertoires d'accueil des utilisateurs par les administrateurs Windows ou par tout autre utilisateur (accès public).

Avant de commencer

Les partages de home Directory sur la machine virtuelle de stockage (SVM) doivent être configurés avec des noms de partage dynamiques précédés d'un tilde (~). Les cas suivants illustrent les conditions de dénomination des partages :

Nom de partage du répertoire racine	Exemple de commande pour se connecter au partage
~%d~%w	net use * \\IPAddress\~domain~user/u:credentials
~%w	net use * \\IPAddress\~user/u:credentials
~abc~%w	net use * \\IPAddress\abc~user/u:credentials

Étape

1. Effectuez l'action appropriée :

Si vous souhaitez activer ou désactiver l'accès aux répertoires d'accueil des utilisateurs à...	Entrez les informations suivantes...
Administrateurs Windows	vserver cifs home-directory modify -vserver vserver_name -is-home-dirs -access-for-admin-enabled {true false} La valeur par défaut est true.
Tout utilisateur (accès public)	a. Définissez le niveau de privilège sur avancé : set -privilege advanced b. Activer ou désactiver l'accès : `vserver cifs home-directory modify -vserver vserver_name -is-home-dirs-access-for-public-enabled {true

L'exemple suivant permet l'accès public aux répertoires locaux des utilisateurs :

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

Informations associées

[Affichage des informations sur le chemin du répertoire local d'un utilisateur SMB](#)

Configurez l'accès client SMB aux liens symboliques UNIX

Comment ONTAP vous permet de fournir un accès client SMB aux liens symboliques UNIX

Un lien symbolique est un fichier créé dans un environnement UNIX qui contient une référence à un autre fichier ou répertoire. Si un client accède à un lien symbolique, le client est redirigé vers le fichier ou répertoire cible auquel le lien symbolique fait référence. ONTAP prend en charge les liens symboliques relatifs et absolus, y compris les liens filaires (liens absolus avec des cibles en dehors du système de fichiers local).

ONTAP permet aux clients SMB de suivre des liens symboliques UNIX configurés sur la SVM. Cette fonction est facultative et vous pouvez la configurer par partage à l'aide de `-symlink-properties` de la `vserver cifs share create` avec l'un des paramètres suivants :

- Accès en lecture/écriture
- Activé avec accès en lecture seule
- Désactivé en masquant les liens symboliques des clients SMB
- Désactivé sans accès aux liens symboliques des clients SMB

Si vous activez des liens symboliques sur un partage, les liens symboliques relatifs fonctionnent sans configuration supplémentaire.

Si vous activez des liens symboliques sur un partage, les liens symboliques absolus ne fonctionnent pas immédiatement. Vous devez d'abord créer un mappage entre le chemin UNIX du lien symbolique et le chemin SMB de destination. Lors de la création de mappages de liens symboliques absolus, vous pouvez spécifier s'il s'agit d'un lien local ou d'un *widelink* ; les liens vers des systèmes de fichiers sur d'autres périphériques de stockage ou des liens vers des systèmes de fichiers hébergés dans des SVM distincts sur le même système ONTAP. Lorsque vous créez un lien, il doit inclure les informations que le client doit suivre, c'est-à-dire que vous créez un point de reanalyse pour que le client puisse découvrir le point de jonction du répertoire. Si vous créez un lien symbolique absolu vers un fichier ou un répertoire en dehors du partage local mais que vous définissez la localité sur local, ONTAP n'autorise pas l'accès à la cible.



Si un client tente de supprimer un lien symbolique local (absolu ou relatif), seul le lien symbolique est supprimé, pas le fichier ou le répertoire cible. Toutefois, si un client tente de supprimer un lien vers le fil, il peut supprimer le fichier ou le répertoire cible auquel le lien vers le fil vers le fil. ONTAP n'a pas le contrôle sur cela, car le client peut explicitement ouvrir le fichier ou le répertoire cible en dehors du SVM et le supprimer.

• Analyse des points et des services de système de fichiers ONTAP

Un *reparse point* est un objet système de fichiers NTFS qui peut éventuellement être stocké sur des volumes avec un fichier. Les points de reanalyse permettent aux clients SMB de recevoir des services de système de fichiers améliorés ou étendus lorsqu'ils travaillent avec des volumes de style NTFS. Les points de réanalyse se composent d'étiquettes standard identifiant le type de point de réanalyse et le contenu du point de réanalyse pouvant être récupéré par les clients SMB pour un traitement ultérieur par le client. Parmi les types d'objets disponibles pour la fonctionnalité étendue du système de fichiers, ONTAP met en œuvre la prise en charge des liens symboliques NTFS et des points de jonction de répertoire à l'aide de balises de point de reparse. Les clients SMB qui ne peuvent pas comprendre le contenu d'un point de reanalyse le ignorent et ne fournissent pas le service étendu de système de fichiers que le point de reanalyse peut activer.

• Prise en charge des points de jonction de répertoire et de ONTAP pour les liens symboliques

Les points de jonction de répertoire sont des emplacements au sein d'une structure de répertoire de système de fichiers qui peuvent faire référence à des emplacements de remplacement où les fichiers sont stockés, soit sur un chemin différent (liens symboliques), soit sur un périphérique de stockage distinct (liens filaires). Les serveurs ONTAP SMB exposent les points de jonction de répertoire aux clients Windows sous forme de points de reanalyse, ce qui permet aux clients capables d'obtenir le contenu du point de reanalyse à partir de ONTAP lorsqu'un point de jonction de répertoire est en cours de traitement. Ils peuvent ainsi naviguer et se connecter à différents chemins ou périphériques de stockage comme s'ils faisaient partie du même système de fichiers.

• Activation de la prise en charge wdelink à l'aide des options de point de réanalyse


Le `-is-use-junctions-as-reparse-points-enabled` Cette option est activée par défaut dans ONTAP 9. Tous les clients SMB ne prennent pas en charge les widelinks. L'option d'activation des informations peut donc être configurée selon la version du protocole, ce qui permet aux administrateurs de prendre en charge à la fois les clients SMB pris en charge et les clients SMB non pris en charge. Dans ONTAP 9.2 et versions ultérieures, vous devez activer cette option `-widelink-as-reparse-point-versions` Pour chaque protocole client qui accède au partage à l'aide de widelinks, la valeur par défaut est SMB1. Dans les versions antérieures, seules les widelinks accessibles à l'aide de SMB1 par défaut ont été signalés et les systèmes utilisant SMB2 ou SMB3 n'ont pas pu accéder aux widelinks.

Informations associées

- ["Applications de sauvegarde Windows et liens symboliques de style Unix"](#)
- ["Documentation Microsoft : analyse des points"](#)

Limites lors de la configuration de liens symboliques UNIX pour l'accès SMB

Vous devez connaître certaines limites lors de la configuration de liens symboliques UNIX pour l'accès SMB.

Limite	Description
45	<div>Longueur maximale du nom de serveur CIFS que vous pouvez spécifier lors de l'utilisation d'un FQDN pour le nom du serveur CIFS.</div> <div> Vous pouvez également spécifier le nom du serveur CIFS sous la forme d'un nom NetBIOS, limité à 15 caractères.</div>
80	Longueur maximale du nom de partage.
256	Longueur maximale du chemin UNIX que vous pouvez spécifier lors de la création d'un lien symbolique ou lors de la modification du chemin UNIX d'un lien symbolique existant.le chemin UNIX doit commencer par un <code>"/</code> (slash) and end with a <code>"/</code> . Les barres obliques de début et de fin font partie de la limite de 256 caractères.
256	Longueur maximale du chemin CIFS que vous pouvez spécifier lors de la création d'un lien symbolique ou lors de la modification du chemin CIFS d'un lien symbolique existant.le chemin CIFS doit commencer par <code>»/</code> (slash) and end with a <code>"/</code> . Les barres obliques de début et de fin font partie de la limite de 256 caractères.

Informations associées

[Création de mappages de liens symboliques pour les partages SMB](#)

Une option de serveur CIFS contrôle la manière dont les fonctionnalités DFS sont annoncées aux clients SMB lors de la connexion aux partages. Étant donné que ONTAP utilise des référencements DFS lorsque les clients accèdent aux liens symboliques via SMB, vous devez savoir quel est l'impact lorsque cette option est désactivée ou activée.

Une option de serveur CIFS détermine si les serveurs CIFS annoncent automatiquement qu'ils sont compatibles DFS pour les clients SMB. Par défaut, cette option est activée et le serveur CIFS annonce toujours que DFS est capable pour les clients SMB (même lors de la connexion à des partages où l'accès aux liens symboliques est désactivé). Si vous voulez que le serveur CIFS annonce qu'il est compatible avec les clients uniquement lorsqu'ils se connectent à des partages où l'accès aux liens symboliques est activé, vous pouvez désactiver cette option.

Vous devez savoir ce qui se passe lorsque cette option est désactivée :

- Les configurations de partage des liens symboliques ne sont pas modifiées.
- Si le paramètre de partage est défini pour autoriser l'accès à la liaison symbolique (accès en lecture/écriture ou accès en lecture seule), le serveur CIFS transmet les fonctionnalités DFS aux clients se connectant à ce partage.

Les connexions client et l'accès aux liens symboliques se poursuivent sans interruption.

- Si le paramètre de partage est défini sur ne pas autoriser l'accès aux liens symboliques (soit en désactivant l'accès, soit si la valeur du paramètre de partage est nulle), le serveur CIFS n'annonce pas les capacités DFS aux clients se connectant à ce partage.

Comme les clients disposent d'informations en cache sur lesquelles le serveur CIFS prend en charge DFS et qu'il n'est plus publicitaire qu'il est, les clients connectés à des partages où l'accès à la liaison symbolique est désactivé risquent de ne pas pouvoir accéder à ces partages une fois que l'option de serveur CIFS est désactivée. Une fois l'option désactivée, vous devrez peut-être redémarrer les clients connectés à ces partages, ce qui vous permettra de supprimer les informations mises en cache.

Ces modifications ne s'appliquent pas aux connexions SMB 1.0.

Configurez la prise en charge des liens symboliques UNIX sur les partages SMB

Vous pouvez configurer la prise en charge des liens symboliques UNIX sur les partages SMB en spécifiant un paramètre de propriété de partage de liens symboliques lorsque vous créez des partages SMB ou en modifiant à tout moment des partages SMB existants. La prise en charge des liens symboliques UNIX est activée par défaut. Vous pouvez également désactiver la prise en charge des liens symboliques UNIX sur un partage.

Description de la tâche

Lors de la configuration de la prise en charge des liens symboliques UNIX pour les partages SMB, vous pouvez choisir l'un des paramètres suivants :

Réglage	Description
<code>enable</code> (OBSOLÈTE*)	Indique que les liens symboliques sont activés pour l'accès en lecture/écriture.
<code>read_only</code> (OBSOLÈTE*)	Indique que les symlinks sont activés pour l'accès en lecture seule. Ce paramètre ne s'applique pas aux boutons de mode. L'accès Widelink est toujours en lecture-écriture.
<code>hide</code> (OBSOLÈTE*)	Spécifie que les clients SMB ne peuvent pas voir les symlinks.
<code>no-strict-security</code>	Spécifie que les clients suivent des symlinks en dehors des limites de partage.
<code>symlinks</code>	Indique que les symlinks sont activés localement pour l'accès en lecture/écriture. Les annonces DFS ne sont pas générées même si l'option CIFS <code>is-advertise-dfs-enabled</code> est défini sur <code>true</code> . Il s'agit du paramètre par défaut.
<code>symlinks-and-widelinks</code>	Spécifie que les liens symlinks locaux et les widelinks pour l'accès en lecture-écriture. Les annonces DFS sont générées pour les symlinks locaux et les widelinks, même si l'option CIFS <code>is-advertise-dfs-enabled</code> est défini sur <code>false</code> .
<code>disable</code>	Spécifie que les liens symlinks et les liens de fil sont désactivés. Les annonces DFS ne sont pas générées même si l'option CIFS <code>is-advertise-dfs-enabled</code> est défini sur <code>true</code> .
<code>""</code> (nul, non défini)	Désactive les liens symboliques sur le partage.
<code>-</code> (non défini)	Désactive les liens symboliques sur le partage.



*Les paramètres *enable*, *hide* et *read-only* sont obsolètes et peuvent être supprimés dans une version future de ONTAP.

Étapes

1. Configurer ou désactiver la prise en charge des liens symboliques :

Si c'est...	Entrer...
Un nouveau partage SMB	<code>`+vserver cifs share create -vserver vservice_name -share-name share_name -path path -symlink -properties {enable</code>

Si c'est...	Entrer...
hide	read-only
""	-
symlinks	symlinks-and-widelinks
disable},...]+`	Un partage SMB existant
`+vserver cifs share modify -vserver vservice_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},...]+`

2. Vérifiez que la configuration du partage SMB est correcte : `vserver cifs share show -vserver vservice_name -share-name share_name -instance`

Exemple

La commande suivante crée un partage SMB nommé "data1" avec la configuration de lien symbolique UNIX définie sur `enable`:


```
cluster1::> vservers cifs share create -vservers vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vservers cifs share show -vservers vs1 -share-name data1
-instance

Vserver: vs1
Share: data1
CIFS Server NetBIOS Name: VS1
Path: /data1
Share Properties: oplocks
                  browsable
                  changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

Informations associées

[Création de mappages de liens symboliques pour les partages SMB](#)

Créez des mappages de liens symboliques pour les partages SMB

Vous pouvez créer des mappages de liens symboliques UNIX pour les partages SMB. Vous pouvez soit créer un lien symbolique relatif, qui fait référence au fichier ou au dossier par rapport à son dossier parent, soit créer un lien symbolique absolu, qui fait référence au fichier ou au dossier à l'aide d'un chemin absolu.

Description de la tâche

Les Widelinks ne sont pas accessibles à partir de clients Mac OS X si vous utilisez SMB 2.x. Lorsqu'un utilisateur tente de se connecter à un partage à l'aide de liens de liaison d'un client Mac OS X, la tentative échoue. Toutefois, vous pouvez utiliser des liens de mode avec les clients Mac OS X si vous utilisez SMB 1.

Étapes

1. Pour créer des mappages de liens symboliques pour les partages SMB : `vservers cifs symlink create -vservers virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

`-vservers virtual_server_name` Spécifie le nom de la machine virtuelle de stockage (SVM).

`-unix-path path` Spécifie le chemin UNIX. Le chemin UNIX doit commencer par une barre oblique (/) et doit se terminer par une barre oblique (/).

`-share-name share_name` Spécifie le nom du partage SMB à mapper.

`-cifs-path path` Spécifie le chemin CIFS. Le chemin CIFS doit commencer par une barre oblique (/) et doit se terminer par une barre oblique (/).

`-cifs-server server_name` Spécifie le nom du serveur CIFS. Le nom du serveur CIFS peut être spécifié sous la forme d'un nom DNS (par exemple, mynetwork.cifs.server.com), d'une adresse IP ou d'un nom NetBIOS. Le nom NetBIOS peut être déterminé à l'aide du `vserver cifs show` commande. Si ce paramètre facultatif n'est pas spécifié, la valeur par défaut est le nom NetBIOS du serveur CIFS local.

`-locality local|free|widelink` spécifie s'il faut créer un lien local, un lien libre ou un lien symbolique étendu. Un lien symbolique local correspond au partage SMB local. Un lien symbolique libre peut être mappé n'importe où sur le serveur SMB local. Un lien symbolique étendu correspond à n'importe quel partage SMB du réseau. Si vous ne spécifiez pas ce paramètre facultatif, la valeur par défaut est `local`.

`-home-directory true false` indique si le partage cible est un répertoire de base. Même si ce paramètre est facultatif, vous devez définir ce paramètre sur `true` lorsque le partage cible est configuré en tant que répertoire de base. La valeur par défaut est `false`.

Exemple

La commande suivante crée un mappage de lien symbolique sur le SVM nommé vs1. Il a le chemin UNIX `/src/`, Le nom de partage SMB "SOURCE", le chemin CIFS `/mycompany/source/`, Et l'adresse IP `123.123.123.123` du serveur CIFS, et c'est un lien de type `widelink`.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Informations associées

[Configuration de la prise en charge des liens symboliques UNIX sur les partages SMB](#)

Commandes permettant de gérer les mappages de liens symboliques

Il existe des commandes ONTAP spécifiques permettant de gérer les mappages de liens symboliques.

Les fonctions que vous recherchez...	Utilisez cette commande...
Créer un mappage de lien symbolique	<code>vserver cifs symlink create</code>
Affiche des informations sur les mappages de liens symboliques	<code>vserver cifs symlink show</code>
Modifier un mappage de lien symbolique	<code>vserver cifs symlink modify</code>

Les fonctions que vous recherchez...	Utilisez cette commande...
Supprimer un mappage de lien symbolique	<code>vserver cifs symlink delete</code>

Consultez la page man pour chaque commande pour plus d'informations.

Applications de sauvegarde Windows et liens symboliques de style Unix

Lorsqu'une application de sauvegarde s'exécutant sous Windows rencontre un lien symbolique de style Unix (symlink), le lien est suivi et les données sont sauvegardées. Depuis ONTAP 9.15.1, vous avez la possibilité de sauvegarder les liens symboliques au lieu des données. Cette fonctionnalité est entièrement prise en charge avec les solutions ONTAP FlexGroups et FlexVols.

Présentation

Avant de modifier la façon dont ONTAP gère les liens symboliques au cours d'une opération de sauvegarde Windows, vous devez connaître les avantages, les concepts clés et les options de configuration.

Avantages

Lorsque cette fonction est désactivée ou indisponible, chaque lien symbolique est parcouru et les données auxquelles elle est liée sont sauvegardées. C'est pourquoi il est parfois possible de sauvegarder des données inutiles et, dans certains cas, l'application risque de se retrouver en boucle. La sauvegarde des liens symboliques permet d'éviter ces problèmes. Et comme les fichiers symlink sont très petits par rapport aux données dans la plupart des cas, les sauvegardes prennent moins de temps. La réduction des opérations d'E/S permet également d'améliorer les performances globales du cluster.

Environnement de serveur Windows

Cette fonction est prise en charge pour les applications de sauvegarde s'exécutant sous Windows. Vous devez comprendre les aspects techniques pertinents de l'environnement avant de l'utiliser.

Attributs étendus

Windows prend en charge les attributs étendus (EA) qui forment collectivement des métadonnées supplémentaires éventuellement associées aux fichiers. Ces attributs sont utilisés par diverses applications, telles que le sous-système Windows pour Linux, comme décrit à la section ["Autorisations de fichier pour WSL"](#). Les applications peuvent demander des attributs étendus pour chaque fichier lors de la lecture de données à partir de ONTAP.

Les liens symboliques sont renvoyés dans les attributs étendus lorsque la fonction est activée. Par conséquent, une application de sauvegarde doit fournir une prise en charge EA standard utilisée pour stocker les métadonnées. Certains utilitaires Windows prennent en charge et conservent les attributs étendus. Toutefois, si le logiciel de sauvegarde ne prend pas en charge la sauvegarde et la restauration des attributs étendus, il ne conservera pas les métadonnées associées à chaque fichier et ne traitera pas correctement les liens symboliques.

Configuration Windows

Les applications de sauvegarde exécutées sur un serveur Microsoft Windows peuvent bénéficier d'un privilège spécial leur permettant de contourner la sécurité normale des fichiers. Pour ce faire, vous devez généralement ajouter les applications au groupe opérateurs de sauvegarde. Les applications peuvent ensuite sauvegarder et restaurer les fichiers selon les besoins, ainsi que réaliser d'autres opérations système connexes. Le protocole

SMB utilisé par les applications de sauvegarde est subtils changements qui peuvent être détectés par ONTAP lors de la lecture et de l'écriture des données.

De formation

La fonction de sauvegarde de lien symbolique a plusieurs exigences, notamment :

- Votre cluster exécute ONTAP 9.15.1 ou une version ultérieure.
- Application de sauvegarde Windows bénéficiant de privilèges de sauvegarde spéciaux.
- L'application de sauvegarde doit également prendre en charge les attributs étendus et les demander pendant les opérations de sauvegarde.
- La fonctionnalité de sauvegarde ONTAP symlink est activée pour le SVM de données applicable.

Options de configuration

Outre l'interface de ligne de commandes de ONTAP, vous pouvez également gérer cette fonctionnalité via l'API REST. Voir "[Nouveautés de l'API REST ONTAP et de l'automatisation](#)" pour plus d'informations. La configuration déterminant la façon dont ONTAP traite les symlinks de style Unix doit être effectuée séparément pour chaque SVM.

Activez la fonction de sauvegarde de lien symbolique dans ONTAP

Une option de configuration a été ajoutée à une commande CLI existante avec ONTAP 9.15.1. Vous pouvez utiliser cette option pour activer ou désactiver le traitement des liens symboliques de style Unix.

Avant de commencer

Passez en revue le de base [De formation](#). Par ailleurs :

- Être capable de porter vos privilèges d'interface de ligne de commandes au niveau avancé.
- Déterminer le SVM de données à modifier Le SVM `vs1` est utilisé dans la commande exemple.

Étapes

1. Définissez le niveau de privilège avancé.

```
set privilege advanced
```

2. Activer la sauvegarde du fichier symlink.

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

Utilisez BranchCache pour mettre en cache le contenu du partage SMB dans une succursale

Utilisez BranchCache pour mettre en cache le contenu du partage SMB dans une présentation destinée aux succursales

BranchCache a été développé par Microsoft afin de permettre la mise en cache du contenu sur les ordinateurs locaux pour les clients. L'implémentation par ONTAP de BranchCache permet de réduire l'utilisation du réseau étendu (WAN) et de réduire le

temps de réponse d'accès lorsque les utilisateurs d'une succursale accèdent au contenu stocké sur des serveurs virtuels de stockage (SVM) avec SMB.

Si vous configurez BranchCache, les clients Windows BranchCache récupèrent le contenu du SVM, puis le mettent en cache sur un ordinateur au sein de la succursale. Si un autre client BranchCache du bureau de succursale demande le même contenu, le SVM procède d'abord à l'authentification et autorise l'utilisateur à demander. La SVM détermine ensuite si le contenu en cache est toujours à jour et, le cas échéant, elle envoie les métadonnées client relatives au contenu en cache. Le client utilise ensuite les métadonnées pour récupérer le contenu directement à partir du cache local.

Informations associées

[Utilisation de fichiers hors ligne pour permettre la mise en cache de fichiers pour une utilisation hors ligne](#)

Exigences et directives

Prise en charge de BranchCache

Notez bien les versions de BranchCache prises en charge par ONTAP.

ONTAP prend en charge BranchCache 1 et le BranchCache 2 optimisé :

- Lorsque vous configurez BranchCache sur le serveur SMB pour le serveur de stockage virtuel (SVM), vous pouvez activer BranchCache 1, BranchCache 2 ou toutes les versions.

Par défaut, toutes les versions sont activées.

- Si vous n'activez que BranchCache 2, les ordinateurs clients Windows du bureau distant doivent prendre en charge BranchCache 2.

Seuls les clients SMB 3.0 ou version ultérieure prennent en charge BranchCache 2.

Pour plus d'informations sur les versions de BranchCache, consultez la bibliothèque Microsoft TechNet.

Informations associées

["Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"](https://technet.microsoft.com/en-us/library/)

Exigences de prise en charge des protocoles réseau

Pour implémenter ONTAP BranchCache, vous devez connaître les exigences en matière de protocoles réseau.

Vous pouvez implémenter la fonction ONTAP BranchCache sur des réseaux IPv4 et IPv6 à l'aide de SMB 2.1 ou version ultérieure.

Tous les serveurs CIFS et les succursales qui participent à l'implémentation de BranchCache doivent activer le protocole SMB 2.1 ou version ultérieure. Avec SMB 2.1, les extensions de protocole permettent à un client de participer à un environnement de BranchCache. Il s'agit de la version minimale du protocole SMB qui prend en charge BranchCache. SMB 2.1 prend en charge BranchCache version 1.

Si vous souhaitez utiliser BranchCache version 2, SMB 3.0 est la version minimale prise en charge. SMB 3.0 doit être activé sur tous les serveurs CIFS et les succursales qui participent à une implémentation de BranchCache 2.

Si vous disposez de bureaux distants où certains clients prennent uniquement en charge SMB 2.1 et que certains clients prennent en charge SMB 3.0, vous pouvez implémenter une configuration de BranchCache sur le serveur CIFS, qui prend en charge la mise en cache de BranchCache 1 et BranchCache 2.



Même si la fonctionnalité de BranchCache de Microsoft prend en charge l'utilisation des protocoles HTTP/HTTPS et SMB comme protocoles d'accès aux fichiers, ONTAP BranchCache ne prend en charge que SMB.

Configuration requise pour la version des hôtes ONTAP et Windows

Avant de configurer BranchCache, les hôtes Windows du ONTAP et des succursales doivent répondre à certaines exigences de version.

Avant de configurer BranchCache, vous devez vérifier que la version de ONTAP est compatible avec le cluster et les clients des succursales participantes et prennent en charge SMB 2.1 ou version ultérieure, et prend en charge la fonctionnalité BranchCache. Si vous configurez le mode cache hébergé, vous devez également vous assurer que vous utilisez un hôte pris en charge pour le serveur de cache.

BranchCache 1 est pris en charge sur les versions ONTAP et hôtes Windows suivantes :

- Serveur de contenu : serveur virtuel de stockage (SVM) avec ONTAP
- Serveur de cache : Windows Server 2008 R2 ou Windows Server 2012 ou version ultérieure
- Poste ou client : Windows 7 Enterprise, Windows 7 Édition intégrale, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 ou version ultérieure

BranchCache 2 est pris en charge sur les versions ONTAP et les hôtes Windows suivants :

- Serveur de contenu : SVM avec ONTAP
- Serveur de cache : Windows Server 2012 ou version ultérieure
- Poste ou client : Windows 8 ou Windows Server 2012 ou version ultérieure

Les raisons pour lesquelles ONTAP invalide des hachages de BranchCache

Pour planifier votre configuration de BranchCache, ONTAP permet de déterminer les raisons pour lesquelles des hachages sont validés. Elle vous aide à choisir le mode de fonctionnement à configurer et à choisir les partages qui permettent d'activer BranchCache.

ONTAP doit gérer BranchCache pour vérifier que des hachages sont valides. Si un hachage n'est pas valide, ONTAP invalide le hachage et calcule un nouveau hachage la prochaine fois que le contenu est demandé, en supposant que BranchCache est toujours activé.

Des hachages de ONTAP valident les données pour les raisons suivantes :

- La clé de serveur est modifiée.

Si la clé du serveur est modifiée, ONTAP invalide tous les hachages du magasin de hachage.

- Le hachage est transféré depuis le cache, car la taille maximale du magasin de hachage de BranchCache a été atteinte.

Il s'agit d'un paramètre ajustable et peut être modifié pour répondre à vos exigences métier.

- Un fichier est modifié via un accès SMB ou NFS.
- Un fichier pour lequel des hachages sont calculés est restauré à l'aide de l' `snap restore` commande.
- Un volume qui contient des partages SMB qui sont activés pour BranchCache est restauré à l'aide du `snap restore` commande.

Directives pour choisir l'emplacement du magasin de hachage

Lors de la configuration de BranchCache, vous pouvez choisir l'emplacement de stockage des hachages et la taille du magasin de hachage. Comprendre les instructions à suivre lors du choix de l'emplacement et de la taille du magasin de hachage peut vous aider à planifier la configuration de BranchCache sur un SVM compatible CIFS.

- Vous devez localiser le magasin de hachage sur un volume où les mises à jour atime sont autorisées.

Le temps d'accès sur un fichier de hachage est utilisé pour conserver les fichiers fréquemment utilisés dans le magasin de hachage. Si les mises à jour atime sont désactivées, l'heure de création est utilisée à cette fin. Il est préférable d'utiliser atime pour suivre les fichiers fréquemment utilisés.

- Vous ne pouvez pas stocker des hachages sur des systèmes de fichiers en lecture seule, tels que les destinations SnapMirror et les volumes SnapLock.
- Si la taille maximale du magasin de hachage est atteinte, des hachages plus anciens sont vidés pour faire de la place à de nouveaux hachages.

Vous pouvez augmenter la taille maximale du magasin de hachage pour réduire la quantité de hachages vidés du cache.

- Si le volume sur lequel vous stockez des hachages est indisponible ou saturé, ou si une communication interne au cluster pose un problème, là où le service de BranchCache ne peut pas récupérer les informations de hachage, les services de BranchCache ne sont pas disponibles.

Le volume peut être indisponible parce qu'il est hors ligne ou parce que l'administrateur du stockage a spécifié un nouvel emplacement pour le magasin de hachage.

Cela ne cause pas de problèmes d'accès aux fichiers. Si l'accès au magasin de hachage est entravé, ONTAP renvoie une erreur définie par Microsoft au client, ce qui entraîne la demande du client concernant le fichier à l'aide de la requête de lecture SMB normale.

Informations associées

[Configurez BranchCache sur le serveur SMB](#)

[Modifier la configuration de BranchCache](#)

Recommandations de BranchCache

Avant de configurer BranchCache, il est important de tenir compte de certaines recommandations lorsque vous décidez des partages SMB que vous souhaitez activer la mise en cache de BranchCache.

Veillez à respecter les recommandations suivantes lorsque vous décidez du mode d'exploitation à utiliser et

des partages SMB pour activer BranchCache :

- Grâce à la mise en cache à distance des données, BranchCache est moins bénéfique.
- Les services de BranchCache sont avantageux pour les partages contenant du contenu de fichier, réutilisé par plusieurs clients distants ou par du contenu de fichier accessible de manière répétée par un seul utilisateur distant.
- Prenez l'activation de la mise en cache pour du contenu en lecture seule, tel que les données de copies Snapshot et de destinations SnapMirror.

Configurer BranchCache

Configurer la présentation de BranchCache

Vous pouvez configurer BranchCache sur votre serveur SMB à l'aide des commandes ONTAP. Pour implémenter BranchCache, vous devez également configurer vos clients et, éventuellement, vos serveurs de cache hébergés dans les succursales où vous souhaitez mettre en cache le contenu.

Si vous configurez BranchCache pour permettre la mise en cache partage par partage, vous devez activer BranchCache sur les partages SMB pour lesquels vous souhaitez fournir des services de mise en cache de BranchCache.

Configuration requise pour la configuration de BranchCache

Une fois que vous avez atteint certains prérequis, vous pouvez configurer BranchCache.

Les exigences suivantes doivent être respectées avant de configurer BranchCache sur le serveur CIFS pour le SVM :

- ONTAP doit être installé sur tous les nœuds du cluster.
- CIFS doit être sous licence et un serveur SMB doit être configuré. La licence SMB est incluse avec "ONTAP One". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.
- La connectivité réseau IPv4 ou IPv6 doit être configurée.
- Pour BranchCache 1, SMB 2.1 ou version ultérieure doit être activé.
- Pour BranchCache 2, SMB 3.0 doit être activé et les clients Windows distants doivent prendre en charge BranchCache 2.

Configurez BranchCache sur le serveur SMB

Vous pouvez configurer BranchCache pour fournir des services de BranchCache sur la base de chaque partage. Vous pouvez également configurer BranchCache pour activer automatiquement la mise en cache sur tous les partages SMB.

Description de la tâche

Vous pouvez configurer BranchCache sur des SVM.

- Vous pouvez créer une configuration de BranchCache pour tous les partages si vous souhaitez proposer des services de mise en cache pour tout le contenu contenu contenu contenu contenu dans tous les partages SMB sur le serveur CIFS.

- Vous pouvez créer une configuration de BranchCache par partage si vous souhaitez proposer des services de mise en cache pour le contenu contenu contenu hébergé dans des partages SMB sélectionnés sur le serveur CIFS.

Vous devez spécifier les paramètres suivants lors de la configuration de BranchCache :

Paramètres requis	Description
<i>Nom du SVM</i>	BranchCache est configuré pour chaque SVM. Vous devez spécifier sur quel SVM compatible CIFS vous souhaitez configurer le service de BranchCache.
<i>Chemin vers magasin de hachage</i>	<p>Les hachages de BranchCache sont stockés dans des fichiers réguliers sur le volume du SVM. Vous devez spécifier le chemin d'accès à un répertoire existant dans lequel ONTAP doit stocker les données de hachage. le chemin de hachage BranchCache doit être accessible en lecture-écriture. Les chemins en lecture seule, tels que les répertoires Snapshot, ne sont pas autorisés. Vous pouvez stocker les données de hachage dans un volume contenant d'autres données ou créer un volume distinct pour stocker les données de hachage.</p> <p>Si le SVM est une source de reprise d'activité du SVM, le chemin de hachage ne peut pas se trouver sur le volume root. En effet, le volume racine n'est pas répliqué vers la destination de reprise après incident.</p> <p>Le chemin de hachage peut contenir des blancs et des caractères de nom de fichier valides.</p>

Vous pouvez éventuellement spécifier les paramètres suivants :

Paramètres facultatifs	Description
<i>Versions prises en charge</i>	ONTAP prend en charge BranchCache 1 et 2. Vous pouvez activer la version 1, la version 2 ou les deux versions. La valeur par défaut est d'activer les deux versions.

Paramètres facultatifs	Description
<i>Taille maximale du magasin de hachage</i>	Vous pouvez spécifier la taille à utiliser pour le magasin de données de hachage. Si les données de hachage dépassent cette valeur, ONTAP supprime des hachages plus anciens pour faire de la place à des hachages plus récents. La taille par défaut du magasin de hachage est de 1 Go. BranchCache fonctionne plus efficacement si des hachages ne sont pas éliminés de manière trop agressive. Si vous déterminez que les hachages sont fréquemment ignorés car le magasin de hachage est plein, vous pouvez augmenter la taille du magasin de hachage en modifiant la configuration de BranchCache.
<i>Clé du serveur</i>	Vous pouvez spécifier une clé de serveur utilisée par le service BranchCache pour empêcher les clients d'imiter le serveur BranchCache. Si vous ne spécifiez pas de clé de serveur, une clé est générée de manière aléatoire lors de la création de la configuration de BranchCache. Vous pouvez définir la clé du serveur à une valeur spécifique. Ainsi, si plusieurs serveurs fournissent des données de BranchCache pour les mêmes fichiers, les clients peuvent utiliser des hachages à partir de n'importe quel serveur à l'aide de la même clé de serveur. Si la clé du serveur contient des espaces, vous devez inclure la clé du serveur entre guillemets.
<i>Mode de fonctionnement</i>	<p>Par défaut, BranchCache est activé par partage.</p> <ul style="list-style-type: none"> • Pour créer une configuration de BranchCache dans laquelle vous activez BranchCache par partage, vous pouvez soit spécifier ce paramètre facultatif, soit <code>per-share</code>. • Pour activer automatiquement BranchCache sur tous les partages, vous devez définir le mode de fonctionnement sur <code>all-shares</code>.

Étapes

1. SMB 2.1 et 3.0 si nécessaire :

- Définissez le niveau de privilège sur avancé : `set -privilege advanced`
- Vérifier les paramètres du SVM SMB configurés pour déterminer si toutes les versions nécessaires de SMB sont activées : `vserver cifs options show -vserver vserver_name`
- Si nécessaire, activez SMB 2.1 : `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

La commande active SMB 2.0 et SMB 2.1.

- Si nécessaire, activez SMB 3.0 : `vserver cifs options modify -vserver vserver_name`

```
-smb3-enabled true
```

e. Retour au niveau de privilège admin : `set -privilege admin`

2. Configurer BranchCache : `vserver cifs branchcache create -vserver vserver_name -hash -store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all}] [-server-key text] -operating-mode {per-share|all-shares}`

Le chemin de stockage de hachage spécifié doit exister et doit résider sur un volume géré par la SVM. Le chemin doit également être situé sur un volume accessible en lecture-écriture. La commande échoue si le chemin d'accès est en lecture seule ou n'existe pas.

Si vous souhaitez utiliser la même clé de serveur pour d'autres configurations de BranchCache du SVM, enregistrez la valeur que vous entrez pour la clé du serveur. La clé du serveur n'apparaît pas lorsque vous affichez des informations sur la configuration de BranchCache.

3. Vérifiez que la configuration de BranchCache est correcte : `vserver cifs branchcache show -vserver vserver_name`

Exemples

Les commandes suivantes vérifient que SMB 2.1 et 3.0 sont activées et configurent BranchCache pour activer automatiquement la mise en cache sur tous les partages SMB sur le SVM vs1 :

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1:*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1:*> set -privilege admin

cluster1:> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1:> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares

```

Les commandes suivantes vérifient que SMB 2.1 et 3.0 sont activées, configurent BranchCache pour permettre la mise en cache par partage sur le SVM vs1 et vérifient la configuration de BranchCache :

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs options show -vsserver vs1 -fields smb2-
enabled,smb3-enabled
vsserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vsserver cifs branchcache create -vsserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vsserver cifs branchcache show -vsserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share

```

Informations associées

[Exigences et directives : prise en charge de la version de BranchCache](#)

[Où trouver des informations sur la configuration de BranchCache dans le bureau distant](#)

[Créez un partage SMB compatible BranchCache](#)

[Activez BranchCache sur un partage SMB existant](#)

[Modifier la configuration de BranchCache](#)

[Désactivez BranchCache sur les partages SMB](#)

[Supprimez la configuration de BranchCache sur les SVM](#)

Où trouver des informations sur la configuration de BranchCache dans le bureau distant

Une fois BranchCache configuré sur le serveur SMB, vous devez installer et configurer BranchCache sur les ordinateurs clients et, éventuellement, sur les serveurs de mise en cache de votre bureau distant. Microsoft fournit des instructions pour configurer BranchCache dans le bureau distant.

Les instructions de configuration des clients des succursales et, éventuellement, des serveurs de mise en cache pour utiliser BranchCache sont disponibles sur le site Web Microsoft BranchCache.

["Microsoft BranchCache Docs : nouveautés"](#)

Configurez des partages SMB compatibles avec BranchCache

Configurer les partages SMB compatibles avec BranchCache

Une fois que vous avez configuré BranchCache sur le serveur SMB et dans la succursale, vous pouvez activer BranchCache sur des partages SMB contenant du contenu que vous souhaitez autoriser les clients des succursales à mettre en cache.

La mise en cache de BranchCache peut être activée sur tous les partages SMB sur le serveur SMB ou sur la base du partage par partage.

- Si vous activez BranchCache sur le partage à partage, vous pouvez activer BranchCache pendant la création du partage ou en modifiant les partages existants.

Si vous activez la mise en cache sur un partage SMB existant, ONTAP commence des hachages de calcul et envoie des métadonnées aux clients demandant du contenu dès que vous activez BranchCache sur ce partage.

- Les clients qui disposent d'une connexion SMB existante vers un partage n'bénéficient pas de la prise en charge de BranchCache si ce partage est ensuite activé.

ONTAP annonce la prise en charge de BranchCache pour un partage au moment de la configuration de la session SMB. Les clients qui ont déjà établi des sessions lorsque BranchCache est activé doivent se déconnecter, puis se reconnecter pour utiliser le contenu mis en cache pour ce partage.



Si BranchCache sur un partage SMB est ensuite désactivé, ONTAP arrête d'envoyer les métadonnées au client demandeur. Un client qui a besoin de données l'extrait directement du serveur de contenu (serveur SMB).

Créez un partage SMB compatible BranchCache

Vous pouvez activer BranchCache sur un partage SMB lors de la création du partage en configurant le `branchcache` propriété de partage.

Description de la tâche

- Si BranchCache est activé sur le partage SMB, le partage doit disposer de la configuration des fichiers hors ligne pour la mise en cache manuelle.

Il s'agit du paramètre par défaut lorsque vous créez un partage.

- Vous pouvez également spécifier d'autres paramètres de partage facultatifs lorsque vous créez le partage avec BranchCache.
- Vous pouvez définir le `branchcache` Propriété sur un partage, même si BranchCache n'est pas configuré et activé sur le serveur virtuel de stockage (SVM).

Toutefois, si vous souhaitez que le partage offre du contenu en cache, vous devez configurer et activer BranchCache sur le SVM.

- Puisqu'aucune propriété de partage par défaut n'est appliquée au partage lorsque vous utilisez le `-share -properties` paramètre, vous devez spécifier toutes les autres propriétés de partage que vous souhaitez appliquer au partage en plus de `branchcache` partager la propriété à l'aide d'une liste délimitée par des virgules.
- Pour plus d'informations, consultez la page de manuel du `vserver cifs share create` commande.

Étape

1. Création d'un partage SMB compatible avec BranchCache :

```
vserver cifs share create -vserver vserver_name -share-name share_name -path
path -share-properties branchcache[,...]
```

2. Vérifiez que la propriété de partage BranchCache est définie sur le partage SMB à l'aide du `vserver cifs share show` commande.

Exemple

La commande suivante crée un partage SMB avec fonction de BranchCache nommé « data » avec le chemin d'accès de `/data` Sur la SVM `vs1`. Par défaut, le paramètre `fichiers hors ligne` est défini sur `manual`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
      Vserver: vs1
      Share: data
CIFS Server NetBIOS Name: VS1
      Path: /data
      Share Properties: branchcache
                       oplocks
                       browsable
                       changenotify
      Symlink Properties: enable
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
      Share Comment: -
      Share ACL: Everyone / Full Control
      File Attribute Cache Lifetime: -
      Volume Name: data
      Offline Files: manual
      Vscan File-Operations Profile: standard
```

Informations associées

[Désactivation de BranchCache sur un partage SMB unique](#)

Activez BranchCache sur un partage SMB existant

Vous pouvez activer BranchCache sur un partage SMB existant en ajoutant le `branchcache` partager la propriété dans la liste existante des propriétés de partage.

Description de la tâche

- Si BranchCache est activé sur le partage SMB, le partage doit disposer de la configuration des fichiers hors ligne pour la mise en cache manuelle.

Si le paramètre fichiers hors ligne du partage existant n'est pas défini sur mise en cache manuelle, vous devez le configurer en modifiant le partage.

- Vous pouvez définir le `branchcache` Propriété sur un partage, même si BranchCache n'est pas configuré et activé sur le serveur virtuel de stockage (SVM).

Toutefois, si vous souhaitez que le partage offre du contenu en cache, vous devez configurer et activer BranchCache sur le SVM.

- Lorsque vous ajoutez le `branchcache` la propriété de partage sur le partage, les paramètres de partage existants et les propriétés de partage sont conservés.

La propriété de partage BranchCache est ajoutée à la liste existante des propriétés de partage. Pour plus d'informations sur l'utilisation du `vserver cifs share properties add` commandes, consultez les pages de manuels.

Étapes

1. Si nécessaire, configurez le paramètre de partage de fichiers hors ligne pour la mise en cache manuelle :
 - a. Déterminez ce que le paramètre de partage de fichiers hors ligne est défini à l'aide de l' `vserver cifs share show` commande.
 - b. Si le paramètre de partage de fichiers hors ligne n'est pas défini sur manuel, remplacez-le par la valeur `requis` : `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. Activer BranchCache sur un partage SMB existant : `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Vérifiez que la propriété de partage BranchCache est définie sur le partage SMB : `vserver cifs share show -vserver vserver_name -share-name share_name`

Exemple

La commande suivante permet d'activer BranchCache sur un partage SMB existant nommé « data2 » avec le chemin d'accès de `/data2` Sur la SVM vs1 :


```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

        Vservice: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     showsnapshot
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
        Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vservice cifs share properties add -vservice vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

        Vservice: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     showsnapshot
                     changenotify
                     branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
        Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

Gestion et surveillance de la configuration de BranchCache

Modifier les configurations de BranchCache

Vous pouvez modifier la configuration du service de BranchCache sur les SVM, notamment la modification du chemin du répertoire du magasin de hachage, la taille maximale du répertoire, le mode de fonctionnement et les versions de BranchCache prises en charge. Vous pouvez également augmenter la taille du volume contenant le magasin de hachage.

Étapes

1. Effectuez l'action appropriée :

Les fonctions que vous recherchez...	Entrez les informations suivantes...
Modifier la taille du répertoire du magasin de hachage	`vserver cifs branchcache modify -vserver vservice_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
Augmentez la taille du volume contenant le magasin de hachage	`volume size -vserver vservice_name -volume volume_name -new-size new_size[k
m	g
t]` Si le volume contenant le magasin de hachage se remplit, vous pourrez peut-être augmenter la taille du volume. Vous pouvez spécifier la nouvelle taille du volume comme un nombre suivi d'une désignation d'unité.	Modifiez le chemin du répertoire du magasin de hachage
En savoir plus sur " Gestion des volumes FlexVol "	

Les fonctions que vous recherchez...	Entrez les informations suivantes...
<pre>`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true</pre>	<p>false}` Si le SVM est une source de reprise d'activité du SVM, le chemin de hachage ne peut pas se trouver sur le volume root. En effet, le volume racine n'est pas répliqué vers la destination de reprise après incident.</p> <p>Le chemin de hachage BranchCache peut contenir des blancs et des caractères de nom de fichier valides.</p> <p>Si vous modifiez le chemin de hachage, <code>-flush -hashes</code> Est un paramètre requis qui spécifie si vous souhaitez que ONTAP affleure les hachages à partir de l'emplacement de magasin de hachage d'origine. Vous pouvez définir les valeurs suivantes pour le <code>-flush-hashes</code> paramètre :</p> <p>Si vous spécifiez <code>true</code>, ONTAP supprime les hachages dans l'emplacement d'origine et crée de nouveaux hachages à l'emplacement du nouveau, car les nouvelles demandes sont effectuées par des clients compatibles BranchCache.</p> <p>Si vous spécifiez <code>false</code>, les hachages ne sont pas vidés.</p> <p>+</p> <p>Dans ce cas, vous pouvez choisir de réutiliser les hachages existants ultérieurement en retrouvant le chemin du magasin de hachage à l'emplacement d'origine.</p>
Changer le mode de fonctionnement	<pre>`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share</pre>
all-shares	<pre>disable}`</pre> <p>Lors de la modification du mode de fonctionnement, vous devez connaître les éléments suivants :</p> <p>ONTAP annonce la prise en charge de BranchCache pour un partage lors de la configuration de la session SMB.</p> <p>Les clients qui ont déjà établi des sessions lorsque BranchCache est activé doivent se déconnecter, puis se reconnecter pour utiliser le contenu mis en cache pour ce partage.</p>
Modifier la prise en charge de BranchCache	<pre>`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable</pre>
v2-enable	<pre>enable-all}`</pre>

2. Vérifiez les modifications de configuration à l'aide de la `vserver cifs branchcache show` commande.

Affiche des informations sur les configurations de BranchCache

Vous pouvez afficher des informations sur les configurations de BranchCache sur les SVM (Storage Virtual machines), qui peuvent être utilisées lors de la vérification d'une configuration ou lors de la détermination des paramètres actuels avant de modifier une configuration.

Étape

1. Effectuez l'une des opérations suivantes :

Si vous voulez afficher...	Entrez cette commande...
Récapitulatif des informations sur les configurations de BranchCache sur tous les SVM	<code>vserver cifs branchcache show</code>
Informations détaillées sur la configuration d'un SVM spécifique	<code>vserver cifs branchcache show -vserver <i>vserver_name</i></code>

Exemple

L'exemple suivant affiche des informations sur la configuration de BranchCache sur le SVM vs1 :

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Changer la clé du serveur BranchCache

Il est possible de modifier la clé du serveur de BranchCache en modifiant la configuration de BranchCache sur le serveur virtuel de stockage (SVM) et en indiquant une clé de serveur différente.

Description de la tâche

Vous pouvez définir la clé du serveur à une valeur spécifique. Ainsi, si plusieurs serveurs fournissent des données de BranchCache pour les mêmes fichiers, les clients peuvent utiliser des hachages à partir de n'importe quel serveur à l'aide de la même clé de serveur.

Lorsque vous modifiez la clé du serveur, vous devez également vider le cache de hachage. Après avoir effectué des hachages, ONTAP crée des hachages de nouvelles demandes des clients compatibles avec BranchCache.

Étapes

1. Modifiez la clé du serveur à l'aide de la commande suivante : `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

Lors de la configuration d'une nouvelle clé de serveur, vous devez également spécifier `-flush-hashes` et définissez la valeur sur `true`.

2. Vérifiez que la configuration de BranchCache est correcte à l'aide du `vserver cifs branchcache show` commande.

Exemple

L'exemple suivant définit une nouvelle clé de serveur qui contient des espaces et purge le cache de hachage sur la SVM vs1 :

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true
```

```
cluster1::> vserver cifs branchcache show -vserver vs1
```

```

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Informations associées

[Les raisons pour lesquelles ONTAP invalide des hachages de BranchCache](#)

Des hachages de pré-calcul de BranchCache sur des chemins spécifiés

Vous pouvez configurer le service de BranchCache pour précalculer les hachages pour un seul fichier, un répertoire ou tous les fichiers d'une structure de répertoires. Cette fonctionnalité est utile pour calculer des hachages de données dans un partage de BranchCache pendant les heures creuses.

Description de la tâche

Si vous souhaitez collecter un échantillon de données avant d'afficher les statistiques de hachage, vous devez utiliser le `statistics start` et en option `statistics stop` commandes.

- Vous devez spécifier la machine virtuelle de stockage (SVM) et le chemin d'accès sur lequel vous souhaitez précalculer les hachages.
- Vous devez également indiquer si vous voulez que des hachages soient calculés de manière récursive.
- Si vous souhaitez calculer des hachages de façon récursive, le service BranchCache traverse l'intégralité de l'arborescence du répertoire sous le chemin spécifié et calcule des hachages pour chaque objet éligible.

Étapes

1. Des hachages de pré-calcul si vous le souhaitez :

Si vous voulez précalculer des hachages sur...	Entrez la commande...
Un seul fichier ou répertoire	<pre>vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false</pre>
Récursivement sur tous les fichiers d'une structure de répertoires	<pre>vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true</pre>

2. Vérifiez que des hachages sont calculés à l'aide de l' `statistics` commande :

- Affiche les statistiques du `hashd` Objet sur l'instance SVM souhaitée : `statistics show -object hashd -instance vserver_name`
- Vérifiez que le nombre de hachages créés augmente en répétant la commande.

Exemples

L'exemple suivant crée des hachages sur le chemin d'accès `/data` Et sur tous les fichiers et sous-répertoires contenus dans la SVM `vs1` :

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true
```

```
cluster1::> statistics show -object hashd -instance vs1
```

Object: hashd

Instance: vs1

Start-time: 9/6/2012 19:09:54

End-time: 9/6/2012 19:11:15

Cluster: cluster1

Counter	Value
branchcache_hash_created	85
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

```
cluster1::> statistics show -object hashd -instance vs1
```

Object: hashd

Instance: vs1

Start-time: 9/6/2012 19:09:54

End-time: 9/6/2012 19:11:15

Cluster: cluster1

Counter	Value
branchcache_hash_created	92
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

Informations associées

["Configuration du contrôle des performances"](#)

Des hachages à plat du magasin de hachage SVM BranchCache

Vous pouvez vider toutes les hachages en cache du magasin de hachage BranchCache sur la machine virtuelle de stockage (SVM). Cette fonction est utile si vous avez modifié la configuration de BranchCache du bureau de succursale. Par exemple, si vous avez récemment reconfiguré le mode de mise en cache de la mise en cache distribuée au mode de mise en cache hébergée, vous devrez vider le magasin de hachage.

Description de la tâche

Après avoir effectué des hachages, ONTAP crée des hachages de nouvelles demandes des clients compatibles avec BranchCache.

Étape

1. Rincez les hachages à partir du magasin de hachage BranchCache : `vserver cifs branchcache hash-flush -vserver vserver_name`

`vserver cifs branchcache hash-flush -vserver vs1`

Afficher les statistiques de BranchCache

Vous pouvez afficher des statistiques de BranchCache, notamment, afin d'identifier le niveau de mise en cache efficace, déterminer si votre configuration fournit du contenu mis en cache aux clients et déterminer si les fichiers de hachage ont été supprimés pour prendre de l'espace pour les données de hachage les plus récentes.

Description de la tâche

Le `hashd` L'objet statistique contient des compteurs qui fournissent des informations statistiques sur les hachages de BranchCache. Le `cifs` L'objet statistique contient des compteurs qui fournissent des informations statistiques sur l'activité liée à BranchCache. Vous pouvez collecter et afficher les informations relatives à ces objets au niveau de privilège avancé.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by support personnel.  
Do you want to continue? {y|n}: y
```

2. Afficher les compteurs liés à BranchCache à l'aide du `statistics catalog counter show` commande.

Pour plus d'informations sur les compteurs de statistiques, reportez-vous à la page man de cette commande.

```
cluster1::*> statistics catalog counter show -object hashd
```


Object: hashd

Counter	Description

branchcache_hash_created	Number of times a request to generate BranchCache hash for a file succeeded.
branchcache_hash_files_replaced	Number of times a BranchCache hash file was deleted to make room for more recent hash data. This happens if the hash store size is exceeded.
branchcache_hash_rejected	Number of times a request to generate BranchCache hash data failed.
branchcache_hash_store_bytes	Total number of bytes used to store hash data.
branchcache_hash_store_size	Total space used to store BranchCache hash data for the Vserver.
instance_name	Instance Name
instance_uuid	Instance UUID
node_name	System node name
node_uuid	System node id

9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs

Counter	Description

active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
avg_junction_depth	Average number of junctions crossed by SMB and SMB2 path-based commands
branchcache_hash_fetch_fail	Total number of times a request to fetch

```

hash
data failed. These are failures when
attempting to read existing hash data.
It
does not include attempts to fetch hash
data
that has not yet been generated.
branchcache_hash_fetch_ok Total number of times a request to fetch
hash
data succeeded.
branchcache_hash_sent_bytes Total number of bytes sent to clients
requesting hashes.
branchcache_missing_hash_bytes
Total number of bytes of data that had
to be
read by the client because the hash for
that
content was not available on the server.
....Output truncated....

```

3. Collectez les statistiques liées à BranchCache à l'aide du `statistics start` et `statistics stop` commandes.

```

cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11

```

4. Afficher les statistiques de BranchCache collectées à l'aide de `statistics show` commande.

```
cluster1::*> statistics show -object cifs -counter  
branchcache_hash_sent_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0

```
cluster1::*> statistics show -object cifs -counter  
branchcache_missing_hash_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0

5. Retour au niveau de privilège admin : set -privilege admin

```
cluster1::*> set -privilege admin
```

Informations associées

[Affichage des statistiques](#)

["Configuration du contrôle des performances"](#)

Prise en charge des objets de stratégie de groupe BranchCache

ONTAP BranchCache prend en charge les objets de stratégie de groupe (GPO) de

BranchCache, ce qui permet une gestion centralisée de certains paramètres de configuration de BranchCache. Deux GPO sont utilisés pour BranchCache, la publication Hash pour BranchCache et la prise en charge de la version Hash pour BranchCache.

- **Publication Hash pour BranchCache**

La publication Hash pour BranchCache de BranchCache correspond à `-operating-mode` paramètre. Lors des mises à jour de GPO, cette valeur est appliquée aux objets SVM (Storage Virtual machine) contenus dans l'unité organisationnelle à laquelle s'applique la stratégie de groupe.

- **Prise en charge de la version de hachage pour BranchCache**

La prise en charge de la version de hachage pour BranchCache correspond au `-versions` paramètre. Lors des mises à jour de GPO, cette valeur est appliquée aux objets SVM contenus dans l'unité organisationnelle à laquelle la politique de groupe s'applique.

Informations associées

[Application d'objets de stratégie de groupe aux serveurs CIFS](#)

Affiche des informations sur les objets de stratégie de groupe BranchCache

Vous pouvez afficher des informations sur la configuration GPO (Group Policy Object) du serveur CIFS pour déterminer si des GPO de BranchCache sont définis pour le domaine auquel le serveur CIFS appartient et, le cas échéant, quels sont les paramètres autorisés. Vous pouvez également déterminer si les paramètres GPO de BranchCache sont appliqués au serveur CIFS.

Description de la tâche

Bien qu'un paramètre GPO soit défini au sein du domaine auquel le serveur CIFS appartient, il n'est pas nécessairement appliqué à l'unité organisationnelle contenant la machine virtuelle de stockage (SVM) compatible CIFS. Le paramètre GPO appliqué est le sous-ensemble de tous les GPO définis qui sont appliqués à la SVM compatible CIFS. Les paramètres BranchCache appliqués via les GPO remplacent les paramètres appliqués via l'interface CLI.

Étapes

1. Affichez le paramètre GPO de BranchCache défini pour le domaine Active Directory à l'aide du `vserver cifs group-policy show-defined` commande.



Cet exemple n'affiche pas tous les champs de sortie disponibles pour la commande. La sortie est tronquée.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
    GPO Name: Default Domain Policy
```

```
    Level: Domain
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

```
    GPO Name: Resultant Set of Policy
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication for Mode BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

2. Affichez le paramètre GPO de BranchCache appliqué au serveur CIFS à l'aide de `vserver cifs group-policy show-applied` commande. ``



Cet exemple n'affiche pas tous les champs de sortie disponibles pour la commande. La sortie est tronquée.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
    GPO Name: Default Domain Policy
```

```
        Level: Domain
```

```
        Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

```
    GPO Name: Resultant Set of Policy
```

```
        Level: RSOP
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

Informations associées

[Activation ou désactivation de la prise en charge de GPO sur un serveur CIFS](#)

Désactiver BranchCache sur les partages SMB

Désactivez BranchCache sur les partages SMB

Si vous ne souhaitez pas fournir de services de mise en cache de BranchCache sur certains partages SMB, mais que vous pouvez ensuite fournir des services de mise en cache, vous pouvez désactiver BranchCache sur le partage à partager. Si BranchCache est configuré pour assurer la mise en cache sur tous les partages, mais que vous souhaitez désactiver temporairement tous les services de mise en cache, vous pouvez modifier la configuration de BranchCache afin d'arrêter la mise en cache automatique sur tous les partages.

Si BranchCache sur un partage SMB est ensuite désactivé après son activation, ONTAP arrête d'envoyer les métadonnées au client qui demande. Client qui a besoin de données la récupère directement depuis le serveur

de contenu (serveur CIFS sur la machine virtuelle de stockage (SVM)).

Informations associées

[Configuration de partages SMB compatibles avec BranchCache](#)

Désactivez BranchCache sur un partage SMB unique

Si vous ne souhaitez pas offrir de services de mise en cache sur certains partages qui proposaient déjà du contenu en cache, vous pouvez désactiver BranchCache sur un partage SMB existant.

Étape

1. Saisissez la commande suivante : `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

La propriété de partage BranchCache est supprimée. Les autres propriétés de partage appliquées restent en vigueur.

Exemple

La commande suivante désactive BranchCache sur un partage SMB existant nommé « data2 » :

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

        Vservice: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
                     branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vservice cifs share properties remove -vservice vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

        Vservice: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```


Arrêt de la mise en cache automatique sur tous les partages SMB

Si votre configuration de BranchCache permet automatiquement la mise en cache de tous les partages SMB sur chaque serveur virtuel de stockage (SVM), vous pouvez modifier la configuration de BranchCache afin d'arrêter automatiquement la mise en cache du contenu pour tous les partages SMB.

Description de la tâche

Pour arrêter la mise en cache automatique sur tous les partages SMB, il est possible de basculer le mode d'exploitation de BranchCache vers la mise en cache par partage.

Étapes

1. Configurer BranchCache pour arrêter la mise en cache automatique sur tous les partages SMB : `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Vérifiez que la configuration de BranchCache est correcte : `vserver cifs branchcache show -vserver vserver_name`

Exemple

La commande suivante modifie la configuration de BranchCache sur le serveur de stockage virtuel (SVM, précédemment appelé vServer) vs1 pour arrêter la mise en cache automatique sur tous les partages SMB :

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Désactivation ou activation de BranchCache sur le SVM

Que se passe-t-il lorsque vous désactivez ou réactivez BranchCache sur le serveur CIFS

Si vous avez déjà configuré BranchCache, mais que vous ne souhaitez pas que les clients des succursales utilisent le contenu en cache, vous pouvez désactiver la mise en cache sur le serveur CIFS. Vous devez savoir ce qui se passe lorsque vous désactivez BranchCache.


Lorsque vous désactivez BranchCache, ONTAP ne calcule plus de hachages et n'envoie plus les métadonnées au client qui demande. Toutefois, l'accès aux fichiers n'est pas interrompu. Par la suite, lorsque des clients compatibles avec BranchCache demandent des informations de métadonnées pour le contenu auquel ils doivent accéder, ONTAP répond par une erreur définie par Microsoft, ce qui entraîne l'envoi d'une seconde demande par le client, demandant le contenu réel. En réponse à la demande de contenu, le serveur CIFS envoie le contenu réel stocké sur la machine virtuelle de stockage (SVM).

Une fois que BranchCache est désactivé sur le serveur CIFS, les partages SMB n'annoncent pas les fonctionnalités de BranchCache. Pour accéder aux données lors de nouvelles connexions SMB, les clients font des requêtes SMB en lecture standard.

Vous pouvez réactiver BranchCache sur le serveur CIFS à tout moment.

- Comme le magasin de hachage n'est pas supprimé lorsque vous désactivez BranchCache, ONTAP peut utiliser les hachages stockés pour répondre aux demandes de hachage après la réactivation de BranchCache, à condition que le hachage demandé soit toujours valide.
- Tout client qui a établi des connexions SMB vers des partages compatibles avec BranchCache au cours de la désactivation de BranchCache n'est pas pris en charge si BranchCache est ensuite réactivé.

En effet, ONTAP annonce la prise en charge de BranchCache pour un partage au moment de la configuration de la session SMB. Les clients qui ont établi des sessions vers des partages compatibles BranchCache alors que ce dernier était désactivé doivent se déconnecter et se reconnecter pour utiliser le contenu en cache pour ce partage.



Si vous ne souhaitez pas enregistrer le magasin de hachage après avoir désactivé BranchCache sur un serveur CIFS, vous pouvez le supprimer manuellement. Si vous réactivez BranchCache, vous devez vous assurer que le répertoire du magasin de hachage existe. Une fois que BranchCache est activé à nouveau, les partages compatibles avec BranchCache publient des fonctionnalités de BranchCache. ONTAP crée de nouvelles hachages lorsque de nouvelles demandes sont faites par des clients compatibles avec BranchCache.

Désactiver ou activer BranchCache

Vous pouvez désactiver BranchCache sur le serveur virtuel de stockage (SVM) en changeant le mode d'exploitation BranchCache en disabled. Vous pouvez activer BranchCache à tout moment en modifiant le mode d'exploitation afin d'offrir soit des services de BranchCache par partage, soit automatiquement pour tous les partages.

Étapes

1. Exécutez la commande appropriée :

Les fonctions que vous recherchez...	Puis entrez les informations suivantes...
Désactivez BranchCache	<code>vserver cifs branchcache modify -vserver vserver_name -operating-mode disable</code>
Activez BranchCache par partage	<code>vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share</code>
Activez BranchCache pour tous les partages	<code>vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares</code>

2. Vérifiez que le mode de fonctionnement de BranchCache est configuré avec le paramètre souhaité :

```
vserver cifs branchcache show -vserver vserver_name
```

Exemple

L'exemple suivant désactive BranchCache sur le SVM vs1 :

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

Supprimez la configuration de BranchCache sur les SVM

Que se passe-t-il lorsque vous supprimez la configuration de BranchCache

Si vous avez déjà configuré BranchCache, mais que vous ne souhaitez pas que le serveur de stockage virtuel (SVM) puisse continuer à fournir du contenu en cache, vous pouvez supprimer la configuration de BranchCache sur le serveur CIFS. Vous devez connaître ce qui se passe lorsque vous supprimez la configuration.

Lorsque vous supprimez la configuration, ONTAP supprime du cluster les informations de configuration du SVM et arrête le service de BranchCache. Vous pouvez choisir si ONTAP doit supprimer le magasin de hachage sur la SVM.

La suppression de la configuration de BranchCache n'interrompt pas l'accès des clients compatibles avec BranchCache. Par la suite, lorsque les clients compatibles avec BranchCache demandent des informations de métadonnées sur les connexions SMB existantes pour du contenu déjà mis en cache, ONTAP répond par une erreur définie par Microsoft, ce qui entraîne l'envoi par le client d'une seconde demande, demandant le contenu réel. En réponse à la demande de contenu, le serveur CIFS envoie le contenu réel stocké sur le SVM.

Une fois la configuration de BranchCache supprimée, les partages SMB n'annoncent pas les fonctionnalités de BranchCache. Pour accéder au contenu qui n'avait pas encore été mis en cache par de nouvelles connexions SMB, les clients effectuent des requêtes SMB en lecture standard.

Supprimez la configuration de BranchCache

La commande que vous utilisez pour supprimer le service de BranchCache sur le serveur de stockage virtuel (SVM) diffère selon que vous souhaitez supprimer ou conserver des hachages existants.

Étape

1. Exécutez la commande appropriée :

Les fonctions que vous recherchez...	Puis entrez les informations suivantes...
Supprimez la configuration de BranchCache et supprimez des hachages existants	<code>vserver cifs branchcache delete -vserver vserver_name -flush-hashes true</code>
Supprimez la configuration de BranchCache, mais conservez des hachages existants	<code>vserver cifs branchcache delete -vserver vserver_name -flush-hashes false</code>

Exemple

L'exemple suivant supprime la configuration de BranchCache sur le SVM vs1 et supprime toutes les hachages existants :

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes  
true
```

Utilisation de BranchCache lors du rétablissement

Il est important de comprendre ce qui se passe lorsque vous restaurez ONTAP vers une version qui ne prend pas en charge BranchCache.

- Lorsque vous restaurez vers une version d'ONTAP qui ne prend pas en charge BranchCache, les partages SMB n'publient pas de fonctionnalités de BranchCache pour les clients compatibles avec BranchCache. Ainsi, les clients ne demandent pas d'informations de hachage.

À la place, ils demandent le véritable contenu à l'aide de demandes de lecture SMB normales. En réponse à la demande de contenu, le serveur SMB envoie le contenu réel qui est stocké sur la machine virtuelle de stockage (SVM).

- Lorsqu'un nœud qui héberge un magasin de hachage est rétabli dans une version qui ne prend pas en charge BranchCache, l'administrateur du stockage doit restaurer manuellement la configuration de BranchCache à l'aide d'une commande imprimée pendant la restauration.

Cette commande supprime la configuration de BranchCache et des hachages.

Une fois la restauration terminée, l'administrateur du stockage peut supprimer manuellement le répertoire qui contient le magasin de hachage si nécessaire.

Informations associées

[Suppression de la configuration de BranchCache sur les SVM](#)

Améliorez les performances de la copie à distance Microsoft

Améliorer les performances de copie à distance Microsoft

Microsoft Offloaded Data Transfer (ODX), également appelé *copy Offload*, permet le transfert direct de données au sein d'un périphérique de stockage compatible ou entre ces périphériques, sans transférer les données via l'ordinateur hôte.

ONTAP prend en charge ODX à la fois pour les protocoles SMB et SAN. La source peut être un serveur CIFS ou une LUN et la destination peut être un serveur CIFS ou une LUN.

Dans les transferts de fichiers non ODX, les données sont lues à partir de la source et transférées sur le réseau vers l'ordinateur client. L'ordinateur client transfère les données via le réseau vers la destination. En résumé, l'ordinateur client lit les données à partir de la source et les écrit vers la destination. Grâce aux transferts de fichiers ODX, les données sont copiées directement de la source vers la destination.

Les copies déchargées d'ODX étant effectuées directement entre le stockage source et le stockage de destination, les performances sont considérablement améliorées. Les avantages obtenus en termes de performances comprennent l'accélération du délai de copie entre la source et la destination, la réduction de l'utilisation des ressources (CPU, mémoire) sur le client et la réduction de l'utilisation de la bande passante E/S du réseau.

Dans les environnements SMB, cette fonctionnalité n'est disponible que lorsque le client et le serveur de stockage prennent en charge SMB 3.0 et la fonctionnalité ODX. Dans les environnements SAN, cette fonctionnalité n'est disponible que lorsque le client et le serveur de stockage prennent en charge la fonctionnalité ODX. Les ordinateurs clients qui prennent en charge ODX et où ODX est activé automatiquement et de manière transparente utilisent le transfert de fichiers déchargés lors du déplacement ou de la copie des fichiers. ODX est utilisé par glisser-déposer des fichiers via l'Explorateur Windows ou utiliser des commandes de copie de fichier en ligne de commande, ou bien si une application client génère des demandes de copie de fichiers.

Informations associées

[Amélioration des temps de réponse client en fournissant des référencements de nœuds automatiques SMB avec Auto Location](#)

["Configuration SMB pour Microsoft Hyper-V et SQL Server"](#)

Fonctionnement d'ODX

L'allègement de la charge de copies (ODX) utilise un mécanisme basé sur des jetons pour la lecture et l'écriture des données dans et entre des serveurs CIFS compatibles avec ODX. Au lieu d'acheminer les données via l'hôte, le serveur CIFS envoie un petit jeton qui représente les données au client. Le client ODX présente ce token au serveur de destination, qui peut ensuite transférer les données représentées par ce token de la source vers la destination.

Lorsqu'un client ODX apprend que le serveur CIFS prend en charge ODX, il ouvre le fichier source et demande un jeton au serveur CIFS. Après l'ouverture du fichier de destination, le client utilise le jeton pour demander au serveur de copier les données directement de la source vers la destination.

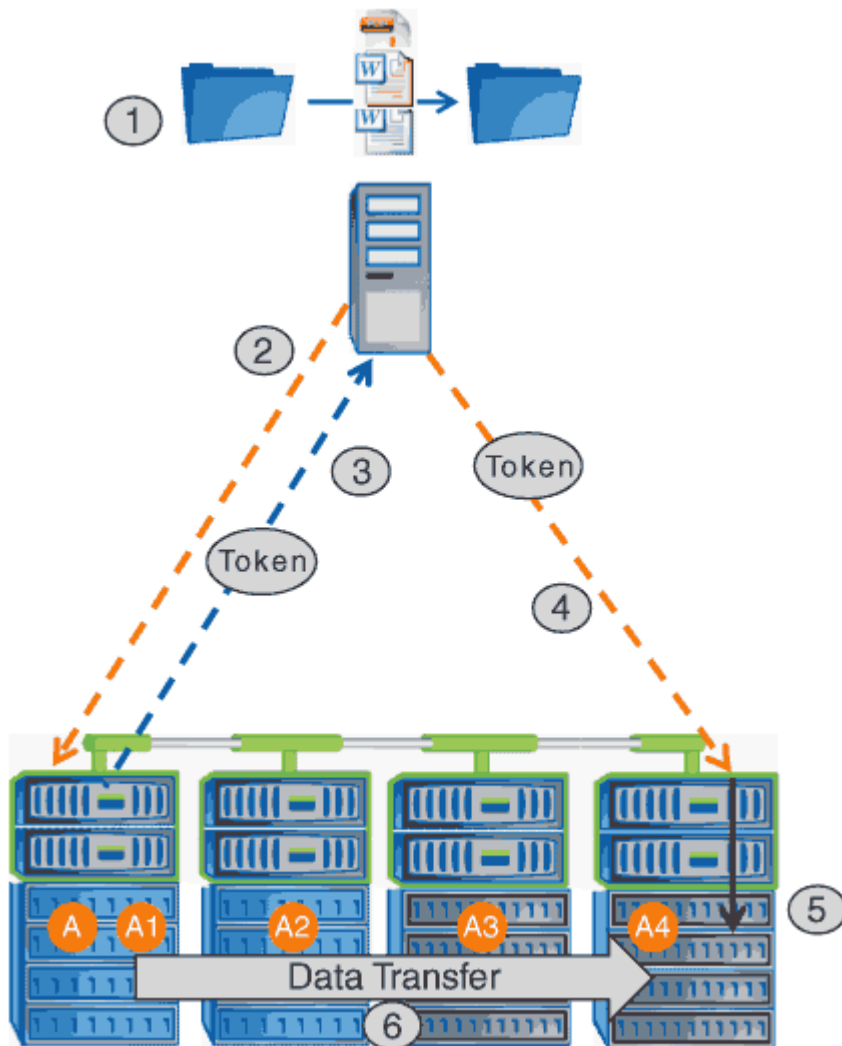


La source et la destination peuvent se trouver sur le même SVM (Storage Virtual machine) ou sur différents SVM, selon le cadre de l'opération de copie.

Ce token sert de représentation des données à un point dans le temps. Par exemple, lorsque vous copiez des données entre des emplacements de stockage, un token représentant un segment de données est renvoyé au client requérant, que le client copie vers la destination, ce qui élimine la nécessité de copier les données sous-jacentes via le client.

ONTAP prend en charge les jetons représentant 8 Mo de données. Des copies ODX de plus de 8 Mo sont effectuées à l'aide de plusieurs jetons, chaque jeton représentant 8 Mo de données.

La figure suivante décrit les étapes du processus de copie d'ODX :



1. Un utilisateur copie ou déplace un fichier à l'aide de l'Explorateur Windows, d'une interface de ligne de commande ou dans le cadre d'une migration d'un serveur virtuel, ou une application crée des copies ou des déplacements de fichiers.
2. Le client compatible ODX convertit automatiquement cette demande de transfert en requête d'ODX.

La demande ODX envoyée au serveur CIFS contient une demande de jeton.

3. Si ODX est activé sur le serveur CIFS et que la connexion est via SMB 3.0, le serveur CIFS génère un jeton, qui est une représentation logique des données sur la source.
4. Le client reçoit un jeton représentant les données et l'envoie avec la demande d'écriture au serveur CIFS de destination.

Il s'agit des seules données copiées sur le réseau de la source vers le client, puis du client vers la destination.

5. Ce jeton est fourni au sous-système de stockage.
6. La SVM effectue en interne la copie ou déplacement.

Si le fichier copié ou déplacé dépasse 8 Mo, plusieurs jetons sont nécessaires pour effectuer la copie. Les étapes 2 à 6 ont été effectuées selon les besoins pour compléter la copie.



En cas de défaillance de la copie ODX déchargée, l'opération de copie ou de déplacement retourne aux lectures et écritures traditionnelles de la copie ou du déplacement. De même, si le serveur CIFS de destination ne prend pas en charge ODX ou ODX est désactivé, l'opération de copie ou de déplacement retourne aux opérations classiques de lecture et d'écriture pour la copie ou de déplacement.

Conditions requises pour l'utilisation d'ODX

Avant de pouvoir utiliser ODX pour la réduction des déchargements de copies avec votre machine virtuelle de stockage (SVM), vous devez prendre en compte certaines exigences.

Configuration requise pour la version ONTAP

Les versions d'ONTAP prennent en charge ODX pour la réduction des copies.

Conditions requises pour la version SMB

- ONTAP prend en charge ODX avec SMB 3.0 et versions ultérieures.
- SMB 3.0 doit être activé sur le serveur CIFS pour que ODX puisse être activé :
 - L'activation d'ODX active également SMB 3.0, si elle n'est pas déjà activée.
 - La désactivation de SMB 3.0 désactive également ODX.

Configuration requise pour le serveur et le client Windows

Avant de pouvoir utiliser ODX pour la réduction des tâches de copie, le client Windows doit prendre en charge cette fonctionnalité.

Le "[Matrice d'interopérabilité NetApp](#)" Contient les informations les plus récentes sur les clients Windows pris en charge.

Besoins en termes de volume

- Les volumes source doivent être d'au moins 1.25 Go.
- Si vous utilisez des volumes compressés, le type de compression doit être adaptatif et seule la taille de groupe de compression de 8 Ko est prise en charge.

Le type de compression secondaire n'est pas pris en charge.

Instructions d'utilisation d'ODX

Avant de pouvoir utiliser ODX pour l'allègement de la charge des copies, vous devez prendre connaissance des instructions. Par exemple, vous devez connaître les types de volumes que vous pouvez utiliser ODX, et connaître les considérations d'ODX au sein du cluster et entre clusters.

Règles relatives aux volumes

- ODX ne peut pas être utilisé pour l'allègement de la charge des copies avec les configurations de volume suivantes :

- La taille du volume source est inférieure à 1.25 Go

La taille du volume doit être supérieure ou égale à 1.25 Go pour utiliser ODX.

- Volumes en lecture seule

ODX n'est pas utilisé pour les fichiers et les dossiers résidant dans des miroirs de partage de charge ou dans des volumes de destination SnapMirror ou SnapVault.

- Si le volume source n'est pas déduplicé

- Les copies ODX sont prises en charge uniquement pour les copies intra-cluster.

Vous ne pouvez pas utiliser ODX pour copier des fichiers ou des dossiers vers un volume d'un autre cluster.

Autres lignes directrices

- Dans les environnements SMB, pour utiliser ODX pour l'allègement de la charge des copies, les fichiers doivent être d'une taille supérieure ou égale à 256 Ko.

Les fichiers plus petits sont transférés à l'aide d'une opération de copie traditionnelle.

- La fonctionnalité de déchargement des copies d'ODX utilise la déduplication dans le cadre du processus de copie.

Si vous ne souhaitez pas que la déduplication s'exécute sur les volumes SVM lors de la copie ou du déplacement de données, vous devez désactiver la décharge des copies ODX sur ce SVM.

- L'application qui effectue le transfert de données doit être écrite pour prendre en charge ODX.

Les opérations applicatives prenant en charge ODX sont les suivantes :

- Les opérations de gestion Hyper-V, telles que la création et la conversion de disques durs virtuels (VHD), la gestion des copies Snapshot et la copie de fichiers entre les machines virtuelles
- Opérations de l'Explorateur Windows
- Commandes de copie Windows PowerShell
- Commandes de copie de l'invite de commande Windows

Robocopy à l'invite de commandes Windows prend en charge ODX.



Les applications doivent être exécutées sur des serveurs Windows ou des clients prenant en charge ODX.

+

Pour plus d'informations sur les applications ODX prises en charge sur les serveurs et clients Windows, consultez la bibliothèque Microsoft TechNet.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Cas d'utilisation d'ODX

Vous devez tenir compte des cas d'utilisation d'ODX sur des SVM afin de pouvoir déterminer dans quelles circonstances ODX vous fournit des avantages en matière de performances.

Par défaut, les serveurs et clients Windows qui prennent en charge ODX utilisent la fonction d'allègement de la charge des copies pour copier des données sur des serveurs distants. Si le serveur ou le client Windows ne prend pas en charge ODX, ou si l'allègement de la charge des copies ODX échoue à tout moment, l'opération de copie ou de déplacement retourne aux lectures et écritures classiques pour la copie ou le déplacement.

Les cas d'utilisation suivants prennent en charge l'utilisation de copies et de déplacements d'ODX :

- Intra-volume

Les fichiers ou LUN source et de destination se trouvent dans le même volume.

- Inter-volume, même nœud, même SVM

Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur le même nœud. Les données sont détenues par le même SVM.

- Inter-volumes, nœuds différents, même SVM

Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par le même SVM.

- Inter-SVM, même nœud

Les fichiers source et de destination ou les LUN se trouvent sur des volumes différents situés sur le même nœud. Les données sont détenues par différents SVM.

- Inter-SVM, nœuds différents

Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par différents SVM.

- Inter-cluster

Les LUN source et de destination se trouvent sur des volumes différents, sur différents nœuds, sur l'ensemble des clusters. Ceci n'est pris en charge que pour SAN et ne fonctionne pas pour CIFS.

Il existe d'autres cas d'utilisation spéciaux :

- Dans l'implémentation de ONTAP ODX, vous pouvez utiliser ODX pour copier des fichiers entre des partages SMB et des disques virtuels connectés FC ou iSCSI.

Vous pouvez utiliser Windows Explorer, l'interface de ligne de commande Windows ou PowerShell, Hyper-V ou d'autres applications prenant en charge ODX pour copier ou déplacer des fichiers de manière transparente à l'aide de l'allègement de la charge des copies ODX entre les partages SMB et les LUN connectés, à condition que les partages SMB et les LUN soient sur le même cluster.

- Hyper-V fournit des cas d'utilisation supplémentaires pour la décharge de copies ODX :

- Vous pouvez utiliser le pass-through ODX qui décharge les copies et Hyper-V pour copier des données

dans ou sur des fichiers de disque dur virtuel (VHD), ou pour copier des données entre les partages SMB mappés et les LUN iSCSI connectés au sein du même cluster.

Ainsi, des copies des systèmes d'exploitation invités peuvent être transmis au stockage sous-jacent.

- Lors de la création de VHD de taille fixe, ODX permet d'initialiser le disque avec des zéros, à l'aide d'un jeton bien connu mis à zéro.
- L'allègement de la charge des copies d'ODX est utilisé pour la migration du stockage de machines virtuelles si le stockage source et cible est situé sur le même cluster.



Pour tirer parti des cas d'utilisation liés au délestage des copies ODX par Hyper-V, le système d'exploitation invité doit prendre en charge ODX. Les disques du système d'exploitation invité doivent être des disques SCSI pris en charge par le stockage (SMB ou SAN) prenant en charge ODX. Les disques IDE du système d'exploitation invité ne prennent pas en charge le pass-through ODX.

Activer ou désactiver ODX

Vous pouvez activer ou désactiver ODX sur des SVM. Par défaut, est d'activer la prise en charge de l'allègement de la charge des copies (ODX) si SMB 3.0 est également activé.

Avant de commencer

SMB 3.0 doit être activé.

Description de la tâche

Si vous désactivez SMB 3.0, ONTAP désactive également SMB ODX. Si vous réactivez SMB 3.0, vous devez réactiver manuellement SMB ODX.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Si vous voulez que l'allègement de la charge des copies ODX soit...	Entrez la commande...
Activé	<code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled true</code>
Désactivé	<code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled false</code>

3. Retour au niveau de privilège admin : `set -privilege admin`

Exemple

L'exemple suivant active la décharge de la copie ODX sur le SVM vs1 :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

Informations associées

Options de serveur SMB disponibles

Améliorer le temps de réponse des clients en fournissant des référencements de nœuds automatiques SMB avec Auto Location

Améliorer le temps de réponse des clients en fournissant des référencements de nœuds automatiques SMB avec vue d'ensemble de l'emplacement automatique

Auto Location utilise les référencements automatiques des nœuds SMB pour augmenter les performances des clients SMB sur les machines virtuelles de stockage (SVM). Les référencements automatiques du nœud reconnectent automatiquement le client demandeur à une LIF sur le SVM du nœud qui héberge le volume dans lequel résident les données, ce qui peut améliorer les temps de réponse du client.

Lorsqu'un client SMB se connecte à un partage SMB hébergé sur le SVM, il peut se connecter à l'aide d'une LIF qui se trouve sur un nœud qui ne possède pas les données demandées. Le nœud auquel le client est connecté accède aux données détenues par un autre nœud via le réseau de cluster. Le client peut bénéficier de temps de réponse plus rapides si la connexion SMB utilise une LIF située sur le nœud contenant les données demandées :

- ONTAP fournit cette fonctionnalité à l'aide des référencements Microsoft DFS pour informer les clients SMB qu'un fichier ou dossier demandé dans l'espace de noms est hébergé quelque part.

Un nœud fait une recommandation lorsqu'il détermine qu'il existe une LIF de SVM sur le nœud qui contient les données.

- Les référencements de nœuds automatiques sont pris en charge pour les adresses IP LIF IPv4 et IPv6.
- Les renvois sont effectués en fonction de l'emplacement de la racine du partage auquel le client est connecté.
- Le renvoi se produit pendant la négociation avec les PME.

Le renvoi est effectué avant l'établissement de la connexion. Après que ONTAP désigne le client SMB au nœud cible, la connexion est établie et le client accède aux données via le chemin LIF référencé à partir de ce point. Les clients accèdent ainsi plus rapidement aux données et évitent toute communication supplémentaire avec le cluster.



Si un partage couvre plusieurs points de jonction et que certaines des jonctions sont vers les volumes contenus sur les autres nœuds, les données du partage sont réparties sur plusieurs nœuds. Étant donné que ONTAP fournit des référencements locaux à la racine du partage, ONTAP doit utiliser le réseau cluster pour récupérer les données contenues dans ces volumes non locaux. Avec ce type d'architecture de namespace, les référencements automatiques des nœuds ne peuvent pas être significatifs pour les performances.

Si le nœud qui héberge les données ne dispose pas de LIF disponible, ONTAP établit la connexion en utilisant la LIF choisie par le client. Une fois qu'un fichier est ouvert par un client SMB, il continue à accéder au fichier via la même connexion référencée.

Si, pour une raison quelconque, le serveur CIFS ne peut pas faire de recommandation, le service SMB ne subit aucune perturbation. La connexion SMB est établie comme si les référencements de nœuds automatiques n'étaient pas activés.

Informations associées

[Amélioration des performances de la copie à distance Microsoft](#)

Exigences et directives pour l'utilisation de référencements de nœuds automatiques

Avant de pouvoir utiliser les référencements de nœud automatiques SMB, également appelés *autolocalisation*, vous devez connaître certaines exigences, y compris les versions de ONTAP qui prennent en charge la fonctionnalité. Vous devez également connaître les versions du protocole SMB prises en charge et d'autres directives spéciales.

Version ONTAP et conditions requises pour les licences

- Tous les nœuds du cluster doivent exécuter une version de ONTAP qui prend en charge les référencements de nœuds automatiques.
- Les Widelinks doivent être activés sur un partage SMB pour utiliser l'autolocalisation.
- CIFS doit être sous licence et un serveur SMB doit exister sur les SVM. La licence SMB est incluse avec "ONTAP One". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.

Version requise du protocole SMB

- Pour les SVM, ONTAP prend en charge les référencements de nœuds automatiques sur toutes les versions de SMB.

Exigences des clients PME

Tous les clients Microsoft pris en charge par ONTAP prennent en charge les référencements automatiques des nœuds SMB.

La matrice d'interopérabilité contient les dernières informations sur les clients Windows pris en charge par ONTAP.

["Matrice d'interopérabilité NetApp"](#)

Configuration requise pour Data LIF

Si vous souhaitez utiliser une LIF de données comme référence potentielle pour les clients SMB, vous devez créer des LIF de données avec NFS et CIFS activés.

Les référencements de nœuds automatiques peuvent ne fonctionner que si le nœud cible contient des LIFs de données qui sont activées uniquement pour le protocole NFS ou uniquement pour le protocole SMB.

Si cette exigence n'est pas respectée, l'accès aux données n'est pas affecté. Le client SMB mappe le partage à l'aide de la LIF d'origine que le client a utilisée pour se connecter à la SVM.

Exigences d'authentification NTLM lors de la connexion SMB référencée

L'authentification NTLM doit être autorisée sur le domaine contenant le serveur CIFS et sur les domaines contenant des clients qui souhaitent utiliser des référencements de nœud automatiques.

Lors d'une recommandation, le serveur SMB renvoie une adresse IP au client Windows. Étant donné que l'authentification NTLM est utilisée lors de la connexion à l'aide d'une adresse IP, l'authentification Kerberos n'est pas réalisée pour les connexions mentionnées.

Cela se produit car le client Windows ne peut pas créer le nom principal de service utilisé par Kerberos (qui est de la forme `service/NetBIOS name` et `service/FQDN`), ce qui signifie que le client ne peut pas demander un ticket Kerberos au service.

Instructions pour l'utilisation de renvois de nœuds automatiques avec la fonction home Directory

Lorsque les partages sont configurés avec la propriété de partage de répertoire personnel activée, il peut y avoir un ou plusieurs chemins de recherche de répertoire racine configurés pour une configuration de répertoire personnel. Les chemins de recherche peuvent pointer vers les volumes contenus dans chaque nœud contenant des volumes du SVM. Les clients reçoivent une recommandation et, si une LIF de données locale active est disponible, connectez-vous via une LIF référencée qui est locale au home Directory de l'utilisateur.

Il existe des directives lorsque les clients SMB 1.0 accèdent aux home directories dynamiques avec l'activation automatique des référencements de nœuds. En effet, les clients SMB 1.0 nécessitent le renvoi automatique de nœud avant d'avoir été authentifiés, c'est-à-dire avant que le serveur SMB ait le nom de l'utilisateur. Cependant, l'accès au répertoire local SMB fonctionne correctement pour les clients SMB 1.0 si les instructions suivantes sont vraies :

- Les répertoires locaux SMB sont configurés pour utiliser des noms simples, tels que "%W" (nom d'utilisateur Windows) ou "%u" (nom d'utilisateur UNIX mappé), et non des noms de style de nom de domaine, tels que "%d\%W" (nom-domaine\nom-utilisateur).
- Lors de la création de partages de répertoires locaux CIFS, les noms de partages de répertoire racine CIFS sont configurés avec des variables ("%W" ou "%u"), et non avec des noms statiques, tels que "HOME".

Pour les clients SMB 2.x et SMB 3.0, il n'y a pas de directives spéciales lors de l'accès aux répertoires locaux en utilisant des référencements de nœuds automatiques.

Instructions relatives à la désactivation des référencements de nœuds automatiques sur les serveurs CIFS avec les connexions existantes désignées

Si vous désactivez les référencements de nœuds automatiques après l'activation de l'option, les clients actuellement connectés à une LIF référencée conservent la connexion référencée. Étant donné que ONTAP utilise les référencements DFS comme mécanisme pour les référencements automatiques des nœuds SMB,

les clients peuvent même se reconnecter au LIF référencé après que vous avez désactivé l'option jusqu'à ce que le renvoi DFS mis en cache du client pour les connexions mentionnées soit trop court. Cela est vrai même dans le cas d'une restauration vers une version de ONTAP qui ne prend pas en charge les référencements de nœuds automatiques. Les clients continuent d'utiliser les référencements jusqu'à ce que la référence DFS soit hors du cache du client.

La géolocalisation automatique utilise les référencements automatiques des nœuds SMB pour augmenter les performances des clients SMB en orientant les clients vers la LIF sur le nœud qui possède le volume de données d'un SVM. Lorsqu'un client SMB se connecte à un partage SMB hébergé sur un SVM, il peut se connecter à l'aide d'une LIF sur un nœud qui ne détient pas les données demandées et utilise un réseau d'interconnexion de cluster pour récupérer les données. Le client peut bénéficier de temps de réponse plus rapides si la connexion SMB utilise une LIF située sur le nœud contenant les données demandées.

ONTAP fournit cette fonctionnalité à l'aide des référencements DFS (système de fichiers distribués Microsoft) pour informer les clients SMB qu'un fichier ou dossier demandé dans l'espace de noms est hébergé quelque part. Un nœud fait une recommandation lorsqu'il détermine qu'il existe une LIF de SVM sur le nœud qui contient les données. Les renvois sont effectués en fonction de l'emplacement de la racine du partage auquel le client est connecté.

Le renvoi se produit pendant la négociation avec les PME. Le renvoi est effectué avant l'établissement de la connexion. Après que ONTAP désigne le client SMB au nœud cible, la connexion est établie et le client accède aux données via le chemin LIF référencé à partir de ce point. Les clients accèdent ainsi plus rapidement aux données et évitent toute communication supplémentaire avec le cluster.

Instructions pour l'utilisation de renvois de nœuds automatiques avec des clients Mac OS

Les clients Mac OS X ne prennent pas en charge les renvois de nœuds automatiques SMB, même si le système d'exploitation Mac prend en charge le système de fichiers distribué (DFS, Distributed File System) de Microsoft. Les clients Windows effectuent une demande de recommandation DFS avant de se connecter à un partage SMB. ONTAP fournit une référence à une LIF de données située sur le même nœud qui héberge les données requises, ce qui entraîne une amélioration des temps de réponse du client. Bien que le système d'exploitation Mac prend en charge DFS, les clients Mac OS ne se comportent pas exactement comme les clients Windows dans cette zone.

Informations associées

[Comment ONTAP rend possible les répertoires locaux dynamiques](#)

["Gestion du réseau"](#)

["Matrice d'interopérabilité NetApp"](#)

Prise en charge des référencements automatiques des nœuds SMB

Avant d'activer les référencements automatiques des nœuds SMB, sachez que certaines fonctionnalités ONTAP ne prennent pas en charge les référencements.

- Les types de volumes suivants ne prennent pas en charge les référencements automatiques des nœuds SMB :
 - Membres en lecture seule d'un miroir de partage de charge
 - Volume de destination d'un miroir de protection des données
- Les référencements des nœuds ne bougent pas parallèlement à un déplacement LIF.

Lorsqu'un client utilise une connexion référencée sur une connexion SMB 2.x ou SMB 3.0 et qu'une LIF de

données se déplace sans interruption, le client continue d'utiliser la même connexion référencée, même si la LIF n'est plus locale des données.

- Les référencements de nœuds ne se déplacent pas parallèlement à un déplacement des volumes.

Lorsqu'un client utilise une connexion référencée sur une connexion SMB et qu'un déplacement de volume se produit, le client continue à utiliser la même connexion référencée, même si le volume n'est plus situé sur le même nœud que la LIF de données.

Activez ou désactivez les référencements automatiques des nœuds SMB

Vous pouvez activer les référencements automatiques des nœuds SMB pour augmenter les performances d'accès des clients SMB. Vous pouvez désactiver les référencements automatiques des nœuds si vous ne souhaitez pas que ONTAP fait des référencements aux clients SMB.

Avant de commencer

Un serveur CIFS doit être configuré et exécuté sur la machine virtuelle de stockage (SVM).

Description de la tâche

La fonctionnalité de référencements automatiques des nœuds SMB est désactivée par défaut. Vous pouvez activer ou désactiver cette fonctionnalité sur chaque SVM si nécessaire.

Cette option est disponible au niveau de privilège avancé.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Activez ou désactivez les référencements automatiques des nœuds SMB si nécessaire :

Si vous voulez que les référencements automatiques des nœuds SMB soient...	Saisissez la commande suivante...
Activé	<code>vserver cifs options modify -vserver vserver_name -is-referral-enabled true</code>
Désactivé	<code>vserver cifs options modify -vserver vserver_name -is-referral-enabled false</code>

Le paramètre d'option prend effet pour les nouvelles sessions SMB. Les clients ayant une connexion existante ne peuvent utiliser la référence de nœud que lorsque leur délai d'expiration de cache existant expire.

3. Basculer vers le niveau de privilège admin : `set -privilege admin`

Informations associées

[Options de serveur SMB disponibles](#)

Pour déterminer le nombre de connexions SMB mentionnées, vous pouvez surveiller l'activité de renvoi automatique des nœuds à l'aide du `statistics` commande. En surveillant les référencements, vous pouvez déterminer dans quelle mesure les référencements automatiques localise des connexions sur des nœuds hébergeant les partages et si vous devez redistribuer vos LIFs de données pour fournir un meilleur accès local aux partages sur le serveur CIFS.

Description de la tâche

Le `cifs` Objet fournit plusieurs compteurs au niveau de privilèges avancés qui sont utiles lors du suivi des référencements automatiques des nœuds SMB :

- `node_referral_issued`

Nombre de clients ayant été aiguillage vers le nœud racine du partage après que le client ait connecté via une LIF hébergée par un nœud différent du nœud racine du partage.

- `node_referral_local`

Nombre de clients connectés via une LIF hébergée par le même nœud qui héberge la racine du partage. L'accès local offre généralement des performances optimales.

- `node_referral_not_possible`

Nombre de clients qui n'ont pas été aiguillage vers le nœud hébergeant la racine du partage après connexion à une LIF hébergée par un nœud différent du nœud racine du partage. En effet, une LIF de données actives pour le nœud racine du partage n'a pas été trouvée.

- `node_referral_remote`

Nombre de clients connectés via une LIF hébergée par un nœud différent du nœud qui héberge la racine du partage. L'accès à distance peut affecter les performances.

Vous pouvez surveiller les statistiques de référence automatique des nœuds sur votre SVM en collectant et en affichant les données d'une période donnée (échantillon). Vous pouvez afficher les données de l'échantillon si vous n'arrêtez pas la collecte de données. L'arrêt de la collecte de données vous donne un échantillon fixe. L'option ne pas arrêter la collecte de données vous permet d'obtenir des données mises à jour que vous pouvez utiliser pour comparer à des requêtes précédentes. La comparaison peut vous aider à identifier les tendances en matière de performances.



Pour évaluer et utiliser les informations que vous recueillez à partir du `statistics` command, vous devez comprendre la distribution des clients dans vos environnements.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Afficher les statistiques de référence de nœud automatique à l'aide du `statistics` commande.

Cet exemple affiche les statistiques d'aiguillage automatique des nœuds en recueillant et en visualisant les données d'une période d'échantillonnage :

- a. Lancez la collection : `statistics start -object cifs -instance vs1 -sample-id sample1`

```
Statistics collection is being started for Sample-id: sample1
```

- b. Attendez que le délai de collecte souhaité s'écoule.

- c. Arrêter la collection : `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

- d. Afficher les statistiques de référence automatique des nœuds : `statistics show -sample-id sample1 -counter node`

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1
```

Counter	Value
node_name	node1
node_referral_issued	0
node_referral_local	1
node_referral_not_possible	2
node_referral_remote	2
...	
node_name	node2
node_referral_issued	2
node_referral_local	1
node_referral_not_possible	0
node_referral_remote	2
...	

Le résultat affiche des compteurs pour tous les nœuds participant au SVM vs1. Pour plus de clarté, seuls les champs de sortie liés aux statistiques de renvoi automatique de nœud sont fournis dans l'exemple.

3. Retour au niveau de privilège admin : `set -privilege admin`

Informations associées

[Affichage des statistiques](#)

"Configuration du contrôle des performances"

Surveiller les informations de renvoi automatique de nœud SMB côté client à l'aide d'un client Windows

Pour déterminer les références faites du point de vue du client, vous pouvez utiliser Windows `dfsutil.exe` informatique.

Le kit Remote Server Administration Tools (RSAT) disponible avec les clients Windows 7 et versions ultérieures contient le `dfsutil.exe` informatique. Cet utilitaire vous permet d'afficher des informations sur le contenu du cache de référence ainsi que des informations sur chaque référence que le client utilise actuellement. Vous pouvez également utiliser l'utilitaire pour effacer le cache de référence du client. Pour plus d'informations, consultez la bibliothèque Microsoft TechNet.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Sécurité des dossiers sur les partages dotés d'une énumération basée sur l'accès

Assurez la sécurité des dossiers sur les partages dotés d'une vue d'ensemble de l'énumération basée sur l'accès

Lorsque l'énumération basée sur l'accès (ABE) est activée sur un partage SMB, les utilisateurs qui n'ont pas l'autorisation d'accéder à un dossier ou un fichier contenu dans le partage (que ce soit par le biais de restrictions d'autorisation individuelles ou de groupe) ne voient pas cette ressource partagée affichée dans leur environnement, bien que le partage lui-même reste visible.

Les propriétés de partage conventionnelles vous permettent de spécifier quels utilisateurs (individuellement ou en groupes) ont l'autorisation d'afficher ou de modifier les fichiers ou dossiers contenus dans le partage. Cependant, elles ne vous permettent pas de contrôler si les dossiers ou les fichiers contenus dans le partage sont visibles pour les utilisateurs qui ne disposent pas de l'autorisation d'y accéder. Cela peut poser des problèmes si les noms de ces dossiers ou fichiers dans le partage décrivent des informations sensibles, telles que les noms des clients ou des produits en cours de développement.

L'énumération basée sur l'accès (ABE) étend les propriétés de partage pour inclure l'énumération des fichiers et dossiers dans le partage. ABE vous permet donc de filtrer l'affichage des fichiers et dossiers dans le partage en fonction des droits d'accès des utilisateurs. C'est-à-dire que le partage lui-même est visible pour tous les utilisateurs, mais les fichiers et les dossiers du partage peuvent être affichés ou masqués par les utilisateurs désignés. En plus de protéger les informations sensibles sur votre lieu de travail, ABE vous permet de simplifier l'affichage de grandes structures de répertoires pour le bénéfice des utilisateurs qui n'ont pas besoin d'accéder à toute votre gamme de contenus. Par exemple, le partage lui-même est visible pour tous les utilisateurs, mais les fichiers et dossiers du partage peuvent être affichés ou masqués.

Découvrez "[Impact sur les performances lors de l'utilisation d'une énumération basée sur SMB/CIFS](#)".

Activez ou désactivez l'énumération basée sur l'accès pour les partages SMB

Vous pouvez activer ou désactiver l'énumération basée sur l'accès (ABE) sur les partages SMB afin d'autoriser ou d'empêcher les utilisateurs de voir les ressources partagées qu'ils ne disposent pas des autorisations d'accès.

Description de la tâche

Par défaut, ABE est désactivé.

Étapes

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez...	Entrez la commande...
Activer ABE sur un nouveau partage	<code>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration</code> Vous pouvez spécifier des paramètres de partage facultatifs supplémentaires et d'autres propriétés de partage lorsque vous créez un partage SMB. Pour plus d'informations, consultez la page de manuel du <code>vserver cifs share create</code> commande.
Activer ABE sur un partage existant	<code>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration</code> Les propriétés de partage existantes sont conservées. La propriété partage ABE est ajoutée à la liste existante des propriétés de partage.
Désactivez ABE sur un partage existant	<code>vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration</code> Les autres propriétés de partage sont conservées. Seule la propriété partage ABE est supprimée de la liste des propriétés de partage.

2. Vérifiez que la configuration du partage est correcte à l'aide du `vserver cifs share show` commande.

Exemples

L'exemple suivant crée un partage ABE SMB nommé "sales" avec un chemin de `/sales` Sur la SVM `vs1`. Le partage est créé avec `access-based-enumeration` en tant que propriété de partage :

```
cluster1::> vservice cifs share create -vservice vs1 -share-name sales -path
/sales -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vservice cifs share show -vservice vs1 -share-name sales

          Vservice: vs1
          Share: sales
CIFS Server NetBIOS Name: VS1
          Path: /sales
      Share Properties: access-based-enumeration
                        oplocks
                        browsable
                        changenotify
      Symlink Properties: enable
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
          Share Comment: -
          Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
          Volume Name: -
          Offline Files: manual
Vscan File-Operations Profile: standard
```

L'exemple suivant ajoute le access-based-enumeration Partagez la propriété dans un partage SMB nommé "data2":

```
cluster1::> vservice cifs share properties add -vservice vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vservice cifs share show -vservice vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
-----
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

Informations associées

[Ajout ou suppression de propriétés de partage sur un partage SMB existant](#)

Activez ou désactivez l'énumération basée sur l'accès à partir d'un client Windows

Vous pouvez activer ou désactiver l'énumération basée sur l'accès (ABE) sur des partages SMB à partir d'un client Windows, ce qui vous permet de configurer ce paramètre de partage sans avoir à vous connecter au serveur CIFS.



Le `abecmd` Utilitaire non disponible dans les nouvelles versions de Windows Server et des clients Windows. Elle a été publiée dans le cadre de Windows Server 2008. Le support de Windows Server 2008 a pris fin le 14 janvier 2020.

Étapes

1. À partir d'un client Windows prenant en charge ABE, entrez la commande suivante : `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

Pour plus d'informations sur le `abecmd` Consultez la documentation de votre client Windows.

Dépendances de nommage des fichiers et des répertoires NFS et SMB

Présentation des dépendances de nommage des fichiers et des répertoires NFS et SMB

Les conventions d'appellation des fichiers et des répertoires dépendent à la fois des systèmes d'exploitation des clients réseau et des protocoles de partage de fichiers, en plus des paramètres de langue sur le cluster ONTAP et les clients.

Le système d'exploitation et les protocoles de partage de fichiers déterminent ce qui suit :

- Caractères un nom de fichier peut utiliser
- Sensibilité à la casse d'un nom de fichier

ONTAP prend en charge les caractères multi-octets dans les noms de fichier, de répertoire et de `qtree`, en fonction de la version de ONTAP utilisée.

Caractères un nom de fichier ou de répertoire peut utiliser

Si vous accédez à un fichier ou à un répertoire à partir de clients ayant différents systèmes d'exploitation, vous devez utiliser des caractères valides dans les deux systèmes d'exploitation.

Par exemple, si vous utilisez UNIX pour créer un fichier ou un répertoire, n'utilisez pas de deux-points (:) dans le nom car le deux-points n'est pas autorisé dans les noms de fichiers ou de répertoires MS-DOS. Comme les restrictions sur les caractères valides varient d'un système d'exploitation à l'autre, consultez la documentation de votre système d'exploitation client pour plus d'informations sur les caractères interdits.

Sensibilité à la casse des noms de fichiers et de répertoires dans un environnement multiprotocole

Les noms de fichiers et de répertoires sont sensibles à la casse pour les clients NFS et non sensibles à la casse, mais ils préservent la casse pour les clients SMB. Vous devez comprendre les implications dans un environnement multiprotocole et les actions nécessaires lorsque vous spécifiez le chemin lors de la création des partages SMB et lors de l'accès aux données au sein des partages.

Si un client SMB crée un répertoire nommé `testdir`, Les clients SMB et NFS affichent le nom de fichier comme `testdir`. Toutefois, si un utilisateur SMB tente par la suite de créer un nom de répertoire `TESTDIR`, Le nom n'est pas autorisé car, pour le client SMB, ce nom existe actuellement. Si un utilisateur NFS crée par la suite un répertoire nommé `TESTDIR`, Les clients NFS et SMB affichent le nom du répertoire différemment,

comme suit :

- Sur les clients NFS, vous voyez les deux noms de répertoire tels qu'ils ont été créés, par exemple `testdir` et `TESTDIR`, car les noms de répertoire sont sensibles à la casse.
- Les clients SMB utilisent les 8.3 noms pour faire la distinction entre les deux répertoires. Un répertoire porte le nom du fichier de base. Un nom de fichier 8.3 est attribué aux répertoires supplémentaires.
 - Sur les clients SMB, vous voyez `testdir` et `TESTDI~1`.
 - ONTAP crée le `TESTDI~1` nom du répertoire pour différencier les deux répertoires.

Dans ce cas, vous devez utiliser le nom 8.3 lorsque vous spécifiez un chemin de partage lors de la création ou de la modification d'un partage sur un SVM (Storage Virtual machine).

De la même manière pour les fichiers, si un client SMB crée `test.txt`, Les clients SMB et NFS affichent le nom de fichier comme `test.txt`. Toutefois, si un utilisateur SMB tente par la suite de le créer `Test.txt`, Le nom n'est pas autorisé car, pour le client SMB, ce nom existe actuellement. Si un utilisateur NFS crée par la suite un fichier nommé `Test.txt`, Les clients NFS et SMB affichent le nom de fichier différemment, comme suit :

- Sur les clients NFS, les deux noms de fichiers sont ceux qu'ils ont créés, `test.txt` et `Test.txt`, car les noms de fichiers sont sensibles à la casse.
- Les clients SMB utilisent les 8.3 noms pour distinguer les deux fichiers. Un fichier porte le nom du fichier de base. Un nom de fichier 8.3 est attribué aux fichiers supplémentaires.
 - Sur les clients SMB, vous voyez `test.txt` et `TEST~1.TXT`.
 - ONTAP crée le `TEST~1.TXT` nom de fichier pour différencier les deux fichiers.



Si vous avez activé ou modifié le mappage de caractères à l'aide des commandes `Vserver CIFS Character-mapping`, une recherche Windows sensible à la casse devient normalement sensible à la casse.

Comment ONTAP crée des noms de fichiers et de répertoires

ONTAP crée et conserve deux noms pour les fichiers ou les répertoires de tout répertoire ayant accès à partir d'un client SMB : le nom long et le nom d'origine au format 8.3.

Pour les noms de fichier ou de répertoire dépassant le nom de huit caractères ou la limite d'extension de trois caractères (pour les fichiers), ONTAP génère un nom de format 8.3 comme suit :

- Il tronque le nom de fichier ou de répertoire d'origine à six caractères, si le nom dépasse six caractères.
- Il ajoute un tilde (~) et un nombre, un à cinq, aux noms de fichier ou de répertoire qui ne sont plus uniques après être tronqués.

S'il manque des nombres parce qu'il y a plus de cinq noms similaires, il crée un nom unique qui n'a aucune relation avec le nom original.

- Dans le cas des fichiers, il tronque l'extension du nom de fichier à trois caractères.

Par exemple, si un client NFS crée un fichier nommé `specifications.html`, Le nom de fichier au format 8.3 créé par ONTAP est `specif~1.htm`. Si ce nom existe déjà, ONTAP utilise un numéro différent à la fin du nom du fichier. Par exemple, si un client NFS crée un autre fichier nommé `specifications_new.html`, le

Comment ONTAP gère les noms de fichier, de répertoire et de qtree à plusieurs octets

À partir de ONTAP 9.5, la prise en charge des noms codés UTF-8 de 4 octets permet la création et l'affichage des noms de fichier, de répertoire et d'arborescence qui incluent des caractères supplémentaires Unicode à l'extérieur du plan multilingue de base (BMP). Dans les versions précédentes, ces caractères supplémentaires ne s'affichent pas correctement dans les environnements multiprotocoles.

Pour activer la prise en charge des noms codés UTF-8 à 4 octets, un nouveau code de langue *utf8mb4* est disponible pour l'*vserver* et *volume* familles de commandement.

Vous devez créer un volume de l'une des manières suivantes :

- Réglage du volume `-language` explicitement option : `volume create -language utf8mb4 {...}`
- Hériter du volume `-language` Option d'un SVM qui a été créé avec ou modifié pour l'option : `vserver [create|modify] -language utf8mb4 {...}``volume create {...}`
- Dans ONTAP 9.6 et les versions antérieures, vous ne pouvez pas modifier les volumes existants pour le support *utf8mb4* ; vous devez créer un nouveau volume prêt pour *utf8mb4*, puis migrer les données à l'aide d'outils de copie basés sur le client.

Vous pouvez mettre à jour les SVM pour la prise en charge de *utf8mb4*, mais les volumes existants conservent leurs codes de langue d'origine.

Si vous utilisez ONTAP 9.7P1 ou une version ultérieure, vous pouvez modifier les volumes existants pour *utf8mb4* avec une demande de support. Pour plus d'informations, voir ["Est-il possible de modifier la langue du volume après sa création dans ONTAP ?"](#).

- À partir de ONTAP 9.8, vous pouvez utiliser le `[-language <Language code>]` Paramètre permettant de changer le langage de volume de *.UTF-8 à *utf8mb4*. Pour modifier la langue d'un volume, contactez ["Support NetApp"](#).



Les noms de LUN portant des caractères UTF-8 de 4 octets ne sont pas pris en charge actuellement.

- Les données de caractères Unicode sont généralement représentées dans les applications de systèmes de fichiers Windows utilisant le format de transformation Unicode 16 bits (UTF-16) et dans les systèmes de fichiers NFS utilisant le format de transformation Unicode 8 bits (UTF-8).

Dans les versions antérieures à ONTAP 9.5, les noms, y compris les caractères supplémentaires UTF-16 créés par les clients Windows, étaient correctement affichés sur d'autres clients Windows mais n'étaient pas traduits correctement en UTF-8 pour les clients NFS. De même, les noms comportant des caractères supplémentaires UTF-8 par les clients NFS créés n'ont pas été correctement traduits en UTF-16 pour les clients Windows.

- Lorsque vous créez des noms de fichier sur des systèmes exécutant ONTAP 9.4 ou une version antérieure contenant des caractères supplémentaires valides ou non valides, ONTAP rejette le nom de fichier et renvoie une erreur de nom de fichier non valide.

Pour éviter ce problème, utilisez uniquement des caractères BMP dans les noms de fichiers et évitez d'utiliser des caractères supplémentaires, ou mettez à niveau vers ONTAP 9.5 ou version ultérieure.

À partir de ONTAP 9, les caractères Unicode sont autorisés dans les noms de qtree.

- Vous pouvez utiliser le volume `qtree` Famille de commandes ou System Manager pour définir ou modifier les noms des qtree.
- Les noms des qtrees peuvent inclure des caractères multi-octets au format Unicode, comme les caractères japonais et chinois.
- Dans les versions antérieures à ONTAP 9.5, seuls les caractères BMP (c'est-à-dire ceux qui pouvaient être représentés en 3 octets) étaient pris en charge.



Dans les versions antérieures à ONTAP 9.5, le Junction-path du volume parent du qtree peut contenir des noms de qtree et de répertoire avec des caractères Unicode. Le volume `show` La commande affiche ces noms correctement lorsque le volume parent a un paramètre de langue UTF-8. Cependant, si la langue du volume parent n'est pas l'un des paramètres de langue UTF-8, certaines parties du chemin de jonction sont affichées à l'aide d'un nom de remplacement NFS numérique.

- Dans les versions 9.5 et ultérieures, les noms des qtree prennent en charge des caractères de 4 octets, à condition que le qtree se trouve dans un volume activé pour `utf8m4`.

Configurez le mappage de caractères pour la conversion de nom de fichier SMB sur des volumes

Les clients NFS peuvent créer des noms de fichiers contenant des caractères non valides pour les clients SMB et certaines applications Windows. Vous pouvez configurer le mappage de caractères pour la conversion de noms de fichiers sur des volumes pour permettre aux clients SMB d'accéder aux fichiers avec des noms NFS qui ne seraient autrement pas valides.

Description de la tâche

Lorsque les fichiers créés par des clients NFS sont accessibles par des clients SMB, ONTAP recherche le nom du fichier. Si le nom n'est pas un nom de fichier SMB valide (par exemple, s'il comporte un caractère «`:`»») inclus, ONTAP renvoie le nom de fichier 8.3 qui est conservé pour chaque fichier. Cependant, cela cause des problèmes pour les applications qui codent des informations importantes dans des noms de fichiers longs.

Par conséquent, si vous partagez un fichier entre des clients sur des systèmes d'exploitation différents, vous devez utiliser des caractères dans les noms de fichiers valides dans les deux systèmes d'exploitation.

Cependant, si vous avez des clients NFS qui créent des noms de fichier contenant des caractères qui ne sont pas des noms de fichier valides pour les clients SMB, vous pouvez définir une carte qui convertit les caractères NFS non valides en caractères Unicode acceptés par SMB et certaines applications Windows. Par exemple, cette fonctionnalité prend en charge les applications CATIA MCAD et Mathematica, ainsi que d'autres applications qui ont cette exigence.

Vous pouvez configurer le mappage de caractères sur une base volume par volume.

Lors de la configuration du mappage de caractères sur un volume, vous devez garder à l'esprit les éléments suivants :

- Le mappage de caractères n'est pas appliqué à travers les points de jonction.

Vous devez configurer explicitement le mappage de caractères pour chaque volume de jonction.

- Vous devez vous assurer que les caractères Unicode utilisés pour représenter des caractères non valides

ou illégaux sont des caractères qui n'apparaissent normalement pas dans les noms de fichiers ; sinon, des mappages indésirables se produisent.

Par exemple, si vous essayez de mapper un deux-points (:) à un tiret (-) mais que le tiret (-) a été utilisé correctement dans le nom de fichier, un client Windows essayant d'accéder à un fichier nommé ""a-b" aurait sa demande mappée au nom NFS de ""a:b" (pas le résultat souhaité).

- Après l'application du mappage de caractères, si le mappage contient toujours un caractère Windows non valide, ONTAP revient aux noms de fichier Windows 8.3.
- Dans les notifications FPolicy, les journaux d'audit NAS et les messages de suivi de sécurité, les noms de fichiers mappés sont affichés.
- Lors de la création d'une relation SnapMirror de type DP, le mappage de caractères du volume source n'est pas répliqué sur le volume DP de destination.
- Sensibilité à la casse : comme les noms Windows mappés se transforment en noms NFS, la recherche des noms suit la sémantique NFS. Ainsi, les recherches NFS sont sensibles à la casse. Cela signifie que les applications qui accèdent aux partages mappés ne doivent pas se fier au comportement non sensible à la casse de Windows. Cependant, le nom 8.3 est disponible, et cela n'est pas sensible à la casse.
- Mappages partiels ou non valides : après le mappage d'un nom pour revenir aux clients faisant une énumération de répertoire (« dir »), le nom Unicode obtenu est vérifié pour la validité de Windows. Si ce nom contient toujours des caractères non valides ou s'il n'est pas valide pour Windows (par exemple, il se termine par "." ou vierge), le nom 8.3 est renvoyé à la place du nom non valide.

Étape

1. Configurer le mappage de caractères : +

```
vserver cifs character-mapping create -vserver vserver_name -volume volume_name  
-mapping mapping_text, ... +
```

Le mappage se compose d'une liste de paires de caractères source-cible séparées par «»:». Les caractères sont des caractères Unicode saisis à l'aide de chiffres hexadécimaux. Par exemple : 3C:E03C. +

La première valeur de chaque mapping_text La paire séparée par deux-points est la valeur hexadécimale du caractère NFS que vous souhaitez traduire, et la seconde est la valeur Unicode utilisée par SMB. Les paires de mappage doivent être uniques (un mappage un-à-un doit exister).

- Mappage de source +

Le tableau suivant montre le jeu de caractères Unicode autorisé pour le mappage de source :

+

Caractère Unicode	Caractère imprimé	Description
0x01-0x19	Sans objet	Caractères de contrôle sans impression
0x5C		Barre oblique inversée
0x3A	:	Deux-points
0x2A	*	Astérisque

Caractère Unicode	Caractère imprimé	Description
0x3F	?	Point d'interrogation
0x22	«	Devis
0x3C	<	Inférieur à
0x3E	>	Supérieur à
0x7C		
Ligne verticale	0xb1	±

- Mappage de cible

Vous pouvez spécifier des caractères cibles dans la « zone d'utilisation privée » d'Unicode dans la plage suivante : U+E0000...U+F8FF.

Exemple

La commande suivante crée un mappage de caractères pour un volume nommé « `dates` » sur la machine virtuelle de stockage (SVM) vs1 :

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show
```

Vserver	Volume Name	Character Mapping
vs1	data	3c:e17c, 3e:f17d, 2a:f745

Informations associées

[Création et gestion des volumes de données dans les espaces de noms NAS](#)

Commandes permettant de gérer les mappages de caractères pour la conversion de noms de fichiers SMB

Vous pouvez gérer le mappage de caractères en créant, en modifiant, en affichant des informations sur et en supprimant des mappages de caractères de fichiers utilisés pour la conversion de noms de fichiers SMB sur des volumes FlexVol.

Les fonctions que vous recherchez...	Utilisez cette commande...
Créer de nouveaux mappages de caractères de fichier	<code>vserver cifs character-mapping create</code>

Les fonctions que vous recherchez...	Utilisez cette commande...
Affiche des informations sur les mappages de caractères de fichier	<code>vserver cifs character-mapping show</code>
Modifier les mappages de caractères de fichier existants	<code>vserver cifs character-mapping modify</code>
Supprimer les mappages de caractères de fichier	<code>vserver cifs character-mapping delete</code>

Pour plus d'informations, consultez la page man pour chaque commande

Informations associées

[Configuration du mappage de caractères pour la conversion de noms de fichiers SMB sur des volumes](#)

Offrez un accès client S3 aux données NAS

Présentation multiprotocole S3

Depuis ONTAP 9.12.1, vous pouvez activer les clients exécutant le protocole S3 pour accéder aux données qui sont servies aux clients qui utilisent les protocoles NFS et SMB sans nouveau formatage. Ainsi, les données NAS peuvent continuer à être servies aux clients NAS, tout en présentant les données d'objet aux clients S3 qui exécutent des applications S3 (par exemple, le data mining et l'intelligence artificielle).

La fonctionnalité multiprotocole S3 répond à deux cas d'utilisation :

1. Accès aux données NAS existantes à l'aide de clients S3

Si vos données existantes ont été créées à l'aide de clients NAS classiques (NFS ou SMB) et sont situées sur des volumes NAS (volumes FlexVol ou FlexGroup), vous pouvez désormais utiliser les outils d'analytique des clients S3 pour accéder à ces données.

2. Stockage back-end pour les clients modernes capables d'exécuter des E/S avec les protocoles NAS et S3

Vous pouvez désormais fournir un accès intégré pour des applications telles que Spark et Kafka qui peuvent lire et écrire les mêmes données à l'aide des protocoles NAS et S3.

Fonctionnement du protocole multiprotocole S3

ONTAP multiprotocole permet de présenter le même jeu de données que la hiérarchie de fichiers ou qu'en tant qu'objets dans un compartiment. Pour ce faire, ONTAP crée des « compartiments NAS S3 » qui permettent aux clients S3 de créer, lire, supprimer et énumérer des fichiers dans le stockage NAS à l'aide de requêtes d'objets S3. Ce mappage est conforme à la configuration de sécurité NAS, en observant les autorisations d'accès aux fichiers et aux répertoires ainsi qu'en écrivant dans la piste d'audit de sécurité si nécessaire.

Ce mappage est effectué en présentant une hiérarchie de répertoires NAS spécifiée comme un compartiment S3. Chaque fichier de la hiérarchie de répertoires est représenté comme un objet S3 dont le nom est relatif à partir du répertoire mappé vers le bas, avec des limites de répertoire représentées par le caractère de barre oblique ('/').

Les utilisateurs standard de ONTAP-defined S3 peuvent accéder à ce stockage, conformément aux règles de compartiment définies pour le compartiment correspondant au répertoire NAS. Pour que cela soit possible, des mappages doivent être définis entre les utilisateurs S3 et SMB/NFS. Les informations d'identification de l'utilisateur SMB/NFS seront utilisées pour la vérification des autorisations NAS et incluses dans tous les enregistrements d'audit résultant de ces accès.

Lorsqu'un fichier est créé par des clients SMB ou NFS, il est immédiatement placé dans un répertoire, et donc visible aux clients, avant l'écriture des données. Les clients S3 s'attendent à une sémantique différente, où le nouvel objet n'est pas visible dans le namespace tant que toutes ses données n'ont pas été écrites. Le mappage de S3 sur le stockage NAS crée des fichiers avec la sémantique S3, afin de rendre les fichiers invisibles en externe jusqu'à la fin de la commande de création S3.

Protection des données par compartiments NAS S3

Les « compartiments » NAS S3 sont simplement des mappages des données NAS pour les clients S3, ils ne sont pas des compartiments S3 standard. Par conséquent, il n'est pas nécessaire de protéger les compartiments NAS S3 à l'aide de la fonctionnalité NetApp SnapMirror S3. À la place, vous pouvez protéger les volumes contenant des compartiments NAS S3 à l'aide de la réplication asynchrone de volume SnapMirror. La fonction SnapMirror synchrone et la reprise d'activité SVM ne sont pas prises en charge.

À partir de ONTAP 9.14.1, les compartiments NAS S3 sont pris en charge dans les agrégats en miroir et sans miroir pour les configurations MetroCluster IP et FC.

En savoir plus sur ["Réplication asynchrone SnapMirror"](#).

Audit des compartiments NAS S3

Les compartiments NAS S3 ne sont pas des compartiments S3 classiques. L'audit S3 ne peut donc pas être configuré pour l'audit de l'accès. En savoir plus sur ["Audit S3"](#).

Cependant, les fichiers et les répertoires NAS mappés dans des compartiments NAS S3 peuvent être audités pour les événements d'accès à l'aide de procédures d'audit ONTAP conventionnelles. Les opérations S3 peuvent ainsi déclencher des événements d'audit NAS, à l'exception de ce qui suit :

- Si l'accès client S3 est refusé par la configuration de la règle S3 (groupe ou règle de compartiment), l'audit NAS pour l'événement n'est pas lancé. En effet, les autorisations S3 sont vérifiées avant la vérification des audits des SVM.
- Si le fichier cible d'une requête GET S3 est de taille 0, le contenu 0 est renvoyé à la demande GET et l'accès en lecture n'est pas consigné.
- Si le fichier cible d'une requête GET S3 se trouve dans un dossier pour lequel l'utilisateur n'a pas d'autorisation « traverse », la tentative d'accès échoue et l'événement n'est pas enregistré.

Découvrez ["Audit des événements NAS sur les SVM"](#).

Interopérabilité S3 et NAS

Sauf mention contraire, les compartiments NAS ONTAP S3 prennent en charge les fonctionnalités NAS standard et S3.

La fonctionnalité NAS n'est pas prise en charge par les compartiments NAS S3

Un niveau de capacité FabricPool

Les compartiments NAS S3 ne peuvent pas être configurés en tant que Tier de capacité pour FabricPool.

La fonctionnalité S3 n'est pas prise en charge par les compartiments NAS S3

Métadonnées d'utilisateur AWS

- Les paires de valeurs-clés reçues dans le cadre des métadonnées S3 ne sont pas stockées sur le disque avec les données d'objet dans la version actuelle.
- Les en-têtes de demande avec le préfixe "x-amz-META" sont ignorés.

Balises AWS

- Sur les demandes d'initialisation D'objet PUT et multipart, les en-têtes avec le préfixe "x-amz-tagging" sont ignorés.
- Les demandes de mise à jour des balises sur un fichier existant (c'est-à-dire une requête PUT, GET et Delete avec la chaîne de requête ?tagging) sont rejetées par une erreur.

Gestion des versions

Il n'est pas possible de spécifier la gestion des versions dans la configuration du mappage des compartiments.

- Les demandes qui incluent des spécifications de version non nulles (versionID=xyz query-string) reçoivent des réponses d'erreur.
- Les demandes visant à affecter l'état de gestion des versions d'un compartiment sont rejetées avec des erreurs.

Opérations en plusieurs parties

Les opérations suivantes ne sont pas prises en charge :

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- ListMultipartUpload

Exigences de données NAS pour l'accès des clients S3

Il est important de comprendre qu'il existe des incompatibilités inhérentes lors du mappage des fichiers NAS et des répertoires pour l'accès S3. Il peut être nécessaire d'ajuster la hiérarchie des fichiers NAS avant de les transférer à l'aide de compartiments NAS S3.

Un compartiment NAS S3 fournit un accès S3 à un répertoire NAS en effectuant le mappage de ce répertoire à l'aide de la syntaxe du compartiment S3, et les fichiers de l'arborescence sont considérés comme des objets. Les noms d'objet sont les chemins d'accès délimités par des barres obliques des fichiers par rapport au répertoire spécifié dans la configuration du compartiment S3.

Ce mappage impose une certaine exigence lorsque les fichiers et les répertoires sont gérés à l'aide de compartiments NAS S3 :

- Les noms S3 sont limités à 1024 octets. Les fichiers dont les chemins d'accès sont plus longs ne sont donc pas accessibles via S3.
- Les noms de fichiers et de répertoires sont limités à 255 caractères, de sorte qu'un nom d'objet ne peut pas comporter plus de 255 caractères consécutifs non-slash ("/")

- Un chemin SMB délimité par des caractères de barre oblique inverse («\») apparaîtra à S3 comme un nom d'objet contenant des caractères de barre oblique («/ »).
- Certaines paires de noms d'objets S3 légaux ne peuvent pas coexister dans l'arborescence de répertoires NAS mappée. Par exemple, les noms d'objet S3 légal "part1/part2" et "part1/part2/part3" correspondent à des fichiers qui ne peuvent pas exister simultanément dans l'arborescence du répertoire NAS, "part1/part2" étant un fichier du premier nom et un répertoire de l'autre.
 - Si "part1/part2" est un fichier existant, la création S3 de "part1/part2/part3" échouera.
 - Si "part1/part2/part3" est un fichier existant, la création ou la suppression S3 de "part1/part2" échouera.
 - La création d'objet S3 correspondant au nom d'un objet existant remplace l'objet existant (dans des compartiments sans version). La gestion est assurée dans le NAS, mais la correspondance est obligatoire. Les exemples ci-dessus ne peuvent pas entraîner la suppression de l'objet existant car les noms entrent en collision et ne correspondent pas.

Alors qu'un magasin d'objets est conçu pour prendre en charge un grand nombre de noms arbitraires, une structure d'annuaire NAS peut rencontrer des problèmes de performance si un très grand nombre de noms sont placés dans un répertoire. En particulier, les noms sans barre oblique (/) dans ces caractères seront tous placés dans le répertoire racine du mappage NAS. Les applications qui utilisent de manière intensive les noms qui ne sont pas « compatibles avec le NAS » seraient mieux hébergées dans un compartiment de magasin d'objets réel plutôt que dans un mappage NAS.

Activez l'accès au protocole S3 aux données NAS

L'activation de l'accès au protocole S3 consiste à s'assurer qu'un SVM compatible avec NAS répond aux mêmes exigences qu'un serveur compatible S3, notamment l'ajout d'un serveur de magasin d'objets et la vérification des exigences en matière de réseau et d'authentification.

Pour les nouvelles installations ONTAP, il est recommandé d'activer l'accès par le protocole S3 à un SVM après sa configuration afin d'assurer le service des données NAS aux clients. Pour en savoir plus sur la configuration du protocole NAS, voir :

- ["Configuration NFS"](#)
- ["Configuration SMB"](#)

Avant de commencer

Les éléments suivants doivent être configurés avant d'activer le protocole S3 :

- Les licences existent pour le protocole S3 et les protocoles NAS souhaités (NFS, SMB ou les deux).
- Un SVM est configuré pour les protocoles NAS souhaités.
- Les serveurs NFS et/ou SMB existent.
- DNS et tous les autres services requis sont configurés.
- Les données NAS sont exportées ou partagées vers les systèmes clients.

Description de la tâche

Un certificat d'autorité de certification (CA) est nécessaire pour activer le trafic HTTPS des clients S3 vers le SVM compatible avec S3. Les certificats CA provenant de trois sources peuvent être utilisés :


- Nouveau certificat auto-signé ONTAP sur le SVM.

- Certificat ONTAP signé automatiquement sur le SVM.
- Un certificat tiers.

Vous pouvez utiliser les mêmes LIF de données pour le compartiment S3/NAS que pour le service des données NAS. Si des adresses IP spécifiques sont requises, reportez-vous à la section "[Création de LIF de données](#)". Une règle de données de service S3 est nécessaire pour activer le trafic de données S3 sur les LIF. Vous pouvez modifier la règle de service existante de la SVM afin d'inclure S3.

Lorsque vous créez le serveur objet S3, vous devez préparer le nom du serveur S3 en tant que nom de domaine complet (FQDN) que les clients utiliseront pour l'accès S3. Le FQDN du serveur S3 ne doit pas commencer par un nom de compartiment.

System Manager

1. Activez S3 sur une machine virtuelle de stockage avec les protocoles NAS configurés.
 - a. Cliquez sur **stockage > Storage VMs**, sélectionnez une VM de stockage compatible NAS, cliquez sur Paramètres, puis cliquez  sous S3.
 - b. Sélectionnez le type de certificat. Que vous sélectionniez un certificat généré par le système ou l'un de vos propres certificats, il sera nécessaire d'accéder au client.
 - c. Saisissez les interfaces réseau.
2. Si vous avez sélectionné le certificat généré par le système, les informations de certificat s'affichent lorsque la création de la nouvelle machine virtuelle de stockage est confirmée. Cliquez sur **Download** et enregistrez-le pour accéder au client.
 - La clé secrète ne s'affiche plus.
 - Si vous avez besoin de nouveau des informations de certificat : cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.

CLI

1. Vérifier que le protocole S3 est autorisé sur la SVM :

```
vserver show -fields allowed-protocols
```
2. Enregistrer le certificat de clé publique pour ce SVM.
Si vous avez besoin d'un nouveau certificat auto-signé ONTAP, reportez-vous à la section "[Créer et installer un certificat d'autorité de certification sur le SVM](#)".
3. Mettre à jour la stratégie de données de service
 - a. Afficher la politique de données de service pour la SVM

```
network interface service-policy show -vserver svm_name
```
 - b. Ajoutez le data-core et data-s3-server services s'ils ne sont pas présents.

```
network interface service-policy add-service -vserver svm_name -policy policy_name -service data-core,data-s3-server
```
4. Vérifier que les LIF de données du SVM répondent à vos exigences :

```
network interface show -vserver svm_name
```
5. Création du serveur S3 :

```
vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]
```

Vous pouvez spécifier des options supplémentaires lors de la création du serveur S3 ou à tout moment ultérieurement.

- HTTPS est activé par défaut sur le port 443. Vous pouvez modifier le numéro de port à l'aide de l'option `-Secure-Listener-port`.
Lorsque HTTPS est activé, des certificats CA sont requis pour une intégration correcte avec SSL/TLS. À partir de ONTAP 9.15.1, TLS 1.3 est pris en charge avec le stockage objet S3.
 - HTTP est désactivé par défaut ; lorsqu'il est activé, le serveur écoute le port 80. Vous pouvez l'activer avec l'option `-is-http-enabled` ou modifier le numéro de port avec l'option `-port` d'écoute.
Lorsque HTTP est activé, toutes les demandes et réponses sont envoyées en clair sur le réseau.
1. Vérifiez que S3 est configuré comme vous le souhaitez :


```
vserver object-store-server show
```

Exemple

La commande suivante vérifie les valeurs de configuration de tous les serveurs de stockage objet :

```
cluster1::> vserver object-store-server show
```

```
Vserver: vs1
```

```
Object Store Server Name: s3.example.com
Administrative State: up
Listener Port For HTTP: 80
Secure Listener Port For HTTPS: 443
HTTP Enabled: false
HTTPS Enabled: true
Certificate for HTTPS Connections: svml_ca
Comment: Server comment
```

Créez un compartiment NAS S3

Un compartiment NAS S3 est un mappage entre un nom de compartiment S3 et un chemin NAS. Les compartiments NAS S3 vous permettent d'offrir un accès S3 à n'importe quelle partie d'un namespace de SVM avec des volumes et une structure de répertoires existants.

Avant de commencer

- Un serveur d'objets S3 est configuré dans une SVM contenant des données NAS.
- Les données NAS sont conformes à la ["Exigences en matière d'accès client S3"](#).

Description de la tâche

Vous pouvez configurer les compartiments NAS S3 pour spécifier tout ensemble de fichiers et de répertoires dans le répertoire racine de la SVM.

Vous pouvez également définir des règles de compartiment qui permettent ou non l'accès aux données NAS selon n'importe quelle combinaison de ces paramètres :

- Fichiers et répertoires
- Autorisations utilisateur et groupe
- Opérations S3

Il peut par exemple s'avérer nécessaire de définir des règles de compartiment distinctes pour accorder l'accès aux données en lecture seule à un grand groupe d'utilisateurs, tandis qu'un groupe limité peut effectuer des opérations sur un sous-ensemble de ces données.

Les « compartiments » NAS S3 étant des mappages et non des compartiments S3, les propriétés suivantes des compartiments S3 standard ne s'appliquent pas aux compartiments NAS S3.

- `aggr-list \ aggr-list-multiplier \ storage-service-level \ volume \ size \ exclude-aggr-list \ qos-policy-`

group

Aucun volume ou qtrees n'est créé lors de la configuration des compartiments NAS S3.

- **Le rôle \ est -protégé \ est -protégé-sur-ONTAP \ est -protégé-sur-cloud** + les compartiments NAS S3 ne sont pas protégés ou mis en miroir à l'aide de SnapMirror S3, mais ils utilisent à la place la protection SnapMirror classique disponible au niveau de la granularité du volume.
- **etat-versionnage**
Les volumes NAS disposent généralement de la technologie Snapshot pour enregistrer différentes versions. Cependant, la gestion de version n'est pas disponible dans les compartiments NAS S3.
- **utilisation logique \ nombre-objets**
Des statistiques équivalentes sont disponibles pour les volumes NAS via les commandes de volume.

System Manager

Ajoutez un nouveau compartiment NAS S3 sur une machine virtuelle de stockage compatible NAS.

1. Cliquez sur **stockage > compartiments**, puis sur **Ajouter**.
2. Entrez un nom pour le compartiment NAS S3 et sélectionnez la machine virtuelle de stockage, ne saisissez pas de taille, puis cliquez sur **plus d'options**.
3. Entrez un nom de chemin d'accès valide ou cliquez sur Parcourir pour le sélectionner dans une liste de noms de chemin valides.
Lorsque vous entrez un chemin d'accès valide, les options qui ne sont pas pertinentes pour la configuration du NAS S3 sont masquées.
4. Si vous avez déjà mappé des utilisateurs S3 aux utilisateurs NAS et aux groupes créés, vous pouvez configurer leurs autorisations, puis cliquez sur **Enregistrer**.
Vous devez avoir déjà mappé des utilisateurs S3 à des utilisateurs NAS avant de configurer les autorisations de cette étape.

Sinon, cliquez sur **Save** pour terminer la configuration du compartiment NAS S3.

CLI

Création d'un compartiment NAS S3 dans un SVM contenant des systèmes de fichiers NAS.

```
vserver object-store-server bucket create -vserver svm_name -bucket  
bucket_name -type nas -nas-path junction_path [-comment text]
```

Exemple :

```
cluster1::> vserver object-store-server bucket create -bucket testbucket -type  
nas -path /vol1
```

Activez les utilisateurs client S3

Pour permettre aux utilisateurs clients S3 d'accéder aux données NAS, vous devez mapper les noms d'utilisateur S3 aux utilisateurs NAS correspondants, puis leur accorder la permission d'accéder aux données NAS à l'aide des politiques de service de compartiment.

Avant de commencer

Les noms d'utilisateur pour l'accès client (utilisateurs clients LINUX/UNIX, Windows et S3) doivent déjà exister.

Description de la tâche

Le mappage d'un nom d'utilisateur S3 avec un utilisateur LINUX/UNIX ou Windows correspondant permet de vérifier les autorisations sur les fichiers NAS qui doivent être honorés lors de l'accès à ces fichiers par des clients S3. Les mappages S3 vers NAS sont spécifiés en fournissant un nom d'utilisateur S3 *Pattern*, qui peut être exprimé sous la forme d'un nom unique ou d'une expression régulière POSIX, et un nom d'utilisateur LINUX/UNIX ou Windows *Replace*.

En l'absence de mappage de nom, le mappage de nom par défaut sera utilisé, où le nom d'utilisateur S3 lui-même sera utilisé comme nom d'utilisateur UNIX et nom d'utilisateur Windows. Vous pouvez modifier les mappages de noms d'utilisateur UNIX et Windows par défaut avec l' `vserver object-store-server modify` commande.

Seule la configuration locale de mappage de noms est prise en charge ; LDAP n'est pas prise en charge.

Une fois que les utilisateurs S3 sont mappés aux utilisateurs NAS, vous pouvez accorder des autorisations aux utilisateurs spécifiant les ressources (répertoires et fichiers) auxquelles ils ont accès et les actions qu'ils sont autorisés ou non à y effectuer.

System Manager

1. Créez des mappages de noms locaux pour les clients UNIX ou Windows (ou les deux).
 - a. Cliquez sur **stockage > compartiments**, puis sélectionnez la machine virtuelle de stockage compatible S3/NAS.
 - b. Sélectionnez **Paramètres**, puis cliquez sur → **mappage de noms** (sous **utilisateurs et groupes hôtes**).
 - c. Dans les mosaïques **S3 à Windows** ou **S3 à UNIX** (ou les deux), cliquez sur **Ajouter**, puis entrez les noms d'utilisateur **Pattern** (S3) et **Remplacement** (NAS) souhaités.
2. Création d'une politique de compartiment pour fournir un accès client
 - a. Cliquez sur **stockage > compartiments**, cliquez sur ⓘ en regard du compartiment S3 souhaité, puis cliquez sur **Modifier**.
 - b. Cliquez sur **Ajouter** et indiquez les valeurs souhaitées.
 - **Principal** - fournir des noms d'utilisateur S3 ou utiliser la valeur par défaut (tous les utilisateurs).
 - **Effet** - sélectionnez **Autoriser** ou **refuser**.
 - **Actions** - Entrez des actions pour ces utilisateurs et ressources. L'ensemble des opérations de ressources que le serveur de magasin d'objets prend actuellement en charge pour les compartiments NAS S3 sont : `GetObject`, `PutObject`, `DeleteObject`, `ListBucketAcl`, `GetObjectAcl`, `GetObjectTagging`, `PutObjectTagging`, `DeleteObjectTagging`, `GetBuckeLocation`, `GetBucketVersioning`, `PutBuckeVersioning` et `ListBuckeVersions`. Les caractères génériques sont acceptés pour ce paramètre.
 - **Ressources** - Entrez les chemins de dossier ou de fichier dans lesquels les actions sont autorisées ou refusées, ou utilisez les valeurs par défaut (répertoire racine du compartiment).

CLI

1. Créez des mappages de noms locaux pour les clients UNIX ou Windows (ou les deux).

```
vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix}  
-position integer -pattern s3_user_name -replacement nas_user_name
```

 - `-position` - numéro de priorité pour l'évaluation de la cartographie; saisissez 1 ou 2.
 - `-pattern` - Un nom d'utilisateur S3 ou une expression régulière
 - `-replacement` - un nom d'utilisateur windows ou unix

Exemples

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1  
-replacement win_user_1  
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1  
-replacement unix_user_1
```

1. Création d'une politique de compartiment pour fournir un accès client

```
vserver object-store-server bucket policy add-statement -vserver svm_name  
-bucket bucket_name -effect {deny|allow} -action list_of_actions -principal  
list_of_users_or_groups -resource [-sid alphanumeric_text]
```

 - `-effect {deny|allow}` - indique si l'accès est autorisé ou refusé lorsqu'un utilisateur demande une action.

- `-action <Action>, ...` - spécifie les opérations de ressources qui sont autorisées ou refusées. L'ensemble des opérations de ressources que le serveur de magasin d'objets prend actuellement en charge pour les compartiments NAS S3 sont : `GetObject`, `PutObject`, `DeleteObject`, `ListBucketAcl`, `GetObjectAcl`, `GetObjectTagging`, `PutObjectTagging`, `DeleteObjectTagging`, `GetBucketLocation`, `GetBucketVersioning`, `PutBucketVersioning` et `ListBucketVersions`. Les caractères génériques sont acceptés pour ce paramètre.
- `-principal <Objectstore Principal>, ...` - valide l'utilisateur demandant un accès par rapport aux utilisateurs ou aux groupes du serveur de magasin d'objets spécifiés dans ce paramètre.
 - Un groupe de serveurs de stockage d'objets est spécifié en ajoutant un groupe de préfixe/ au nom du groupe.
 - `-principal` - (le caractère de trait d'union) donne accès à tous les utilisateurs.
- `-resource <text>, ...` - spécifie le compartiment, le dossier ou l'objet pour lequel les autorisations d'autorisation/de refus sont définies. Les caractères génériques sont acceptés pour ce paramètre.
- `[-sid <SID>]` - spécifie un commentaire texte facultatif pour l'instruction de stratégie de compartiment de serveur de magasin d'objets.

Exemples

```
cluster1::> vsriver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vsriver object-store-server bucket policy statement create
-vsriver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

Configuration SMB pour Microsoft Hyper-V et SQL Server

Présentation de la configuration SMB pour Microsoft Hyper-V et SQL Server

Les fonctionnalités de ONTAP assurent la continuité de l'activité pour deux applications Microsoft sur le protocole SMB : Microsoft Hyper-V et Microsoft SQL Server.

Vous devez appliquer ces procédures pour implémenter une continuité de l'activité SMB dans les circonstances suivantes :

- L'accès de base aux fichiers du protocole SMB a été configuré.
- Vous souhaitez activer les partages de fichiers SMB 3.0 ou version ultérieure résidant sur les SVM pour stocker les objets suivants :
 - Fichiers de machines virtuelles Hyper-V.
 - Bases de données système SQL Server

Informations associées

Pour plus d'informations sur la technologie ONTAP et l'interaction avec les services externes, consultez ces

rapports techniques :

["Rapport technique de NetApp 4172 : Microsoft Hyper-V sur SMB 3.0 avec les meilleures pratiques de ONTAP"](#)

["Rapport technique NetApp 4369 : meilleures pratiques pour Microsoft SQL Server et SnapManager 7.2 for SQL Server avec clustered Data ONTAP"](#)

Configuration de ONTAP pour Microsoft Hyper-V et SQL Server sur les solutions SMB

Vous pouvez utiliser les partages de fichiers SMB 3.0 et versions ultérieures disponibles en permanence pour stocker les fichiers des machines virtuelles Hyper-V ou les bases de données du système SQL Server et les bases de données des utilisateurs sur des volumes résidant dans des SVM, tout en assurant la continuité de l'activité à la fois pour les événements planifiés et non planifiés.

Microsoft Hyper-V sur SMB

Pour créer une solution Hyper-V sur SMB, vous devez d'abord configurer ONTAP afin de fournir des services de stockage aux serveurs Microsoft Hyper-V. En outre, vous devez également configurer les clusters Microsoft (s'ils utilisent une configuration en cluster), les serveurs Hyper-V, les connexions SMB 3.0 disponibles en continu vers les partages hébergés par le serveur CIFS, et, éventuellement, les services de sauvegarde pour protéger les fichiers de machines virtuelles stockés sur les volumes de SVM.



Les serveurs Hyper-V doivent être configurés sur Windows 2012 Server ou version ultérieure. Les configurations de serveur Hyper-V autonomes et en cluster sont toutes deux prises en charge.

- Pour plus d'informations sur la création de clusters Microsoft et de serveurs Hyper-V, consultez le site Web de Microsoft.
- SnapManager for Hyper-V est une application basée sur hôte qui facilite les services de sauvegarde rapides basés sur des copies Snapshot. Elle est conçue pour s'intégrer aux configurations Hyper-V sur SMB.

Pour plus d'informations sur l'utilisation de SnapManager avec les configurations Hyper-V sur SMB, voir le *SnapManager for Hyper-V installation and Administration Guide*.

Microsoft SQL Server sur SMB

Pour créer une solution SQL Server sur SMB, vous devez d'abord configurer ONTAP afin de fournir des services de stockage pour l'application Microsoft SQL Server. En outre, vous devez également configurer les clusters Microsoft (en cas d'utilisation d'une configuration en cluster). Vous devez ensuite installer et configurer SQL Server sur les serveurs Windows et créer des connexions SMB 3.0 disponibles en continu vers les partages hébergés par le serveur CIFS. Vous pouvez choisir de configurer les services de sauvegarde pour protéger les fichiers de base de données stockés sur des volumes SVM.



SQL Server doit être installé et configuré sur Windows 2012 Server ou version ultérieure. Les configurations autonomes et en cluster sont prises en charge.

- Pour plus d'informations sur la création de clusters Microsoft et l'installation et la configuration de SQL Server, consultez le site Web de Microsoft.

- Le plug-in SnapCenter pour Microsoft SQL Server est une application basée sur hôte qui facilite les services de sauvegarde rapides et basés sur des copies Snapshot, conçus pour s'intégrer aux configurations SQL Server sur SMB.

Pour plus d'informations sur l'utilisation du plug-in SnapCenter pour Microsoft SQL Server, consultez le ["Plug-in SnapCenter pour Microsoft SQL Server" documentation](#) :

Continuité de l'activité pour Hyper-V et SQL Server over SMB

En termes de continuité de l'activité pour Hyper-V et SQL Server over SMB

La continuité de l'activité pour Hyper-V et SQL Server over SMB se réfère à la combinaison de fonctionnalités permettant aux serveurs d'application et aux machines virtuelles ou bases de données contenues de rester en ligne et d'assurer une disponibilité continue au cours de nombreuses tâches administratives. Cela inclut les temps d'indisponibilité planifiés et non planifiés de l'infrastructure de stockage.

La continuité de l'activité pour les serveurs applicatifs via SMB est prise en charge :

- Takeover et Giveback planifiées
- Basculement non planifié
- Mise à niveau
- Transfert d'agrégats planifié (ARL)
- Migration et basculement de LIF
- Déplacement de volume planifié

Protocoles qui garantissent la continuité de l'activité sur SMB

Outre la commercialisation de SMB 3.0, Microsoft a lancé de nouveaux protocoles qui fournissent les fonctionnalités nécessaires à la continuité de l'activité pour Hyper-V et SQL Server over SMB.

ONTAP utilise ces protocoles pour assurer la continuité de l'activité des serveurs applicatifs sur SMB :

- SMB 3.0
- Témoin

Concepts clés de la continuité de l'activité pour Hyper-V et SQL Server sur SMB

Avant de configurer la solution Hyper-V ou SQL Server sur SMB, certains concepts relatifs à la continuité de l'activité doivent être abordés.

• Partage disponible en continu

Partage SMB 3.0 avec la propriété de partage disponible en continu. Les clients qui se connectent via des partages disponibles en permanence peuvent survivre aux événements perturbateur tels que le basculement, le rétablissement et le transfert d'agrégats.

• Nœud

Un contrôleur unique membre d'un cluster. Pour faire la distinction entre les deux nœuds d'une paire SFO, un nœud est parfois appelé *local node* et l'autre nœud est parfois appelé *Partner node* ou *remote node*. Le propriétaire principal du stockage est le nœud local. Le propriétaire secondaire, qui prend le contrôle du stockage en cas de défaillance du propriétaire principal, est le nœud partenaire. Chaque nœud est le principal propriétaire de son stockage et du secondaire pour le stockage de son partenaire.

- **Transfert d'agrégats sans interruption**

Capacité à déplacer un agrégat entre les nœuds partenaires au sein d'une paire SFO dans un cluster sans interrompre les applications client.

- **Basculement sans interruption**

Voir *Takeover*.

- **Migration de LIF sans interruption**

La possibilité d'effectuer une migration de LIF sans interrompre les applications client qui sont connectées au cluster via cette LIF. Pour les connexions SMB, cette opération est uniquement possible pour les clients qui se connectent via SMB 2.0 ou version ultérieure.

- * Continuité de l'activité*

La possibilité d'effectuer les principales opérations de gestion et de mise à niveau ONTAP, et de résister aux défaillances de nœud sans interrompre les applications client. Ce terme fait référence à la collecte de fonctionnalités de basculement sans interruption, de mise à niveau sans interruption et de migration dans son ensemble.

- * Mise à niveau sans interruption*

Capacité à mettre à niveau le matériel ou les logiciels des nœuds sans perturber les applications.

- **Déplacement de volume sans interruption**

La capacité de déplacer librement un volume au sein du cluster sans interrompre les applications qui utilisent ce volume. Pour les connexions SMB, toutes les versions de SMB prennent en charge le déplacement de volumes sans interruption.

- **Poignées permanentes**

Propriété de SMB 3.0 qui permet aux connexions disponibles en continu de se reconnecter de façon transparente au serveur CIFS en cas de déconnexion. Tout comme les poignées durables, les poignées permanentes sont conservées par le serveur CIFS pendant un certain temps après la perte de la communication avec le client connecté. Toutefois, les pointeurs permanents bénéficient d'une résilience supérieure à celle des poignées durables. En plus de donner au client la possibilité de récupérer la poignée dans une fenêtre de 60 secondes après reconnexion, le serveur CIFS refuse l'accès à tout autre client demandant l'accès au fichier pendant cette fenêtre de 60 secondes.

Des informations relatives aux pointeurs permanents sont mises en miroir sur le stockage persistant du partenaire SFO, qui permet aux clients disposant de pointeurs permanents déconnectés de récupérer les pointeurs durables après un événement où le partenaire SFO est propriétaire du stockage du nœud. En plus d'assurer la continuité de l'activité en cas de déplacement de LIF (dont la prise en charge est durable), des pointeurs permanents assurent la continuité de l'activité pendant le basculement, le rétablissement et le transfert d'agrégats.

- **OFS-retour**

Retour d'agrégats à leurs locaux lors d'une récupération après un événement de basculement.

- **Paire SFO**

Si l'un des deux nœuds cesse de fonctionner, une paire de nœuds dont les contrôleurs sont configurés pour transmettre des données les uns aux autres. Selon le modèle du système, les deux contrôleurs peuvent se trouver dans un seul châssis ou les contrôleurs peuvent se trouver dans un châssis distinct. Appelée paire HA dans un cluster à deux nœuds.

- *** Prise de contrôle***

Processus par lequel le partenaire prend le contrôle du stockage en cas de défaillance du propriétaire principal de ce stockage. Dans le cadre du SFO, le basculement et le basculement sont synonymes.

La fonctionnalité SMB 3.0 prend en charge la continuité de l'activité sur les partages SMB

SMB 3.0 apporte une fonctionnalité essentielle qui permet la continuité de l'activité pour les partages Hyper-V et SQL Server sur SMB. Cela inclut le `continuously-available` Partagez la propriété et un type de descripteur de fichier appelé *persistent handle* qui permettent aux clients SMB de récupérer l'état ouvert du fichier et de rétablir de façon transparente les connexions SMB.

Des pointeurs permanents peuvent être accordés aux clients compatibles SMB 3.0 qui se connectent à un partage avec l'ensemble de propriétés de partage disponible en continu. Si la session SMB est déconnectée, le serveur CIFS conserve les informations relatives à l'état de descripteur permanent. Le serveur CIFS bloque les autres requêtes client pendant la période de 60 secondes pendant laquelle le client est autorisé à se reconnecter, ce qui permet au client avec le descripteur permanent de récupérer le descripteur après une déconnexion du réseau. Les clients avec pointeurs permanents peuvent se reconnecter en utilisant l'une des LIF de données sur la machine virtuelle de stockage (SVM), en reconnectant via la même LIF ou via une autre LIF.

Le transfert, le basculement et le rétablissement d'agrégats s'effectuent tous entre les paires SFO. Pour gérer de manière transparente la déconnexion et la reconnexion des sessions avec des fichiers dotés de pointeurs permanents, le nœud partenaire conserve une copie de toutes les informations de verrouillage de descripteur permanent. Que l'événement soit planifié ou non, le partenaire SFO peut gérer les reconnexions de la poignée persistante sans interruption. Grâce à cette nouvelle fonctionnalité, les connexions SMB 3.0 au serveur CIFS peuvent basculer en toute transparence vers une autre LIF de données affectée à la SVM, selon les temps d'événements perturbateurs.

Bien que l'utilisation de pointeurs permanents permette au serveur CIFS de basculer en toute transparence sur des connexions SMB 3.0, en cas de défaillance, l'application Hyper-V bascule vers un autre nœud du cluster Windows Server, le client n'a aucun moyen de récupérer les descripteurs de fichiers de ces pointeurs déconnectés. Dans ce scénario, les descripteurs de fichier à l'état déconnecté peuvent potentiellement bloquer l'accès à l'application Hyper-V s'il est redémarré sur un autre nœud. « Failover Clustering » fait partie de SMB 3.0 qui répond à ce scénario en fournissant un mécanisme permettant d'invalides des pointeurs obsolètes en conflit. Grâce à ce mécanisme, un cluster Hyper-V peut restaurer rapidement les données en cas de panne des nœuds de cluster Hyper-V.

Comment le protocole Witness traite l'amélioration du basculement transparent

Le protocole Witness propose des fonctionnalités de basculement client améliorées pour

les partages SMB 3.0 disponibles en continu (partages CA). Témoin facilite le basculement plus rapide car il évite toute période de restauration de basculement LIF. Cette notification avertit les serveurs d'applications lorsqu'un nœud est indisponible sans nécessiter l'attente de la connexion SMB 3.0.

Le basculement est transparent, car les applications s'exécutant sur le client ne savent pas qu'un basculement a eu lieu. Si Witness n'est pas disponible, le basculement s'effectue toujours avec succès, mais le basculement sans Witness s'avère moins efficace.

Le basculement amélioré par témoin est possible lorsque les conditions suivantes sont respectées :

- Il ne peut être utilisé qu'avec des serveurs CIFS compatibles SMB 3.0 sur lesquels SMB 3.0 est activé.
- Les partages doivent utiliser SMB 3.0 avec l'ensemble de propriétés de partage de disponibilité continue.
- Le partenaire SFO du nœud sur lequel les serveurs d'applications sont connectés doit disposer d'au moins une LIF de données opérationnelles attribuée au SVM (Storage Virtual machine) qui héberge les données des serveurs applicatifs.



Le protocole Witness fonctionne entre les paires SFO. Étant donné que les LIF peuvent migrer vers n'importe quel nœud du cluster, n'importe quel nœud peut avoir besoin d'être le témoin de son partenaire SFO. Le protocole Witness ne peut pas permettre le basculement rapide des connexions SMB sur un nœud donné si le SVM hébergeant les données des serveurs d'applications ne dispose pas d'une LIF de données active sur le nœud partenaire. Par conséquent, chaque nœud du cluster doit disposer d'au moins une LIF de données pour chaque SVM hébergeant l'une de ces configurations.

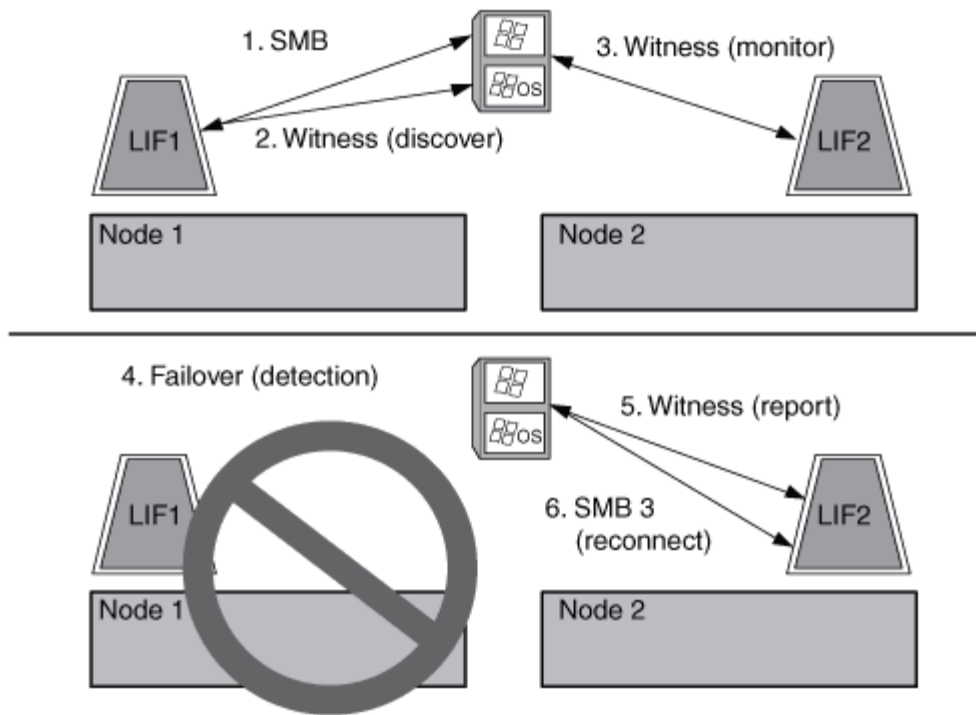
- Les serveurs d'applications doivent se connecter au serveur CIFS en utilisant le nom du serveur CIFS stocké dans DNS au lieu d'utiliser des adresses IP LIF individuelles.

Fonctionnement du protocole Witness

ONTAP implémente le protocole Witness en utilisant le partenaire SFO d'un nœud comme témoin. En cas de défaillance, le partenaire détecte rapidement la panne et en informe le client SMB.

Le protocole Witness fournit un basculement amélioré à l'aide du processus suivant :

1. Lorsque le serveur d'applications établit une connexion SMB disponible en continu pour Node1, le serveur CIFS informe le serveur d'applications que Witness est disponible.
2. Le serveur d'application demande les adresses IP du serveur Witness à partir du nœud 1 et reçoit une liste des adresses IP LIF de données Node2 (le partenaire SFO) attribuées à la machine virtuelle de stockage (SVM).
3. Le serveur d'application choisit l'une des adresses IP, crée une connexion témoin à Node2 et s'enregistre pour être averti si la connexion disponible en continu sur Node1 doit être déplacé.
4. Si un événement de basculement se produit sur le nœud 1, Witness simplifie les événements de basculement, mais n'est pas impliqué dans le rétablissement.
5. Témoin détecte l'événement de basculement et informe le serveur d'application via la connexion Witness que la connexion SMB doit passer à Node2.
6. Le serveur d'application déplace la session SMB sur Node2 et restaure la connexion sans interruption de l'accès client.



Partage de sauvegardes avec VSS distant

Présentation de VSS distant pour les sauvegardes basées sur le partage

Vous pouvez utiliser VSS distant pour effectuer des sauvegardes basées sur les partages des fichiers de machines virtuelles Hyper-V stockés sur un serveur CIFS.

Microsoft Remote VSS (Volume Shadow Copy Services) est une extension de l'infrastructure Microsoft VSS existante. Avec Remote VSS, Microsoft a étendu l'infrastructure VSS pour prendre en charge la copie Shadow des partages SMB. De plus, des applications serveur telles qu'Hyper-V peuvent stocker des fichiers VHD sur des partages de fichiers SMB. Avec ces extensions, il est possible d'effectuer des clichés instantanés cohérents avec les applications pour les machines virtuelles qui stockent des données et des fichiers de configuration sur des partages.

Concepts de VSS distant

Vous devez connaître certains concepts requis pour comprendre l'utilisation de VSS distant (Volume Shadow Copy Service) par les services de sauvegarde avec des configurations Hyper-V sur SMB.

- **VSS (Volume Shadow Copy Service)**

Technologie Microsoft utilisée pour effectuer des copies de sauvegarde ou des snapshots de données sur un volume spécifique à un point dans le temps spécifique. VSS coordonne entre les serveurs de données, les applications de sauvegarde et les logiciels de gestion du stockage afin d'assurer la création et la gestion de sauvegardes cohérentes.

- **VSS distant (Remote Volume Shadow Copy Service)**

Technologie Microsoft utilisée pour créer des copies de sauvegarde basées sur les partages de données qui sont cohérentes avec les données à un point spécifique dans le temps où les données sont accessibles via les partages SMB 3.0. Également connu sous le nom *Volume Shadow Copy Service*.

- **Copie fantôme**

Un jeu de données dupliqué contenu dans le partage à un instant bien défini dans le temps. Des clichés instantanés sont utilisés pour créer des sauvegardes ponctuelles cohérentes des données, permettant ainsi au système ou aux applications de continuer à mettre à jour les données sur les volumes d'origine.

- **Ensemble de copies ombré**

Collection d'une ou plusieurs clichés instantanés, chaque copie fantôme correspondant à un partage. Les clichés instantanés dans un jeu de clichés instantanés représentent tous les partages qui doivent être sauvegardés dans la même opération. Le client VSS de l'application VSS-enabled identifie les clichés instantanés à inclure dans l'ensemble.

- **Shadow Copy set Automatic Recovery**

La partie du processus de sauvegarde pour les applications de sauvegarde VSS distantes dans lesquelles le répertoire de réplica contenant les clichés instantanés est cohérent à un point dans le temps. Au début de la sauvegarde, le client VSS de l'application déclenche l'application pour qu'elle prenne des points de contrôle logiciels sur les données planifiées pour la sauvegarde (les fichiers de la machine virtuelle dans le cas d'Hyper-V). Le client VSS autorise alors les applications à continuer. Une fois le jeu de clichés instantanés créé, Remote VSS rend le jeu de clichés instantanés inscriptible et expose la copie inscriptible aux applications. L'application prépare le jeu de clichés instantanés pour la sauvegarde en effectuant une restauration automatique à l'aide du point de contrôle du logiciel précédemment effectué. La récupération automatique place les clichés instantanés dans un état cohérent en détournant les modifications apportées aux fichiers et répertoires depuis la création du point de contrôle. La restauration automatique est une étape facultative pour les sauvegardes VSS.

- **ID de copie fantôme**

GUID qui identifie de manière unique une copie en double.

- **ID jeu de copies ombré**

GUID qui identifie de manière unique une collection d'ID de copie en double sur le même serveur.

- **SnapManager pour Hyper-V**

Logiciel qui automatise et simplifie les opérations de sauvegarde et de restauration pour Microsoft Windows Server 2012 Hyper-V. SnapManager for Hyper-V utilise VSS distant avec restauration automatique pour sauvegarder des fichiers Hyper-V sur des partages SMB.

Informations associées

[Concepts clés de la continuité de l'activité pour Hyper-V et SQL Server sur SMB](#)

[Partage de sauvegardes avec VSS distant](#)

Exemple de structure de répertoire utilisée par VSS distant

VSS distant traverse la structure de répertoire qui stocke les fichiers de machine virtuelle Hyper-V lorsqu'il crée des clichés instantanés. Il est important de comprendre la structure de répertoires appropriée afin de pouvoir créer des sauvegardes de fichiers de machines virtuelles.

Une structure de répertoire prise en charge pour la création réussie de clichés instantanés est conforme aux

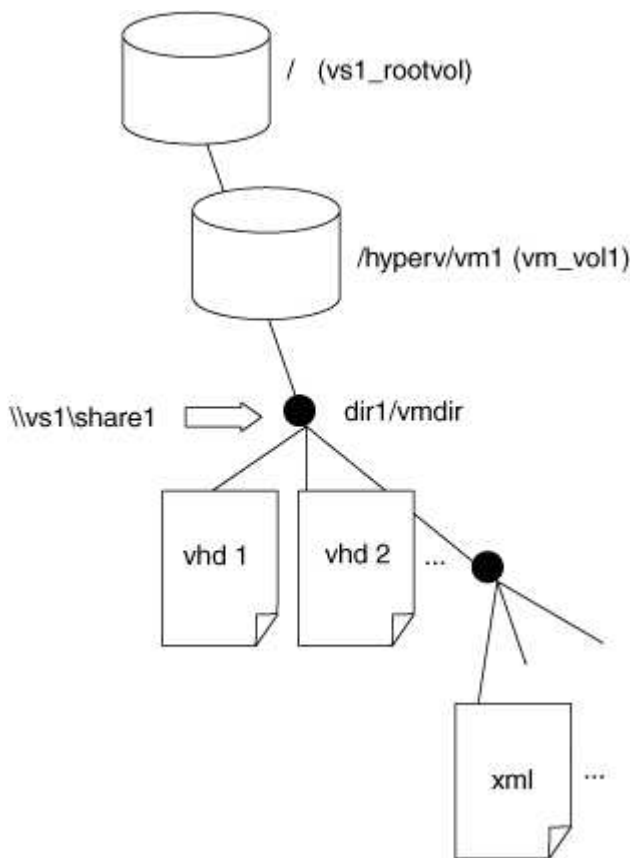
exigences suivantes :

- Seuls les répertoires et les fichiers réguliers sont présents dans la structure de répertoires utilisée pour stocker les fichiers de la machine virtuelle.

La structure du répertoire ne contient pas de jonctions, de liens ou de fichiers non réguliers.

- Tous les fichiers d'une machine virtuelle résident dans un même partage.
- La structure de répertoire utilisée pour stocker les fichiers de la machine virtuelle ne dépasse pas la profondeur configurée dans le répertoire de clichés instantanés.
- Le répertoire racine du partage contient uniquement des fichiers ou des répertoires de machine virtuelle.

Dans l'illustration suivante, le volume nommé `vm_vol1` est créé avec un point de jonction à `/hyperv/vm1` Sur la machine virtuelle de stockage (SVM) `vs1`. Les sous-répertoires contenant les fichiers de la machine virtuelle sont créés sous le point de jonction. Les fichiers de machine virtuelle du serveur Hyper-V sont accessibles sur `share1` qui a le chemin `/hyperv/vm1/dir1/vmdir`. Le service Shadow Copy crée des clichés instantanés de tous les fichiers de la machine virtuelle qui sont contenus dans la structure de répertoires sous `share1` (jusqu'à la profondeur configurée dans le répertoire Shadow Copy).



Comment SnapManager for Hyper-V gère les sauvegardes VSS distantes pour Hyper-V sur SMB

Vous pouvez utiliser SnapManager for Hyper-V pour gérer les services de sauvegarde VSS distants. Les avantages du service géré de sauvegarde SnapManager for Hyper-V sont nombreux, car il permet de créer des ensembles de sauvegarde peu gourmands en espace.

Les optimisations vers SnapManager pour les sauvegardes gérées Hyper-V sont les suivantes :

- L'intégration de SnapDrive avec ONTAP permet d'optimiser les performances lors de la détection de l'emplacement de partage SMB.

ONTAP fournit à SnapDrive le nom du volume où réside le partage.

- SnapManager for Hyper-V spécifie la liste des fichiers de machine virtuelle dans les partages SMB que le service Shadow Copy doit copier.

En fournissant une liste ciblée de fichiers de machine virtuelle, le service de clichés instantanés n'a pas besoin de créer de clichés instantanés de tous les fichiers du partage.

- Le serveur virtuel de stockage (SVM) conserve les copies Snapshot pour SnapManager pour Hyper-V utilisées pour les restaurations.

Il n'y a pas de phase de sauvegarde. La sauvegarde est la copie Snapshot compacte.

SnapManager for Hyper-V fournit des fonctionnalités de sauvegarde et de restauration pour HyperV sur SMB, en utilisant le processus suivant :

1. Préparation de l'opération de copie en double

Le client VSS de l'application SnapManager pour Hyper-V configure le jeu de clichés instantanés. Le client VSS collecte des informations sur les partages à inclure dans le jeu de clichés instantanés et fournit ces informations à ONTAP. Un ensemble peut contenir une ou plusieurs clichés instantanés et une copie en double correspond à un partage.

2. Création du jeu de clichés instantanés (si la restauration automatique est utilisée)

Pour chaque partage inclus dans le jeu de clichés instantanés, ONTAP crée une copie « shadow » et rend la copie « shadow Copy » accessible en écriture.

3. Exposition du jeu de clichés instantanés

Une fois que ONTAP a créé les clichés instantanés, ils sont exposés à SnapManager for Hyper-V de sorte que les enregistreurs VSS de l'application peuvent effectuer une restauration automatique.

4. Restauration automatique du jeu de clichés instantanés

Au cours de la création du jeu de clichés instantanés, il y a une période pendant laquelle des modifications actives sont apportées aux fichiers inclus dans le jeu de sauvegardes. Les VSS writer de l'application doivent mettre à jour les clichés instantanés pour s'assurer qu'ils sont dans un état complètement cohérent avant la sauvegarde.



La méthode d'exécution de la restauration automatique est spécifique à l'application. VSS distant n'est pas impliqué dans cette phase.

5. Finalisation et nettoyage du jeu de clichés instantanés

Le client VSS informe ONTAP après la fin de la restauration automatique. Le jeu de copies « shadow » est en lecture seule, puis prêt pour la sauvegarde. Lorsque vous utilisez SnapManager pour Hyper-V pour la sauvegarde, les fichiers d'une copie Snapshot deviennent la sauvegarde. Ainsi, pour la phase de sauvegarde, une copie Snapshot est créée pour chaque volume contenant des partages du jeu de sauvegarde. Une fois la sauvegarde terminée, le jeu de clichés instantanés est supprimé du serveur CIFS.

Comment l'allègement de la charge des copies d'ODX est utilisé avec Hyper-V et SQL Server sur des partages SMB

Offloaded Data Transfer (ODX), également appelé *copy Offload*, permet le transfert direct de données au sein d'un périphérique de stockage compatible ou entre ces périphériques, sans transférer les données via l'ordinateur hôte. Le allègement de la charge des copies ONTAP ODX présente des avantages en termes de performances lors des opérations de copie sur votre serveur applicatif plutôt que sur une installation SMB.

Dans les transferts de fichiers non ODX, les données sont lues à partir du serveur CIFS source et sont transférées sur le réseau vers l'ordinateur client. L'ordinateur client transfère les données via le réseau vers le serveur CIFS de destination. En résumé, l'ordinateur client lit les données à partir de la source et les écrit vers la destination. Grâce aux transferts de fichiers ODX, les données sont copiées directement de la source vers la destination.

Les copies déchargées d'ODX étant effectuées directement entre le stockage source et le stockage de destination, les performances sont considérablement améliorées. Les avantages obtenus en termes de performances comprennent l'accélération du délai de copie entre la source et la destination, la réduction de l'utilisation des ressources (CPU, mémoire) sur le client et la réduction de l'utilisation de la bande passante E/S du réseau.

ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0 continuously available connections.

Les cas d'utilisation suivants prennent en charge l'utilisation de copies et de déplacements d'ODX :

- Intra-volume

Les fichiers ou LUN source et de destination se trouvent dans le même volume.

- Inter-volumes, même nœud, même machine virtuelle de stockage (SVM)

Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur le même nœud. Les données sont détenues par le même SVM.

- Inter-volumes, nœuds différents, même SVM

Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par le même SVM.

- Inter-SVM, même nœud

Les fichiers source et de destination ou les LUN se trouvent sur des volumes différents situés sur le même nœud. Les données sont détenues par différents SVM.

- Inter-SVM, nœuds différents

Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par différents SVM.

Les cas d'utilisation spécifiques pour l'allègement de la charge des copies d'ODX avec les solutions Hyper-V

sont les suivants :

- Vous pouvez utiliser le pass-through ODX qui décharge les copies et Hyper-V pour copier des données dans ou sur des fichiers de disque dur virtuel (VHD), ou pour copier des données entre les partages SMB mappés et les LUN iSCSI connectés au sein du même cluster.

Ainsi, des copies des systèmes d'exploitation invités peuvent être transmis au stockage sous-jacent.

- Lors de la création de VHD de taille fixe, ODX permet d'initialiser le disque avec des zéros, à l'aide d'un jeton bien connu mis à zéro.
- L'allègement de la charge des copies d'ODX est utilisé pour la migration du stockage de machines virtuelles si le stockage source et cible est situé sur le même cluster.



Pour tirer parti des cas d'utilisation liés au déstage des copies ODX par Hyper-V, le système d'exploitation invité doit prendre en charge ODX. Les disques du système d'exploitation invité doivent être des disques SCSI pris en charge par le stockage (SMB ou SAN) prenant en charge ODX. Les disques IDE du système d'exploitation invité ne prennent pas en charge le pass-through ODX.

Voici quelques cas d'utilisation spécifiques des copies ODX utilisées par les solutions SQL Server :

- Vous pouvez utiliser l'allègement de la charge des copies d'ODX pour exporter et importer des bases de données SQL Server entre des partages SMB mappés ou entre des partages SMB et des LUN iSCSI connectés au sein du même cluster.
- L'allègement de la charge de copies (ODX) est utilisé pour les exportations et les importations de bases de données si le stockage source et cible est situé sur le même cluster.

Configuration requise et considérations

Conditions requises pour le ONTAP et les licences

Vous devez connaître certaines exigences en matière de licences et de ONTAP lors de la création de solutions SQL Server ou Hyper-V sur SMB afin de garantir la continuité de l'activité sur les SVM.

Configuration requise pour la version ONTAP

- Hyper-V sur SMB

ONTAP prend en charge la continuité de l'activité sur les partages SMB pour Hyper-V exécutés sous Windows 2012 ou version ultérieure.

- SQL Server sur SMB

ONTAP prend en charge la continuité de l'activité sur les partages SMB pour SQL Server 2012 ou une version ultérieure fonctionnant sous Windows 2012 ou version ultérieure.

Pour obtenir les dernières informations sur les versions prises en charge de ONTAP, Windows Server et SQL Server pour assurer la continuité de l'activité sur les partages SMB, consultez la matrice d'interopérabilité.

["Matrice d'interopérabilité NetApp"](#)

Licences requises

Les licences suivantes sont requises :

- CIFS
- FlexClone (pour Hyper-V sur SMB uniquement)

Cette licence est requise si Remote VSS est utilisé pour les sauvegardes. Le service Shadow Copy utilise FlexClone pour créer des copies instantanées de fichiers qui sont ensuite utilisés lors de la création d'une sauvegarde.

Une licence FlexClone est facultative si vous utilisez une méthode de sauvegarde qui n'utilise pas VSS distant.

La licence FlexClone est incluse dans ["ONTAP One"](#). Si vous n'avez pas ONTAP One, vous devriez ["vérifiez que les licences requises sont installées"](#), et, si nécessaire, ["installez-les"](#).

Exigences LIF relatives au réseau et aux données

Vous devez connaître certaines exigences LIF de réseau et de données lors de la création de configurations SQL Server ou Hyper-V sur SMB afin de garantir la continuité de l'activité).

Exigences en matière de protocoles réseau

- Les réseaux IPv4 et IPv6 sont pris en charge.
- SMB 3.0 ou version ultérieure requis.

SMB 3.0 apporte les fonctionnalités nécessaires pour créer les connexions SMB disponibles en continu nécessaires à la continuité de l'activité.

- Les serveurs DNS doivent contenir des entrées qui mappent le nom du serveur CIFS aux adresses IP attribuées aux LIF de données sur la machine virtuelle de stockage (SVM).

Les serveurs d'applications Hyper-V ou SQL Server font en général plusieurs connexions sur plusieurs LIF de données lors de l'accès aux fichiers de machines virtuelles ou de bases de données. Pour garantir la fonctionnalité appropriée, les serveurs d'applications doivent établir ces connexions SMB en utilisant le nom du serveur CIFS au lieu de créer plusieurs connexions à plusieurs adresses IP uniques.

Témoin exige également l'utilisation du nom DNS du serveur CIFS au lieu d'adresses IP LIF individuelles.

Depuis ONTAP 9.4, SMB Multichannel permet d'améliorer le débit et la tolérance aux pannes des configurations Hyper-V et SQL Server sur SMB. Pour ce faire, vous devez avoir plusieurs cartes réseau 1G, 10G ou plus grandes déployées sur le cluster et les clients.

Configuration requise pour Data LIF

- La SVM hébergeant le serveur d'application sur la solution SMB doit disposer d'au moins une LIF de données opérationnelles sur chaque nœud du cluster.

Les LIFs de données SVM peuvent basculer vers d'autres ports de données du cluster, y compris les nœuds qui n'hébergent pas actuellement les données accessibles par les serveurs applicatifs. De plus, comme le nœud Witness est toujours le partenaire SFO d'un nœud sur lequel le serveur d'applications est

connecté, chaque nœud du cluster est un nœud potentiel Witness.

- Les LIF de données ne doivent pas être configurées pour rétablir automatiquement ces données.

Après un événement de basculement ou de rétablissement, vous devez rétablir manuellement les LIF de données sur leurs ports de rattachement.

- Toutes les adresses IP de la LIF de données doivent disposer d'une entrée dans DNS et toutes les entrées doivent se résoudre au nom du serveur CIFS.

Les serveurs d'applications doivent se connecter aux partages SMB à l'aide du nom du serveur CIFS. Vous ne devez pas configurer les serveurs d'application pour établir des connexions en utilisant les adresses IP de la LIF.

- Si le nom du serveur CIFS est différent du nom du SVM, les entrées DNS doivent être résolus sur le nom du serveur CIFS.

Exigences en termes de volumes et de serveurs SMB pour Hyper-V sur SMB

Vous devez tenir compte de certaines exigences en matière de volume et de serveur SMB lors de la création de configurations Hyper-V sur SMB afin de garantir la continuité de l'activité.

Configuration requise pour les serveurs SMB

- SMB 3.0 doit être activé.

Cette option est activée par défaut.

- L'option de serveur CIFS utilisateur UNIX par défaut doit être configurée avec un compte utilisateur UNIX valide.

Les serveurs d'applications utilisent le compte machine lors de la création d'une connexion SMB. Comme tout accès SMB nécessite que l'utilisateur Windows soit correctement mappé à un compte d'utilisateur UNIX ou au compte d'utilisateur UNIX par défaut, ONTAP doit pouvoir mapper le compte machine du serveur d'applications sur le compte d'utilisateur UNIX par défaut.

- Les référencements de nœuds automatiques doivent être désactivés (cette fonctionnalité est désactivée par défaut).

Si vous souhaitez utiliser les référencements de nœuds automatiques pour l'accès aux données autres que les fichiers des machines Hyper-V, vous devez créer un SVM distinct pour ces données.

- L'authentification Kerberos et NTLM doit être autorisée dans le domaine auquel le serveur SMB appartient.

ONTAP ne fait pas la promotion du service Kerberos pour VSS distant ; par conséquent, le domaine doit être défini pour autoriser NTLM.

- La fonctionnalité Shadow Copy doit être activée.

Cette fonctionnalité est activée par défaut.

- Le compte de domaine Windows utilisé par le service de copie instantanée lors de la création de copies en double doit être membre du groupe local BULILTIN\Administrators ou BULILTIN\Backup Operators du serveur SMB.

Besoins en termes de volume

- Les volumes utilisés pour stocker les fichiers de la machine virtuelle doivent être créés en tant que volumes de sécurité NTFS.

Pour fournir des NDO aux serveurs d'applications utilisant des connexions SMB disponibles en continu, le volume contenant le partage doit être un volume NTFS. En outre, il doit toujours avoir été un volume NTFS. Vous ne pouvez pas modifier un volume mixte de style de sécurité ou un volume de style de sécurité UNIX en un volume de type sécurité NTFS et l'utiliser directement pour les NDO sur des partages SMB. Si vous modifiez un volume de style de sécurité mixte en volume de style de sécurité NTFS et que vous envisagez de l'utiliser pour les NDO sur des partages SMB, vous devez placer manuellement une ACL en haut du volume et propager cette ACL à tous les fichiers et dossiers contenus. Autrement, les migrations de machine virtuelle ou les exportations de fichiers de base de données et les importations où les fichiers sont déplacés vers un autre volume peuvent échouer si les volumes source ou de destination ont été initialement créés sous forme de volumes de sécurité mixtes ou UNIX, puis modifiés vers le style de sécurité NTFS.

- Pour que les opérations de copie en mode « shadow » aient réussi, vous devez disposer de suffisamment d'espace disponible sur le volume.

L'espace disponible doit être au moins aussi grand que l'espace combiné utilisé par tous les fichiers, répertoires et sous-répertoires contenus dans les partages inclus dans le jeu de sauvegarde Shadow Copy. Cette exigence s'applique uniquement aux clichés instantanés avec la restauration automatique.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Besoins en volume et serveur SMB pour SQL Server sur SMB

Pour assurer la continuité de l'activité, vous devez tenir compte des exigences en matière de volumes et de serveurs SMB lors de la création de configurations SQL Server sur SMB.

Configuration requise pour les serveurs SMB

- SMB 3.0 doit être activé.

Cette option est activée par défaut.

- L'option de serveur CIFS utilisateur UNIX par défaut doit être configurée avec un compte utilisateur UNIX valide.

Les serveurs d'applications utilisent le compte machine lors de la création d'une connexion SMB. Comme tout accès SMB nécessite que l'utilisateur Windows soit correctement mappé à un compte d'utilisateur UNIX ou au compte d'utilisateur UNIX par défaut, ONTAP doit pouvoir mapper le compte machine du serveur d'applications sur le compte d'utilisateur UNIX par défaut.

En outre, SQL Server utilise un utilisateur de domaine comme compte de service SQL Server. Le compte de service doit également être mappé à l'utilisateur UNIX par défaut.

- Les référencements de nœuds automatiques doivent être désactivés (cette fonctionnalité est désactivée par défaut).

Si vous souhaitez utiliser les référencements de nœuds automatiques pour l'accès aux données autres

que les fichiers de bases de données SQL Server, vous devez créer un SVM distinct pour ces données.

- Le privilège SeSecurityPrivilege doit être attribué au compte utilisateur Windows utilisé pour installer SQL Server sur ONTAP.

Ce privilège est attribué au groupe local BUILTIN\Administrators du serveur SMB.

Besoins en termes de volume

- Les volumes utilisés pour stocker les fichiers de la machine virtuelle doivent être créés en tant que volumes de sécurité NTFS.

Pour fournir des NDO aux serveurs d'applications utilisant des connexions SMB disponibles en continu, le volume contenant le partage doit être un volume NTFS. En outre, il doit toujours avoir été un volume NTFS. Vous ne pouvez pas modifier un volume mixte de style de sécurité ou un volume de style de sécurité UNIX en un volume de type sécurité NTFS et l'utiliser directement pour les NDO sur des partages SMB. Si vous modifiez un volume de style de sécurité mixte en volume de style de sécurité NTFS et que vous envisagez de l'utiliser pour les NDO sur des partages SMB, vous devez placer manuellement une ACL en haut du volume et propager cette ACL à tous les fichiers et dossiers contenus. Autrement, les migrations de machine virtuelle ou les exportations de fichiers de base de données et les importations où les fichiers sont déplacés vers un autre volume peuvent échouer si les volumes source ou de destination ont été initialement créés sous forme de volumes de sécurité mixtes ou UNIX, puis modifiés vers le style de sécurité NTFS.

- Bien que le volume contenant les fichiers de base de données puisse contenir des jonctions, SQL Server ne traverse pas les jonctions lors de la création de la structure du répertoire de base de données.
- Pour que les opérations de sauvegarde du plug-in SnapCenter pour Microsoft SQL Server réussissent, vous devez disposer de suffisamment d'espace disponible sur le volume.

Le volume sur lequel les fichiers de base de données SQL Server résident doit être suffisamment grand pour contenir la structure du répertoire de base de données et tous les fichiers contenus résidant dans le partage.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Exigences de partage constamment disponibles et considérations pour Hyper-V sur SMB

Vous devez connaître certaines exigences et considérations relatives à la configuration de partages disponibles en continu pour les configurations Hyper-V sur SMB qui prennent en charge la continuité de l'activité.

Exigences en matière de partage

- Les partages utilisés par les serveurs d'applications doivent être configurés avec le jeu de propriétés disponible en continu.

Les serveurs d'application qui se connectent aux partages disponibles en permanence sont dotés de pointeurs permanents qui leur permettent de se reconnecter sans interruption aux partages SMB et de récupérer les verrouillages de fichiers après des événements perturbateurs, tels que le basculement, le rétablissement et le transfert d'agrégats.

- Si vous souhaitez utiliser les services de sauvegarde Remote VSS-enabled, vous ne pouvez pas placer de

fichiers Hyper-V dans des partages contenant des jonctions.

Dans le cas de la récupération automatique, la création de clichés instantanés échoue si une jonction est détectée lors du déplacement du partage. Dans le cas non auto-Recovery, la création de la copie en double ne échoue pas, mais la jonction ne pointe en rien.

- Si vous souhaitez utiliser les services de sauvegarde Remote VSS-enabled avec auto-Recovery, vous ne pouvez pas placer les fichiers Hyper-V dans des partages contenant les éléments suivants :
 - Symlinks, liens rigides ou widelinks
 - Fichiers non standard

La création de la copie en double échoue si des liens ou des fichiers non standard se trouvent dans le partage vers copie en double. Cette exigence s'applique uniquement aux clichés instantanés avec la restauration automatique.

- Pour que les opérations de clichés instantanés réussisse, vous devez disposer d'un espace disponible suffisant sur le volume (pour Hyper-V sur SMB uniquement).

L'espace disponible doit être au moins aussi grand que l'espace combiné utilisé par tous les fichiers, répertoires et sous-répertoires contenus dans les partages inclus dans le jeu de sauvegarde Shadow Copy. Cette exigence s'applique uniquement aux clichés instantanés avec la restauration automatique.

- Les propriétés de partage suivantes ne doivent pas être définies sur les partages disponibles en continu utilisés par les serveurs d'applications :
 - Répertoire de base
 - Mise en cache des attributs
 - BranchCache

Considérations

- Les quotas sont pris en charge par les partages disponibles en permanence.
- La fonctionnalité suivante n'est pas prise en charge pour les configurations Hyper-V sur SMB :
 - Audit
 - FPolicy
- L'analyse antivirus n'est pas réalisée sur les partages SMB avec le `continuously-availability` paramètre défini sur `Yes`.

Exigences en matière de partages disponibles en permanence et considérations pour SQL Server sur SMB

Vous devez connaître certaines exigences et considérations relatives à la configuration de partages disponibles en continu pour les configurations SQL Server sur SMB qui prennent en charge la continuité de l'activité.

Exigences en matière de partage

- Les volumes utilisés pour stocker les fichiers de la machine virtuelle doivent être créés en tant que volumes de sécurité NTFS.

Pour assurer la continuité de l'activité des serveurs applicatifs en utilisant des connexions SMB disponibles

en continu, le volume contenant le partage doit être un volume NTFS. En outre, il doit toujours avoir été un volume NTFS. Vous ne pouvez pas modifier un volume mixte de style de sécurité ou un volume de style de sécurité UNIX en un volume NTFS de type sécurité, et l'utiliser directement pour la continuité de l'activité sur les partages SMB. Si vous remplacez un volume de style de sécurité mixte par un volume de style de sécurité NTFS et que vous prévoyez de l'utiliser pour assurer la continuité des opérations sur des partages SMB, vous devez placer manuellement une liste de contrôle d'accès en haut du volume et la propager à tous les fichiers et dossiers contenus. Autrement, les migrations de machine virtuelle ou les exportations de fichiers de base de données et les importations où les fichiers sont déplacés vers un autre volume peuvent échouer si les volumes source ou de destination ont été initialement créés sous forme de volumes de sécurité mixtes ou UNIX, puis modifiés vers le style de sécurité NTFS.

- Les partages utilisés par les serveurs d'applications doivent être configurés avec le jeu de propriétés disponible en continu.

Les serveurs d'application qui se connectent aux partages disponibles en permanence sont dotés de pointeurs permanents qui leur permettent de se reconnecter sans interruption aux partages SMB et de récupérer les verrouillages de fichiers après des événements perturbateurs, tels que le basculement, le rétablissement et le transfert d'agrégats.

- Bien que le volume contenant les fichiers de base de données puisse contenir des jonctions, SQL Server ne traverse pas les jonctions lors de la création de la structure du répertoire de base de données.
- Pour que les opérations du plug-in SnapCenter pour Microsoft SQL Server réussissent, vous devez disposer de suffisamment d'espace disponible sur le volume.

Le volume sur lequel les fichiers de base de données SQL Server résident doit être suffisamment grand pour contenir la structure du répertoire de base de données et tous les fichiers contenus résidant dans le partage.

- Les propriétés de partage suivantes ne doivent pas être définies sur les partages disponibles en continu utilisés par les serveurs d'applications :
 - Répertoire de base
 - Mise en cache des attributs
 - BranchCache

Partager des considérations

- Les quotas sont pris en charge par les partages disponibles en permanence.
- La fonctionnalité suivante n'est pas prise en charge dans les configurations SQL Server sur SMB :
 - Audit
 - FPolicy
- L'analyse antivirus n'est pas réalisée sur les partages SMB avec le `continuously-availability` ensemble de propriétés de partage.

Considérations relatives à VSS distant pour les configurations Hyper-V sur SMB

Vous devez tenir compte de certains éléments à prendre en compte lors de l'utilisation de solutions de sauvegarde Remote VSS-enabled pour les configurations Hyper-V over SMB.

Considérations générales de VSS distant

- Un maximum de 64 partages peut être configuré par serveur d'applications Microsoft.

L'opération de copie en double échoue si plus de 64 partages se trouvent dans un jeu de clichés instantanés. Il s'agit d'une condition requise par Microsoft.

- Un seul jeu de clichés instantanés actif par serveur CIFS est autorisé.

Une opération de copie en double échouera si une opération de copie en double est en cours sur le même serveur CIFS. Il s'agit d'une condition requise par Microsoft.

- Aucune jonction n'est autorisée dans la structure de répertoire sur laquelle VSS distant crée une copie en double.
 - Dans le cas de la restauration automatique, la création de clichés instantanés échouera si une jonction est rencontrée lors du déplacement du partage.
 - Dans le cas de restauration non automatique, la création de clichés instantanés ne échoue pas, mais la jonction ne pointe en rien.

Considérations relatives à la VSS distante qui ne s'appliquent qu'aux clichés instantanés avec restauration automatique

Certaines limites s'appliquent uniquement aux clichés instantanés avec restauration automatique.

- Une profondeur maximale de répertoire de cinq sous-répertoires est autorisée pour la création de clichés instantanés.

Il s'agit de la profondeur du répertoire sur laquelle le service Shadow Copy crée un jeu de sauvegarde Shadow Copy. La création de clichés instantanés échoue si les répertoires contenant un fichier de machine virtuelle sont imbriqués de plus de cinq niveaux. Cela permet de limiter la traversée de répertoire lors du clonage du partage. La profondeur maximale de répertoire peut être modifiée à l'aide d'une option de serveur CIFS.

- La quantité d'espace disponible sur le volume doit être adéquate.

L'espace disponible doit être au moins aussi grand que l'espace combiné utilisé par tous les fichiers, répertoires et sous-répertoires contenus dans les partages inclus dans le jeu de sauvegarde Shadow Copy.

- Aucun lien ou fichier non régulier n'est autorisé dans la structure de répertoires sur laquelle VSS distant crée une copie en double.

La création de la copie en double échoue si des liens ou des fichiers non standard se trouvent dans le partage vers la copie en double. Le processus de clonage ne les prend pas en charge.

- Les répertoires ne sont pas autorisés à ACL NFSv4.

Bien que la création de clichés instantanés conserve les listes de contrôle d'accès NFSv4 sur les fichiers, les listes de contrôle d'accès NFSv4 sur les répertoires sont perdues.

- Un maximum de 60 secondes est autorisé à créer un jeu de clichés instantanés.

Les spécifications Microsoft permettent de créer le jeu de clichés instantanés pendant 60 secondes au maximum. Si le client VSS ne peut pas créer l'ensemble de clichés instantanés dans ce délai, l'opération de copie en double échoue ; ceci limite donc le nombre de fichiers dans un jeu de clichés instantanés. Le nombre réel de fichiers ou de machines virtuelles pouvant être inclus dans un jeu de sauvegardes varie ;

ce nombre dépend de nombreux facteurs et doit être déterminé pour chaque environnement du client.

Conditions d'allègement de la charge des copies d'ODX pour SQL Server et Hyper-V sur SMB

L'allègement de la charge des copies (ODX) doit être activé pour migrer les fichiers de machines virtuelles ou pour exporter et importer les fichiers de base de données directement depuis la source vers l'emplacement de stockage de destination, sans envoyer de données par le biais des serveurs applicatifs. Certaines exigences sont à prendre en compte lors de l'utilisation de l'allègement de la charge des copies d'ODX avec les solutions SQL Server et Hyper-V sur SMB.

L'utilisation de l'allègement de la charge des copies (ODX) offre des performances importantes. Cette option de serveur CIFS est activée par défaut.

- SMB 3.0 doit être activé pour utiliser l'allègement de la charge des copies (ODX).
- Les volumes source doivent être d'au moins 1.25 Go.
- La déduplication doit être activée sur les volumes utilisés avec l'allègement de la charge des copies.
- Si vous utilisez des volumes compressés, le type de compression doit être adaptatif et seule la taille de groupe de compression de 8 Ko est prise en charge.

Le type de compression secondaire n'est pas pris en charge

- Pour utiliser le délestage des copies ODX pour migrer des invités Hyper-V dans et entre les disques, les serveurs Hyper-V doivent être configurés pour utiliser des disques SCSI.

La valeur par défaut consiste à configurer des disques IDE, mais l'allègement de charge des copies d'ODX ne fonctionne pas lorsque les invités sont migrés si des disques sont créés à l'aide de disques IDE.

Recommandations concernant les configurations SQL Server et Hyper-V sur SMB

Pour être certain que vos configurations SQL Server et Hyper-V sur SMB sont robustes et opérationnelles, vous devez connaître les meilleures pratiques recommandées lors de la configuration des solutions.

Recommandations générales

- Séparez les fichiers du serveur d'applications des données générales de l'utilisateur.

Si possible, consacrer un SVM complet et son stockage aux données du serveur d'applications.

- Pour obtenir les meilleures performances, n'activez pas la signature SMB sur les SVM utilisés pour stocker les données du serveur d'applications.
- Pour des performances optimales et une meilleure tolérance aux pannes, SMB Multichannel permet de fournir plusieurs connexions entre ONTAP et les clients au cours d'une seule session SMB.
- Ne créez pas de partages disponibles en permanence sur d'autres partages que ceux utilisés dans la configuration Hyper-V ou SQL Server sur SMB.
- Désactiver l'alerte de modification sur les partages utilisés pour la disponibilité continue.
- N'effectuez pas de déplacement de volume simultanément au transfert d'agrégats (ARL), car les phases

de l'ARL sont suspendues.

- Pour les solutions Hyper-V sur SMB, utilisez des disques iSCSI invités lors de la création de machines virtuelles en cluster. Partagée .VHDX Les fichiers ne sont pas pris en charge par Hyper-V sur SMB dans les partages ONTAP SMB.

Planifiez la configuration Hyper-V ou SQL Server sur SMB

Renseignez la fiche technique de configuration des volumes

Cette fiche fournit un moyen simple d'enregistrer les valeurs nécessaires lors de la création de volumes pour les configurations SQL Server et Hyper-V sur SMB.

Pour chaque volume, vous devez spécifier les informations suivantes :

- Nom de la machine virtuelle de stockage (SVM)

Le nom du SVM est identique pour tous les volumes.

- Nom du volume
- Nom de l'agrégat

Vous pouvez créer des volumes sur des agrégats situés sur n'importe quel nœud du cluster.

- Taille
- Un chemin de jonction

Lorsque vous créez des volumes utilisés pour stocker des données de serveur d'applications, vous devez garder à l'esprit les éléments suivants :

- Si le volume racine n'a pas de style de sécurité NTFS, vous devez spécifier le style de sécurité comme NTFS lorsque vous créez le volume.

Par défaut, les volumes héritent du style de sécurité du volume root du SVM.

- Les volumes doivent être configurés avec la garantie d'espace du volume par défaut.
- Vous pouvez éventuellement configurer le paramètre de gestion de l'espace de dimensionnement automatique.
- Vous devez définir l'option qui détermine la réserve d'espace de copie Snapshot sur 0.
- La politique Snapshot appliquée au volume doit être désactivée.

Si la SVM Snapshot policy est désactivée, il n'est donc pas nécessaire de spécifier une policy Snapshot pour les volumes. Les volumes héritent de la politique Snapshot pour le SVM. Si la politique Snapshot de la SVM n'est pas désactivée et qu'elle est configurée pour créer des copies Snapshot, vous devez spécifier une policy Snapshot au niveau du volume, et cette policy doit être désactivée. Les sauvegardes Shadow Copy et les sauvegardes SQL Server gèrent la création et la suppression de copies Snapshot.

- Vous ne pouvez pas configurer de miroirs de partage de charge pour les volumes.

Les chemins de jonction sur lesquels vous prévoyez de créer des partages que les serveurs d'applications doivent être choisis de sorte qu'aucun volume relié par jonction ne se trouve sous le point d'entrée du partage.

Par exemple, si vous souhaitez stocker des fichiers de machine virtuelle sur quatre volumes nommés « vol1 »,

« vol2 », « vol3 » et « vol4 », vous pouvez créer l'espace de noms indiqué dans l'exemple. Vous pouvez ensuite créer des partages pour les serveurs d'applications aux chemins suivants : /data1/vol1, /data1/vol2, /data2/vol3, et /data2/vol4.

Vserver	Volume	Junction		Junction Path	Junction Path Source
		Active			
vs1	data1	true		/data1	RW_volume
vs1	vol1	true		/data1/vol1	RW_volume
vs1	vol2	true		/data1/vol2	RW_volume
vs1	data2	true		/data2	RW_volume
vs1	vol3	true		/data2/vol3	RW_volume
vs1	vol4	true		/data2/vol4	RW_volume

Types d'information	Valeurs
<i>Volume 1 : nom du volume, agrégat, taille, Junction path</i>	
<i>Volume 2 : nom du volume, agrégat, taille, chemin de jonction</i>	
<i>Volume 3 : nom du volume, agrégat, taille, chemin de jonction</i>	
<i>Volume 4 : nom du volume, agrégat, taille, chemin de jonction</i>	
<i>Volume 5 : nom du volume, agrégat, taille, chemin de jonction</i>	
<i>Volume 6 : nom du volume, agrégat, taille, chemin de jonction</i>	
<i>Volumes supplémentaires : nom du volume, agrégat, taille, Junction path</i>	

Remplissez la fiche de configuration du partage SMB

Cette fiche vous permet d'enregistrer les valeurs dont vous avez besoin lors de la création de partages SMB disponibles en continu pour les configurations SQL Server et Hyper-V sur SMB.

Informations sur les propriétés des partages SMB et les paramètres de configuration

Pour chaque partage, vous devez spécifier les informations suivantes :

- Nom de la machine virtuelle de stockage (SVM)

Le nom du SVM est identique pour tous les partages

- Nom de partage
- Chemin
- Propriétés du partage

Vous devez configurer les deux propriétés de partage suivantes :

- `oplocks`
- `continuously-available`

Les propriétés de partage suivantes ne doivent pas être définies :

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
 - Les symlinks doivent être désactivés (la valeur de l' `-symlink-properties` le paramètre doit être nul `[""]`).

Informations sur les chemins de partage

Si vous utilisez VSS distant pour sauvegarder les fichiers Hyper-V, il est important de choisir les chemins de partage à utiliser lors des connexions SMB des serveurs Hyper-V vers les emplacements de stockage dans lesquels sont stockés les fichiers des machines virtuelles. Bien que les partages peuvent être créés à tout moment dans l'espace de noms, les chemins pour les partages utilisés par les serveurs Hyper-V ne doivent pas contenir de volumes reliés. Les opérations de copie en double ne peuvent pas être effectuées sur des chemins de partage qui contiennent des points de jonction.

SQL Server ne peut pas traverser les jonctions lors de la création de la structure du répertoire de la base de données. Vous ne devez pas créer de chemins de partage pour SQL Server contenant des points de jonction.

Par exemple, si vous souhaitez stocker des fichiers de machine virtuelle ou de base de données sur des volumes « vol1 », « vol2 », « vol3 » et « vol4 », vous devez créer des partages pour les serveurs d'applications aux chemins suivants : `/data1/vol1`, `/data1/vol2`, `/data2/vol3`, et `/data2/vol4`.

Vserver	Volume	Junction		Junction Path	Junction Source
		Active	Junction Path		
vs1	data1	true	/data1		RW_volume
vs1	vol1	true	/data1/vol1		RW_volume
vs1	vol2	true	/data1/vol2		RW_volume
vs1	data2	true	/data2		RW_volume
vs1	vol3	true	/data2/vol3		RW_volume
vs1	vol4	true	/data2/vol4		RW_volume



Bien que vous puissiez créer des partages sur le /data1 et /data2 chemins de gestion administrative, vous ne devez pas configurer les serveurs d'applications pour utiliser ces partages pour stocker des données.

Fiche de planification

Types d'information	Valeurs
<i>Volume 1 : nom du partage SMB et chemin</i>	
<i>Volume 2 : nom et chemin du partage SMB</i>	
<i>Volume 3 : nom et chemin du partage SMB</i>	
<i>Volume 4 : nom et chemin du partage SMB</i>	
<i>Volume 5 : nom et chemin du partage SMB</i>	
<i>Volume 6 : nom et chemin du partage SMB</i>	
<i>Volume 7 : nom et chemin du partage SMB</i>	
<i>Volumes supplémentaires : noms et chemins de partage SMB</i>	

Créez des configurations ONTAP pour la continuité de l'activité avec Hyper-V et SQL Server over SMB

Créez des configurations ONTAP pour la continuité de l'activité grâce à la présentation Hyper-V et SQL Server sur SMB

Vous devez effectuer plusieurs étapes de configuration ONTAP pour préparer les installations Hyper-V et SQL Server qui assurent la continuité de l'activité sur SMB.

Avant de créer la configuration ONTAP pour la continuité de l'activité avec Hyper-V et SQL Server sur SMB, les tâches suivantes doivent être effectuées :

- Les services de temps doivent être configurés sur le cluster.
- La mise en réseau doit être configurée pour le SVM.
- Le SVM doit être créé.
- Les interfaces LIF de données doivent être configurées sur le SVM.
- DNS doit être configuré sur le SVM.
- Les services de noms souhaités doivent être configurés pour la SVM.
- Le serveur SMB doit être créé.

Informations associées

Vérifier que les authentifications Kerberos et NTLMv2 sont autorisées (Hyper-V sur les partages SMB)

La continuité de l'activité pour Hyper-V over SMB requiert que le serveur CIFS d'un SVM de données et le serveur Hyper-V autorisent l'authentification Kerberos et NTLMv2. Vous devez vérifier les paramètres du serveur CIFS et des serveurs Hyper-V qui contrôlent les méthodes d'authentification autorisées.

Description de la tâche

L'authentification Kerberos est requise lors de la mise en place d'une connexion de partage disponible en continu. Une partie du processus VSS distant utilise l'authentification NTLMv2. Par conséquent, les connexions utilisant les deux méthodes d'authentification doivent être prises en charge dans les configurations Hyper-V sur SMB.

Les paramètres suivants doivent être configurés pour autoriser l'authentification Kerberos et NTLMv2 :

- Les export policy pour SMB doivent être désactivées sur le serveur virtuel de stockage (SVM).

Les authentifications Kerberos et NTLMv2 sont toujours activées sur les SVM, mais les règles d'exportation peuvent être utilisées pour limiter l'accès en fonction de la méthode d'authentification.

Les export policy pour SMB sont facultatives et désactivées par défaut. Si les règles d'exportation sont désactivées, l'authentification Kerberos et NTLMv2 sont autorisées par défaut sur un serveur CIFS.

- Le domaine auquel le serveur CIFS et les serveurs Hyper-V appartiennent doit autoriser l'authentification Kerberos et NTLMv2.

L'authentification Kerberos est activée par défaut sur les domaines Active Directory. Toutefois, l'authentification NTLMv2 peut être refusée, en utilisant des paramètres de stratégie de sécurité ou des stratégies de groupe.

Étapes

1. Effectuer les opérations suivantes pour vérifier que les export policies sont désactivée sur le SVM:

- a. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

- b. Vérifiez que le `-is-exportpolicy-enabled` L'option de serveur CIFS est définie sur `false`:

```
vserver cifs options show -vserver vserver_name -fields vserver,is-exportpolicy-enabled
```

- c. Retour au niveau de privilège admin :

```
set -privilege admin
```

2. Si les export policy pour SMB ne sont pas désactivées, désactivez-les :

```
vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false
```

3. Vérifiez que les authentifications NTLMv2 et Kerberos sont autorisées dans le domaine.

Pour plus d'informations sur la détermination des méthodes d'authentification autorisées dans le domaine, consultez la bibliothèque Microsoft TechNet.

4. Si le domaine n'autorise pas l'authentification NTLMv2, activez l'authentification NTLMv2 en utilisant l'une des méthodes décrites dans la documentation Microsoft.

Exemple

Les commandes suivantes vérifient que les export policies pour SMB sont désactivées sur le SVM vs1 :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-----  -----
vs1      false

cluster1::*> set -privilege admin
```

Vérifiez que les comptes de domaine sont mis en correspondance avec l'utilisateur UNIX par défaut

Hyper-V et SQL Server utilisent des comptes de domaine pour créer des connexions SMB à des partages disponibles en continu. Pour réussir la création de la connexion, le compte d'ordinateur doit être mappé avec un utilisateur UNIX. Le moyen le plus pratique pour y parvenir est de mapper le compte d'ordinateur à l'utilisateur UNIX par défaut.

Description de la tâche

Hyper-V et SQL Server utilisent les comptes d'ordinateur de domaine pour créer des connexions SMB. En outre, SQL Server utilise un compte d'utilisateur de domaine comme compte de service qui établit également des connexions SMB.

Lorsque vous créez un SVM (Storage Virtual machine), ONTAP crée automatiquement l'utilisateur par défaut nommé « pcuser » (avec un UID sur 65534) Et le groupe nommé « pcuser » (avec un GID de 65534), et ajoute l'utilisateur par défaut au groupe « pcuser ». Si vous configurez une solution Hyper-V sur SMB sur un SVM existant avant de mettre à niveau le cluster vers Data ONTAP 8.2, l'utilisateur et le groupe par défaut risquent de ne pas exister. Dans le cas contraire, vous devez les créer avant de configurer l'utilisateur UNIX par défaut du serveur CIFS.

Étapes

1. Déterminez s'il existe un utilisateur UNIX par défaut :

```
vserver cifs options show -vserver vserver_name
```

2. Si l'option utilisateur par défaut n'est pas définie, déterminez si un utilisateur UNIX peut être désigné comme utilisateur UNIX par défaut :

```
vserver services unix-user show -vserver vserver_name
```

3. Si l'option utilisateur par défaut n'est pas définie et qu'il n'y a pas d'utilisateur UNIX qui peut être désigné comme utilisateur UNIX par défaut, créez l'utilisateur UNIX par défaut et le groupe par défaut, puis ajoutez l'utilisateur par défaut au groupe.

Généralement, l'utilisateur par défaut est nommé « pcuser » et doit être affecté à l'UID de 65534. Le groupe par défaut est généralement attribué au nom de groupe « pcuser ». Le GID affecté au groupe doit être de 65534.

- a. Créez le groupe par défaut :

```
vserver services unix-group create -vserver vserver_name -name pcuser -id 65534
```

- b. Créez l'utilisateur par défaut et ajoutez l'utilisateur par défaut au groupe par défaut :

```
vserver services unix-user create -vserver vserver_name -user pcuser -id 65534 -primary-gid 65534
```

- c. Vérifiez que l'utilisateur par défaut et le groupe par défaut sont correctement configurés :

```
vserver services unix-user show -vserver vserver_name
```

```
vserver services unix-group show -vserver vserver_name -members
```

4. Si l'utilisateur par défaut du serveur CIFS n'est pas configuré, effectuez les opérations suivantes :

- a. Configurez l'utilisateur par défaut :

```
vserver cifs options modify -vserver *vserver_name -default-unix-user pcuser*
```

- b. Vérifiez que l'utilisateur UNIX par défaut est configuré correctement :

```
vserver cifs options show -vserver vserver_name
```

5. Pour vérifier que le compte de l'ordinateur du serveur d'application correspond correctement à l'utilisateur par défaut, mappez un disque sur un partage résidant sur le SVM et confirmez que l'utilisateur Windows correspond au mappage utilisateur UNIX à l'aide de `vserver cifs session show` commande.

Pour plus d'informations sur l'utilisation de cette commande, consultez les pages de manuels.

Exemple

Les commandes suivantes déterminent que l'utilisateur par défaut du serveur CIFS n'est pas défini, mais déterminent que l'utilisateur « pcuser » et le groupe « pcuser » existent. L'utilisateur « pcuser » est attribué en tant qu'utilisateur par défaut du serveur CIFS sur le SVM vs1.

```
cluster1::> vserver cifs options show
```

Vserver: vs1

Client Session Timeout : 900
Default Unix Group : -
Default Unix User : -
Guest Unix User : -
Read Grants Exec : disabled
Read Only Delete : disabled
WINS Servers : -

cluster1::> vsriver services unix-user show

Vserver	User Name	User ID	Group ID	Full Name
vs1	nobody	65535	65535	-
vs1	pcuser	65534	65534	-
vs1	root	0	1	-

cluster1::> vsriver services unix-group show -members

Vserver	Name	ID
vs1	daemon	1
	Users: -	
vs1	nobody	65535
	Users: -	
vs1	pcuser	65534
	Users: -	
vs1	root	0
	Users: -	

cluster1::> vsriver cifs options modify -vserver vs1 -default-unix-user pcuser

cluster1::> vsriver cifs options show

Vserver: vs1

Client Session Timeout : 900
Default Unix Group : -
Default Unix User : pcuser
Guest Unix User : -
Read Grants Exec : disabled
Read Only Delete : disabled
WINS Servers : -

Vérifier que le style de sécurité du volume root du SVM est défini sur NTFS

Pour assurer la continuité de l'activité pour Hyper-V et SQL Server sur SMB, des volumes doivent être créés avec le style de sécurité NTFS. Comme le style de sécurité du volume root est appliqué par défaut aux volumes créés sur la machine virtuelle de stockage (SVM), le style de sécurité du volume root doit être défini sur NTFS.

Description de la tâche

- Vous pouvez spécifier le style de sécurité du volume root au moment de la création de la SVM.
- Si le SVM n'est pas créé avec le volume root défini sur le style de sécurité NTFS, vous pouvez changer le style de sécurité plus tard en utilisant le `volume modify` commande.

Étapes

1. Déterminer la méthode de sécurité actuelle du volume root du SVM :

```
volume show -vserver vs1 -fields vs1,volume,security-style
```

2. Si le volume racine n'est pas un volume de style de sécurité NTFS, remplacez le style de sécurité par NTFS :

```
volume modify -vserver vs1 -volume vs1_root -security-style ntfs
```

3. Vérifier que le volume root du SVM est défini sur le style de sécurité NTFS :

```
volume show -vserver vs1 -fields vs1,volume,security-style
```

Exemple

Les commandes suivantes vérifient que le style de sécurité du volume root est NTFS sur le SVM vs1 :

```
cluster1::> volume show -vserver vs1 -fields vs1,volume,security-style
vs1      volume      security-style
-----
vs1      vs1_root     unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style ntfs

cluster1::> volume show -vserver vs1 -fields vs1,volume,security-style
vs1      volume      security-style
-----
vs1      vs1_root     ntfs
```

Vérifiez que les options requises pour les serveurs CIFS sont configurées

Vous devez vérifier que les options des serveurs CIFS requis sont activées et configurées conformément aux exigences de continuité de l'activité pour Hyper-V et SQL

Server sur SMB.

Description de la tâche

- SMB 2.x et SMB 3.0 doivent être activés.
- L'allègement de la charge des copies (ODX) doit être activé pour que l'allègement de la performance des copies soit délesté.
- Les services VSS Shadow Copy doivent être activés si la solution Hyper-V sur SMB utilise des services de sauvegarde VSS distants (Hyper-V uniquement).

Étapes

1. Vérifier que les options des serveurs CIFS requis sont activées sur la machine virtuelle de stockage (SVM) :

- a. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

- b. Saisissez la commande suivante :

```
vserver cifs options show -vserver vserver_name
```

Les options suivantes doivent être définies sur `true`:

- `-smb2-enabled`
- `-smb3-enabled`
- `-copy-offload-enabled`
- `-shadowcopy-enabled` (Hyper-V uniquement)

2. Si l'une des options n'est pas définie sur `true`, effectuez les opérations suivantes :
 - a. Réglez-les sur `true` à l'aide du `vserver cifs options modify` commande.
 - b. Vérifiez que les options sont définies sur `true` à l'aide du `vserver cifs options show` commande.
3. Retour au niveau de privilège admin :

```
set -privilege admin
```

Exemple

Les commandes suivantes vérifient que les options requises pour la configuration Hyper-V sur SMB sont activées sur le SVM vs1. Dans l'exemple, l'allègement de la charge des copies (ODX) doit être activé pour répondre aux exigences des options.

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::~*> vservers cifs options show -vservers vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vservers smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
-----
vs1      true          true          false          true

cluster-1::~*> vservers cifs options modify -vservers vs1 -copy-offload
-enabled true

cluster-1::~*> vservers cifs options show -vservers vs1 -fields copy-offload-
enabled
vservers copy-offload-enabled
-----
vs1      true

cluster1::~*> set -privilege admin

```

Configurez SMB Multichannel pour des performances et une redondance optimales

Depuis ONTAP 9.4, vous pouvez configurer SMB Multichannel pour fournir plusieurs connexions entre ONTAP et les clients dans une seule session SMB. L'amélioration du débit et de la tolérance aux pannes pour les configurations Hyper-V et SQL Server sur SMB.

Avant de commencer

La fonctionnalité SMB Multichannel ne peut être utilisée que lorsque les clients négocient avec SMB 3.0 ou une version ultérieure. SMB 3.0 et versions ultérieures sont activés par défaut sur le serveur ONTAP SMB.

Description de la tâche

Les clients SMB détectent et utilisent automatiquement plusieurs connexions réseau si une configuration adéquate est identifiée sur le cluster ONTAP.

Le nombre de connexions simultanées dans une session SMB dépend des cartes réseau que vous avez déployées :

- **NIC 1G sur le client et le cluster ONTAP**

Le client établit une connexion par carte réseau et lie la session à toutes les connexions.

- **Cartes réseau 10G et de capacité supérieure sur le client et le cluster ONTAP**

Le client établit jusqu'à quatre connexions par carte réseau et lie la session à toutes les connexions. Le client peut établir des connexions sur plusieurs cartes réseau 10G et supérieures.

Vous pouvez également modifier les paramètres suivants (privilège avancé) :

- `-max-connections-per-session`

Nombre maximum de connexions autorisées par session multicanal. La valeur par défaut est 32 connexions.

Si vous souhaitez activer plus de connexions que la configuration par défaut, vous devez effectuer des ajustements comparables à la configuration client, qui possède également une valeur par défaut de 32 connexions.

- `-max-lifs-per-session`

Nombre maximum d'interfaces réseau annoncées par session multicanal. La valeur par défaut est 256 interfaces réseau.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Activez SMB Multichannel sur le serveur SMB :

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel  
-enabled true
```

3. Vérifiez que ONTAP signale les sessions SMB multicanaux :

```
vserver cifs session show
```

4. Retour au niveau de privilège admin :

```
set -privilege admin
```

Exemple

L'exemple suivant affiche les informations relatives à toutes les sessions SMB, affichant plusieurs connexions pour une seule session :

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                               Open
Idle
IDs      ID      Workstation      Windows User      Files
Time
-----
-----
138683,
138684,
138685    1      10.1.1.1      DOMAIN\
4s
Administrator
```

L'exemple suivant affiche des informations détaillées sur une session SMB avec l'ID-session 1 :

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -
```

Création de volumes de données NTFS

Vous devez créer des volumes de données NTFS sur la machine virtuelle de stockage (SVM) avant de pouvoir configurer les partages disponibles en continu pour une


utilisation avec Hyper-V ou SQL Server sur les serveurs d’applications SMB. Utilisez la fiche de configuration des volumes pour créer vos volumes de données.

Description de la tâche

Vous pouvez utiliser des paramètres facultatifs pour personnaliser un volume de données. Pour plus d’informations sur la personnalisation des volumes, reportez-vous à la section ["Gestion du stockage logique"](#).

Lorsque vous créez vos volumes de données, vous ne devez pas créer de points de jonction au sein d’un volume contenant les éléments suivants :

- Hyper-V Files pour lesquels ONTAP crée des clichés instantanés
- Fichiers de base de données SQL Server sauvegardés à l’aide de SQL Server



Si vous créez par inadvertance un volume utilisant un style de sécurité mixte ou UNIX, vous ne pouvez pas le remplacer par un volume de style de sécurité NTFS, puis l'utiliser directement pour créer des partages disponibles en continu pour assurer la continuité de l'activité. La continuité de l'activité pour Hyper-V et SQL Server over SMB ne fonctionne pas correctement, sauf si les volumes utilisés dans la configuration sont créés en tant que volumes de sécurité NTFS. vous devez supprimer le volume et recréer le volume avec le style de sécurité NTFS, Vous pouvez également mapper le volume sur un hôte Windows et appliquer une liste de contrôle d'accès en haut du volume et propager la liste de contrôle d'accès à tous les fichiers et dossiers du volume.

Étapes

1. Créez le volume de données en entrant la commande appropriée :

Si vous souhaitez créer un volume dans un SVM où le root volume Security style...	Entrez la commande...
NTFS	<code>volume create -vserver vsERVER_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -junction-path path</code>
Pas NTFS	<code>volume create -vserver vsERVER_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -security-style ntfs -junction-path path</code>

2. Vérifiez que la configuration de volume est correcte :

```
volume show -vserver vsERVER_name -volume volume_name
```

Créer des partages SMB disponibles en permanence

Une fois les volumes de données créés, vous pouvez créer les partages disponibles en continu que les serveurs d’applications utilisent pour accéder aux fichiers de la machine virtuelle et de configuration Hyper-V ainsi qu’aux fichiers de la base de données SQL Server. Vous devez utiliser la fiche de configuration du partage lors de la création des

partages SMB.

Étapes

1. Afficher des informations sur les volumes de données existants et leurs Junction paths :

```
volume show -vserver vs1 -junction
```

2. Créer un partage SMB disponible en continu :

```
vserver cifs share create -vserver vs1 -share-name share_name -path  
path -share-properties oplocks,continuously-available -symlink "" [-comment  
text]
```

- Vous pouvez éventuellement ajouter un commentaire à la configuration du partage.
 - Par défaut, la propriété de partage de fichiers hors ligne est configurée sur le partage et est définie sur manual.
 - ONTAP crée le partage avec l'autorisation de partage par défaut Windows de Everyone / Full Control.
3. Répétez l'étape précédente pour tous les partages de la fiche de configuration du partage.
 4. Vérifiez que votre configuration est correcte à l'aide du `vserver cifs share show` commande.
 5. Configurez les autorisations de fichiers NTFS sur les partages disponibles en permanence en mappant un lecteur sur chaque partage et en configurant les autorisations de fichiers à l'aide de la fenêtre **Propriétés Windows**.

Exemple

Les commandes suivantes créent un partage disponible en continu nommé « data2 » sur la machine virtuelle de stockage (SVM, précédemment appelé vServer) vs1. Les symlinks sont désactivés en définissant l' `-symlink` paramètre à "" :

```

cluster1::> volume show -vserver vs1 -junction

Vserver    Volume      Junction
-----
vs1        data        true       /data       RW_volume
vs1        data1       true       /data/data1 RW_volume
vs1        data2       true       /data/data2 RW_volume
vs1        vs1_root    -          /           -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

Vserver: vs1
Share: data2
CIFS Server NetBIOS Name: VS1
Path: /data/data2
Share Properties: oplocks
                  continuously-available
Symlink Properties: -
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard

```

Ajoutez le privilège SeSecurityPrivilege au compte d'utilisateur (pour SQL Server des partages SMB)

Le compte d'utilisateur de domaine utilisé pour installer le serveur SQL doit être affecté au privilège "SeSecurityPrivilege" pour effectuer certaines actions sur le serveur CIFS qui exigent des privilèges non attribués par défaut aux utilisateurs de domaine.

Ce dont vous avez besoin

Le compte de domaine utilisé pour installer SQL Server doit déjà exister.

Description de la tâche

Lors de l'ajout du privilège au compte du programme d'installation de SQL Server, ONTAP peut valider le compte en contactant le contrôleur de domaine. La commande peut échouer si ONTAP ne parvient pas à contacter le contrôleur de domaine.

Étapes

1. Ajoutez le privilège "SeSecurityPrivilege" :


```
vserver cifs users-and-groups privilege add-privilege -vserver vserver_name  
-user-or-group-name account_name -privileges SeSecurityPrivilege
```

La valeur pour le `-user-or-group-name` Paramètre est le nom du compte utilisateur de domaine utilisé pour l'installation de SQL Server.

2. Vérifiez que le privilège est appliqué au compte :

```
vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-  
group-name account_name
```

Exemple

La commande suivante ajoute le privilège "SeSecurityPrivilege" au compte du programme d'installation de SQL Server dans le domaine D'EXEMPLE pour la machine virtuelle de stockage (SVM) vs1 :

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver  
vs1 -user-or-group-name EXAMPLE\SQLInstaller -privileges  
SeSecurityPrivilege  
  
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1  
Vserver      User or Group Name      Privileges  
-----  
vs1          EXAMPLE\SQLInstaller  SeSecurityPrivilege
```

Configurer la profondeur du répertoire de copie « shadow » VSS (pour les partages Hyper-V sur SMB)

Vous pouvez également configurer la profondeur maximale des répertoires dans les partages SMB sur lesquels vous souhaitez créer des clichés instantanés. Ce paramètre est utile si vous souhaitez contrôler manuellement le niveau maximal de sous-répertoires sur lesquels ONTAP doit créer des clichés instantanés.

Ce dont vous avez besoin

La fonction VSS Shadow Copy doit être activée.

Description de la tâche

La valeur par défaut est de créer des clichés instantanés pour un maximum de cinq sous-répertoires. Si la valeur est définie sur 0, ONTAP crée des clichés instantanés pour tous les sous-répertoires.



Bien que vous puissiez spécifier que la profondeur du répertoire du jeu de clichés instantanés inclut plus de cinq sous-répertoires ou tous les sous-répertoires, Microsoft a besoin que la création du jeu de clichés instantanés soit terminée dans les 60 secondes. La création d'un jeu de clichés instantanés échoue s'il ne peut pas être terminé dans ce délai. La profondeur du répertoire de copie en double que vous choisissez ne doit pas entraîner le dépassement du délai de création.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Définissez la profondeur du répertoire de copie fantôme VSS au niveau souhaité :

```
vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth  
integer
```

```
vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
```

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

Gérez les configurations Hyper-V et SQL Server sur SMB

Configurez les partages existants pour assurer la disponibilité sans interruption

Vous pouvez modifier les partages existants pour devenir des partages disponibles en permanence que les serveurs d'applications Hyper-V et SQL Server utilisent pour accéder sans interruption aux fichiers de configuration et des machines virtuelles Hyper-V et aux fichiers de base de données SQL Server.

Description de la tâche

Vous ne pouvez pas utiliser un partage existant comme partage disponible en continu pour assurer la continuité de l'activité avec des serveurs applicatifs sur SMB si le partage présente les caractéristiques suivantes :

- Si le `homedirectory` la propriété partager est définie sur ce partage
- Si le partage contient des symlinks ou des widelinks activés
- Si le partage contient des volumes sous la racine du partage

Vous devez vérifier que les deux paramètres de partage suivants sont correctement définis :

- Le `-offline-files` le paramètre est défini sur l'un ou l'autre `manual` (valeur par défaut) ou `none`.
- Les symlinks doivent être désactivés.

Les propriétés de partage suivantes doivent être configurées :

- `continuously-available`
- `oplocks`

Les propriétés de partage suivantes ne doivent pas être définies. S'ils sont présents dans la liste des propriétés de partage actuelles, ils doivent être supprimés du partage disponible en continu :

- `attributecache`
- `branchcache`

Étapes

1. Afficher les paramètres de partage actuels et la liste actuelle des propriétés de partage configurées :

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
```

2. Si nécessaire, modifiez les paramètres de partage pour désactiver les liens symboliques et définissez les fichiers hors ligne sur manuel à l'aide de la `vserver cifs share modify` commande.
 - Vous pouvez désactiver les symlinks en définissant la valeur de l' `-symlink` paramètre à `""`.
 - Vous pouvez définir le `-offline-files` paramètre au réglage correct en spécifiant `manual`.
3. Ajoutez la `continuously-available` propriété de partage et, si nécessaire, la `oplocks` propriété de partage :

```
vserver cifs share properties add -vserver <vserver_name> -share-name  
<share_name> -share-properties continuously-available[,oplock]
```

Si le `oplocks` la propriété de partage n'est pas déjà définie, vous devez l'ajouter avec `continuously-available` propriété de partage.

4. Supprimez toutes les propriétés de partage qui ne sont pas prises en charge sur les partages disponibles en continu :

```
vserver cifs share properties remove -vserver <vserver_name> -share-name  
<share_name> -share-properties properties[,...]
```

Vous pouvez supprimer une ou plusieurs propriétés de partage en spécifiant les propriétés de partage avec une liste délimitée par des virgules.

5. Vérifiez que le `-symlink` et `-offline-files` les paramètres sont correctement réglés :

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>  
-fields symlink-properties,offline-files
```

6. Vérifiez que la liste des propriétés de partage configurées est correcte :

```
vserver cifs share properties show -vserver <vserver_name> -share-name  
<share_name>
```

Exemples

L'exemple suivant montre comment configurer un partage existant nommé « share1 » sur la machine virtuelle de stockage (SVM) « vs1 » pour les NDO avec un serveur d'application sur SMB :

- Les liens symboliques sont désactivés sur le partage en définissant le `-symlink` paramètre sur `""`.
- Le `-offline-file` le paramètre est modifié et défini sur `manual`.
- Le `continuously-available` la propriété de partage est ajoutée au partage.

- Le `oplocks` la propriété de partage figure déjà dans la liste des propriétés de partage ; il n'est donc pas nécessaire de l'ajouter.
- Le `attributecache` la propriété de partage est supprimée du partage.
- Le `browsable` La propriété de partage est facultative pour un partage disponible en continu utilisé pour les NDO avec des serveurs d'application sur SMB et est conservée comme une des propriétés de partage.

```
cluster1::> vsriver cifs share show -vsriver vs1 -share-name share1
```

```

        Vserver: vs1
        Share: share1
CIFS Server NetBIOS Name: vs1
        Path: /data
        Share Properties: oplocks
                        browsable
                        attributecache
        Symlink Properties: enable
        File Mode Creation Mask: -
        Directory Mode Creation Mask: -
        Share Comment: -
        Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: data
        Offline Files: documents
Vscan File-Operations Profile: standard
```

```
cluster1::> vsriver cifs share modify -vsriver vs1 -share-name share1
-offline-file manual -symlink ""
```

```
cluster1::> vsriver cifs share properties add -vsriver vs1 -share-name
share1 -share-properties continuously-available
```

```
cluster1::> vsriver cifs share properties remove -vsriver vs1 -share-name
share1 -share-properties attributecache
```

```
cluster1::> vsriver cifs share show -vsriver vs1 -share-name share1
-fields symlink-properties,offline-files
vsriver  share-name symlink-properties offline-files
```

```
-----
vs1      share1      -                      manual
```

```
cluster1::> vsriver cifs share properties show -vsriver vs1 -share-name
share1
```

```

        Vserver: vs1
        Share: share1
Share Properties: oplocks
                browsable
                continuously-available
```

Activez ou désactivez les clichés instantanés VSS pour les sauvegardes Hyper-V sur SMB

Si vous utilisez une application de sauvegarde VSS pour sauvegarder les fichiers de machine virtuelle Hyper-V stockés sur des partages SMB, la copie Shadow VSS doit être activée. Vous pouvez désactiver la copie « shadow Copy VSS » si vous n'utilisez pas d'applications de sauvegarde « VSS Aware ». La valeur par défaut est d'activer la copie fantôme VSS.

Description de la tâche

Vous pouvez activer ou désactiver les clichés instantanés VSS à tout moment.

Étapes

- 1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

- 2. Effectuez l'une des opérations suivantes :

Si vous voulez que les clichés instantanés VSS soient...	Entrez la commande...
Activé	<code>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true</code>
Désactivé	<code>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false</code>

- 3. Retour au niveau de privilège admin :

```
set -privilege admin
```

Exemple

Les commandes suivantes permettent d'activer les clichés instantanés VSS sur le SVM vs1 :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

Utilisez les statistiques pour surveiller l'activité Hyper-V et SQL Server sur SMB

Déterminez les objets statistiques et les compteurs disponibles

Avant d'obtenir des informations sur les statistiques de hachage CIFS, SMB, d'audit et de BranchCache, ainsi que sur les performances, vous devez connaître les objets et compteurs disponibles, à partir desquels vous pouvez obtenir des données.

Étapes

- 1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

- 2. Effectuez l'une des opérations suivantes :

Si vous voulez déterminer...	Entrer...
Les objets disponibles	<code>statistics catalog object show</code>
Objets spécifiques disponibles	<code>statistics catalog object show object <i>object_name</i></code>
Quels compteurs sont disponibles	<code>statistics catalog counter show object <i>object_name</i></code>

Pour plus d'informations sur les objets et les compteurs disponibles, consultez les pages de manuels.

- 3. Retour au niveau de privilège admin :

```
set -privilege admin
```

Exemples

La commande suivante affiche la description des objets statistiques sélectionnés relatifs à l'accès CIFS et SMB au cluster, comme s'il s'affiche au niveau de privilège avancé :

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog object show -object audit
      audit_ng          CM object for exporting audit_ng
performance counters
```

```
cluster1::*> statistics catalog object show -object cifs
      cifs              The CIFS object reports activity of the
                        Common Internet File System protocol
                        ...
```

```
cluster1::*> statistics catalog object show -object nblade_cifs
      nblade_cifs      The Common Internet File System (CIFS)
                        protocol is an implementation of the
Server
                        ...
```

```
cluster1::*> statistics catalog object show -object smb1
      smb1             These counters report activity from the
SMB
                        revision of the protocol. For information
                        ...
```

```
cluster1::*> statistics catalog object show -object smb2
      smb2             These counters report activity from the
                        SMB2/SMB3 revision of the protocol. For
                        ...
```

```
cluster1::*> statistics catalog object show -object hashd
      hashd           The hashd object provides counters to
measure
                        the performance of the BranchCache hash
daemon.
```

```
cluster1::*> set -privilege admin
```

La commande suivante affiche des informations sur certains compteurs de `cifs` objet tel qu'il apparaît au niveau de privilège avancé :



Cet exemple n'affiche pas tous les compteurs disponibles pour le `cifs` objet ; la sortie est tronquée.


```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

Counter	Description
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
...	...

```
cluster2::> statistics start -object client -sample-id
```

Object: client

Counter	Value
cifs_ops	0
cifs_read_ops	0
cifs_read_recv_ops	0
cifs_read_recv_size	0B
cifs_read_size	0B
cifs_write_ops	0
cifs_write_recv_ops	0
cifs_write_recv_size	0B
cifs_write_size	0B
instance_name	vserver_1:10.72.205.179
instance_uuid	2:10.72.205.179
local_ops	0
mount_ops	0

[...]

Affiche les statistiques SMB

Vous pouvez afficher différentes statistiques SMB pour surveiller les performances et

diagnostiquer les problèmes.

Étapes

1. Utilisez le `statistics start` et en option `statistics stop` commandes pour collecter un échantillon de données.
2. Effectuez l'une des opérations suivantes :

Pour afficher les statistiques de...	Saisissez la commande suivante...
Toutes les versions de SMB	<code>statistics show -object cifs</code>
SMB 1.0	<code>statistics show -object smb1</code>
SMB 2.x et SMB 3.0	<code>statistics show -object smb2</code>
Sous-système SMB du nœud	<code>statistics show -object nblade_cifs</code>

En savoir plus sur le `statistics` commandes :

- ["statistiques affichées"](#)
- ["début des statistiques"](#)
- ["fin des statistiques"](#)

Vérifiez que la configuration permet la continuité de l'activité

Utilisez le contrôle de l'état de l'intégrité pour déterminer si l'état de la continuité de l'activité fonctionne correctement

Le contrôle de l'état fournit des informations relatives à l'état du système sur le cluster. Le contrôle de l'état surveille les configurations Hyper-V et SQL Server sur SMB pour assurer la continuité de l'activité pour les serveurs applicatifs. Si l'état est dégradé, vous pouvez afficher des détails sur le problème, y compris la cause probable et les actions de récupération recommandées.

Il y a plusieurs moniteurs de santé. ONTAP contrôle à la fois l'état global du système et l'état de santé des personnes. Le contrôle de l'état de connectivité des nœuds contient le sous-système CIFS-NDO. Le contrôle dispose d'un ensemble de règles d'intégrité qui déclenchent des alertes si certaines conditions physiques peuvent entraîner des interruptions et, si une condition de perturbation existe, génère des alertes et fournit des informations sur les actions correctives à mettre en œuvre. Pour les configurations NDO sur SMB, des alertes sont générées dans les deux conditions suivantes :

L'ID d'alerte	Gravité	Condition
HaNotReadyCifsNdo_Alert	Majeur	Un ou plusieurs fichiers hébergés par un volume dans un agrégat du nœud ont été ouverts via un partage SMB disponible en continu, avec la promesse de persistance en cas de défaillance. Cependant, la relation de haute disponibilité avec le partenaire n'est pas configurée ou n'est pas saine.
NoStandbyLifCifsNdo_Alert	Mineur	Le SVM (Storage Virtual machine) transmet activement les données via SMB via un nœud, et les fichiers SMB sont ouverts de manière continue sur des partages disponibles. Cependant, son nœud partenaire n'expose pas de LIF de données actives pour la SVM.

Affichez l'état de l'opération sans interruption grâce à la surveillance de l'état du système

Vous pouvez utiliser le `system health` Commandes permettant d'afficher des informations relatives à l'état global du cluster et à l'état de santé du sous-système CIFS-NDO, de répondre aux alertes, de configurer les alertes futures et d'afficher des informations sur la configuration du contrôle de l'état.

Étapes

1. Surveillez l'état de l'état de santé en effectuant l'action appropriée :

Si vous voulez afficher...	Entrez la commande...
L'état d'intégrité du système, qui reflète l'état global des moniteurs d'état individuels	system health status show
Informations sur l'état de santé du sous-système CIFS-NDO	system health subsystem show -subsystem CIFS-NDO -instance

2. Afficher des informations sur la configuration de la surveillance des alertes CIFS-NDO en effectuant les actions appropriées :

Pour afficher des informations sur...	Entrez la commande...
La configuration et l'état du contrôle de l'état du sous-système CIFS-NDO, tels que les nœuds contrôlés, l'état d'initialisation et l'état	system health config show -subsystem CIFS-NDO

Pour afficher des informations sur...	Entrez la commande...
CIFS-NDO signale qu'un contrôle de l'état peut générer	system health alert definition show -subsystem CIFS-NDO
Règles de contrôle de l'état de la CONTINUITÉ de l'ACTIVITÉ CIFS qui déterminent la date d'émission des alertes	system health policy definition show -monitor node-connect



Utilisez le `-instance` paramètre pour afficher des informations détaillées.

Exemples

Le résultat suivant affiche des informations sur l'état d'intégrité global du cluster et le sous-système CIFS-NDO :

```
cluster1::> system health status show
Status
-----
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                Subsystem: CIFS-NDO
                Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
Number of Suppressed Alerts: 0
                        Node: node2
Subsystem Refresh Interval: 5m
```

Le résultat suivant affiche des informations détaillées sur la configuration et l'état du contrôle de l'état du sous-système CIFS-NDO :

```

cluster1::> system health config show -subsystem CIFS-NDO -instance

Node: node1
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

Node: node2
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

```

Vérifiez la configuration du partage SMB disponible en continu

Pour prendre en charge la continuité de l'activité, les partages SMB Hyper-V et SQL Server doivent être configurés en tant que partages disponibles en continu. En outre, vous devez vérifier certains autres paramètres de partage. Vérifiez que les partages sont correctement configurés pour assurer la continuité de l'activité des serveurs applicatifs en cas d'événements planifiés ou non.

Description de la tâche

Vous devez vérifier que les deux paramètres de partage suivants sont correctement définis :

- Le `-offline-files` le paramètre est défini sur l'un ou l'autre `manual` (valeur par défaut) ou `none`.
- Les symlinks doivent être désactivés.

Pour garantir la continuité de l'activité, les propriétés de partage suivantes doivent être définies :

- `continuously-available`
- `oplocks`

Les propriétés de partage suivantes ne doivent pas être définies :

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

Étapes

1. Vérifiez que les fichiers hors ligne sont définis sur `manual` ou `disabled` et que les symlinks sont désactivés :

```
vserver cifs shares show -vserver vserver_name
```

2. Vérifiez que les partages SMB sont configurés pour une disponibilité continue :

```
vserver cifs shares properties show -vserver vserver_name
```

Exemples

L'exemple suivant présente le paramètre de partage d'un partage nommé « `sunrel'` » sur la machine virtuelle de stockage (SVM, anciennement appelée Vserver) `vs1`. Les fichiers hors ligne sont définis sur `manual` et les symlinks sont désactivés (désignés par un tiret dans le `Symlink Properties` sortie de champ) :

```
cluster1::> vservers cifs share show -vservers vs1 -share-name share1
Vserver: vs1
Share: share1
CIFS Server NetBIOS Name: VS1
Path: /data/share1
Share Properties: oplocks
continuously-available
Symlink Properties: -
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
```

L'exemple suivant affiche les propriétés de partage d'un partage nommé «`sunre1'» sur la SVM vs1 :

```
cluster1::> vservers cifs share properties show -vservers vs1 -share-name
share1
Vserver      Share      Properties
-----
vs1          share1    oplocks
continuously-available
```

Vérifiez l'état du LIF

Même si vous configurez des SVM (Storage Virtual machines) avec des configurations Hyper-V et SQL Server over SMB pour avoir des LIF sur chaque nœud d'un cluster, au cours des opérations quotidiennes, certaines LIF peuvent être déplacées vers des ports sur un autre nœud. Vous devez vérifier le statut de la LIF et prendre les mesures correctives nécessaires.

Description de la tâche

Pour assurer la prise en charge transparente et sans interruption de l'activité, chaque nœud d'un cluster doit disposer d'au moins une LIF pour le SVM et toutes les LIF doivent être associées à un port de rattachement. Si certaines des LIF configurées ne sont actuellement pas associées à leur port de base, vous devez résoudre un problème de port, puis rétablir les LIF sur leur port de base.

Étapes

1. Afficher les informations relatives aux LIFs configurées pour le SVM :

```
network interface show -vservers vservers_name
```

Dans cet exemple, «`lites1` » n'est pas situé sur le port d'attache.

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
vs1					
	lif1	up/up	10.0.0.128/24	node2	e0d
false					
	lif2	up/up	10.0.0.129/24	node2	e0d
true					

2. Si certaines des LIFs ne se trouvent pas sur leurs ports de home, effectuez les opérations suivantes :

a. Pour chaque LIF, déterminez ce que le port de base de la LIF est :

```
network interface show -vserver vs1 -lif lif1 -fields home-node,home-port
```

```
network interface show -vserver vs1 -lif lif1 -fields home-node,home-port
```

vserver	lif	home-node	home-port
-----	----	-----	-----
vs1	lif1	node1	e0d

b. Pour chaque LIF, déterminez si le port de base de la LIF est active :

```
network port show -node node1 -port e0d -fields port,link
```

```
network port show -node node1 -port e0d -fields port,link
```

node	port	link
-----	----	----
node1	e0d	up

+

Dans cet exemple, « lif1 » doit être remigré vers son port d'origine, node1:e0d.

3. Si l'une des interfaces réseau du port de Home port auxquelles les LIFs doivent être associées, elles ne se trouvent pas dans le up état, résolvez le problème afin que ces interfaces soient utilisées.

4. Si besoin, rrestaurez les LIF sur leurs ports de base :

```
network interface revert -vserver vs1 -lif lif1
```



```
network interface revert -vserver vs1 -lif lif1
```

5. Vérifier que chaque nœud du cluster dispose d'une LIF active pour le SVM :

```
network interface show -vserver vserver_name
```

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
-----	-----	-----	-----	-----	-----	-----

vs1						
	lif1	up/up	10.0.0.128/24	node1	e0d	
true						
	lif2	up/up	10.0.0.129/24	node2	e0d	
true						

Déterminez si les sessions SMB sont disponibles en continu

Affiche les informations relatives aux sessions SMB

Vous pouvez afficher des informations sur les sessions SMB établies, notamment la connexion SMB et l'ID de session ainsi que l'adresse IP du poste de travail à l'aide de la session. Vous pouvez afficher des informations sur la version du protocole SMB de la session et son niveau de protection disponible en continu, ce qui vous aide à déterminer si cette session prend en charge la continuité de l'activité.

Description de la tâche

Vous pouvez afficher les informations de toutes les sessions de votre SVM sous forme récapitulative. Cependant, dans de nombreux cas, la quantité de sortie renvoyée est importante. Vous pouvez personnaliser les informations affichées dans la sortie en spécifiant des paramètres facultatifs :

- Vous pouvez utiliser l'option `-fields` paramètre pour afficher la sortie des champs que vous choisissez.

Vous pouvez entrer `-fields ?` pour déterminer les champs que vous pouvez utiliser.

- Vous pouvez utiliser le `-instance` Paramètre pour afficher des informations détaillées sur les sessions SMB établies.
- Vous pouvez utiliser le `-fields` ou le `-instance` paramètre seul ou associé à d'autres paramètres facultatifs.

Étapes

1. Effectuez l'une des opérations suivantes :

Pour afficher les informations de session SMB...	Saisissez la commande suivante...
Pour toutes les sessions sur le SVM sous forme résumée	vserver cifs session show -vserver <i>vserver_name</i>
Sur un ID de connexion spécifié	vserver cifs session show -vserver <i>vserver_name</i> -connection-id integer
À partir d'une adresse IP de poste de travail spécifiée	vserver cifs session show -vserver <i>vserver_name</i> -address <i>workstation_IP_address</i>
Sur une adresse IP LIF spécifiée	vserver cifs session show -vserver <i>vserver_name</i> -lif -address <i>LIF_IP_address</i>
Sur un nœud spécifié	<i>**vserver cifs session show -vserver vserver_name -node {node_name</i>
<i>local}**</i>	D'un utilisateur Windows spécifié
vserver cifs session show -vserver <i>vserver_name</i> -windows-user <i>user_name</i> Le format de <i>user_name</i> est [domain]\user.	Avec un mécanisme d'authentification spécifié

<p>Pour afficher les informations de session SMB...</p>	<p>Saisissez la commande suivante...</p>
<p>vserver cifs session show -vserver vserver_name -auth -mechanism authentication_mechanism</p> <p>La valeur pour -auth -mechanism peut être l'une des suivantes :</p> <ul style="list-style-type: none"> • NTLMv1 • NTLMv2 • Kerberos • Anonymous 	<p>Avec une version de protocole spécifiée</p>

<p>Pour afficher les informations de session SMB...</p>	<p>Saisissez la commande suivante...</p>
<p>vserver cifs session show -vserver vserver_name -protocol-version protocol_version</p> <p>La valeur pour -protocol-version peut être l'une des suivantes :</p> <ul style="list-style-type: none"> • SMB1 • SMB2 • SMB2_1 • SMB3 • SMB3_1 	<p>Avec un niveau spécifié de protection disponible en continu</p>

Pour afficher les informations de session SMB...

Saisissez la commande suivante...

```
vserver cifs  
session show  
-vserver  
vserver_name  
-continuously  
-available  
continuously_avail  
able_protection_le  
vel
```

Avec un état de session de signature SMB spécifié

La valeur pour
-continuously
-available peut être
l'une des suivantes :

- No
- Yes
- Partial

Exemples

La commande suivante affiche les informations relatives aux sessions sur le SVM vs1 établies à partir d'un poste de travail avec l'adresse IP 10.1.1.1 :

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:      node1
Vserver:   vs1
Connection Session
ID          ID      Workstation      Windows User      Open      Idle
-----
3151272279,
3151272280,
3151272281  1        10.1.1.1        DOMAIN\joe        2         23s
```

La commande suivante affiche des informations détaillées pour les sessions avec protection disponible en continu sur le SVM vs1. La connexion a été établie à l'aide du compte de domaine.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation IP address: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\SERVER1$
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: Yes
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

La commande suivante affiche les informations relatives aux sessions sur une session utilisant SMB 3.0 et SMB Multichannel sur le SVM vs1. Dans l'exemple, l'utilisateur connecté à ce partage à un client SMB 3.0 en utilisant l'adresse IP du LIF ; par conséquent, le mécanisme d'authentification par défaut est NTLMv2. La connexion doit se faire à l'aide de l'authentification Kerberos pour se connecter à une protection disponible en continu.

continu.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

Node: node1
Vserver: vs1
Session ID: 1
**Connection IDs: 3151272607,31512726078,3151272609
Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

Affiche des informations sur les fichiers SMB ouverts

Vous pouvez afficher des informations sur les fichiers SMB ouverts, notamment la connexion SMB et l'ID de session, le volume hôte, le nom du partage et le chemin du partage. Vous pouvez également afficher des informations sur le niveau de protection disponible en continu d'un fichier, ce qui permet de déterminer si un fichier ouvert est dans un état qui prend en charge la continuité de l'activité.

Description de la tâche

Vous pouvez afficher des informations sur les fichiers ouverts dans une session SMB établie. Les informations affichées sont utiles lorsque vous devez déterminer les informations de session SMB pour des fichiers particuliers dans une session SMB.

Par exemple, si vous disposez d'une session SMB où certains fichiers ouverts sont ouverts avec une protection disponible en continu et certains ne sont pas ouverts avec une protection disponible en continu (valeur pour le `-continuously-available` champ dans `vserver cifs session show` la sortie de la commande est `Partial`), vous pouvez déterminer quels fichiers ne sont pas disponibles en continu à l'aide de cette commande.

Vous pouvez afficher les informations de tous les fichiers ouverts sur des sessions SMB établies sur des SVM (Storage Virtual machines) sous forme de récapitulatif à l'aide de `vserver cifs session file show` commande sans paramètres facultatifs.

Cependant, dans de nombreux cas, la quantité de production renvoyée est importante. Vous pouvez personnaliser les informations affichées dans la sortie en spécifiant des paramètres facultatifs. Cela peut être utile lorsque vous souhaitez afficher des informations pour un petit sous-ensemble de fichiers ouverts uniquement.

- Vous pouvez utiliser l'option `-fields` paramètre pour afficher la sortie sur les champs de votre choix.

Vous pouvez utiliser ce paramètre seul ou en combinaison avec d'autres paramètres facultatifs.


- Vous pouvez utiliser le `-instance` Paramètre pour afficher des informations détaillées sur les fichiers SMB ouverts.

Vous pouvez utiliser ce paramètre seul ou en combinaison avec d'autres paramètres facultatifs.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez afficher des fichiers SMB ouverts...	Saisissez la commande suivante...
Sur le SVM sous forme résumée	<code>vserver cifs session file show -vserver vserver_name</code>
Sur un nœud spécifié	<code>`*vserver cifs session file show -vserver vserver_name -node {node_name</code>
<code>local}*</code>	Sur un ID de fichier spécifié
<code>vserver cifs session file show -vserver vserver_name -file-id integer</code>	Sur un ID de connexion SMB spécifié
<code>vserver cifs session file show -vserver vserver_name -connection-id integer</code>	Sur un ID de session SMB spécifié
<code>vserver cifs session file show -vserver vserver_name -session-id integer</code>	Sur l'agrégat d'hébergement spécifié
<code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code>	Sur le volume spécifié
<code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code>	Sur le partage SMB spécifié

Si vous souhaitez afficher des fichiers SMB ouverts...	Saisissez la commande suivante...
<code>vserver cifs session file show</code> <code>-vserver vserver_name -share</code> <code>share_name</code>	Sur le chemin SMB spécifié
<code>vserver cifs session file show</code> <code>-vserver vserver_name -path path</code>	Avec le niveau spécifié de protection disponible en continu
<code>vserver cifs session file show</code> <code>-vserver vserver_name -continuously</code> <code>-available</code> <code>continuously_available_status</code> La valeur pour <code>-continuously-available</code> peut être l'une des suivantes : <ul style="list-style-type: none">• No• Yes <div><p>Si l'état disponible en continu est de No, cela signifie que ces fichiers ouverts ne peuvent pas être rétablis sans interruption à partir du basculement et du rétablissement. Ils ne peuvent pas non plus récupérer d'une relocalisation générale entre les partenaires dans une relation de haute disponibilité.</p></div>	Avec l'état reconnecté spécifié

D'autres paramètres facultatifs peuvent être utilisés pour affiner les résultats de sortie. Consultez la page man pour plus d'informations

Exemples

L'exemple suivant affiche les informations sur les fichiers ouverts sur le SVM vs1 :

```
cluster1::> vserver cifs session file show -vserver vs1
Node:      node1
Vserver:   vs1
Connection: 3151274158
Session:   1
File       File       Open Hosting      Continuously
ID         Type        Mode Volume       Share            Available
-----
41         Regular    r    data          data            Yes
Path: \mytest.rtf
```

L'exemple suivant affiche des informations détaillées sur les fichiers SMB ouverts avec l'ID de fichier 82 sur le SVM vs1 :

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

Node: node1
Vserver: vs1
File ID: 82
Connection ID: 104617
Session ID: 1
File Type: Regular
Open Mode: rw
Aggregate Hosting File: aggr1
Volume Hosting File: data1
CIFS Share: data1
Path from CIFS Share: windows\win8\test\test.txt
Share Mode: rw
Range Locks: 1
Continuously Available: Yes
Reconnected: No
```

Gestion du stockage SAN

Concepts RELATIFS AU SAN

Provisionnement DE SAN avec iSCSI

Dans les environnements SAN, les systèmes de stockage sont des cibles qui disposent de périphériques de stockage cibles. Pour iSCSI et FC, les périphériques cibles de stockage sont appelés LUN (unités logiques). Pour NVMe (non-volatile Memory Express) sur Fibre Channel, les périphériques de stockage cibles sont appelés « namespaces ».

Vous configurez le stockage en créant des LUN pour iSCSI et FC, ou en créant des espaces de noms pour NVMe. Les LUN ou les espaces de noms sont ensuite accessibles par les hôtes via les réseaux de protocole Internet Small Computer Systems interface (iSCSI) ou Fibre Channel (FC).

Pour se connecter aux réseaux iSCSI, les hôtes peuvent utiliser des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de bus hôte iSCSI dédiés.

Pour la connexion aux réseaux FC, les hôtes nécessitent des HBA FC ou des CNA.

Les protocoles FC pris en charge sont les suivants :

- FC
- FCoE
- NVMe

Noms et connexions réseau du nœud cible iSCSI

Les nœuds cibles iSCSI peuvent se connecter au réseau de plusieurs façons :

- Plus de interfaces Ethernet utilisent un logiciel intégré à ONTAP.
- Via plusieurs interfaces système, avec une interface utilisée pour iSCSI qui transmet également le trafic pour d'autres protocoles, tels que les protocoles SMB et NFS.
- Utilisation d'un adaptateur cible unifié (UTA) ou d'un adaptateur réseau convergé (CNA).

Chaque nœud iSCSI doit avoir un nom de nœud.

Les deux formats, ou les indicateurs de type, pour les noms de nœud iSCSI sont *iqn* et *eui*. La cible iSCSI du SVM utilise toujours l'indicateur de type *iqn*. L'initiateur peut utiliser l'indicateur de type *iqn* ou *eui*.

Nom de nœud du système de stockage

Chaque SVM exécutant iSCSI possède un nom de nœud par défaut basé sur un nom de domaine inverse et un numéro de codage unique.

Le nom du nœud est affiché au format suivant :

`iqn.1992-08.com.netapp:sn.unique-encoding-number`

L'exemple suivant montre le nom de nœud par défaut d'un système de stockage avec un numéro d'encodage

unique :

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

Port TCP pour iSCSI

Le protocole iSCSI est configuré dans ONTAP pour utiliser le port TCP numéro 3260.

ONTAP ne prend pas en charge la modification du numéro de port pour iSCSI. Le numéro de port 3260 est enregistré dans le cadre de la spécification iSCSI et ne peut être utilisé par aucune autre application ou service.

Informations associées

["Documentation NetApp : configuration de l'hôte SAN ONTAP"](#)

Gestion de services iSCSI

Gestion de services iSCSI

Vous pouvez gérer la disponibilité du service iSCSI sur les interfaces logiques iSCSI de la machine virtuelle de stockage (SVM) à l'aide de la `vserver iscsi interface enable` ou `vserver iscsi interface disable` commandes.

Par défaut, le service iSCSI est activé sur toutes les interfaces logiques iSCSI.

Mise en œuvre d'iSCSI sur l'hôte

iSCSI peut être implémenté sur l'hôte à l'aide du matériel ou du logiciel.

Vous pouvez implémenter iSCSI de l'une des manières suivantes :

- Utilisation d'un logiciel initiateur qui utilise les interfaces Ethernet standard de l'hôte.
- Via un adaptateur de bus hôte iSCSI (HBA) : un adaptateur HBA iSCSI apparaît au système d'exploitation hôte comme un adaptateur de disque SCSI avec disques locaux.
- Utilisation d'un adaptateur TOE (TCP Offload Engine) qui décharge le traitement TCP/IP.

Le traitement du protocole iSCSI est toujours exécuté par le logiciel hôte.

Fonctionnement de l'authentification iSCSI

Au cours de la phase initiale d'une session iSCSI, l'initiateur envoie une demande de connexion au système de stockage pour démarrer une session iSCSI. Le système de stockage autorise ou refuse la demande de connexion, ou détermine qu'aucun identifiant n'est requis.

Les méthodes d'authentification iSCSI sont les suivantes :

- CHAP (Challenge Handshake Authentication Protocol) - l'initiateur se connecte à l'aide d'un nom d'utilisateur et d'un mot de passe CHAP.

Vous pouvez spécifier un mot de passe CHAP ou générer un mot de passe hexadécimal secret. Il existe deux types de noms d'utilisateur et de mots de passe CHAP :

- Inbound : le système de stockage authentifie l'initiateur.

Les paramètres entrants sont requis si vous utilisez l'authentification CHAP.

- Outbound—il s'agit d'un paramètre facultatif permettant à l'initiateur d'authentifier le système de stockage.

Vous ne pouvez utiliser les paramètres sortants que si vous définissez un nom d'utilisateur et un mot de passe entrants sur le système de stockage.

- Deny—l'accès de l'initiateur est refusé au système de stockage.
- Aucune—le système de stockage ne nécessite pas d'authentification pour l'initiateur.

Vous pouvez définir la liste des initiateurs et leurs méthodes d'authentification. Vous pouvez également définir une méthode d'authentification par défaut qui s'applique aux initiateurs qui ne figurent pas dans cette liste.

Informations associées

["Options Windows de chemins d'accès multiples avec Data ONTAP : Fibre Channel et iSCSI"](#)

Gestion de la sécurité de l'initiateur iSCSI

ONTAP offre un certain nombre de fonctionnalités permettant de gérer la sécurité des initiateurs iSCSI. Vous pouvez définir une liste d'initiateurs iSCSI et la méthode d'authentification pour chacun d'entre eux, afficher les initiateurs et leurs méthodes d'authentification associées dans la liste d'authentification, ajouter et supprimer des initiateurs de la liste d'authentification et définir la méthode d'authentification par défaut de l'initiateur iSCSI pour les initiateurs qui ne figurent pas dans la liste.

Isolation du terminal iSCSI

À partir de ONTAP 9.1, les commandes de sécurité iSCSI existantes ont été améliorées pour accepter une plage d'adresses IP, ou plusieurs adresses IP.

Tous les initiateurs iSCSI doivent fournir des adresses IP d'origine lors de l'établissement d'une session ou d'une connexion avec une cible. Cette nouvelle fonctionnalité empêche un initiateur de se connecter au cluster si l'adresse IP d'origine n'est pas prise en charge ou inconnue, fournissant un schéma d'identification unique. Tout initiateur provenant d'une adresse IP non prise en charge ou inconnue aura son login rejeté au niveau de la couche de session iSCSI, empêchant l'initiateur d'accéder à n'importe quelle LUN ou volume du cluster.

Mettez en œuvre cette nouvelle fonctionnalité à l'aide de deux nouvelles commandes pour faciliter la gestion des entrées préexistantes.

Ajouter une plage d'adresses initiateur

Améliorez la gestion de la sécurité de l'initiateur iSCSI en ajoutant une plage d'adresses IP ou plusieurs adresses IP avec le `vserver iscsi security add-initiator-address-range` commande.

```
cluster1::> vserver iscsi security add-initiator-address-range
```

Supprimer la plage d'adresses initiateurs

Supprimez une ou plusieurs adresses IP avec le `vserver iscsi security remove-initiator-address-range` commande.

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

Qu'est-ce que l'authentification CHAP

Le protocole CHAP (Challenge Handshake Authentication Protocol) permet une communication authentifiée entre les initiateurs et les cibles iSCSI. Lorsque vous utilisez l'authentification CHAP, vous définissez des noms d'utilisateur et des mots de passe CHAP sur l'initiateur et le système de stockage.

Au cours de la phase initiale d'une session iSCSI, l'initiateur envoie une demande de connexion au système de stockage pour démarrer la session. La demande de connexion inclut le nom d'utilisateur CHAP de l'initiateur et l'algorithme CHAP. Le système de stockage répond par un défi CHAP. L'initiateur fournit une réponse CHAP. Le système de stockage vérifie la réponse et authentifie l'initiateur. Le mot de passe CHAP est utilisé pour calculer la réponse.

Consignes d'utilisation de l'authentification CHAP

Vous devez suivre certaines directives lors de l'utilisation de l'authentification CHAP.

- Si vous définissez un nom d'utilisateur et un mot de passe entrants sur le système de stockage, vous devez utiliser le même nom d'utilisateur et le même mot de passe pour les paramètres CHAP sortants sur l'initiateur. Si vous définissez également un nom d'utilisateur et un mot de passe sortants sur le système de stockage pour activer l'authentification bidirectionnelle, vous devez utiliser le même nom d'utilisateur et le même mot de passe pour les paramètres CHAP entrants sur l'initiateur.
- Vous ne pouvez pas utiliser les mêmes nom d'utilisateur et mot de passe pour les paramètres entrant et sortant sur le système de stockage.
- Les noms d'utilisateur CHAP peuvent comporter entre 1 et 128 octets.

Un nom d'utilisateur nul n'est pas autorisé.

- Les mots de passe CHAP (secrets) peuvent être de 1 à 512 octets.

Les mots de passe peuvent être des valeurs ou des chaînes hexadécimales. Pour les valeurs hexadécimales, entrez la valeur avec un préfixe « 0x » ou « 0X ». Un mot de passe nul n'est pas autorisé.



ONTAP permet d'utiliser des caractères spéciaux, des lettres non anglaises, des chiffres et des espaces pour les mots de passe CHAP (secrets). Toutefois, cette condition est soumise à des restrictions sur les hôtes. Si l'un de ces éléments n'est pas autorisé par votre hôte spécifique, ils ne peuvent pas être utilisés.

Par exemple, l'initiateur logiciel Microsoft iSCSI nécessite que les mots de passe CHAP d'initiateur et de cible soient d'au moins 12 octets si le cryptage IPsec n'est pas utilisé. La longueur maximale du mot de passe est de 16 octets, qu'IPsec soit utilisé ou non.

Si vous souhaitez restrictions supplémentaires, la documentation de l'initiateur doit s'afficher.

Comment utiliser les listes d'accès de l'interface iSCSI pour limiter les interfaces de l'initiateur peut améliorer les performances et la sécurité

Les listes d'accès à l'interface iSCSI peuvent être utilisées pour limiter le nombre de LIF d'un SVM auxquelles un initiateur peut accéder, ce qui améliore les performances et la sécurité.

Lorsqu'un initiateur commence une session de découverte à l'aide d'un iSCSI `SendTargets` Commande, il reçoit les adresses IP associées à la LIF (network interface) qui figurent dans la liste d'accès. Par défaut, tous les initiateurs ont accès à toutes les LIFs iSCSI du SVM. Vous pouvez utiliser la liste d'accès pour limiter le nombre de LIF d'un SVM auquel un initiateur a accès.

iSNS (Internet Storage Name Service)

Le service iSNS (Internet Storage Name Service) est un protocole qui permet la découverte et la gestion automatisées des périphériques iSCSI sur un réseau de stockage TCP/IP. Un serveur iSNS conserve des informations sur les périphériques iSCSI actifs sur le réseau, y compris leurs adresses IP, les noms d'IQN iSCSI et les groupes de portails.

Vous pouvez obtenir un serveur iSNS auprès d'un fournisseur tiers. Si un serveur iSNS est configuré et activé pour l'initiateur et la cible, vous pouvez utiliser la LIF de gestion d'une machine virtuelle de stockage (SVM) pour enregistrer toutes les LIFs iSCSI de ce SVM sur le serveur iSNS. Une fois l'enregistrement terminé, l'initiateur iSCSI peut interroger le serveur iSNS pour découvrir toutes les LIFs de ce SVM particulier.

Si vous décidez d'utiliser un service iSNS, vous devez vous assurer que vos SVM (Storage Virtual machines) sont correctement enregistrés auprès d'un serveur iSNS (Internet Storage Name Service).

Si vous ne disposez pas d'un serveur iSNS sur votre réseau, vous devez configurer manuellement chaque cible pour qu'elle soit visible par l'hôte.

Que fait un serveur iSNS

Un serveur iSNS utilise le protocole iSNS (Internet Storage Name Service) pour gérer les informations relatives aux périphériques iSCSI actifs sur le réseau, y compris leurs adresses IP, noms de nœuds iSCSI (IQN) et groupes de portails.

Le protocole iSNS permet la découverte et la gestion automatisées des périphériques iSCSI sur un réseau de stockage IP. Un initiateur iSCSI peut interroger le serveur iSNS pour détecter les périphériques cibles iSCSI.

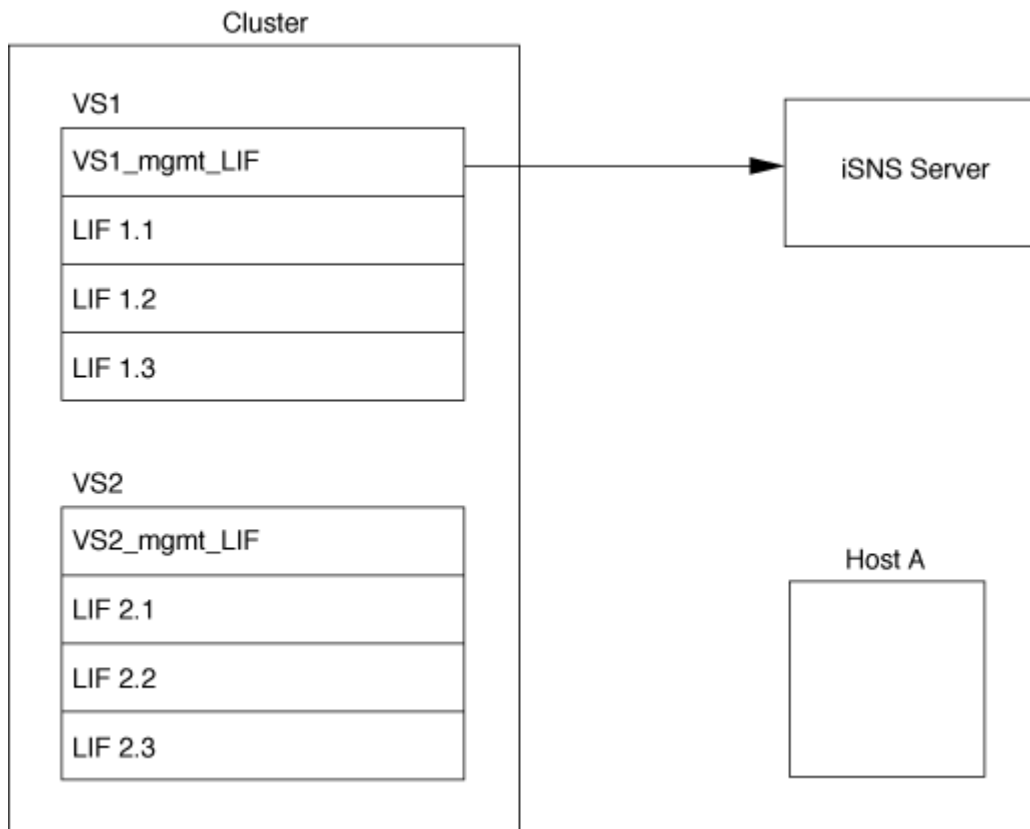
NetApp ne fournit pas ni ne revende de serveurs iSNS. Vous pouvez obtenir ces serveurs auprès d'un fournisseur pris en charge par NetApp.

Interaction des SVM avec un serveur iSNS

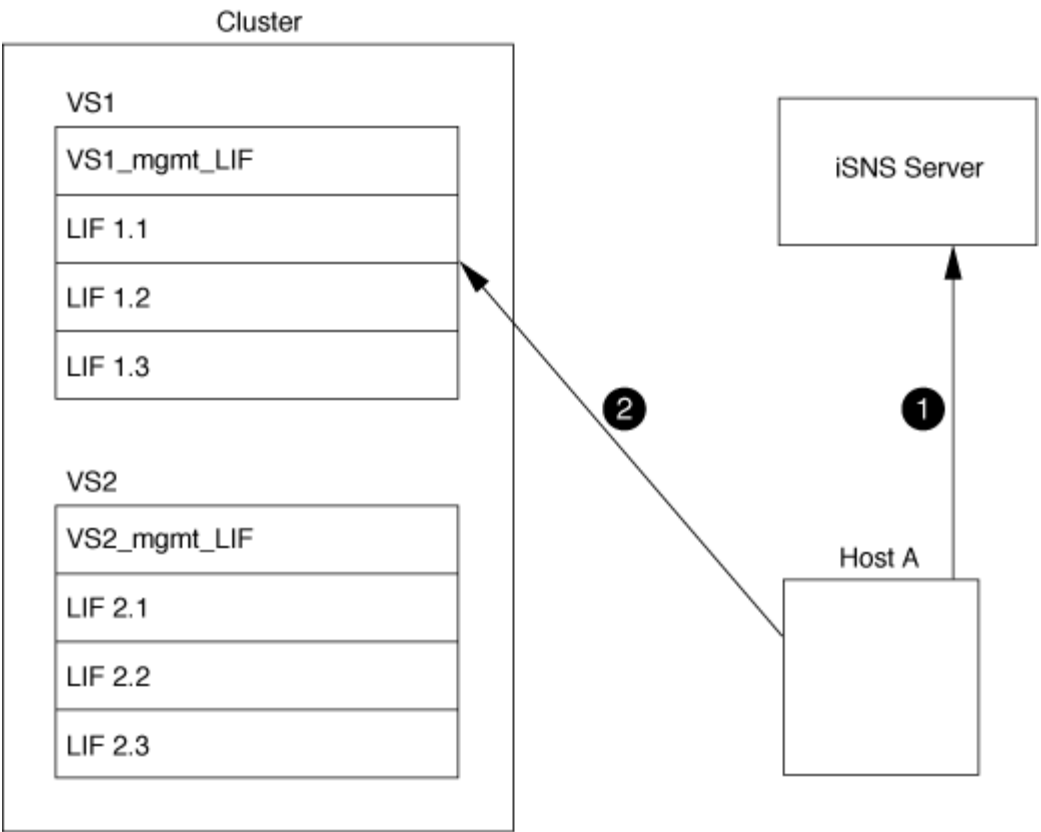
Le serveur iSNS communique avec chaque machine virtuelle de stockage (SVM) via la LIF de gestion des SVM. La LIF de gestion enregistre toutes les informations de nom de nœud cible iSCSI, d'alias et de portail avec le service iSNS pour un SVM spécifique.

Dans l'exemple suivant, le SVM « VS1 » utilise la LIF de gestion du SVM « VS1_mgmt_lif » pour s'enregistrer sur le serveur iSNS. Lors de l'enregistrement iSNS, un SVM envoie toutes les LIFs iSCSI via la LIF de gestion du SVM au serveur iSNS. Une fois l'enregistrement iSNS terminé, le serveur iSNS dispose d'une liste de toutes les LIFs desservant iSCSI dans « VS1 ». Si un cluster contient plusieurs SVM, chaque SVM doit

s'enregistrer individuellement sur le serveur iSNS pour utiliser le service iSNS.



Dans l'exemple suivant, une fois que le serveur iSNS a terminé l'enregistrement avec la cible, l'hôte A peut découvrir toutes les LIFs pour « VS1 » via le serveur iSNS comme indiqué à l'étape 1. Une fois que l'hôte A a terminé la découverte des LIFs pour « VS1 », l'hôte A peut établir une connexion avec l'une des LIFs dans « VS1 », comme indiqué à l'étape 2. L'hôte A ne connaît aucune des LIFs dans « VS2 » jusqu'à ce que la LIF de gestion « VS2_mgmt_LIF » pour les registres « VS2 » avec le serveur iSNS.



Cependant, si vous définissez les listes d'accès de l'interface, l'hôte ne peut utiliser que les LIFs définies dans la liste d'accès de l'interface pour accéder à la cible.

Après la configuration initiale d'iSNS, ONTAP met automatiquement à jour le serveur iSNS lorsque les paramètres de configuration de la SVM changent.

Un délai de quelques minutes peut se produire entre le moment où vous apportez les modifications de configuration et l'envoi de la mise à jour par ONTAP au serveur iSNS. Forcer une mise à jour immédiate des informations iSNS sur le serveur iSNS : `vserver iscsi isns update`

Commandes de gestion d'iSNS

ONTAP fournit des commandes pour gérer votre service iSNS.

Les fonctions que vous recherchez...	Utilisez cette commande...
Configurez un service iSNS	<code>vserver iscsi isns create</code>
Démarrez un service iSNS	<code>vserver iscsi isns start</code>
Modifiez un service iSNS	<code>vserver iscsi isns modify</code>
Affiche la configuration du service iSNS	<code>vserver iscsi isns show</code>
Forcer une mise à jour des informations iSNS enregistrées	<code>vserver iscsi isns update</code>

Arrêtez un service iSNS	<code>vserver iscsi isns stop</code>
Supprimez un service iSNS	<code>vserver iscsi isns delete</code>
Affichez la page man pour une commande	<code>man <i>command name</i></code>

Consultez la page man pour chaque commande pour plus d'informations.

Provisionnement SAN avec FC

Vous devez connaître les concepts importants requis pour comprendre comment ONTAP met en œuvre un FC SAN.

Comment les nœuds cibles FC se connectent au réseau

Les systèmes de stockage et les hôtes ont des adaptateurs afin qu'ils puissent être connectés aux commutateurs FC avec des câbles.

Lorsqu'un nœud est connecté au SAN FC, chaque SVM enregistre le WWPN (World Wide Port Name) de sa LIF avec le service Switch Fabric Name. Le WWNN du SVM et le WWPN de chaque LIF sont automatiquement affectés par le ONTAP.



La connexion directe aux nœuds des hôtes avec FC n'est pas prise en charge, NPIV est requis et un commutateur doit être utilisé.avec les sessions iSCSI, la communication fonctionne avec les connexions soit acheminées par le réseau, soit à connexion directe. Cependant, ces deux méthodes sont prises en charge par ONTAP.

Identification des nœuds FC

Chaque SVM configuré avec FC est identifié par un nom de nœud mondial (WWNN).

Comment les WWPN sont utilisés

Les WWPN identifient chaque LIF dans un SVM configuré pour prendre en charge FC. Ces LIF utilisent les ports FC physiques de chaque nœud du cluster, qui peuvent être des cartes cibles FC, UTA ou UTA2 configurées en tant que FC ou FCoE dans les nœuds.

- Création d'un groupe initiateur

Les WWPN des HBA de l'hôte servent à créer un groupe initiateur. Un groupe initiateur permet de contrôler l'accès des hôtes à des LUN spécifiques. Vous pouvez créer un groupe initiateur en spécifiant une collection de WWPN des initiateurs dans un réseau FC. Lorsque vous mappez une LUN sur un système de stockage sur un groupe initiateur, vous pouvez accorder à tous les initiateurs de ce groupe l'accès à cette LUN. Si le WWPN d'un hôte ne se trouve pas dans un groupe initiateur mappé sur une LUN, cet hôte n'a pas accès à la LUN. Cela signifie que les LUN n'apparaissent pas comme des disques sur cet hôte.

Vous pouvez également créer des jeux de ports pour rendre une LUN visible uniquement sur des ports cibles spécifiques. Un ensemble de ports se compose d'un groupe de ports FC target. Vous pouvez lier un groupe initiateur à un ensemble de ports. N'importe quel hôte du groupe initiateur peut accéder aux LUN qu'en vous connectant aux ports cibles de l'ensemble de ports.

- Identification unique des LIF FC

Les WWPN identifient de manière unique chaque interface logique FC. Le système d'exploitation hôte utilise la combinaison de WWNN et de WWPN pour identifier les SVM et les LIF FC. Certains systèmes d'exploitation nécessitent une liaison permanente pour s'assurer que la LUN apparaît au même ID cible sur l'hôte.

Fonctionnement des affectations de noms à l'échelle mondiale

Les noms dans le monde sont créés de manière séquentielle dans ONTAP. Cependant, en raison de la manière dont ONTAP les affecte, ils peuvent sembler être affectés dans un ordre non séquentiel.

Chaque adaptateur possède un WWPN et un WWNN préconfigurés, mais ONTAP n'utilise pas ces valeurs préconfigurées. En revanche, ONTAP attribue ses propres WWPN ou WWN, en fonction des adresses MAC des ports Ethernet intégrés.

Les noms mondiaux peuvent sembler non séquentiels lorsqu'ils sont affectés pour les raisons suivantes :

- Des noms mondiaux sont attribués à l'ensemble des nœuds et des SVM (Storage Virtual machine) dans le cluster.
- Les noms partout dans le monde libérés sont recyclés et ajoutés au pool de noms disponibles.

Identification des commutateurs FC

Les switches Fibre Channel possèdent un nom de nœud mondial (WWNN) pour le périphérique lui-même et un WWPN (World Port Name) pour chacun de ses ports.

Le diagramme suivant montre par exemple comment les WWPN sont affectés à chacun des ports d'un commutateur Brocade à 16 ports. Pour plus de détails sur le numéro des ports pour un commutateur particulier, reportez-vous à la documentation fournie par le fournisseur pour ce commutateur.



Port **0**, WWPN 20:**00**:00:60:69:51:06:b4

Port **1**, WWPN 20:**01**:00:60:69:51:06:b4

Port **14**, WWPN 20: **0e**:00:60:69:51:06:b4

Port **15**, WWPN 20:******:00:60:69:51:06:b4

Provisionnement SAN avec NVMe

Depuis la version ONTAP 9.4, NVMe/FC est pris en charge dans un environnement SAN. NVMe/FC permet aux administrateurs de stockage de provisionner des espaces de noms et des sous-systèmes, puis de les mapper aux sous-systèmes, de la même manière que les LUN sont provisionnées et mappées aux groupes pour FC et iSCSI.

Un namespace NVMe est une quantité de mémoire non volatile pouvant être formatée dans des blocs logiques. Les espaces de noms sont l'équivalent de LUN pour les protocoles FC et iSCSI, et un sous-système NVMe est similaire à un groupe initiateur. Un sous-système NVMe peut être associé à des initiateurs afin que les espaces de noms dans le sous-système soient accessibles par les initiateurs associés.



Bien qu'ils soient similaires à leur fonction, les espaces de noms NVMe ne prennent pas en charge toutes les fonctionnalités prises en charge par les LUN.

À partir de ONTAP 9.5, une licence est requise pour la prise en charge de l'accès aux données côté hôte avec NVMe. Si NVMe est activé dans ONTAP 9.4, une période de grâce de 90 jours est accordée pour l'acquisition de la licence après la mise à niveau vers ONTAP 9.5. Si vous l'avez "ONTAP One", Les licences NVMe sont incluses. Vous pouvez activer la licence à l'aide de la commande suivante :

```
system license add -license-code NVMe_license_key
```

Informations associées

["Rapport technique NetApp 4684 : implémentation et configuration des SAN modernes avec NVMe/FC"](#)

Volumes SAN

Présentation des volumes SAN

ONTAP propose trois options de provisionnement de base : le provisionnement fin, le provisionnement fin et le provisionnement semi-lourd. Chaque option utilise différentes méthodes pour gérer l'espace volume et les besoins en espace pour les technologies de partage de blocs ONTAP. Comprendre le fonctionnement des options vous permet de choisir la meilleure option pour votre environnement.



Il n'est pas recommandé d'installer des LUN SAN et des partages NAS dans le même volume FlexVol. Vous devez provisionner des volumes FlexVol distincts pour vos LUN SAN, et vous devez en particulier provisionner des volumes FlexVol distincts pour vos partages NAS. Cela simplifie les déploiements de gestion et de réplication, tout en parallèle à la prise en charge des volumes FlexVol dans Active IQ Unified Manager (anciennement OnCommand Unified Manager).

Provisionnement fin pour les volumes

Lors de la création d'un volume à provisionnement fin, ONTAP ne réserve aucun espace supplémentaire lors de la création du volume. Au fur et à mesure de l'écriture des données sur le volume, le volume demande le stockage dont il a besoin depuis l'agrégat pour prendre en charge l'opération d'écriture. L'utilisation de volumes à provisionnement fin vous permet d'effectuer un surengagement de votre agrégat. Ce dernier risque donc de ne pas pouvoir sécuriser l'espace requis lorsqu'il vient à manquer d'espace.

Vous créez un volume FlexVol à provisionnement fin en paramétrant son unité `-space-guarantee` option à `none`.

Provisionnement lourd pour les volumes

Lorsqu'un volume à provisionnement lourd est créé, la mémoire ONTAP réserve suffisamment de stockage de l'agrégat pour garantir l'écriture à tout moment de n'importe quel bloc du volume. Lorsque vous configurez un volume pour utiliser le provisionnement lourd, vous pouvez utiliser n'importe quelle fonction d'efficacité du stockage ONTAP, comme la compression et la déduplication, pour ainsi compenser les plus importantes

besoins en stockage initial.

Vous créez un volume FlexVol à provisionnement lourd en définissant sa valeur `-space-slo` (objectif de niveau de service) à `thick`.

Provisionnement semi-lourd pour les volumes

Lorsqu'un volume utilisant un provisionnement semi-lourd est créé, ONTAP met de côté l'espace de stockage de l'agrégat pour tenir compte de la taille du volume. Si le volume manque d'espace disponible parce que les blocs sont utilisés par les technologies de partage de blocs, ONTAP supprime un effort de suppression des objets de protection (copies Snapshot et fichiers FlexClone et LUN) afin de libérer l'espace qu'ils conservent. Tant que la ONTAP peut supprimer les objets de données de protection assez rapidement pour prendre en charge l'espace requis pour les écrasements, les opérations d'écriture sont continues. Il s'agit là d'une garantie d'écriture « meilleur effort ».

Remarque : la fonctionnalité suivante n'est pas prise en charge sur les volumes qui utilisent le provisionnement semi-épais :

- des technologies d'efficacité du stockage telles que la déduplication, la compression et la compaction
- Microsoft Offloaded Data Transfer (ODX)

Vous créez un volume FlexVol à provisionnement semi-lourd en paramétrant son option `-space-slo` (objectif de niveau de service) à `semi-thick`.

À utiliser avec des fichiers et des LUN réservés en espace

Une LUN ou un fichier réservé à l'espace est un fichier pour lequel le stockage est alloué lors de sa création. Par le passé, NetApp a utilisé le terme « LUN à provisionnement fin » pour désigner une LUN dont la réservation d'espace est désactivée (LUN non réservée d'espace).

Remarque : les fichiers non réservés à l'espace ne sont généralement pas appelés « fichiers à provisionnement fin ».

Le tableau suivant récapitule les principales différences de manière à utiliser les trois options de provisionnement de volumes avec des fichiers et des LUN réservés à l'espace :

Provisionnement de volume	Réservation d'espace LUN/fichier	Écrasements	Données de protection ²	Efficacité du stockage ³
Épais	Pris en charge	Garanti ¹	Résultats garantis	Pris en charge
Fin	Aucun effet	Aucune	Résultats garantis	Pris en charge
Semi-épais	Pris en charge	Meilleur effort ¹	Meilleur effort	Non pris en charge

Notes

1. Pour garantir le remplacement ou fournir une garantie de remplacement sans effort, la réservation d'espace est activée sur la LUN ou le fichier.
2. Les données de protection incluent des copies Snapshot, ainsi que les fichiers FlexClone et les LUN marqués pour la suppression automatique (clones de sauvegarde).

3. L'efficacité du stockage inclut la déduplication, la compression, tous les fichiers FlexClone et LUN non marqués pour la suppression automatique (clones actifs) et les sous-fichiers FlexClone (utilisés pour le déchargement des copies).

Prise en charge des LUN SCSI à provisionnement fin

ONTAP prend en charge les LUN T10 SCSI à provisionnement fin ainsi que les LUN NetApp à provisionnement fin. Le provisionnement fin SCSI T10 permet aux applications hôtes de prendre en charge les fonctionnalités SCSI, notamment la récupération d'espace LUN et la surveillance de l'espace LUN pour les environnements en blocs. Le provisionnement fin SCSI T10 doit être pris en charge par votre logiciel hôte SCSI.

Vous utilisez ONTAP `space-allocation` Paramètre permettant d'activer/de désactiver la prise en charge du provisionnement fin T10 sur une LUN. Vous utilisez ONTAP `space-allocation enable` Paramètre permettant d'activer le provisionnement fin SCSI T10 sur une LUN.

Le `[-space-allocation {enabled|disabled}]` Commande dans le manuel de référence des commandes ONTAP contient plus d'informations pour activer/désactiver la prise en charge du provisionnement fin T10 et activer le provisionnement fin SCSI T10 sur un LUN.

["Référence de commande ONTAP"](#)

Configurer les options de provisionnement de volumes

Vous pouvez configurer un volume pour le provisionnement fin, le provisionnement lourd ou le provisionnement semi-lourd.

Description de la tâche

Réglage du `-space-slo` option à `thick` assure les éléments suivants :

- Le volume entier est préalloué dans l'agrégat. Vous ne pouvez pas utiliser `volume create` ou `volume modify` commande pour configurer les volumes `-space-guarantee` option.
- 100 % de l'espace requis pour les écrasements est réservé. Vous ne pouvez pas utiliser `volume modify` commande pour configurer les volumes `-fractional-reserve` option

Réglage du `-space-slo` option à `semi-thick` assure les éléments suivants :

- Le volume entier est préalloué dans l'agrégat. Vous ne pouvez pas utiliser `volume create` ou `volume modify` commande pour configurer les volumes `-space-guarantee` option.
- Aucun espace n'est réservé aux écrasements. Vous pouvez utiliser le `volume modify` commande pour configurer les volumes `-fractional-reserve` option.
- La suppression automatique des copies Snapshot est activée.

Étape

1. Configurez les options de provisionnement des volumes :

```
volume create -vserver vservers_name -volume volume_name -aggregate
aggregate_name -space-slo none|thick|semi-thick -space-guarantee none|volume
```

Le `-space-guarantee` par défaut, l'option est `none` Pour les systèmes AFF et pour les volumes non-AFF DP. Sinon, elle est définie par défaut sur `volume`. Pour les volumes FlexVol existants, utilisez le

volume modify commande permettant de configurer les options de provisionnement.

La commande suivante configure vol1 sur SVM vs1 pour le provisionnement fin :

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-guarantee none
```

La commande suivante configure vol1 sur le SVM vs1 pour le provisionnement Thick :

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo thick
```

La commande suivante configure vol1 sur le SVM vs1 pour le provisionnement semi-lourd :

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-thick
```

Options de configuration de volume SAN

Vous devez définir différentes options sur le volume contenant votre LUN. La méthode de définition des options du volume détermine la quantité d'espace disponible pour les LUN du volume.

Croissance automatique

Vous pouvez activer ou désactiver la croissance automatique. Si vous la activez, la croissance automatique permet à ONTAP d'augmenter automatiquement la taille du volume jusqu'à une taille maximale que vous prédéterminez. L'espace doit être disponible dans l'agrégat contenant pour prendre en charge la croissance automatique du volume. Par conséquent, si vous activez la croissance automatique, vous devez surveiller l'espace libre dans l'agrégat contenant et en ajouter d'autres si nécessaire.

Le nombre de disques automatique ne peut pas être déclenché pour prendre en charge la création de snapshots. Si vous tentez de créer une copie Snapshot et que l'espace disponible sur le volume est insuffisant, la création de snapshots échoue, même si la croissance automatique est activée.

Si la croissance automatique est désactivée, la taille de votre volume reste la même.

Autoshrink

Vous pouvez activer ou désactiver Autoshrink. Si vous l'activez, la fonction autoshrink permet à ONTAP de diminuer automatiquement la taille globale d'un volume lorsque la quantité d'espace consommée dans le volume diminue un seuil prédéfini. Le stockage est ainsi plus efficace, ce qui entraîne le déclenchement des volumes pour libérer automatiquement l'espace libre inutilisé.

Suppression automatique de l'instantané

La suppression automatique du Snapshot supprime automatiquement les copies Snapshot lorsque l'une des opérations suivantes se produit :

- Le volume est presque plein.
- L'espace réservé de l'instantané est presque plein.
- L'espace de réserve d'écrasement est plein.

Vous pouvez configurer la suppression automatique de Snapshot de manière à supprimer les copies Snapshot du plus ancien au plus récent ou du plus récent au plus ancien. La suppression automatique des snapshots ne supprime pas les copies Snapshot liées aux copies Snapshot dans les volumes ou les LUN clonés.

Si votre volume a besoin d'espace supplémentaire et que vous avez activé la croissance automatique et la suppression automatique des snapshots, par défaut, ONTAP tente d'acquérir l'espace nécessaire en activant la croissance automatique en premier. Si l'espace suffisant n'est pas acquis via la croissance automatique, la suppression automatique des snapshots est déclenchée.

Réserve Snapshot

La réserve Snapshot définit la quantité d'espace dans le volume réservé pour les copies Snapshot. L'espace alloué à la réserve Snapshot ne peut pas être utilisé à d'autres fins. Si tout l'espace alloué à la réserve Snapshot est utilisé, les copies Snapshot commencent à consommer de l'espace supplémentaire sur le volume.

Nécessité de déplacer des volumes dans des environnements SAN

Avant de déplacer un volume qui contient des LUN ou des espaces de noms, vous devez répondre à certaines exigences.

- Pour les volumes contenant une ou plusieurs LUN, vous devez disposer d'au moins deux chemins par LUN (LIF) qui se connectent à chaque nœud du cluster.

Cela élimine les points de défaillance uniques et permet au système de résister aux défaillances des composants.

- Pour les volumes contenant des espaces de noms, le cluster doit exécuter ONTAP 9.6 ou version ultérieure.

Le déplacement de volumes n'est pas pris en charge dans les configurations NVMe qui exécutent ONTAP 9.5.

Considérations relatives à la définition de la réserve fractionnaire

La réserve fractionnaire de remplacement, également appelée *LUN Overwrite Reserve*, permet de désactiver la réserve de remplacements pour les LUN et les fichiers réservés à l'espace dans un volume FlexVol. Cela peut vous aider à optimiser l'utilisation du stockage, mais si votre environnement est affecté par des opérations d'écriture qui échouent à cause du manque d'espace, vous devez comprendre les exigences de cette configuration.

Le paramètre de réserve fractionnaire est exprimé sous forme de pourcentage ; les seules valeurs valides sont 0 et 100 pour cent. Le paramètre de réserve fractionnaire est un attribut du volume.

Définition de la réserve fractionnaire sur 0 meilleure exploitation du stockage. Cependant, une application qui accède aux données d'un volume peut subir une interruption de service des données si son espace est

insuffisant, même avec la garantie du volume définie sur `volume`. Toutefois, grâce à une configuration et à une utilisation appropriées du volume, vous pouvez réduire les risques d'échec des écritures. ONTAP propose une garantie d'écriture « meilleur effort » pour les volumes dont la réserve fractionnaire est définie sur 0 lorsque *tous* des conditions suivantes sont remplies :

- La déduplication n'est pas utilisée
- La compression n'est pas utilisée
- Les sous-fichiers FlexClone ne sont pas utilisés
- Tous les fichiers FlexClone et les LUN FlexClone sont activés pour la suppression automatique

Ce n'est pas le paramètre par défaut. Vous devez explicitement activer la suppression automatique lors de sa création ou en modifiant le fichier FlexClone ou la LUN après sa création.

- ODX et l'allègement de la charge des copies FlexClone ne sont pas utilisés
- La garantie du volume est définie sur `volume`
- La réservation d'espace fichier ou LUN est `enabled`
- La réserve Snapshot du volume est définie sur 0
- La suppression automatique de la copie Snapshot du volume est `enabled` avec un niveau d'engagement de `destroy`, une liste de destruction de `lun_clone`, `vol_clone`, `cifs_share`, `file_clone`, `sfsr`, et un déclencheur de `volume`

Ce paramètre permet également de s'assurer que les fichiers FlexClone et les LUN FlexClone sont supprimés lorsque nécessaire.

Notez que si le taux de modification est élevé, dans de rares cas, la suppression automatique de la copie Snapshot peut se situer derrière et que l'espace du volume est insuffisant, même si tous les paramètres de configuration ci-dessus sont utilisés.

Vous avez également la possibilité d'utiliser la fonctionnalité de croissance automatique de volumes pour réduire la probabilité de suppression automatique des copies Snapshot de volumes. Si vous activez la capacité de croissance automatique, vous devez surveiller l'espace libre dans l'agrégat associé. Si l'agrégat devient suffisamment complet que le volume n'a pas pu croître, la quantité de copies Snapshot sera probablement supprimée lorsque l'espace libre dans le volume est épuisé.

Si vous ne pouvez pas remplir l'ensemble des conditions ci-dessus et que vous devez vous assurer que l'espace du volume est insuffisant, vous devez définir le paramètre de réserve fractionnaire du volume sur 100. Cela nécessite davantage d'espace disponible à l'avance, mais garantit que les opérations de modification des données réussiront même si les technologies répertoriées ci-dessus sont en cours d'utilisation.

La valeur par défaut et les valeurs autorisées pour le paramètre de réserve fractionnaire dépendent de la garantie du volume :

Garantie de volume	Réserve fractionnaire par défaut	Valeurs autorisées
Volumétrie	100	0, 100
Aucune	0	0, 100

Gestion de l'espace côté hôte SAN

Dans un environnement à provisionnement fin, la gestion de l'espace côté hôte complète le processus de gestion de l'espace depuis le système de stockage qui a été libéré dans le système de fichiers hôte.

Un système de fichiers hôte contient des métadonnées pour suivre les blocs disponibles pour stocker de nouvelles données et les blocs contenant des données valides qui ne doivent pas être écrasés. Ces métadonnées sont stockées au sein de la LUN. Lorsqu'un fichier est supprimé dans le système de fichiers hôte, les métadonnées du système de fichiers sont mises à jour pour marquer les blocs de ce fichier comme espace libre. L'espace total disponible du système de fichiers est ensuite recalculé pour inclure les blocs récemment libérés. Sur le système de stockage, ces mises à jour de métadonnées n'apparaissent aucune différence entre les autres écritures effectuées par l'hôte. Par conséquent, le système de stockage n'a pas conscience que des suppressions se sont produits.

Cela crée un écart entre la quantité d'espace libre signalée par l'hôte et la quantité d'espace libre signalée par le système de stockage sous-jacent. Supposons par exemple que vous avez affecté un nouveau LUN de 200 Go provisionné à l'hôte par votre système de stockage. L'hôte et le système de stockage indiquent 200 Go d'espace libre. L'hôte écrit alors 100 Go de données. À ce stade, l'hôte et le système de stockage indiquent 100 Go d'espace utilisé et 100 Go d'espace inutilisé.

Vous supprimez ensuite 50 Go de données de votre hôte. À ce stade, votre hôte indique 50 Go d'espace utilisé et 150 Go d'espace inutilisé. Toutefois, votre système de stockage indique 100 Go d'espace utilisé et 100 Go d'espace inutilisé.

La gestion de l'espace côté hôte utilise différentes méthodes pour concilier la différence d'espace entre l'hôte et le système de stockage.

Gestion simplifiée de l'hôte avec SnapCenter

Le logiciel SnapCenter permet de simplifier certaines des tâches de gestion et de protection des données associées aux solutions de stockage iSCSI et FC. SnapCenter est un package de gestion facultatif pour les hôtes Windows et UNIX.

Le logiciel SnapCenter peut être utilisé pour créer facilement des disques virtuels à partir de pools de stockage qui peuvent être distribués sur plusieurs systèmes de stockage, ainsi que pour automatiser des tâches de provisionnement du stockage et simplifier le processus de création de copies Snapshot et de clones à partir de copies Snapshot cohérentes avec les données hôtes.

Consultez la documentation des produits NetApp pour plus d'informations sur ["SnapCenter"](#).

Liens connexes

["Activez l'allocation d'espace pour les LUN SCSI à provisionnement fin"](#)

À propos des igroups

Les groupes initiateurs sont des tableaux des WWPN des hôtes du protocole FC ou des noms des nœuds hôtes iSCSI. Vous pouvez définir des groupes initiateurs et les mapper sur des LUN pour contrôler l'accès des initiateurs aux LUN.

Généralement, vous souhaitez que tous les ports initiateurs ou initiateurs logiciels de l'hôte puissent accéder à une LUN. Si vous utilisez un logiciel de chemins d'accès multiples ou que vous disposez d'hôtes en cluster, chaque port d'initiateur ou initiateur logiciel de chaque hôte en cluster a besoin de chemins redondants vers la

même LUN.

Vous pouvez créer des groupes initiateurs spécifiant les initiateurs auxquels les initiateurs ont accès aux LUN avant ou après leur création. Vous devez toutefois créer des groupes initiateurs avant de pouvoir mapper une LUN sur un groupe initiateur.

Plusieurs groupes initiateurs peuvent avoir plusieurs initiateurs. Vous pouvez également avoir le même initiateur. Toutefois, vous ne pouvez pas mapper une LUN sur plusieurs groupes initiateurs qui ont le même initiateur. Un initiateur ne peut pas être membre des igroups de différents otypes.

Exemple de mode d'accès des groupes initiateurs aux LUN

Vous pouvez créer plusieurs igroups pour définir quels LUN sont disponibles pour vos hôtes. Par exemple, si vous disposez d'un cluster hôte, vous pouvez utiliser des igroups pour s'assurer que des LUN spécifiques ne sont visibles que pour un seul hôte du cluster ou pour tous les hôtes du cluster.

Le tableau suivant montre comment quatre groupes initiateurs accèdent aux LUN pour quatre hôtes différents qui accèdent au système de stockage. Les hôtes en cluster (Host3 et Host4) sont tous deux membres du même groupe initiateur (groupe3) et peuvent accéder aux LUN mappées à ce groupe initiateur. Le groupe initiateur nommé groupe4 contient les WWPN de Host4 pour stocker les informations locales qui ne sont pas destinées à être vues par son partenaire.

Hôtes avec WWPN HBA, IQN ou EUI	igroups	WWPN, IQN et EUI ajoutés aux igroups	LUN mappées aux igroups
Host1, chemin unique (initiateur de logiciel iSCSI) iqn.1991-05.com.microsoft:host1	groupe 1	iqn.1991-05.com.microsoft:host1	/vol/vol2/lun1
Host2, multipath (deux HBA) 10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	groupe 2	10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	/vol/vol2/lun2
Host3, multipath, cluster avec l'hôte 4 10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02	groupe 3	10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	/vol/vol2/mtree1/lun3

Hôtes avec WWPN HBA, IQN ou EUI	igroups	WWPN, IQN et EUI ajoutés aux igroups	LUN mappées aux igroups
Host4, multichemin, cluster (non visible sur Host3)	groupe4	10:00:00:00:c9:2b:51:2c	/vol/vol2/qtrees2/lun4
10:00:00:00:c9:2b:51:2c		10:00:00:00:c9:2b:47:a2	/vol/vol2/qtrees1/lun5
10:00:00:00:c9:2b:47:a2			

Spécifiez les WWPN des initiateurs et les noms des nœuds iSCSI pour un groupe initiateur

Lorsque vous créez un groupe initiateur, vous pouvez spécifier les noms des nœuds iSCSI et les WWPN des initiateurs ou les ajouter ultérieurement. Si vous choisissez de spécifier les noms des nœuds iSCSI d'initiateur et les WWPN lorsque vous créez la LUN, ils peuvent être supprimés plus tard, si nécessaire.

Suivez les instructions de la documentation Host Utilities pour obtenir les WWPN et rechercher les noms de nœud iSCSI associés à un hôte spécifique. Pour les hôtes exécutant le logiciel ESX, utilisez Virtual Storage Console.

Virtualisation du stockage avec copie auxiliaire VMware et Microsoft

Présentation de la virtualisation du stockage avec VMware et Microsoft Copy Offload

VMware et Microsoft prennent en charge des opérations de déchargement des copies afin d'augmenter les performances et le débit du réseau. Vous devez configurer votre système pour qu'il réponde aux exigences des environnements des systèmes d'exploitation VMware et Windows et utilise leurs fonctions respectives de déchargement des copies.

Lorsque vous utilisez les copies VMware et Microsoft auxiliaires dans les environnements virtualisés, vos LUN doivent être alignées. Les LUN non alignés peuvent dégrader les performances.

Avantages liés à l'utilisation d'un environnement SAN virtualisé

La création d'un environnement virtualisé à l'aide de serveurs virtuels de stockage (SVM) et de LIF vous permet d'étendre votre environnement SAN à tous les nœuds du cluster.

- Gestion distribuée

Vous pouvez vous connecter à n'importe quel nœud du SVM afin d'administrer tous les nœuds d'un cluster.

- Un meilleur accès aux données

Avec MPIO et ALUA, vous avez accès à vos données via n'importe quelle LIF iSCSI ou FC active pour la SVM.

- Contrôle de l'accès aux LUN

Si vous utilisez SLM et des ensembles de ports, vous pouvez limiter les LIF qu'un initiateur peut utiliser pour accéder aux LUN.

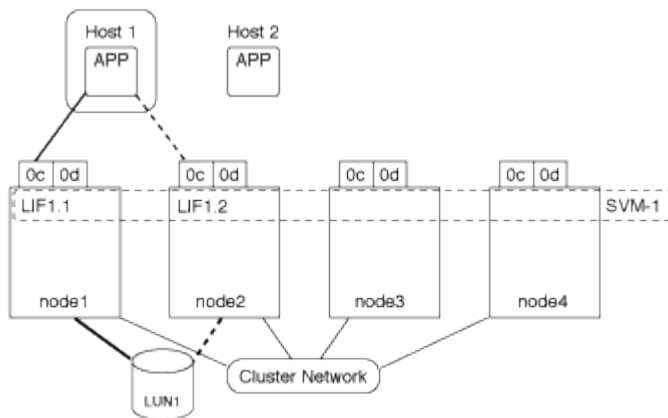
Fonctionnement de l'accès aux LUN dans un environnement virtualisé

Dans un environnement virtualisé, les LIF permettent aux hôtes (clients) d'accéder aux LUN via des chemins optimisés et non optimisés.

Une LIF est une interface logique qui connecte le SVM à un port physique. Bien que plusieurs SVM puissent avoir plusieurs LIF sur le même port, une LIF appartient à un SVM. Vous pouvez accéder aux LUN via les LIFs du SVM.

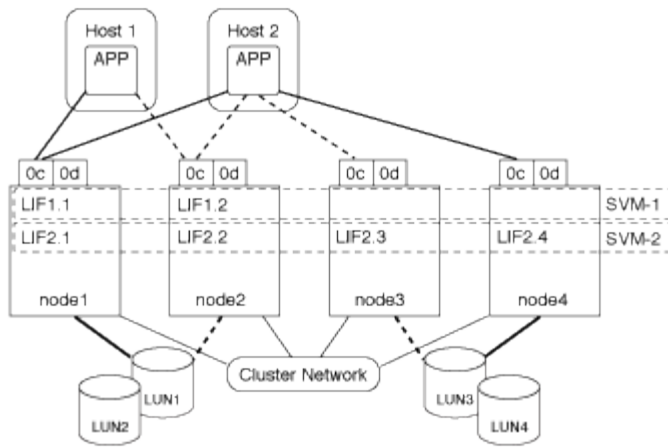
Exemple d'accès à une LUN avec un seul SVM dans un cluster

Dans l'exemple suivant, l'hôte 1 se connecte à LIF1.1 et LIF1.2 au SVM-1 pour accéder à LUN1. LIF1.1 utilise le port physique node1:0C et LIF1.2 utilise le node2:0C. LIF1.1 et LIF1.2 n'appartiennent qu'au SVM-1. Si une nouvelle LUN est créée sur le nœud 1 ou 2, pour SVM-1, elle peut utiliser ces mêmes LIF. Si un nouveau SVM est créé, de nouvelles LIF peuvent être créées à l'aide des ports physiques 0C ou 0d sur les deux nœuds.



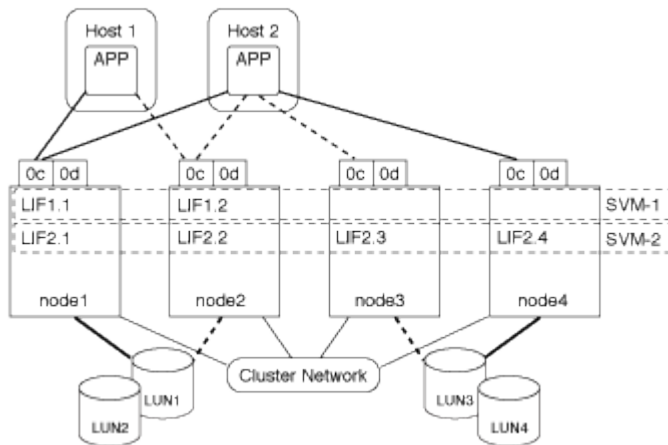
Exemple d'accès LUN avec plusieurs SVM dans un cluster

Un port physique peut prendre en charge plusieurs LIF servant différents SVM. Étant donné que les LIFs sont associées à un SVM particulier, les nœuds de cluster peuvent envoyer le trafic de données entrantes au SVM correct. Dans l'exemple suivant, chaque nœud de 1 à 4 a une LIF pour SVM-2 en utilisant le port physique 0C sur chaque nœud. L'hôte 1 se connecte à LIF1.1 et LIF1.2 du SVM-1 pour accéder à l'utilitaire LUN1. L'hôte 2 se connecte à LIF2-1 et LIF2-2 au SVM-2 pour accéder aux LUN2. Les deux SVM partagent le port physique 0C sur les nœuds 1 et 2. SVM-2 dispose de LIF supplémentaires qui utilisent l'hôte 2 pour accéder aux LUN 3 et 4. Ces LIF utilisent le port physique 0C sur les nœuds 3 et 4. Plusieurs SVM peuvent partager les ports physiques sur les nœuds.



Exemple de chemin actif ou optimisé vers une LUN à partir d'un système hôte

Dans un chemin actif ou optimisé, le trafic de données ne transite pas par le réseau de clusters ; il déplace le chemin le plus direct vers la LUN. Le chemin actif ou optimisé vers LUN1 est via LIF1.1 dans le nœud1, en utilisant le port physique 0C. L'hôte 2 possède deux chemins actifs ou optimisés, un chemin vers le nœud1, LIF2.1, qui partage le port physique 0C et l'autre chemin vers le nœud4, LIF2.4, qui utilise le port physique 0C.



Exemple de chemin d'accès actif ou non optimisé (indirect) vers une LUN depuis un système hôte

Dans un chemin actif ou non optimisé (indirect), le trafic de données transite par le réseau en cluster. Ce problème survient uniquement si tous les chemins actifs ou optimisés d'un hôte ne sont pas disponibles pour gérer le trafic. Si le chemin d'accès de l'hôte 2 vers SVM-2 LIF2.4 est perdu, l'accès à LUN3 et LUN4 traverse le réseau de cluster. L'accès à partir de l'hôte 2 utilise LIF2.3 sur le nœud 3. Ensuite, le trafic entre dans le commutateur de réseau du cluster et sauvegarde vers le nœud4 pour accéder aux LUN3 et LUN4. Il traverse ensuite le commutateur réseau du cluster, puis revient via LIF2.3 à l'hôte 2. Ce chemin actif ou non optimisé est utilisé jusqu'à ce que le chemin vers LIF2.4 soit restauré ou qu'une nouvelle LIF soit créée pour SVM-2 sur un autre port physique du nœud 4.



=
:allow-uri-read:

Améliorer les performances VMware VAAI pour les hôtes ESX

ONTAP prend en charge certaines API VMware vStorage pour l'intégration de baies (VAAI) lorsque l'hôte ESX exécute ESX 4.1 ou une version ultérieure. Ces fonctionnalités permettent de décharger l'hôte ESX vers le système de stockage et d'augmenter le débit du réseau. L'hôte ESX active ces fonctionnalités automatiquement dans l'environnement adéquat.

La fonctionnalité VAAI prend en charge les commandes SCSI suivantes :

- EXTENDED_COPY

Cette fonctionnalité permet à l'hôte de lancer le transfert de données entre les LUN ou au sein d'une LUN sans impliquer l'hôte dans le transfert de données. Résultat : des économies sur les cycles de CPU ESX et une augmentation du débit réseau. La fonctionnalité de copie étendue, également appelée « copie auxiliaire », est utilisée dans les scénarios tels que le clonage d'une machine virtuelle. Lorsqu'elle est invoquée par l'hôte ESX, la fonctionnalité d'allègement de la charge de copie copie copie copie copie copie copie les données du système de stockage plutôt que de passer par le réseau hôte. L'allègement de la charge des copies transfère les données de l'une des manières suivantes :

- Dans une LUN
- Entre les LUN d'un volume
- Entre des LUN sur des volumes différents au sein d'une machine virtuelle de stockage (SVM)
- Entre LUN sur différents SVM au sein d'un cluster

Si cette fonctionnalité ne peut pas être invoquée, l'hôte ESX utilise automatiquement les commandes standard DE LECTURE et D'ÉCRITURE pour l'opération de copie.

- WRITE_SAME

Cette fonctionnalité décharge le travail d'écriture d'un modèle répété, tel que tous les zéros, vers une baie de stockage. L'hôte ESX utilise cette fonctionnalité lors d'opérations telles que le remplissage sans fichier.

- COMPARE_AND_WRITE

Cette fonctionnalité contourne certaines limites de simultanéité d'accès aux fichiers, ce qui accélère les

opérations comme le démarrage des machines virtuelles.

Conditions d'utilisation de l'environnement VAAI

Les fonctionnalités VAAI font partie du système d'exploitation ESX et sont automatiquement appelées par l'hôte ESX lors de la configuration de l'environnement approprié.

Les exigences environnementales sont les suivantes :

- L'hôte ESX doit exécuter ESX 4.1 ou version ultérieure.
- Le système de stockage NetApp hébergeant le datastore VMware doit exécuter ONTAP.
- (Copie auxiliaire uniquement) la source et la destination de l'opération de copie VMware doivent être hébergées sur le même système de stockage au sein du même cluster.



La fonctionnalité d'allègement de la charge des copies ne prend actuellement pas en charge la copie des données entre datastores VMware hébergés sur des systèmes de stockage différents.

Déterminez si les fonctions VAAI sont prises en charge par ESX

Pour vérifier si le système d'exploitation ESX prend en charge les fonctionnalités VAAI, vous pouvez vérifier le client vSphere ou utiliser tout autre moyen d'accéder à l'hôte. ONTAP prend en charge les commandes SCSI par défaut.

Vous pouvez vérifier les paramètres avancés de votre hôte ESX pour déterminer si les fonctionnalités VAAI sont activées. Le tableau indique quelles commandes SCSI correspondent aux noms de contrôle ESX.

Commande SCSI	Nom du contrôle ESX (fonctionnalité VAAI)
COPIE ÉTENDUE	HardwareAcceleratedMove
WRITE_SAME	HardwareAcceleratedInit
COMPARER_ET_ÉCRIRE	HardwareAcceleratedLocking

Microsoft Offloaded Data Transfer (ODX)

Microsoft Offloaded Data Transfer (ODX), également appelé *copy Offload*, permet le transfert direct de données au sein d'un périphérique de stockage ou entre des périphériques de stockage compatibles sans transférer les données via l'ordinateur hôte.

ONTAP prend en charge ODX à la fois pour les protocoles SMB et SAN.

Dans les transferts de fichiers non ODX, les données sont lues à partir de la source et transférées sur le réseau vers l'hôte. L'hôte transfère les données via le réseau vers la destination. Dans le transfert de fichier ODX, les données sont copiées directement de la source vers la destination sans passer par l'hôte.

Les copies déchargées d'ODX sont effectuées directement entre la source et la destination. Par conséquent, des copies sont réalisées au sein d'un même volume pour des performances élevées. Elles offrent notamment une durée de copie plus rapide pour les mêmes copies de volume, une utilisation réduite du processeur et de

la mémoire sur le client et une utilisation réduite de la bande passante E/S du réseau. Si les copies se trouvent sur plusieurs volumes, les gains de performances peuvent être négligeables par rapport aux copies basées sur l'hôte.

Pour les environnements SAN, ODX n'est disponible que lorsqu'il est pris en charge par l'hôte et le système de stockage. Les ordinateurs clients qui prennent en charge ODX et où ODX est activé automatiquement et de manière transparente utilisent le transfert de fichiers déchargés lors du déplacement ou de la copie des fichiers. ODX est utilisé que les fichiers par glisser-déposer soient via l'Explorateur Windows ou qu'il utilise des commandes de copie de fichier en ligne de commande ou qu'une application client lance des demandes de copie de fichiers.

Conditions requises pour l'utilisation d'ODX

Si vous prévoyez d'utiliser ODX pour la réduction des volumes de copies, vous devez connaître les considérations relatives à la prise en charge des volumes, les exigences système et les fonctionnalités logicielles requises.

Pour utiliser ODX, votre système doit disposer des éléments suivants :

- ONTAP

ODX est automatiquement activé dans les versions prises en charge de ONTAP.

- Volume source minimum de 2 Go

Pour des performances optimales, le volume source doit être supérieur à 260 Go.

- Prise en charge d'ODX sur le client Windows

ODX est pris en charge par Windows Server 2012 ou version ultérieure et dans Windows 8 ou version ultérieure. La matrice d'interopérabilité contient les dernières informations sur les clients Windows pris en charge.

["Matrice d'interopérabilité NetApp"](#)

- Prise en charge des applications de copie pour ODX

ODX doit être prise en charge par l'application qui effectue le transfert de données. Les opérations applicatives prenant en charge ODX sont les suivantes :

- Les opérations de gestion Hyper-V, telles que la création et la conversion de disques durs virtuels (VHD), la gestion des copies Snapshot et la copie de fichiers entre les machines virtuelles
- Opérations de l'Explorateur Windows
- Commandes de copie Windows PowerShell
- Commandes de copie de l'invite de commande Windows

La bibliothèque Microsoft TechNet contient plus d'informations sur les applications ODX prises en charge sur les serveurs et les clients Windows.

- Si vous utilisez des volumes compressés, la taille du groupe de compression doit être de 8 Ko.

La taille des groupes de compression 32 K n'est pas prise en charge.

ODX ne fonctionne pas avec les types de volume suivants :

- Volumes source d'une capacité inférieure à 2 Go
- Volumes en lecture seule
- "Volumes FlexCache"



ODX est pris en charge sur les volumes d'origine FlexCache.

- "Volumes provisionnés semi-lourds"

Configuration spéciale pour les fichiers système

Vous pouvez supprimer les fichiers ODX trouvés dans les qtrees. Vous ne devez pas supprimer ou modifier d'autres fichiers système d'ODX à moins d'en obtenir une.

Lors de l'utilisation de la fonctionnalité ODX, des fichiers système d'ODX existent dans tous les volumes du système. Ces fichiers permettent une représentation instantanée des données utilisées lors du transfert d'ODX. Les fichiers système suivants se trouvent au niveau racine de chaque volume qui contient des LUN ou des fichiers vers lesquels les données ont été déchargées :

- `.copy-offload` (un répertoire masqué)
- `.tokens` (fichier sous le masqué `.copy-offload` répertoire)

Vous pouvez utiliser le `copy-offload delete-tokens -path dir_path -node node_name` Commande permettant de supprimer un qtree contenant un fichier ODX.

Cas d'utilisation d'ODX

Vous devez tenir compte des cas d'utilisation d'ODX sur des SVM afin de pouvoir déterminer dans quelles circonstances ODX vous fournit des avantages en matière de performances.

Par défaut, les serveurs et clients Windows qui prennent en charge ODX utilisent la fonction d'allègement de la charge des copies pour copier des données sur des serveurs distants. Si le serveur ou le client Windows ne prend pas en charge ODX, ou si l'allègement de la charge des copies ODX échoue à tout moment, l'opération de copie ou de déplacement retourne aux lectures et écritures classiques pour la copie ou le déplacement.

Les cas d'utilisation suivants prennent en charge l'utilisation de copies et de déplacements d'ODX :

- Intra-volume

Les fichiers ou LUN source et de destination se trouvent dans le même volume.

- Inter-volume, même nœud, même SVM

Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur le même nœud. Les données sont détenues par le même SVM.

- Inter-volumes, nœuds différents, même SVM

Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par le même SVM.

- Inter-SVM, même nœud

Les fichiers source et de destination ou les LUN se trouvent sur des volumes différents situés sur le même

nœud. Les données sont détenues par différents SVM.

- Inter-SVM, nœuds différents

Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par différents SVM.

- Inter-cluster

Les LUN source et de destination se trouvent sur des volumes différents, sur différents nœuds, sur l'ensemble des clusters. Cette fonctionnalité est uniquement prise en charge pour SAN et ne fonctionne pas pour SMB.

Il existe d'autres cas d'utilisation spéciaux :

- Dans l'implémentation de ONTAP ODX, vous pouvez utiliser ODX pour copier des fichiers entre des partages SMB et des disques virtuels connectés FC ou iSCSI.

Vous pouvez utiliser Windows Explorer, l'interface de ligne de commande Windows ou PowerShell, Hyper-V ou d'autres applications prenant en charge ODX pour copier ou déplacer des fichiers de manière transparente à l'aide de l'allègement de la charge des copies ODX entre les partages SMB et les LUN connectés, à condition que les partages SMB et les LUN soient sur le même cluster.

- Hyper-V fournit des cas d'utilisation supplémentaires pour la décharge de copies ODX :
 - Vous pouvez utiliser le pass-through ODX qui décharge les copies et Hyper-V pour copier des données dans ou sur des fichiers de disque dur virtuel (VHD), ou pour copier des données entre les partages SMB mappés et les LUN iSCSI connectés au sein du même cluster.
- Ainsi, des copies des systèmes d'exploitation invités peuvent être transmis au stockage sous-jacent.
- Lors de la création de VHD de taille fixe, ODX permet d'initialiser le disque avec des zéros, à l'aide d'un jeton bien connu mis à zéro.
 - L'allègement de la charge des copies d'ODX est utilisé pour la migration du stockage de machines virtuelles si le stockage source et cible est situé sur le même cluster.



Pour tirer parti des cas d'utilisation liés au délestage des copies ODX par Hyper-V, le système d'exploitation invité doit prendre en charge ODX. Les disques du système d'exploitation invité doivent être des disques SCSI pris en charge par le stockage (SMB ou SAN) prenant en charge ODX. Les disques IDE du système d'exploitation invité ne prennent pas en charge le pass-through ODX.

Administration SAN

Provisionnement SAN

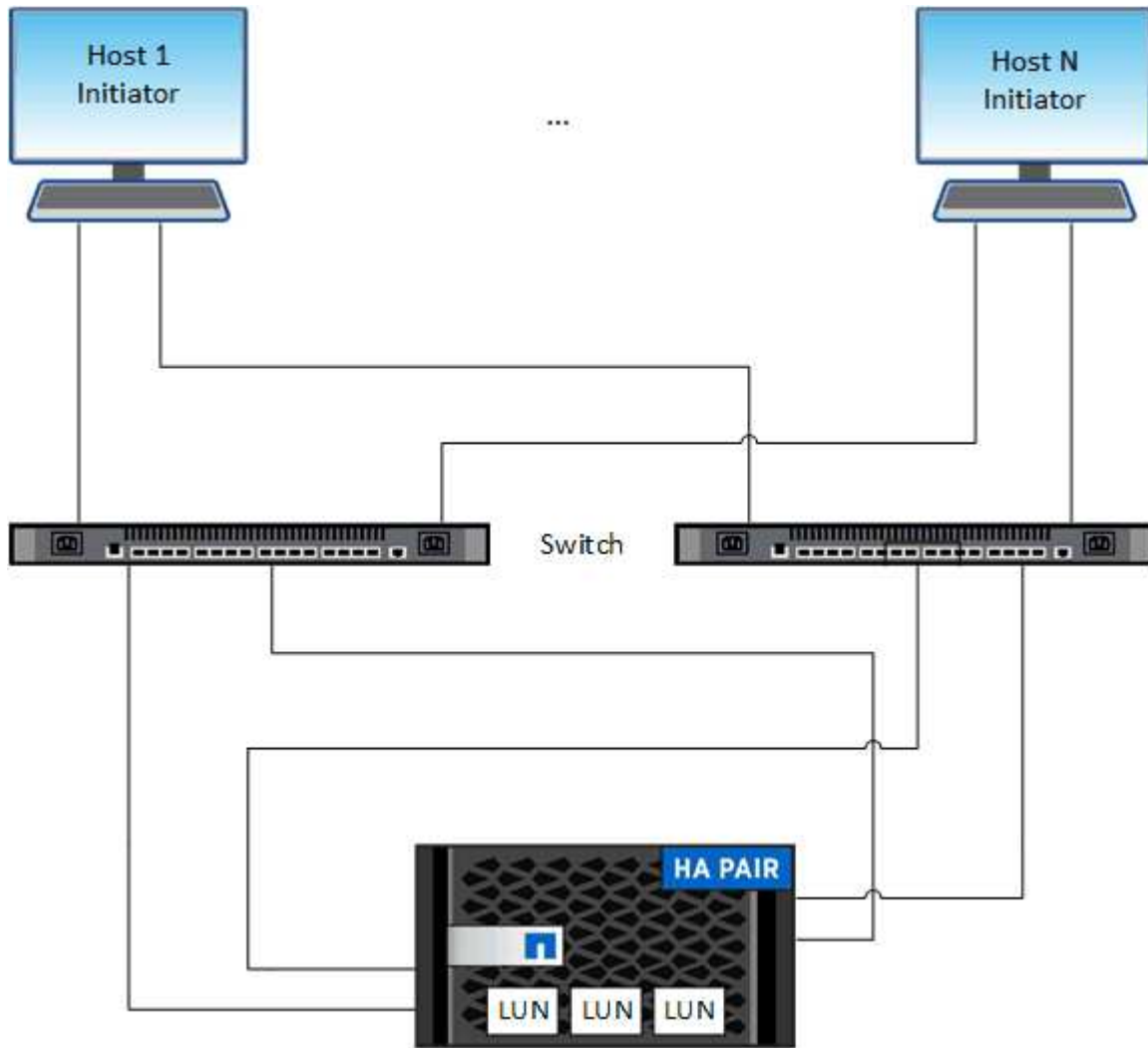
Présentation de la gestion SAN

Le contenu de cette section vous explique comment configurer et gérer les environnements SAN avec l'interface de ligne de commande ONTAP et System Manager dans ONTAP 9.7 et versions ultérieures.

Si vous utilisez System Manager classique (disponible uniquement dans ONTAP 9.7 et versions antérieures), reportez-vous aux rubriques suivantes :

- ["Protocole iSCSI"](#)
- ["Protocole FC/FCoE"](#)

Vous pouvez utiliser les protocoles iSCSI et FC pour fournir le stockage dans un environnement SAN.



Avec iSCSI et FC, les cibles de stockage sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de bloc standard. Vous créez des LUN, puis les mappez sur des groupes initiateurs. Les groupes initiateurs sont des tableaux des WWPS hôtes FC et des noms de nœuds hôtes iSCSI, et contrôlent les initiateurs auxquels les initiateurs ont accès.

Les cibles FC se connectent au réseau via des commutateurs FC et des adaptateurs côté hôte. Elles sont identifiées par des WWPN (World Wide Port Name). Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet standard (NIC), des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs hôtes principaux dédiés (HBA) et sont identifiées par des noms qualifiés iSCSI (IQN).

Configuration des commutateurs pour FCoE

Vous devez configurer les commutateurs pour FCoE avant que votre service FC ne

puisse s'exécuter sur l'infrastructure Ethernet existante.

Ce dont vous avez besoin

- Votre configuration SAN doit être prise en charge.

Pour plus d'informations sur les configurations prises en charge, reportez-vous au ["Matrice d'interopérabilité NetApp"](#).

- Un adaptateur cible unifié (UTA) doit être installé sur votre système de stockage.

Si vous utilisez un UTA2, il doit être défini sur `cna` mode.

- Un adaptateur réseau convergé (CNA) doit être installé sur votre hôte.

Étapes

1. Utilisez la documentation de votre commutateur pour configurer vos commutateurs pour FCoE.
2. Vérifiez que les paramètres DCB de chaque nœud du cluster ont été correctement configurés.

```
run -node node1 -command dcb show
```

Les paramètres DCB sont configurés sur le commutateur. Consultez la documentation du commutateur si les paramètres sont incorrects.

3. Vérifiez que la connexion FCoE fonctionne lorsque l'état en ligne du port cible FC est `true`.

```
fcg adapter show -fields node,adapter,status,state,speed,fabric-  
established,physical-protocol
```

Si l'état en ligne du port FC cible est `false`, consultez la documentation de votre commutateur.

Informations associées

- ["Matrice d'interopérabilité NetApp"](#)
- ["Rapport technique de NetApp 3800 : guide de déploiement de bout en bout de Fibre Channel over Ethernet \(FCoE\)"](#)
- ["Guides de configuration des logiciels Cisco MDS 9000 NX-OS et SAN-OS"](#)
- ["Produits Brocade"](#)

Configuration minimale requise

La configuration des LUN implique la création d'une LUN, la création d'un groupe initiateur et le mappage de celle-ci sur le groupe initiateur. Votre système doit respecter certaines conditions préalables avant de pouvoir configurer vos LUN.

- La matrice d'interopérabilité doit répertorier votre configuration SAN prise en charge.
- Votre environnement SAN doit être conforme aux limites de configuration d'hôtes et de contrôleurs SAN spécifiées dans la ["NetApp Hardware Universe"](#) Pour votre version du logiciel ONTAP.

- Une version prise en charge des utilitaires hôtes doit être installée.

La documentation Host Utilities fournit des informations supplémentaires.

- Vous devez disposer de LIF SAN sur le nœud propriétaire et sur le partenaire HA du nœud propriétaire.

Informations associées

- ["Matrice d'interopérabilité NetApp"](#)
- ["Configuration de l'hôte SAN ONTAP"](#)
- ["Rapport technique de NetApp 4017 : meilleures pratiques liées au SAN Fibre Channel"](#)

Que savoir avant de créer une LUN

Pourquoi la taille réelle des LUN varie légèrement

Concernant la taille de vos LUN, veuillez à tenir compte des points suivants.

- Lorsque vous créez une LUN, la taille réelle de celle-ci peut varier légèrement en fonction du type de système d'exploitation de la LUN. Le type de système d'exploitation de LUN ne peut pas être modifié après la création de la LUN.
- Si vous créez une LUN à sa taille maximale, notez que sa taille réelle peut être légèrement inférieure. ONTAP arrondit la limite par excès pour être légèrement inférieur.
- Les métadonnées de chaque LUN requièrent environ 64 Ko d'espace dans l'agrégat contenant. Lorsque vous créez une LUN, vous devez vous assurer que l'agrégat qui contient dispose d'un espace suffisant pour les métadonnées de la LUN. Si l'agrégat ne contient pas assez d'espace pour les métadonnées de la LUN, certains hôtes risquent de ne pas pouvoir accéder à la LUN.

Consignes d'attribution des ID de LUN

En général, l'ID de LUN par défaut commence par 0 et est attribué par incréments de 1 pour chaque LUN mappée supplémentaire. L'hôte associe l'ID de LUN à l'emplacement et au chemin d'accès de la LUN. La plage de numéros d'ID de LUN valides dépend de l'hôte. Pour plus d'informations, consultez la documentation fournie avec vos utilitaires hôtes.

Consignes de mappage des LUN sur les igroups

- Une LUN ne peut être mappée sur un groupe initiateur qu'une seule fois.
- Il est recommandé de mapper une LUN sur un seul initiateur spécifique via le groupe initiateur.
- Vous pouvez ajouter un seul initiateur à plusieurs groupes initiateurs, mais celui-ci ne peut être mappé qu'à une seule LUN.
- Vous ne pouvez pas utiliser le même ID de LUN pour deux LUN mappées sur le même groupe initiateur.
- Vous devez utiliser le même type de protocole pour les groupes initiateurs et les jeux de ports.


Vérifiez et ajoutez votre licence FC ou iSCSI de protocole

Avant de pouvoir activer l'accès aux blocs pour une machine virtuelle de stockage (SVM) avec FC ou iSCSI, vous devez disposer d'une licence. Les licences FC et iSCSI sont incluses dans ["ONTAP One"](#).

Exemple 6. Étapes

System Manager

Si vous n'avez pas ONTAP One, vérifiez et ajoutez votre licence FC ou iSCSI avec ONTAP System Manager (9.7 et versions ultérieures).

1. Dans System Manager, sélectionnez **Cluster > Paramètres > licences**
2. Si la licence n'est pas répertoriée, sélectionnez  et entrez la clé de licence.
3. Sélectionnez **Ajouter**.

CLI

Si vous n'avez pas ONTAP One, vérifiez et ajoutez votre licence FC ou iSCSI via l'interface de ligne de commande ONTAP.

1. Vérifiez que vous disposez d'une licence active pour FC ou iSCSI.

```
system license show
```

Package	Type	Description	Expiration
Base	site	Cluster Base License	-
NFS	site	NFS License	-
CIFS	site	CIFS License	-
iSCSI	site	iSCSI License	-
FCP	site	FCP License	-

2. Si vous ne disposez pas d'une licence active pour FC ou iSCSI, ajoutez votre code de licence.

```
license add -license-code <your_license_code>
```

Provisionnement du stockage SAN

Cette procédure crée de nouvelles LUN sur une machine virtuelle de stockage existante sur laquelle le protocole FC ou iSCSI est déjà configuré.

Si vous devez créer une nouvelle machine virtuelle de stockage et configurer le protocole FC ou iSCSI, reportez-vous à la section ["Configuration d'un SVM pour FC"](#) ou ["Configuration d'un SVM pour iSCSI"](#).

Si la licence FC n'est pas activée, les LIFs et les SVM semblent être en ligne, mais le statut opérationnel est arrêté.

Les LUN apparaissent sur votre hôte en tant que périphériques de disque.



L'accès ALUA (Asymmetric Logical Unit Access) est toujours activé au cours de la création de LUN. Vous ne pouvez pas modifier le paramètre ALUA.

Vous devez utiliser un zoning unique pour toutes les LIFs FC du SVM pour héberger les initiateurs.

Depuis ONTAP 9.8, lorsque vous provisionnez le stockage, la QoS est activée par défaut. Vous pouvez désactiver QoS ou choisir une règle de QoS personnalisée lors du processus de provisionnement ou ultérieurement.

Exemple 7. Étapes


System Manager

Créer des LUN pour fournir du stockage à un hôte SAN à l'aide du protocole FC ou iSCSI avec ONTAP System Manager (9.7 et versions ultérieures).

Pour effectuer cette tâche à l'aide de System Manager Classic (disponible avec les versions 9.7 et antérieures), reportez-vous à la section ["Configuration iSCSI pour Red Hat Enterprise Linux"](#)

Étapes

- 1. Installez le approprié ["Utilitaires d'hôte SAN"](#) sur votre hôte.
- 2. Dans System Manager, cliquez sur **stockage > LUN**, puis sur **Ajouter**.
- 3. Indiquez les informations requises pour la création de la LUN.
- 4. Vous pouvez cliquer sur **plus d'options** pour effectuer l'une des opérations suivantes, selon votre version de ONTAP.

Option	Disponible à partir de
<ul style="list-style-type: none">• Attribuez la politique de QoS aux LUN au lieu du volume parent<ul style="list-style-type: none">◦ Plus d'options > stockage et optimisation◦ Sélectionnez Performance Service Level.◦ Pour appliquer la stratégie QoS à des LUN individuelles au lieu du volume entier, sélectionnez appliquer ces seuils de performances à chaque LUN.<p>Par défaut, des limites de performances sont appliquées au niveau du volume.</p>	ONTAP 9.10.1
<ul style="list-style-type: none">• Créez un nouveau groupe initiateur à l'aide des groupes initiateurs existants<ul style="list-style-type: none">◦ Plus d'options > INFORMATIONS SUR L'HÔTE◦ Sélectionnez Nouveau groupe initiateur utilisant des groupes initiateurs existants.<div><p>Le type de système d'exploitation d'un groupe initiateur contenant d'autres groupes initiateurs ne peut pas être modifié après sa création.</p></div>	ONTAP 9.9.1
<ul style="list-style-type: none">• Ajoutez une description à votre groupe initiateur ou à votre initiateur hôte<p>La description sert d'alias pour le groupe initiateur ou l'initiateur hôte.</p><ul style="list-style-type: none">◦ Plus d'options > INFORMATIONS SUR L'HÔTE	ONTAP 9.9.1

- Créez votre LUN sur un volume existant

ONTAP 9.9.1

Par défaut une nouvelle LUN est créée dans un nouveau volume.

- **Plus d'options > Ajouter des LUN**
- Sélectionnez **groupes de LUN connexes**.

- Désactivez la QoS ou choisissez une règle de QoS personnalisée

ONTAP 9.8

- **Plus d'options > stockage et optimisation**
- Sélectionnez **Performance Service Level**.



Dans ONTAP 9.9.1 et versions ultérieures, si vous sélectionnez une stratégie de QoS personnalisée, vous pouvez également sélectionner le placement manuel sur un niveau local spécifié.

5. Pour FC, déssegmentation des commutateurs FC par WWPN. Utilisez une zone par initiateur et incluez tous les ports cibles dans chaque zone.

6. Découvrez les LUN sur votre hôte

Pour VMware vSphere, utilisez Virtual Storage Console (VSC) pour détecter et initialiser vos LUN.

7. Initialisez les LUN et, éventuellement, créez des systèmes de fichiers.

8. Vérifiez que l'hôte peut écrire et lire les données sur la LUN.

CLI

Créer des LUN afin de fournir le stockage d'un hôte SAN utilisant le protocole FC ou iSCSI avec l'interface de ligne de commande de ONTAP.

1. Vérifiez que vous disposez d'une licence pour FC ou iSCSI.

```
system license show
```

Package	Type	Description	Expiration
Base	site	Cluster Base License	-
NFS	site	NFS License	-
CIFS	site	CIFS License	-
iSCSI	site	iSCSI License	-
FCP	site	FCP License	-

2. Si vous ne disposez pas de licence pour FC ou iSCSI, utilisez le `license add` commande.

```
license add -license-code <your_license_code>
```

3. Activer votre service de protocole sur le SVM :

Pour iSCSI:

```
vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
```

Pour FC:

```
vserver fcp create -vserver <svm_name> -status-admin up
```

4. Créez deux LIF pour les SVM sur chaque nœud :

```
network interface create -vserver <svm_name> -lif <lif_name> -role  
data -data-protocol <iscsi|fc> -home-node <node_name> -home-port  
<port_name> -address <ip_address> -netmask <netmask>
```

NetApp prend en charge au moins une LIF iSCSI ou FC par nœud pour chaque SVM assurant le service des données. Cependant, deux LIF par nœud sont nécessaires pour assurer la redondance. Pour iSCSI, il est recommandé de configurer au moins deux LIF par nœud dans des réseaux Ethernet distincts.

5. Vérifiez que vos LIF ont été créées et que leur statut opérationnel est online:

```
network interface show -vserver <svm_name> <lif_name>
```

6. Création de vos LUN :

```
lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>  
-size <lun_size> -ostype linux -space-reserve <enabled|disabled>
```

Le nom de LUN ne doit pas dépasser 255 caractères et ne peut pas contenir d'espaces.



L'option NVFAIL est automatiquement activée lorsqu'une LUN est créée dans un volume.

7. Création de vos igroups :

```
igroup create -vserver <svm_name> -igroup <igroup_name> -protocol  
<fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
```

8. Mappage de vos LUN sur des igroups :

```
lun mapping create -vserver <svm_name> -volume <volume_name> -lun  
<lun_name> -igroup <igroup_name>
```

9. Vérifiez que vos LUN sont configurées correctement :

```
lun show -vserver <svm_name>
```

10. En option, ["Créez un port défini et associez-le à un groupe initiateur"](#).
11. Suivez les étapes de la documentation de votre hôte pour activer l'accès aux blocs sur vos hôtes spécifiques.
12. Utilisez les utilitaires hôtes pour terminer le mappage FC ou iSCSI et détecter vos LUN sur l'hôte.

Informations associées

- ["Présentation de L'administration SAN"](#)
- ["Configuration de l'hôte SAN ONTAP"](#)
- ["Afficher et gérer les groupes initiateurs SAN dans System Manager"](#)
- ["Rapport technique de NetApp 4017 : meilleures pratiques liées au SAN Fibre Channel"](#)

Provisionnement NVMe

Présentation de NVMe

Vous pouvez utiliser le protocole NVMe (non-volatile Memory Express) pour fournir du stockage dans un environnement SAN. Le protocole NVMe est optimisé pour les performances du stockage Solid state.

Pour NVMe, les cibles de stockage sont appelées espaces de noms. Un namespace NVMe est une quantité de stockage non volatile pouvant être formatée dans des blocs logiques et présentée à un hôte comme un périphérique de bloc standard. Vous créez des espaces de noms et des sous-systèmes, puis mappez les espaces de noms aux sous-systèmes, de la même manière que les LUN sont provisionnées et mappées aux igroups pour FC et iSCSI.

Les cibles NVMe sont connectées au réseau via une infrastructure FC standard en utilisant des switches FC ou une infrastructure TCP standard à l'aide de switches Ethernet et d'adaptateurs côté hôte.

La prise en charge de NVMe varie selon votre version d'ONTAP. Voir ["Prise en charge et limitations de NVMe"](#) pour plus d'informations.

Qu'est-ce que NVMe

Le protocole NVMe (Nonvolatile Memory Express) est un protocole de transport utilisé pour l'accès aux supports de stockage non volatiles.

NVMe over Fabrics (NVMeoF) est une extension définie par la spécification vers NVMe qui permet une communication basée sur NVMe avec des connexions autres que PCIe. Cette interface permet de connecter

des armoires de stockage externes à un serveur.

Conçue pour fournir un accès efficace aux dispositifs de stockage conçus avec une mémoire non volatile, de la technologie Flash aux technologies de mémoire persistante plus performantes. En tant que telle, elle ne présente pas les mêmes limites que les protocoles de stockage conçus pour les disques durs. Les périphériques Flash et Solid State Devices (SSD) sont un type de mémoire non volatile (NVM). NVM est un type de mémoire qui conserve son contenu pendant une coupure de courant. C'est une méthode qui vous permet d'accéder à cette mémoire.

La vitesse, la productivité, le débit et la capacité accrues sont autant d'avantages pour le transfert de données. Caractéristiques spécifiques :

- NVMe est conçu pour accueillir jusqu'à 64 000 files d'attente.

Chaque file d'attente peut à son tour comporter jusqu'à 64 000 commandes simultanées.

- La technologie NVMe est prise en charge par plusieurs fournisseurs matériels et logiciels
- NVMe est plus productif grâce aux technologies Flash, qui accélèrent les temps de réponse
- NVMe autorise plusieurs requêtes de données pour chaque « demande » envoyée vers le SSD.

NVMe apporte moins de temps à décoder une « recherche » et n'exige pas de verrouillage des threads dans un programme multithread.

- NVMe prend en charge des fonctionnalités qui empêchent les goulots d'étranglement au niveau du CPU et assure une évolutivité massive au fur et à mesure que les systèmes augmentent.

À propos des espaces de noms NVMe

Un namespace NVMe est une quantité de mémoire non volatile (NVM) pouvant être formatée dans des blocs logiques. Les espaces de noms sont utilisés lorsqu'un serveur virtuel de stockage est configuré avec le protocole NVMe et équivalent de LUN pour les protocoles FC et iSCSI.

Un ou plusieurs espaces de noms sont provisionnés et connectés à un hôte NVMe. Chaque espace de noms peut prendre en charge plusieurs tailles de blocs.

Le protocole NVMe donne accès aux espaces de noms via plusieurs contrôleurs. À l'aide des pilotes NVMe, pris en charge sur la plupart des systèmes d'exploitation, les espaces de noms des disques SSD apparaissent comme des périphériques de bloc standard sur lesquels les systèmes de fichiers et les applications peuvent être déployés sans aucune modification.

Un ID d'espace de noms (NSID) est un identifiant utilisé par un contrôleur pour fournir l'accès à un espace de noms. Lors de la définition du NSID pour un hôte ou un groupe d'hôtes, vous configurez également l'accessibilité à un volume par un hôte. Un bloc logique ne peut être mappé qu'à un seul groupe d'hôtes à la fois et un groupe d'hôtes donné ne possède pas de NSID en double.

À propos des sous-systèmes NVMe

Un sous-système NVMe comprend un ou plusieurs contrôleurs NVMe, des espaces de noms, des ports de sous-système NVM, un support de stockage NVM et une interface entre le contrôleur et le support de stockage NVM. Par défaut, lorsque vous créez un namespace NVMe, ce dernier n'est pas mappé sur un sous-système. Vous pouvez également choisir de mapper un sous-système nouveau ou existant.

Informations associées

- ["Provisionner le stockage NVMe"](#)

- ["Mappez un namespace NVMe à un sous-système"](#)
- ["Configuration des hôtes SAN et des clients cloud"](#)

Exigences des licences NVMe

Une licence est requise pour la prise en charge de NVMe à partir de ONTAP 9.5. Si NVMe est activé dans ONTAP 9.4, une période de grâce de 90 jours est accordée pour l'acquisition de la licence après la mise à niveau vers ONTAP 9.5.

Vous pouvez activer la licence à l'aide de la commande suivante :

```
system license add -license-code NVMe_license_key
```

Configuration, prise en charge et limitations de NVMe

À partir de ONTAP 9.4, le ["NVMe \(non-volatile Memory Express\)"](#) le protocole est disponible pour les environnements SAN. FC-NVMe utilise la même configuration physique et la même pratique de segmentation que les réseaux FC traditionnels. Toutefois, cette méthode permet une plus grande bande passante, une augmentation des IOPS et une latence réduite que le FC-SCSI.

Les limites et la prise en charge de NVMe varient en fonction de votre version d'ONTAP, de votre plateforme et de votre configuration. Pour plus de détails sur votre configuration spécifique, reportez-vous au ["Matrice d'interopérabilité NetApp"](#). Pour connaître les limites prises en charge, voir ["Hardware Universe"](#).



Le nombre maximum de nœuds par cluster est disponible dans Hardware Universe sous **mélange de plates-formes pris en charge**.

Configuration

- Vous pouvez configurer votre configuration NVMe à l'aide d'une structure unique ou multistucture.
- Vous devez configurer une LIF de gestion pour chaque SVM prenant en charge SAN.
- L'utilisation de structures de commutateurs FC hétérogènes n'est pas prise en charge, sauf dans le cas de commutateurs lame intégrés.

Des exceptions spécifiques sont répertoriées sur le ["Matrice d'interopérabilité NetApp"](#).

- Les tissus en cascade, à maillage partiel, à maillage complet, à la périphérie du cœur et au directeur sont tous des méthodes standard de connexion des commutateurs FC à un tissu, et toutes sont prises en charge.

Une structure peut comprendre un ou plusieurs commutateurs et les contrôleurs de stockage peuvent être connectés à plusieurs commutateurs.

Caractéristiques

Les fonctionnalités NVMe suivantes sont prises en charge selon votre version d'ONTAP.

Depuis ONTAP...	NVMe prend en charge
-----------------	----------------------

9.15.1	<ul style="list-style-type: none"> Configurations IP MetroCluster à quatre nœuds sur NVMe/TCP
9.14.1	<ul style="list-style-type: none"> Définition de la priorité de l'hôte au niveau du sous-système (QoS au niveau de l'hôte)
9.12.1	<ul style="list-style-type: none"> Configurations IP MetroCluster à quatre nœuds sur NVMe/FC Les configurations MetroCluster ne sont pas prises en charge pour les réseaux NVMe frontaux avant ONTAP 9.12.1. Les configurations MetroCluster ne sont pas prises en charge sur NVMe/TCP.
9.10.1	Redimensionnement d'un espace de noms
9.9.1	<ul style="list-style-type: none"> Coexistence d'espaces de noms et de LUN sur le même volume
9.8	<ul style="list-style-type: none"> Coexistence du protocole <p>Les protocoles SCSI, NAS et NVMe peuvent exister sur la même machine virtuelle de stockage (SVM).</p> <p>Avant ONTAP 9.8, NVMe peut être le seul protocole de la SVM.</p>
9.6	<ul style="list-style-type: none"> blocs de 512 octets et blocs de 4096 octets pour espaces de noms <p>4096 est la valeur par défaut. 512 ne doit être utilisé que si le système d'exploitation hôte ne prend pas en charge les blocs de 4096 octets.</p> <ul style="list-style-type: none"> Déplacement de volumes avec espaces de noms mappés
9.5	<ul style="list-style-type: none"> Basculement/rétablissement d'une paire haute disponibilité multivoie

Protocoles

Les protocoles NVMe suivants sont pris en charge :

Protocole	Depuis ONTAP...	Autorisé par...
TCP	9.10.1	Valeur par défaut
FC	9.4	Valeur par défaut

À partir de ONTAP 9.8, vous pouvez configurer les protocoles SCSI, NAS et NVMe sur la même machine virtuelle de stockage (SVM).

Dans ONTAP 9.7 et les versions antérieures, NVMe est le seul protocole du SVM.

Espaces de noms

Lorsque vous utilisez des espaces de noms NVMe, vous devez connaître les points suivants :

- Vous ne pouvez pas utiliser SnapRestore pour restaurer un espace de noms à partir d'une LUN, ni inversement.
- La garantie d'espace pour les espaces de noms est identique à la garantie d'espace du volume contenant.
- Vous ne pouvez pas créer d'espace de noms sur une transition de volume à partir d'Data ONTAP 7-mode.
- Les espaces de noms ne prennent pas en charge les éléments suivants :
 - Nouvelles appellations
 - Déplacement inter-volume
 - Copie inter-volume
 - Copie à la demande

Restrictions supplémentaires

Les configurations NVMe ne prennent pas en charge les fonctionnalités d'ONTAP suivantes :

- Synchrone
- Virtual Storage Console

Les éléments suivants s'appliquent uniquement aux nœuds exécutant ONTAP 9.4 :

- Les LIFs et namespaces NVMe doivent être hébergés sur le même nœud.
- Le service NVMe doit être créé avant la création du LIF NVMe.

Informations associées

["Bonnes pratiques pour le SAN moderne"](#)

Configuration d'une VM de stockage pour NVMe

Si vous souhaitez utiliser le protocole NVMe sur un nœud, vous devez configurer votre SVM spécifiquement pour NVMe.


Avant de commencer

Vos adaptateurs FC ou Ethernet doivent prendre en charge NVMe. Les adaptateurs pris en charge sont répertoriés dans le ["NetApp Hardware Universe"](#).

Exemple 8. Étapes

System Manager

Configurer une machine virtuelle de stockage pour NVMe avec ONTAP System Manager (9.7 et versions ultérieures).

Pour configurer NVMe sur une nouvelle machine virtuelle de stockage	Pour configurer NVMe sur une VM de stockage existante
<ol style="list-style-type: none">1. Dans System Manager, cliquez sur stockage > machines virtuelles de stockage, puis sur Ajouter.2. Entrez un nom pour la machine virtuelle de stockage.3. Sélectionnez NVMe pour le Protocole d'accès.4. Sélectionnez Activer NVMe/FC ou Activer NVMe/TCP et Enregistrer.	<ol style="list-style-type: none">1. Dans System Manager, cliquez sur stockage > machines virtuelles de stockage.2. Cliquez sur la VM de stockage que vous souhaitez configurer.3. Cliquez sur l'onglet Settings, puis cliquez sur  en regard du protocole NVMe.4. Sélectionnez Activer NVMe/FC ou Activer NVMe/TCP et Enregistrer.

CLI

Configurez une VM de stockage pour NVMe avec l'interface de ligne de commande de ONTAP.

1. Si vous ne souhaitez pas utiliser un SVM existant, créez un :

```
vserver create -vserver <SVM_name>
```

- a. Vérifier que le SVM est créé :

```
vserver show
```

2. Vérifiez que des adaptateurs compatibles NVMe ou TCP sont installés dans votre cluster :

Pour NVMe :

```
network fcp adapter show -data-protocols-supported fc-nvme
```

Pour TCP :

```
network port show
```

3. Si vous exécutez ONTAP 9.7 ou version antérieure, supprimez tous les protocoles du SVM :

```
vserver remove-protocols -vserver <SVM_name> -protocols  
iscsi, fcp, nfs, cifs, ndmp
```

Depuis la version ONTAP 9.8, il n'est pas nécessaire de supprimer d'autres protocoles lors de l'ajout de NVMe.

4. Ajoutez le protocole NVMe au SVM :

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. Si vous exécutez ONTAP 9.7 ou une version antérieure, vérifiez que NVMe est le seul protocole autorisé sur le SVM :

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

NVMe doit être le seul protocole affiché sous le `allowed protocols` colonne.

6. Créez le service NVMe :

```
vserver nvme create -vserver <SVM_name>
```

7. Vérifiez que le service NVMe a été créé :

```
vserver nvme show -vserver <SVM_name>
```

Le Administrative Status Du SVM doit être répertorié comme up.

8. Créez une LIF NVMe/FC :

- Pour ONTAP 9.9.1 ou version antérieure, FC :

```
network interface create -vserver <SVM_name> -lif <lif_name>  
-address <ip address> -netmask <netmask_value> -role data -data  
-protocol fc-nvme -home-node <home_node> -home-port <home_port>
```

- Pour ONTAP 9.10.1 ou version ultérieure, FC ou TCP :

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp | default-data-nvme-fc> -data-protocol
<fcp | fc-nvme | nvme-tcp> -home-node <home_node> -home-port
<home_port> -status-admin up -failover-policy disabled -firewall
-policy data -auto-revert false -failover-group <failover_group>
-is-dns-update-enabled false
```

9. Créer une LIF NVMe/FC sur le nœud partenaire HA :

- Pour ONTAP 9.9.1 ou version antérieure, FC :

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

- Pour ONTAP 9.10.1 ou version ultérieure, FC ou TCP :

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fcp | fc-nvme | nvme-tcp> -home-node <home_node>
-home-port <home_port> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false -failover-group
<failover_group> -is-dns-update-enabled false
```

10. Vérifiez que les LIF NVMe/FC ont été créées :

```
network interface show -vserver <SVM_name>
```

11. Création de volumes sur le même nœud que la LIF :

```
vol create -vserver <SVM_name> -volume <vol_name> -aggregate
<aggregate_name> -size <volume_size>
```

Si un message d'avertissement relatif à la stratégie d'efficacité automatique s'affiche, il peut être ignoré en toute sécurité.

Provisionner le stockage NVMe

Suivez ces étapes pour créer des espaces de noms et provisionner du stockage pour tout hôte NVMe pris en charge sur une machine virtuelle de stockage existante.

Depuis ONTAP 9.8, lorsque vous provisionnez le stockage, la QoS est activée par défaut. Vous pouvez désactiver QoS ou choisir une règle de QoS personnalisée lors du processus de provisionnement ou ultérieurement.

Avant de commencer

Votre VM de stockage doit être configurée pour NVME, et votre transport FC ou TCP doit déjà être configuré.

System Manager

En utilisant ONTAP System Manager (9.7 et versions ultérieures), créez des espaces de noms pour fournir un stockage à l'aide du protocole NVMe.

Étapes

1. Dans System Manager, cliquez sur **stockage > espaces de noms NVMe**, puis sur **Ajouter**.

Si vous devez créer un nouveau sous-système, cliquez sur **plus d'options**.

2. Si vous exécutez ONTAP 9.8 ou version ultérieure et que vous souhaitez désactiver la qualité de service ou choisir une stratégie de qualité de service personnalisée, cliquez sur **plus d'options**, puis, sous **stockage et optimisation**, sélectionnez **niveau de service de performances**.
3. Segmenter vos commutateurs FC par WWPN. Utilisez une zone par initiateur et incluez tous les ports cibles dans chaque zone.
4. Sur votre hôte, découvrez les nouveaux espaces de noms.
5. Initialiser l'espace de noms et le formater avec un système de fichiers.
6. Vérifiez que votre hôte peut écrire et lire les données sur le namespace.

CLI

En utilisant l'interface de ligne de commande d'ONTAP, créez des espaces de noms pour fournir le stockage à l'aide du protocole NVMe.

Cette procédure crée un namespace et un sous-système NVMe sur une VM de stockage existante déjà configurée pour le protocole NVMe, puis mappe l'espace de noms sur le sous-système pour permettre l'accès aux données de votre système hôte.

Si vous devez configurer la machine virtuelle de stockage pour NVMe, reportez-vous à la section ["Configuration d'un SVM pour NVMe"](#).

Étapes

1. Vérifier que le SVM est configuré pour NVMe :

```
vserver show -vserver <svm_name> -fields allowed-protocols
```

NVMe doit s'afficher sous le `allowed-protocols` colonne.

2. Créez le namespace NVMe :

```
vserver nvme namespace create -vserver <svm_name> -path <path> -size  
<size_of_namespace> -ostype <OS_type>
```

3. Créez le sous-système NVMe :

```
vserver nvme subsystem create -vserver <svm_name> -subsystem  
<name_of_subsystem> -ostype <OS_type>
```

Le nom du sous-système NVMe est sensible à la casse. Ils doivent comporter entre 1 et 96 caractères. Les caractères spéciaux sont autorisés.

4. Vérifiez que le sous-système a été créé :

```
vserver nvme subsystem show -vserver <svm_name>
```

Le nvme le sous-système doit s'afficher sous Subsystem colonne.

5. Obtenez le NQN de l'hôte.
6. Ajoutez le NQN hôte au sous-système :

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN>
```

7. Mapper l'espace de noms au sous-système :

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem  
<subsystem_name> -path <path>
```

Un espace de noms ne peut être mappé qu'à un seul sous-système.

8. Vérifiez que l'espace de noms est mappé sur le sous-système :

```
vserver nvme namespace show -vserver <svm_name> -instance
```

Le sous-système doit être répertorié comme Attached subsystem.

Mappez un namespace NVMe à un sous-système

Le mappage d'un namespace NVMe sur un sous-système permet l'accès aux données depuis votre hôte. Vous pouvez mapper un namespace NVMe à un sous-système lors du provisionnement du stockage ou le faire une fois celui-ci provisionné.

À partir de ONTAP 9.14.1, vous pouvez hiérarchiser l'allocation des ressources pour des hôtes spécifiques. Par défaut, lorsqu'un hôte est ajouté au sous-système NVMe, sa priorité est donnée. Vous pouvez utiliser l'interface de ligne de commandes ONTAP pour modifier manuellement la priorité par défaut, de normal à élevée. Les hôtes affectés à une priorité élevée reçoivent un nombre de files d'attente d'E/S et des profondeurs de files d'attente plus importants.



Si vous souhaitez donner une priorité élevée à un hôte ajouté à un sous-système dans ONTAP 9.13.1 ou une version antérieure, vous pouvez le faire [modifiez la priorité de l'hôte](#).

Avant de commencer

Votre espace de noms et votre sous-système doivent déjà être créés. Si vous devez créer un espace de noms et un sous-système, reportez-vous à la section "[Provisionner le stockage NVMe](#)".

Étapes

1. Obtenez le NQN de l'hôte.
2. Ajoutez le NQN hôte au sous-système :

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
```

Si vous souhaitez modifier la priorité par défaut de l'hôte de normal à élevé, utilisez le `-priority high` option. Cette option est disponible à partir de ONTAP 9.14.1.

3. Mapper l'espace de noms au sous-système :

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem  
<subsystem_name> -path <path>
```

Un espace de noms ne peut être mappé qu'à un seul sous-système.

4. Vérifiez que l'espace de noms est mappé sur le sous-système :

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

Le sous-système doit être répertorié comme `Attached subsystem`.

Gérer les LUN

Modifiez la « policy group » QoS de la LUN

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour attribuer ou supprimer des règles de QoS sur plusieurs LUN en même temps.



Si la politique de QoS est attribuée au niveau du volume, elle doit être modifiée au niveau du volume. Vous pouvez modifier la règle de qualité de services au niveau des LUN uniquement s'il a été initialement attribué au niveau des LUN.

Étapes

1. Dans System Manager, cliquez sur **stockage > LUN**.
2. Sélectionnez la ou les LUN à modifier.

Si vous modifiez plusieurs LUN à la fois, les LUN doivent appartenir au même SVM (Storage Virtual machine). Si vous sélectionnez des LUN qui n'appartiennent pas au même SVM, l'option de modification du QoS Policy Group n'est pas affichée.

3. Cliquez sur **plus** et sélectionnez **Modifier groupe de stratégies QoS**.

Convertir une LUN en espace de nom

Depuis ONTAP 9.11.1, vous pouvez utiliser l'interface de ligne de commandes de ONTAP pour convertir un LUN existant en espace de noms NVMe, sans déplacement des données.

Avant de commencer

- La LUN spécifiée ne doit pas disposer d'aucun mappage existant sur un groupe initiateur.
- La LUN ne doit pas se trouver dans un SVM configuré par MetroCluster ou dans une relation de synchronisation active SnapMirror.
- La LUN ne doit pas être un terminal de protocole ni être liée à un terminal de protocole.
- La LUN ne doit pas contenir de préfixe et/ou de flux de suffixe non nul.
- La LUN ne doit pas faire partie d'un snapshot ou du côté destination d'une relation SnapMirror en tant que LUN en lecture seule.

Étape

1. Convertir une LUN en namespace NVMe :

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```


Mettez une LUN hors ligne

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour mettre les LUN hors ligne. Avant ONTAP 9.10.1, vous devez utiliser l'interface de ligne de commandes de ONTAP pour mettre les LUN hors ligne.

System Manager

Étapes

1. Dans System Manager, cliquez sur **stockage> LUN**.
2. Mettre une ou plusieurs LUN hors ligne

Si vous voulez...	Faites cela...
Mettez une LUN hors ligne	En regard du nom de la LUN, cliquez sur  et sélectionnez mettre hors ligne .
Mettre plusieurs LUN hors ligne	<ol style="list-style-type: none">1. Sélectionnez les LUN que vous souhaitez mettre hors ligne.2. Cliquez sur plus et sélectionnez mettre hors ligne.

CLI

Vous ne pouvez mettre une LUN hors ligne qu'à la fois lorsque vous utilisez l'interface de ligne de commandes.

Étape

1. Mettre la LUN hors ligne :

```
lun offline <lun_name> -vserver <SVM_name>
```

Redimensionner une LUN

Vous pouvez augmenter ou réduire la taille d'une LUN.



Les LUN Solaris ne peuvent pas être redimensionnées.

Augmentez la taille d'une LUN

La taille à laquelle vous pouvez augmenter le nombre de LUN dépend de votre version de ONTAP.

Version ONTAP	Taille maximale de LUN
ONTAP 9.12.1P2 et versions ultérieures	128 To pour les plateformes AFF, FAS et ASA
ONTAP 9.8 et versions ultérieures	<ul style="list-style-type: none">• 128 To pour les plateformes de baies SAN 100 % Flash (ASA)• 16 To pour les plateformes non ASA
ONTAP 9.5, 9.6, 9.7	16 TO

ONTAP 9.4 ou version antérieure	<p>10 fois la taille de LUN d'origine, mais pas supérieure à 16 To, ce qui correspond à la taille de LUN maximale.</p> <p>Par exemple, si vous créez une LUN de 100 Go, vous ne pouvez la faire évoluer qu'à 1,000 Go.</p> <p>La taille maximale réelle de la LUN peut ne pas être exactement 16 To. ONTAP arrondit la limite par excès pour être légèrement inférieur.</p>
---------------------------------	---


Il n'est pas nécessaire de mettre la LUN hors ligne pour augmenter la taille. Toutefois, une fois la taille augmentée, vous devez relancer une nouvelle analyse du LUN sur l'hôte pour que l'hôte reconnaisse la modification de taille.

Voir la page [Command Reference du `lun resize`](#) Pour plus d'informations sur le redimensionnement d'une LUN.

Exemple 9. Étapes

System Manager

Augmentez la taille d'une LUN avec ONTAP System Manager (9.7 et versions ultérieures).

1. Dans System Manager, cliquez sur **stockage > LUN**.
2. Cliquez sur  et sélectionnez **Modifier**.
3. Sous **stockage et optimisation**, augmentez la taille du LUN et **Enregistrer**.

CLI

Augmentez la taille d'une LUN à l'aide de l'interface de ligne de commandes de ONTAP.

1. Augmenter la taille de la LUN :

```
lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
-size <lun_size>
```

2. Vérifiez que la taille de LUN augmente :

```
lun show -vserver <SVM_name>
```

Les opérations de ONTAP arrondissent la taille maximale réelle de la LUN. Celle-ci est donc légèrement inférieure à la valeur attendue. Par ailleurs, la taille de LUN réelle peut varier légèrement en fonction du type de système d'exploitation de la LUN. Pour obtenir la valeur redimensionnée exacte, exécutez les commandes suivantes en mode avancé :

```
set -unit B
```

```
lun show -fields max-resize-size -volume volume_name -lun lun_name
```

1. Relancez l'analyse de la LUN sur l'hôte.
2. Suivez la documentation de votre hôte pour que la taille de LUN créée soit visible par le système de fichiers hôte.

Réduisez la taille d'une LUN

Avant de réduire la taille d'une LUN, l'hôte doit migrer les blocs contenant les données de LUN vers le limite de la taille de LUN inférieure. Vous devez utiliser un outil tel que SnapCenter pour vous assurer que la LUN est correctement réduite sans tronquer les blocs contenant des données de LUN. Il est déconseillé de réduire manuellement la taille de la LUN.

Une fois que vous avez réduit la taille de la LUN, ONTAP informe automatiquement l'initiateur que sa taille a diminué. Toutefois, des étapes supplémentaires peuvent être nécessaires sur votre hôte pour reconnaître la nouvelle taille de LUN. Consultez la documentation de votre hôte pour obtenir des informations spécifiques sur la diminution de la taille de la structure de fichiers hôte.

Déplacer une LUN

Vous pouvez déplacer une LUN entre des volumes au sein d'un SVM, mais il n'est pas possible de déplacer une LUN entre ces SVM. Les LUN déplacées entre les volumes d'un SVM sont immédiatement déplacés et sans perte de connectivité.

Ce dont vous avez besoin

Si votre LUN utilise la fonction de mappage de LUN sélectif (SLM), vous devez "[Modifiez la liste des nœuds de création de rapports SLM](#)" Pour inclure le nœud de destination et son partenaire haute disponibilité avant de déplacer la LUN.

Description de la tâche

Les fonctionnalités d'efficacité du stockage, telles que la déduplication, la compression et la compaction, ne sont pas conservées pendant un déplacement de LUN. Elles doivent être de nouveau appliquées une fois le déplacement de LUN terminé.

La protection des données via les copies Snapshot s'effectue au niveau du volume. Par conséquent, lorsque vous déplacez une LUN, elle tombe sous le schéma de protection des données du volume de destination. Si aucune copie Snapshot n'est établie pour le volume de destination, les copies Snapshot de la LUN ne sont pas créées. Par ailleurs, toutes les copies Snapshot de la LUN restent dans le volume d'origine jusqu'à ce que ces copies soient supprimées.

Vous ne pouvez pas déplacer une LUN vers les volumes suivants :

- Volume de destination SnapMirror
- Root volume du SVM

Vous ne pouvez pas déplacer les types de LUN suivants :

- LUN créée à partir d'un fichier
- LUN en état NVFail
- LUN faisant partie d'une relation de partage de charge
- LUN de classe terminal-protocole



Pour les LUN Solaris de type os qui sont de 1 To ou plus, l'hôte peut connaître un délai d'expiration lors du déplacement de LUN. Pour ce type de LUN, vous devez démonter la LUN avant d'initier la migration.


Exemple 10. Étapes

System Manager

Déplacez une LUN avec ONTAP System Manager (9.7 et versions ultérieures).

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour créer un volume lorsque vous déplacez un seul LUN. Dans ONTAP 9.8 et 9.9.1, le volume vers lequel vous déplacez le LUN doit exister avant de lancer le déplacement de LUN.

Étapes

1. Dans System Manager, cliquez sur **stockage> LUN**.
2. Cliquez avec le bouton droit de la souris sur la LUN à déplacer, puis cliquez sur  et sélectionnez **déplacer LUN**.

Dans ONTAP 9.10.1, sélectionnez pour déplacer le LUN vers **un volume existant** ou vers **Nouveau volume**.

Si vous choisissez de créer un nouveau volume, indiquez les spécifications du volume.

3. Cliquez sur **déplacer**.

CLI

Déplacez une LUN avec l'interface de ligne de commandes de ONTAP.

1. Déplacer la LUN :

```
lun move start
```

Pendant une très brève période, la LUN est visible à la fois sur le volume d'origine et sur le volume de destination. Ceci est prévu et résolu à la fin de la transition.

2. Suivre l'état du déplacement et vérifier que l'opération a bien été effectuée :

```
lun move show
```

Informations associées

- ["Mappage de LUN sélectif"](#)

Supprimer les LUN

Vous pouvez supprimer une LUN d'un serveur virtuel de stockage (SVM) si vous n'avez plus besoin de la LUN.

Ce dont vous avez besoin

Pour que vous puissiez le supprimer, vous devez annuler le mappage de la LUN sur son groupe initiateur.

Étapes

1. Vérifiez que l'application ou l'hôte n'utilise pas la LUN.
2. Annulez le mappage de la LUN du groupe initiateur :

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun  
<LUN_name> -igroup <igroup_name>
```

3. Supprimer la LUN :

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. Vérifiez que vous avez supprimé la LUN :

```
lun show -vserver <SVM_name>
```

Vserver	Path	State	Mapped	Type	Size
vs5	/vol/vol16/lun8	online	mapped	windows	10.00GB

Que devez-vous savoir avant de copier des LUN

Avant de copier une LUN, vous devez connaître certaines informations.

Les administrateurs de cluster peuvent copier une LUN sur des serveurs virtuels de stockage (SVM) au sein du cluster à l'aide de `lun copy` commande. Les administrateurs de cluster doivent établir la relation de peering de la machine virtuelle de stockage (SVM) à l'aide de `vserver peer create` Commande avant l'exécution d'une opération de copie de LUN inter-SVM. Il doit y avoir suffisamment d'espace dans le volume source pour un clone SIS.

Les LUN des copies Snapshot peuvent être utilisées comme LUN source pour le `lun copy` commande. Lorsque vous copiez une LUN en utilisant le `lun copy` La copie LUN est immédiatement disponible pour l'accès en lecture et en écriture. La LUN source reste inchangée par la création d'une copie LUN. La LUN source et la copie de LUN existent tous deux en tant que LUN uniques avec différents numéros de série de LUN. Les modifications apportées à la LUN source ne sont pas reflétées dans la copie de LUN, et les modifications apportées à cette copie ne sont pas prises en compte dans la LUN source. Le mappage de LUN de la LUN source n'est pas copié sur la nouvelle LUN ; la copie de LUN doit être mappée.

La protection des données via les copies Snapshot s'effectue au niveau du volume. Par conséquent, si vous copiez une LUN vers un volume différent du volume de la LUN source, celle-ci se trouve sous le schéma de protection des données du volume de destination. Si aucune copie Snapshot n'est établie pour le volume de destination, ces copies ne sont pas créées pour la copie de LUN.

La copie des LUN s'effectue sans interruption.

Vous ne pouvez pas copier les types de LUN suivants :

- LUN créée à partir d'un fichier
- LUN en état NVFAIL
- LUN faisant partie d'une relation de partage de charge
- LUN de classe terminal-protocole

Examen de l'espace configuré et utilisé d'une LUN

En sachant l'espace configuré et l'espace réel utilisé pour vos LUN, vous pouvez déterminer la quantité d'espace que vous pouvez récupérer lors de la récupération de l'espace, la quantité d'espace réservé contenant les données, et la taille totale configurée par rapport à la taille réelle utilisée pour une LUN.

Étape

1. Afficher l'espace configuré et l'espace réel utilisé par une LUN :

```
lun show
```

L'exemple suivant montre l'espace configuré par rapport à l'espace réel utilisé par les LUN dans la machine virtuelle de stockage vs3 (SVM) :

```
lun show -vserver vs3 -fields path, size, size-used, space-reserve
```

vserver	path	size	space-reserve	size-used
vs3	/vol/vol0/lun1	50.01GB	disabled	25.00GB
vs3	/vol/vol0/lun1_backup	50.01GB	disabled	32.15GB
vs3	/vol/vol0/lun2	75.00GB	disabled	0B
vs3	/vol/volspace/lun0	5.00GB	enabled	4.50GB

4 entries were displayed.

Activez l'allocation d'espace pour SAN

Activez l'allocation d'espace pour permettre à vos hôtes et systèmes de stockage de coopérer sur la gestion de l'espace LUN.

Depuis la version ONTAP 9.15.1, l'allocation d'espace est activée par défaut pour les nouvelles LUN créées. L'allocation d'espace avait été désactivée par défaut dans les versions précédentes de ONTAP (9.14.1 et antérieures).

L'activation du `space-allocation` paramètre offre les avantages suivants :

- **ONTAP peut communiquer à un hôte qu'aucun espace libre n'est disponible pour le service d'une écriture:** Cette communication est un moyen plus gracieux pour les hôtes de gérer des situations hors de l'espace. La LUN reste en ligne, mais ne peut pas traiter d'E/S d'écriture tant que l'espace n'est pas

disponible. Les E/S de lecture peuvent toujours être effectuées. L'effet exact sur un système d'exploitation hôte dépend de la configuration de l'hôte. Dans certains cas, le système d'exploitation tente d'écrire E/S jusqu'à ce qu'il réussisse. Dans d'autres cas, le système de fichiers pourrait être mis hors ligne.



Si le `space-allocation` Le paramètre n'est pas activé, une LUN passe à l'état `space-error` Lorsqu'il atteint un seuil d'espace faible et que toutes les E/S échouent. La LUN doit être redéfinie sur `online` après la résolution du problème d'espace. Il peut également être nécessaire de renumériser les périphériques LUN sur l'hôte pour restaurer les chemins et les périphériques à un état opérationnel.

- **Un hôte peut exécuter SCSI UNMAP (parfois appelé TRIM) Opérations:** Ces opérations permettent à un hôte d'identifier des blocs de données sur une LUN qui ne sont plus nécessaires parce qu'ils ne contiennent plus de données valides. L'identification se produit normalement après la suppression du fichier. Le système de stockage peut ensuite désallouer ces blocs de données afin que l'espace puisse être consommé ailleurs. Cette désallocation améliore considérablement l'efficacité globale du stockage, en particulier avec les systèmes de fichiers dont le volume de données est élevé.

Avant de commencer

L'activation de l'allocation d'espace nécessite une configuration hôte capable de gérer correctement les erreurs d'allocation d'espace lorsqu'une écriture ne peut pas être terminée. Valorisation `SCSI UNMAP` Nécessite une configuration pouvant utiliser le provisionnement de blocs logiques tel que défini dans la norme SCSI SBC-3.

Les hôtes suivants prennent actuellement en charge le provisionnement fin SCSI lorsque vous activez l'allocation d'espace :

- Citrix XenServer 6.5 et versions ultérieures
- ESXi 5.0 et versions ultérieures
- Noyau Oracle Linux 6.2 UEK et versions ultérieures
- Red Hat Enterprise Linux 6.2 et versions ultérieures
- SUSE Linux Enterprise Server 11 et versions ultérieures
- Solaris 11.1 et versions ultérieures
- Répertoires de base

L'allocation d'espace n'est pas prise en charge sur les hôtes NVMe.

Description de la tâche

Lorsque vous mettez à niveau votre cluster vers ONTAP 9.15.1, le paramètre d'allocation d'espace pour toutes les LUN créées avant la mise à niveau logicielle reste le même après la mise à niveau, quel que soit le type d'hôte. Par exemple, si une LUN a été créée dans ONTAP 9.13.1 pour un hôte VMware dont l'allocation d'espace est désactivée, l'allocation d'espace sur cette LUN reste désactivée après la mise à niveau vers ONTAP 9.15.1.

Étapes

1. Activer l'allocation d'espace :

```
lun modify -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-space-allocation enabled
```

2. Vérifiez que l'allocation d'espace est activée :

```
lun show -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-fields space-allocation
```

3. Vérifiez que l'allocation d'espace est activée sur le système d'exploitation hôte.



Certaines configurations hôtes, notamment ESX, peuvent reconnaître automatiquement la modification des paramètres et ne nécessitent pas l'intervention de l'utilisateur. D'autres configurations peuvent nécessiter une nouvelle analyse du périphérique. Certains systèmes de fichiers et gestionnaires de volumes peuvent nécessiter des paramètres spécifiques supplémentaires pour activer la récupération d'espace à l'aide de SCSI UNMAP. Le montage des systèmes de fichiers ou le redémarrage complet du système d'exploitation peuvent être nécessaires. Consultez la documentation de votre système d'exploitation spécifique pour obtenir de l'aide.

Contrôlez et surveillez les performances d'E/S des LUN grâce à la QoS de stockage

Vous pouvez contrôler les performances des entrées/sorties (E/S) des LUN en affectant des LUN aux groupes de règles de QoS de stockage. Vous pouvez contrôler les performances d'E/S pour permettre aux workloads d'atteindre des objectifs de performance spécifiques ou de limiter les workloads qui ont un impact négatif sur d'autres workloads.

Description de la tâche

Les groupes de règles appliquent une limite de débit maximal (par exemple, 100 Mo/s). Vous pouvez créer un groupe de règles sans spécifier un débit maximal, ce qui vous permet de contrôler les performances avant de contrôler le workload.

Vous pouvez également attribuer des SVM (Storage Virtual machines) avec des volumes FlexVol et des LUN à des groupes de règles.

Prenez en compte les exigences suivantes concernant l'assignation d'une LUN à un « policy group » :

- La LUN doit être contenue par le SVM auquel appartient le « policy group ».

Vous spécifiez la SVM lors de la création de la « policy group ».

- Si vous attribuez une LUN à une « policy group » alors vous ne pouvez pas attribuer le volume ou SVM contenant la LUN à une « policy group ».

Pour plus d'informations sur l'utilisation de la QoS du stockage, consultez le ["Référence d'administration du système"](#).

Étapes

1. Utilisez le `qos policy-group create` commande pour créer une « policy group ».
2. Utilisez le `lun create` commande ou le `lun modify` commande avec `-qos-policy-group` Paramètre permettant d'affecter une LUN à une « policy group ».
3. Utilisez le `qos statistics` commandes pour afficher les données de performances.

4. Si nécessaire, utiliser l' `qos policy-group modify` commande pour ajuster la limite de débit maximale du groupe de règles.

Outils disponibles pour surveiller efficacement vos LUN

Des outils sont disponibles pour vous aider à contrôler efficacement vos LUN et à éviter un manque d'espace.

- Active IQ Unified Manager est un outil gratuit qui vous permet de gérer tout le stockage sur tous les clusters de votre environnement.
- System Manager est une interface utilisateur graphique intégrée à ONTAP qui vous permet de gérer manuellement les besoins en stockage au niveau du cluster.
- OnCommand Insight offre une vue unique de l'infrastructure de stockage et vous permet de configurer la surveillance automatique, les alertes et le reporting lorsque vos LUN, volumes et agrégats manquent d'espace de stockage.

Capacités et restrictions des LUN migrées

Dans un environnement SAN, une interruption de service est nécessaire lors de la transition d'un volume 7-mode vers ONTAP. Vous devez arrêter vos hôtes pour terminer la transition. Une fois la transition terminée, vous devez mettre à jour vos configurations hôte pour pouvoir commencer à transférer des données dans ONTAP

Vous devez planifier une fenêtre de maintenance au cours de laquelle vous pouvez arrêter vos hôtes et terminer la transition.

Certaines fonctionnalités et restrictions ont un impact sur la gestion des LUN depuis Data ONTAP 7-mode vers ONTAP.

Vous pouvez faire ce qui suit avec les LUN migrées :

- Affichez la LUN à l'aide de `lun show` commande
- Affichez l'inventaire des LUN migrées depuis le volume 7-mode à l'aide de la `transition 7-mode show` commande
- Restaurer un volume à partir d'une copie Snapshot 7-mode

La restauration du volume effectue toutes les transitions de toutes les LUN capturées dans la copie Snapshot

- Restaurez une LUN unique à partir d'une copie Snapshot 7-mode à l'aide de `snapshot restore-file` commande
- Créer un clone d'une LUN dans une copie Snapshot 7-mode
- Restauration d'une plage de blocs à partir d'une LUN capturée dans une copie Snapshot 7-mode
- Créer un FlexClone du volume à l'aide d'une copie Snapshot 7-mode

Vous ne pouvez pas faire ce qui suit avec les LUN migrées :

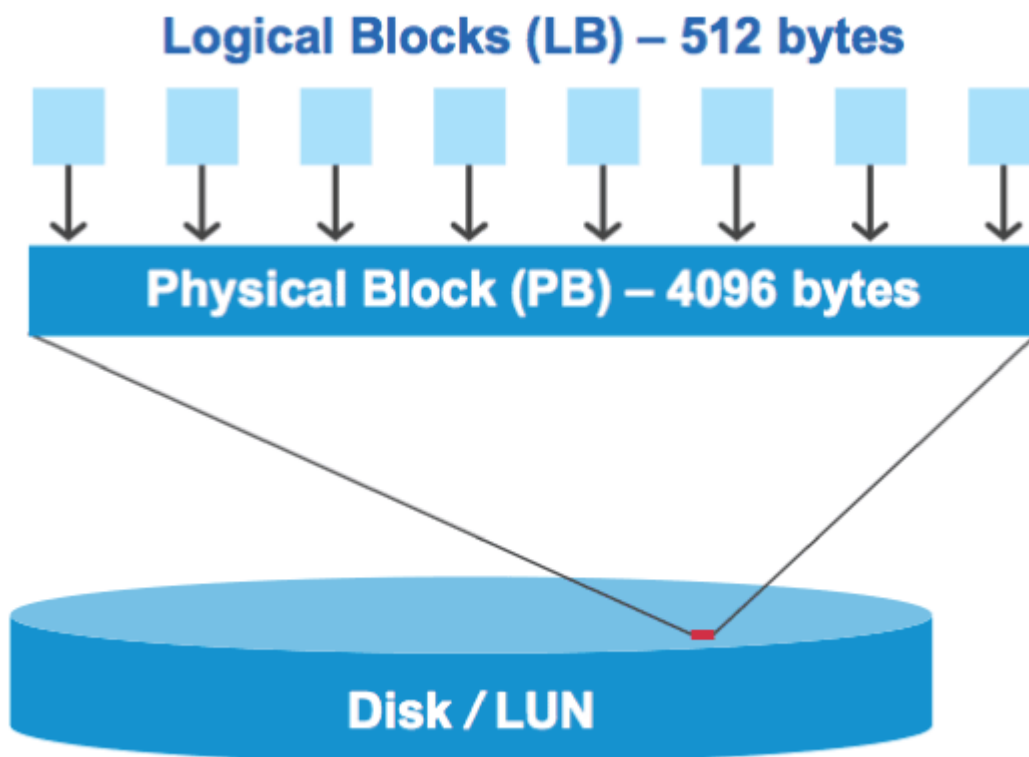
- Accéder aux clones LUN sauvegardés dans le volume par des copies Snapshot

Informations associées

Aperçu des défauts d'alignement des E/S sur les LUN correctement alignées

ONTAP peut signaler des problèmes d'alignement des E/S sur les LUN correctement alignées. En général, ces avertissements relatifs au mauvais alignement peuvent être ignorés tant que vous êtes sûr que votre LUN est correctement provisionnée et que votre table de partitionnement est correcte.

Les LUN et les disques durs fournissent tous deux un stockage sous forme de blocs. Étant donné que la taille de bloc des disques de l'hôte est de 512 octets, les LUN présentent des blocs de cette taille à l'hôte tout en utilisant des blocs de 4 Ko plus volumineux pour stocker les données. Le bloc de données de 512 octets utilisé par l'hôte est appelé bloc logique. Le bloc de données de 4 Ko utilisé par le LUN pour stocker les données est appelé bloc physique. Cela signifie qu'il y a huit blocs logiques de 512 octets dans chaque bloc physique de 4 Ko.



Le système d'exploitation hôte peut lancer une opération de lecture ou d'écriture d'E/S sur n'importe quel bloc logique. Les opérations d'E/S n'ont pas été considérées comme alignées lorsqu'elles commencent au premier bloc logique du bloc physique. Si une opération d'E/S commence au démarrage d'un bloc logique qui n'est pas toujours le début d'un bloc physique, les E/S sont considérées comme mal alignées. ONTAP détecte automatiquement l'alignement incorrect et le signale sur le LUN. Toutefois, l'alignement incorrect des E/S n'entraîne pas nécessairement l'alignement incorrect de la LUN. Il est possible de signaler des E/S mal alignées sur les LUN correctement alignées.

Si vous avez besoin d'une enquête plus approfondie, consultez l'article de la base de connaissances ["Comment identifier les E/S non alignées sur les LUN ?"](#)

Pour plus d'informations sur les outils de correction des problèmes d'alignement, reportez-vous à la documentation suivante : +

- ["Utilitaires d'hôtes unifiés Windows 7.1"](#)
- ["Provisionnez la documentation sur le stockage SAN"](#)

Assurez l'alignement des E/S à l'aide des types de systèmes d'exploitation LUN

Pour ONTAP 9.7 ou version antérieure, vous devez utiliser le LUN ONTAP recommandé `ostype` Valeur qui correspond le mieux à votre système d'exploitation pour aligner les E/S avec le schéma de partitionnement du système d'exploitation.

Le schéma de partition utilisé par le système d'exploitation hôte constitue un facteur important de désalignement des E/S. Une LUN ONTAP `ostype` les valeurs utilisent un décalage spécial appelé « préfixe » pour permettre l'alignement du schéma de partitionnement par défaut utilisé par le système d'exploitation hôte.



Dans certains cas, une table de partitionnement personnalisée peut être nécessaire pour atteindre l'alignement E/S. Cependant, pour `ostype` valeurs dont la valeur « préfixe » est supérieure à 0, Une partition personnalisée peut créer des E/S mal alignées

Pour plus d'informations sur les LUN provisionnées dans ONTAP 9.7 ou une version antérieure, consultez l'article de la base de connaissances ["Comment identifier les E/S non alignées sur les LUN"](#).



Par défaut, les nouvelles LUN provisionnées dans ONTAP 9.8 ou version ultérieure ont un préfixe et un suffixe de taille zéro pour tous les types de LUN OS. Par défaut, les E/S doivent être alignées sur le système d'exploitation hôte pris en charge.

Considérations spéciales d'alignement des E/S pour Linux

Les distributions Linux offrent de nombreuses façons d'utiliser un LUN, notamment en tant que périphériques bruts pour bases de données, divers gestionnaires de volumes et systèmes de fichiers. Il n'est pas nécessaire de créer des partitions sur un LUN lorsqu'il est utilisé en tant que périphérique brut ou en tant que volume physique dans un volume logique.

Pour RHEL 5 et versions antérieures et SLES 10 et versions antérieures, si le LUN doit être utilisé sans gestionnaire de volumes, vous devez partitionner le LUN pour avoir une partition qui commence à un décalage aligné, ce qui est un secteur qui est un multiple de huit blocs logiques.

Considérations spéciales relatives à l'alignement des E/S pour les LUN Solaris

Vous devez tenir compte de divers facteurs pour déterminer si vous devez utiliser le `solaris` `otapez` ou le `solaris_efi` `ostype`.

Voir la ["Solaris Host Utilities - Guide d'installation et d'administration"](#) pour des informations détaillées.

Les LUN de démarrage ESX indiquent un mauvais alignement

Les LUN utilisées comme LUN de démarrage ESX sont généralement signalées par ONTAP comme étant mal alignées. ESX crée plusieurs partitions sur la LUN de démarrage, ce qui complique particulièrement l'alignement. Les LUN de démarrage ESX mal alignées ne sont généralement pas problématiques de performances, car la quantité totale d'E/S mal alignées est faible. Supposant que la LUN ait été correctement provisionnée avec VMware `ostype`, aucune action n'est nécessaire.

Informations associées

["Alignement des partitions/disques du système de fichiers des machines virtuelles invité pour VMware vSphere, les autres environnements virtuels et les systèmes de stockage NetApp"](#)

Méthodes pour résoudre les problèmes lorsque les LUN sont mises hors ligne

Lorsqu'aucun espace n'est disponible pour les écritures, les LUN sont mises hors ligne pour préserver l'intégrité des données. Les LUN peuvent manquer d'espace et les mettre hors ligne pour diverses raisons, et il existe plusieurs façons de résoudre le problème.

Si...	Vous pouvez...
L'agrégat est plein	<ul style="list-style-type: none">• Ajouter des disques.• Utilisez le <code>volume modify</code> commande pour réduire un volume qui dispose d'un espace disponible.• Si vous disposez de volumes Space-Guarantee qui disposent d'espace disponible, définissez la garantie d'espace de volume sur <code>none</code> avec le <code>volume modify</code> commande.
Le volume est plein, mais l'agrégat contenant est disponible	<ul style="list-style-type: none">• Pour les volumes garantis par espace, utilisez <code>volume modify</code> commande pour augmenter la taille du volume.• Pour les volumes à provisionnement fin, utilisez le <code>volume modify</code> commande pour augmenter la taille maximale du volume. <p>Si la croissance automatique de volume n'est pas activée, utiliser <code>volume modify -autogrow -mode</code> pour l'activer.</p> <ul style="list-style-type: none">• Supprimez manuellement les copies Snapshot avec le <code>volume snapshot delete</code> ou utilisez la commande <code>volume snapshot autodelete modify</code> Commande permettant de supprimer automatiquement les copies Snapshot.

Informations associées

["Gestion des disques et des niveaux locaux \(agrégat\)"](#)

["Gestion du stockage logique"](#)

Dépanner les LUN iSCSI non visibles sur l'hôte

Les LUN iSCSI apparaissent en tant que disques locaux vers l'hôte. Si les LUN du système de stockage ne sont pas disponibles en tant que disques sur l'hôte, vérifiez les paramètres de configuration.

Paramètre de configuration	Que faire
Câblage	Vérifiez que les câbles entre l'hôte et le système de stockage sont correctement connectés.
Connectivité réseau	<p>Vérifiez que la connectivité TCP/IP est présente entre l'hôte et le système de stockage.</p> <ul style="list-style-type: none"> À partir de la ligne de commande du système de stockage, envoyez une requête ping aux interfaces hôtes utilisées pour iSCSI : <pre>ping -node node_name -destination host_ip_address_for_iSCSI</pre> À partir de la ligne de commande de l'hôte, envoyez une requête ping aux interfaces du système de stockage utilisées pour iSCSI : <pre>ping -node node_name -destination host_ip_address_for_iSCSI</pre>
Configuration minimale requise	Vérifiez que les composants de votre configuration sont qualifiés. Vérifiez également que vous disposez du niveau de service pack du système d'exploitation hôte, de la version de l'initiateur, de la version de ONTAP et des autres exigences système appropriées. La matrice d'interopérabilité présente les conditions système les plus récentes.
Trames Jumbo	Si vous utilisez des trames Jumbo dans votre configuration, vérifiez que ces trames jumbo sont activées sur tous les périphériques du chemin réseau : la carte réseau Ethernet hôte, le système de stockage et tous les commutateurs.
État du service iSCSI	Vérifiez que le service iSCSI est sous licence et démarré sur le système de stockage.
Connexion à l'initiateur	Vérifiez que l'initiateur est connecté au système de stockage. Si le <code>iscsi initiator show</code> le résultat de la commande affiche qu'aucun initiateur n'est connecté, vérifiez la configuration de l'initiateur sur l'hôte. Vérifiez également que le système de stockage est configuré comme cible de l'initiateur.
Noms des nœuds iSCSI (IQN)	Vérifiez que vous utilisez les noms de nœud d'initiateur corrects dans la configuration de votre groupe initiateur. Sur l'hôte, vous pouvez utiliser les outils et les commandes de l'initiateur pour afficher le nom du nœud initiateur. Les noms de nœud initiateur configurés dans le groupe initiateur et sur l'hôte doivent correspondre.

Paramètre de configuration	Que faire
Mappages de LUN	<p>Vérifiez que les LUN sont mappées sur un groupe initiateur. Sur la console du système de stockage, vous pouvez utiliser l'une des commandes suivantes :</p> <ul style="list-style-type: none"> • <code>lun mapping show</code> Affiche toutes les LUN et les groupes initiateurs sur lesquels ils sont mappés. • <code>lun mapping show -igroup</code> Affiche les LUN mappées sur un groupe initiateur spécifique.
Activation des LIF iSCSI	Vérifiez que les interfaces logiques iSCSI sont activées.

Informations associées

["Matrice d'interopérabilité NetApp"](#)

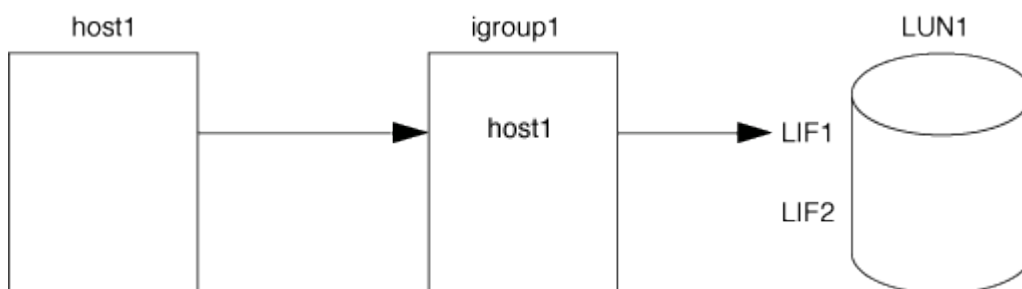
Gestion des igroups et des ensembles de ports

Moyens de limiter l'accès aux LUN avec des ensembles de ports et des igroups

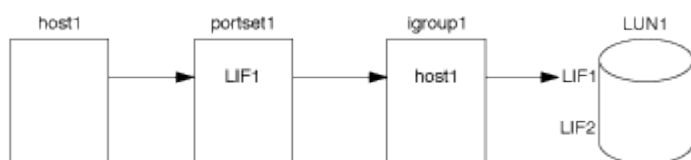
En plus d'utiliser le mappage de LUN sélectif (SLM), vous pouvez limiter l'accès à vos LUN via des igroups et des ensembles de ports.

Les ensembles de ports peuvent être utilisés avec SLM pour restreindre davantage l'accès de certaines cibles à certains initiateurs. Lors de l'utilisation de SLM avec des ensembles de ports, les LUN sont accessibles sur l'ensemble des LIF du portset sur le nœud propriétaire de la LUN et sur le partenaire HA de ce nœud.

Dans l'exemple suivant, initiator1 n'a pas de jeu de ports. Sans ensemble de ports, initiator1 peut accéder à LUN1 via LIF1 et LIF2.



Vous pouvez limiter l'accès à LUN1 en utilisant un ensemble de ports. Dans l'exemple suivant, initiator1 ne peut accéder à LUN1 que via LIF1. Cependant, initiator1 ne peut pas accéder à LUN1 via LIF2 car LIF2 n'est pas dans portset1.



Informations associées

- [Mappage de LUN sélectif](#)

- [Créer un ensemble de ports et lier à un groupe initiateur](#)

Affichez et gérez les initiateurs SAN et igroups

Vous pouvez utiliser System Manager pour afficher et gérer les groupes initiateurs et les initiateurs.

Description de la tâche

- Les groupes initiateurs identifient les hôtes pouvant accéder à des LUN spécifiques sur le système de stockage.
- Une fois qu'un initiateur et des groupes initiateurs sont créés, vous pouvez également les modifier ou les supprimer.
- Pour gérer les groupes initiateurs SAN et les initiateurs, vous pouvez effectuer les tâches suivantes :
 - [\[view-manage-san-igroups\]](#)
 - [\[view-manage-san-inits\]](#)

Afficher et gérer les groupes initiateurs SAN

Vous pouvez utiliser System Manager pour afficher la liste des groupes initiateurs. Dans cette liste, vous pouvez effectuer des opérations supplémentaires.

Étapes

1. Dans System Manager, cliquez sur **hôtes > groupes initiateurs SAN**.

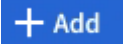
La page affiche la liste des groupes initiateurs. Si la liste est grande, vous pouvez afficher des pages supplémentaires de la liste en cliquant sur les numéros de page dans le coin inférieur droit de la page.

Les colonnes affichent diverses informations sur les igroups. Depuis 9.11.1, l'état de connexion du groupe initiateur est également affiché. Passez le curseur sur les alertes d'état pour afficher les détails.


2. (Facultatif) : vous pouvez effectuer les tâches suivantes en cliquant sur les icônes dans le coin supérieur droit de la liste :

- **Recherche**
- **Télécharger** la liste.
- **Afficher** ou **Masquer** dans la liste.
- **Filtrer** les données de la liste.

3. Vous pouvez effectuer des opérations à partir de la liste :

- Cliquez sur  pour ajouter un groupe initiateur.
- Cliquez sur le nom du groupe initiateur pour afficher la page **Présentation** qui affiche les détails sur le groupe initiateur.

Sur la page **Présentation**, vous pouvez afficher les LUN associées au groupe initiateur et lancer les opérations pour créer des LUN et mapper les LUN. Cliquez sur **tous les initiateurs SAN** pour revenir à la liste principale.

- Passez la souris sur le groupe initiateur, puis cliquez sur  en regard de son nom pour modifier ou supprimer ce groupe.

- Passez le curseur de la souris sur la zone à gauche du nom du groupe initiateur, puis cochez la case. Si vous cliquez sur **+Ajouter au groupe initiateur**, vous pouvez ajouter ce groupe initiateur à un autre groupe initiateur.
- Dans la colonne **Storage VM**, cliquez sur le nom d'une machine virtuelle de stockage pour en afficher les détails.

Afficher et gérer les initiateurs SAN

Vous pouvez utiliser System Manager pour afficher la liste des initiateurs. Dans cette liste, vous pouvez effectuer des opérations supplémentaires.

Étapes

1. Dans System Manager, cliquez sur **hôtes > groupes initiateurs SAN**.

La page affiche la liste des groupes initiateurs.

2. Pour afficher les initiateurs, effectuez les opérations suivantes :

- Cliquez sur l'onglet **FC Initiators** pour afficher la liste des initiateurs FC.
- Cliquez sur l'onglet **initiateurs iSCSI** pour afficher la liste des initiateurs iSCSI.

Les colonnes affichent diverses informations relatives aux initiateurs.

Depuis 9.11.1, le statut de connexion de l'initiateur est également affiché. Passez le curseur sur les alertes d'état pour afficher les détails.

3. (Facultatif) : vous pouvez effectuer les tâches suivantes en cliquant sur les icônes dans le coin supérieur droit de la liste :
 - **Rechercher** la liste des initiateurs particuliers.
 - **Télécharger** la liste.
 - **Afficher** ou **Masquer** dans la liste.
 - **Filtrer** les données de la liste.

Créez un groupe initiateur imbriqué

À partir de la version ONTAP 9.9.1, vous pouvez créer un groupe initiateur qui se compose d'autres groupes initiateurs existants.

1. Dans System Manager, cliquez sur **hôte > groupes d'initiateurs SAN**, puis sur **Ajouter**.
2. Saisissez le nom **Nom** et **Description** du groupe initiateur.

La description sert d'alias de groupe initiateur.

3. Sélectionnez **Storage VM** et **Host Operating System**.



Impossible de modifier le type de système d'exploitation d'un groupe initiateur imbriqué après la création du groupe initiateur.

4. Sous **membres du groupe initiateur**, sélectionnez **Groupe initiateur existant**.

Vous pouvez utiliser **Search** pour rechercher et sélectionner les groupes d'initiateurs à ajouter.

Mappez les igroups sur plusieurs LUN

Depuis la version ONTAP 9.9.1, vous pouvez mapper les groupes initiateurs sur deux ou plusieurs LUN simultanément.

1. Dans System Manager, cliquez sur **stockage > LUN**.
2. Sélectionnez les LUN à mapper.
3. Cliquez sur **plus**, puis sur **mapper aux groupes initiateurs**.



Les igroups sélectionnés sont ajoutés aux LUN sélectionnés. Les mappages existants ne sont pas écrasés.

Créer un ensemble de ports et lier à un groupe initiateur

En plus de l'utilisation "[Mappage de LUN sélectif \(SLM\)](#)", Vous pouvez créer un ensemble de ports et lier l'ensemble de ports à un groupe initiateur pour limiter davantage les LIF qu'un initiateur peut utiliser pour accéder à une LUN.

Si vous n'associez pas un ensemble de ports à un groupe initiateur, tous les initiateurs du groupe initiateur peuvent accéder aux LUN mappées par l'intermédiaire de toutes les LIF du nœud propriétaire de la LUN et du partenaire haute disponibilité du nœud propriétaire.

Ce dont vous avez besoin

Vous devez disposer d'au moins une LIF et un groupe initiateur.

Sauf si vous utilisez des groupes d'interface, deux LIF sont recommandées pour la redondance des protocoles iSCSI et FC. Une seule LIF est recommandée pour les groupes d'interfaces.

Description de la tâche

Il est avantageux d'utiliser des ensembles de ports avec SLM lorsque vous disposez de plus de deux LIF sur un nœud et que vous souhaitez limiter un certain initiateur à un sous-ensemble de LIF. Sans portsets, toutes les cibles du nœud sont accessibles par tous les initiateurs avec accès à la LUN via le nœud propriétaire de la LUN et le partenaire haute disponibilité du nœud propriétaire.

Exemple 11. Étapes

System Manager

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour créer des ensembles de ports et les lier aux groupes initiateurs.

Si vous devez créer un ensemble de ports et le lier à un groupe initiateur dans une version de ONTAP antérieure à 9.10.1, vous devez utiliser la procédure de l'interface de ligne de commandes de ONTAP.

- 1. Dans System Manager, cliquez sur **réseau > Présentation > ensembles de ports**, puis sur **Ajouter**.
- 2. Entrez les informations du nouvel ensemble de ports et cliquez sur **Ajouter**.
- 3. Cliquez sur **hôtes > SAN Initiator Groups**.
- 4. Pour lier l'ensemble de ports à un nouveau groupe initiateur, cliquez sur **Ajouter**.

Pour lier le génération à un groupe initiateur existant, sélectionnez-le, cliquez sur **⋮**, puis sur **Modifier le groupe initiateur**.

Informations associées

["Afficher et gérer les initiateurs et les igroups"](#)

CLI

- 1. Créer un jeu de ports contenant les LIFs appropriées :

```
portset create -vserver vs1 -portset portset0 -protocol iscsi -port-name lif0,lif1
```

Si vous utilisez FC, spécifiez le `protocol` ens. paramètre `fc`. Si vous utilisez iSCSI, spécifiez `protocol` ens. paramètre `iscsi`.

- 2. Connectez le groupe initiateur à l'ensemble de ports :

```
lun igroup bind -vserver vs1 -igroup igroup1 -portset portset0
```

- 3. Vérifiez que vos jeux de ports et vos LIF sont corrects :

```
portset show -vserver vs1
```

Vserver	Portset	Protocol	Port Names	Igroups
vs3	portset0	iscsi	lif0,lif1	igroup1


Gérer les ensembles de ports

En plus de ["Mappage de LUN sélectif \(SLM\)"](#), Vous pouvez utiliser des ensembles de ports pour limiter davantage les LIF qu'un initiateur peut utiliser pour accéder à une LUN.


Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour modifier les interfaces réseau associées

aux ensembles de ports et supprimer les ensembles de ports.

Modifier les interfaces réseau associées à un ensemble de ports

1. Dans System Manager, sélectionnez **réseau > Présentation > Portsets**.
2. Sélectionnez la génération que vous souhaitez modifier, puis  sélectionnez **Modifier génération**.

Supprimer un ensemble de ports

1. Dans System Manager, cliquez sur **réseau > Présentation > ensembles de ports**.
2. Pour supprimer un seul ensemble de ports, sélectionnez-le,  puis sélectionnez **Supprimer les ensembles de ports**.

Pour supprimer plusieurs ensembles de ports, sélectionnez-les et cliquez sur **Supprimer**.

Présentation du mappage de LUN sélectif

Le mappage de LUN sélectif (SLM) réduit le nombre de chemins entre l'hôte et la LUN. Avec SLM, lorsqu'un nouveau mappage de LUN est créé, le LUN est accessible uniquement via des chemins sur le nœud propriétaire de la LUN et son partenaire HA.

SLM permet de gérer un groupe initiateur unique par hôte et prend également en charge les opérations de déplacement de LUN sans interruption qui ne nécessitent pas de manipulation de l'ensemble de ports ou de remappage des LUN.

"Ensembles de ports" Peut être utilisé avec SLM pour restreindre davantage l'accès à certaines cibles à certains initiateurs. Lors de l'utilisation de SLM avec des ensembles de ports, les LUN sont accessibles sur l'ensemble des LIF du portset sur le nœud propriétaire de la LUN et sur le partenaire HA de ce nœud.

SLM est activé par défaut sur tous les nouveaux mappages de LUN.

Déterminez si SLM est activé sur un mappage de LUN

Si votre environnement comporte une combinaison de LUN créées dans une version de ONTAP 9 et de LUN faisant l'objet d'une transition à partir de versions précédentes, vous devrez peut-être déterminer si la fonction de mappage de LUN sélectif (SLM) est activée sur une LUN spécifique.

Vous pouvez utiliser les informations affichées dans la sortie du `lun mapping show -fields reporting-nodes, node` Commande permettant de déterminer si SLM est activé sur votre mappage de LUN. Si SLM n'est pas activé, "-" s'affiche dans les cellules sous la colonne "nœuds de portage" de la sortie de la commande. Si SLM est activé, la liste des nœuds affichée sous la colonne « noeuds » est dupliquée dans la colonne « noeuds de portage ».

Modifiez la liste des noeuds-rapports SLM

Si vous déplacez une LUN ou un volume contenant des LUN vers une autre paire haute disponibilité (HA) au sein du même cluster, vous devez modifier la liste des nœuds de rapport du mappage de LUN sélectif (SLM) avant de lancer le déplacement pour vous assurer que les chemins LUN actifs et optimisés sont maintenus.

Étapes

1. Ajoutez le nœud de destination et son nœud partenaire à la liste « reporting-nodes » de l'agrégat ou du volume :

```
lun mapping add-reporting-nodes -vserver <vserver_name> -path <lun_path>
-igroup <igroup_name> [-destination-aggregate <aggregate_name>|-
destination-volume <volume_name>]
```

Si vous disposez d'une nomenclature établie cohérente, vous pouvez modifier plusieurs mappages de LUN en même temps en utilisant à `igroup_prefix*` la place de `igroup_name`.

2. Relancez l'analyse de l'hôte pour détecter les nouveaux chemins ajoutés.
3. Si votre système d'exploitation le requiert, ajoutez les nouveaux chemins d'accès à votre configuration MPIO (Multi-Path Network I/O).
4. Exécutez la commande pour l'opération de déplacement requise et attendez la fin de l'opération.
5. Vérifier que les E/S sont en cours de maintenance via le chemin actif/optimisé :

```
lun mapping show -fields reporting-nodes
```

6. Supprimez l'ancien propriétaire de LUN et son nœud partenaire de la liste noeuds-rapports :

```
lun mapping remove-reporting-nodes -vserver <vserver_name> -path
<lun_path> -igroup <igroup_name> -remote-nodes
```

7. Vérifiez que la LUN a été supprimée du mappage de LUN existant :

```
lun mapping show -fields reporting-nodes
```

8. Supprimez toute entrée de périphérique obsolète pour le système d'exploitation hôte.
9. Modifiez les fichiers de configuration des chemins d'accès multiples si nécessaire.
10. Relancez l'analyse de l'hôte pour vérifier la suppression des anciens chemins.
Reportez-vous à la documentation de votre hôte pour connaître les étapes spécifiques à suivre pour relancer l'analyse de vos hôtes.

Gérez le protocole iSCSI

Configurez votre réseau pour des performances optimales

Les performances des réseaux Ethernet varient considérablement. Vous pouvez optimiser les performances du réseau utilisé pour iSCSI en sélectionnant des valeurs de configuration spécifiques.

Étapes

1. Connectez l'hôte et les ports de stockage au même réseau.

Il est préférable de se connecter aux mêmes commutateurs. Le routage ne doit jamais être utilisé.

2. Sélectionnez les ports à vitesse la plus élevée disponibles et dédiez-les à iSCSI.

Les 10 ports GbE sont optimaux. Le nombre minimal de ports 1 GbE est égal à 1.

3. Désactiver le contrôle de flux Ethernet pour tous les ports.

Vous devriez voir "[Gestion du réseau](#)" Pour configurer le contrôle de flux du port Ethernet à l'aide de l'interface de ligne de commande.

4. Activez les trames Jumbo (généralement MTU de 9 9000).

Tous les périphériques du chemin d'accès aux données, y compris les initiateurs, les cibles et les commutateurs, doivent prendre en charge les trames Jumbo. Dans le cas contraire, l'activation des trames Jumbo réduit considérablement les performances du réseau.

Configuration d'un SVM pour iSCSI

Pour configurer un SVM (Storage Virtual machine) pour iSCSI, vous devez créer des LIFs pour le SVM et affecter le protocole iSCSI à ces LIFs.


Description de la tâche

Au moins une LIF iSCSI par nœud est nécessaire pour chaque SVM assurant le service des données avec le protocole iSCSI. Pour la redondance, vous devez créer au moins deux LIF par nœud.

Exemple 12. Étapes

System Manager

Configurer une machine virtuelle de stockage pour iSCSI avec ONTAP System Manager (9.7 et versions ultérieures).

Pour configurer iSCSI sur une nouvelle machine virtuelle de stockage	Pour configurer iSCSI sur une machine virtuelle de stockage existante
<ol style="list-style-type: none">1. Dans System Manager, cliquez sur stockage > machines virtuelles de stockage, puis sur Ajouter.2. Entrez un nom pour la machine virtuelle de stockage.3. Sélectionnez iSCSI pour le Protocole d'accès.4. Cliquez sur Activer iSCSI et entrez l'adresse IP et le masque de sous-réseau de l'interface réseau. + chaque nœud doit disposer d'au moins deux interfaces réseau.5. Cliquez sur Enregistrer.	<ol style="list-style-type: none">1. Dans System Manager, cliquez sur stockage > machines virtuelles de stockage.2. Cliquez sur la VM de stockage que vous souhaitez configurer.3. Cliquez sur l'onglet Paramètres, puis cliquez sur  en regard du protocole iSCSI.4. Cliquez sur Activer iSCSI et entrez l'adresse IP et le masque de sous-réseau de l'interface réseau. + chaque nœud doit disposer d'au moins deux interfaces réseau.5. Cliquez sur Enregistrer.

CLI

Configurer une VM de stockage pour iSCSI à l'aide de l'interface de ligne de commande ONTAP.

1. Activer les SVM pour écouter le trafic iSCSI :

```
vserver iscsi create -vserver vserver_name -target-alias vserver_name
```

2. Créer une LIF pour les SVM sur chaque nœud à utiliser pour iSCSI :

- Pour ONTAP 9.6 et versions ultérieures :

```
network interface create -vserver vserver_name -lif lif_name -data  
-protocol iscsi -service-policy default-data-iscsi -home-node node_name  
-home-port port_name -address ip_address -netmask netmask
```

- Pour ONTAP 9.5 et versions antérieures :

```
network interface create -vserver vserver_name -lif lif_name -role data  
-data-protocol iscsi -home-node node_name -home-port port_name -address  
ip_address -netmask netmask
```

3. Vérifiez que vous avez configuré correctement vos LIF :

```
network interface show -vserver vserver_name
```

4. Vérifier que iSCSI est actif et que l'IQN cible pour ce SVM :

```
vserver iscsi show -vserver vserver_name
```

5. Depuis votre hôte, créez des sessions iSCSI vers vos LIF.

Informations associées

["Rapport technique de NetApp 4080 : meilleures pratiques pour le SAN moderne"](#)

Définir une méthode de stratégie de sécurité pour un initiateur

Vous pouvez définir une liste d'initiateurs et leurs méthodes d'authentification. Vous pouvez également modifier la méthode d'authentification par défaut qui s'applique aux initiateurs qui n'ont pas de méthode d'authentification définie par l'utilisateur.

Description de la tâche

Vous pouvez générer des mots de passe uniques à l'aide d'algorithmes de règles de sécurité dans le produit ou vous pouvez spécifier manuellement les mots de passe que vous souhaitez utiliser.



Tous les initiateurs ne prennent pas en charge les mots de passe secrets CHAP hexadécimaux.

Étapes

1. Utilisez le `vserver iscsi security create` commande permettant de créer une méthode de stratégie de sécurité pour un initiateur.

```
vserver iscsi security create -vserver vs2 -initiator iqn.1991-05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name bob2
```

2. Suivez les commandes à l'écran pour ajouter les mots de passe.

Crée une méthode de stratégie de sécurité pour l'initiateur `iqn.1991-05.com.microsoft:host1` avec des noms d'utilisateur et des mots de passe CHAP entrants et sortants.

Informations associées

- [Fonctionnement de l'authentification iSCSI](#)
- [Authentification CHAP](#)

Suppression d'un service iSCSI pour une SVM

Vous pouvez supprimer un service iSCSI pour une machine virtuelle de stockage (SVM) s'il n'est plus nécessaire.

Ce dont vous avez besoin

L'état d'administration du service iSCSI doit être à l'état "down" avant de pouvoir supprimer un service iSCSI. Vous pouvez déplacer l'état d'administration vers le bas à l'aide de `vserver iscsi modify` commande.

Étapes

1. Utilisez le `vserver iscsi modify` Commande permettant d'arrêter les E/S vers la LUN.

```
vserver iscsi modify -vserver vs1 -status-admin down
```

2. Utilisez le `vserver iscsi delete` Commande permettant de supprimer le service iscsi du SVM.

```
vserver iscsi delete -vserver vs_1
```

3. Utilisez le `vserver iscsi show` command Pour vérifier que vous avez supprimé le service iSCSI de la SVM.

```
vserver iscsi show -vserver vs1
```

Obtenez plus de détails dans les restaurations d'erreurs de session iSCSI

L'augmentation du niveau de récupération des erreurs de session iSCSI vous permet de recevoir des informations plus détaillées sur les restaurations d'erreurs iSCSI. L'utilisation d'un niveau de récupération d'erreur plus élevé peut entraîner une réduction mineure des performances de la session iSCSI.

Description de la tâche

Par défaut, ONTAP est configuré pour utiliser le niveau de récupération d'erreur 0 pour les sessions iSCSI. Si vous utilisez un initiateur qui a été qualifié pour la récupération d'erreur de niveau 1 ou 2, vous pouvez choisir d'augmenter le niveau de récupération d'erreur. Le niveau de récupération d'erreur de session modifié n'affecte que les sessions nouvellement créées et n'affecte pas les sessions existantes.

À partir de ONTAP 9.4, le `max-error-recovery-level` cette option n'est pas prise en charge dans le `iscsi show` et `iscsi modify` commandes.

Étapes

1. Entrer en mode avancé :

```
set -privilege advanced
```

2. Vérifiez le paramètre actuel à l'aide du `iscsi show` commande.

```
iscsi show -vserver vs3 -fields max-error-recovery-level
```

```
vserver max-error-recovery-level
-----
vs3      0
```

3. Modifiez le niveau de récupération d'erreur à l'aide de `iscsi modify` commande.

```
iscsi modify -vserver vs3 -max-error-recovery-level 2
```

Enregistrez le SVM avec un serveur iSNS

Vous pouvez utiliser le `vserver iscsi isns` Commande permettant de configurer la machine virtuelle de stockage (SVM) à enregistrer avec un serveur iSNS.

Description de la tâche

Le `vserver iscsi isns create` Commande permet de configurer le SVM pour qu'il s'enregistre avec le serveur iSNS. Le SVM ne fournit pas de commandes permettant de configurer ou de gérer le serveur iSNS.

Pour gérer le serveur iSNS, vous pouvez utiliser les outils d'administration du serveur ou l'interface fournie par le fournisseur pour le serveur iSNS.

Étapes

1. Sur votre serveur iSNS, assurez-vous que votre service iSNS est opérationnel et disponible.
2. Créer la LIF de SVM management sur un port data :

```
network interface create -vserver SVM_name -lif lif_name -role data -data  
-protocol none -home-node home_node_name -home-port home_port -address  
IP_address -netmask network_mask
```

3. Créer un service iSCSI sur votre SVM si celui-ci n'existe pas déjà :

```
vserver iscsi create -vserver SVM_name
```

4. Vérifiez que le service iSCSI a été créé avec succès :

```
iscsi show -vserver SVM_name
```

5. Vérifier qu'une route par défaut existe pour le SVM :

```
network route show -vserver SVM_name
```

6. Si une route par défaut n'existe pas pour le SVM, créer une route par défaut :

```
network route create -vserver SVM_name -destination destination -gateway  
gateway
```

7. Configurer le SVM pour s'enregistrer avec le service iSNS :

```
vserver iscsi isns create -vserver SVM_name -address IP_address
```

Les familles d'adresses IPv4 et IPv6 sont prises en charge. La famille d'adresses du serveur iSNS doit être identique à celle du LIF de gestion des SVM.

Par exemple, vous ne pouvez pas connecter une LIF de gestion SVM avec une adresse IPv4 à un serveur iSNS avec une adresse IPv6.

8. Vérifiez que le service iSNS fonctionne :

```
vserver iscsi isns show -vserver SVM_name
```

9. Si le service iSNS n'est pas en cours d'exécution, démarrez-le :

```
vserver iscsi isns start -vserver SVM_name
```

Résolution des messages d'erreur iSCSI sur le système de stockage

Vous pouvez afficher un certain nombre de messages d'erreur iSCSI courants avec le `event log show` commande. Vous devez savoir ce que signifient ces messages et ce que vous pouvez faire pour résoudre les problèmes qu'ils identifient.

Le tableau suivant contient les messages d'erreur les plus courants et des instructions pour les résoudre :

Messagerie	Explication	Que faire
ISCSI: network interface identifier disabled for use; incoming connection discarded	Le service iSCSI n'est pas activé sur l'interface.	Vous pouvez utiliser le <code>iscsi interface enable</code> Pour activer le service iSCSI sur l'interface. Par exemple : <code>iscsi interface enable -vserver vs1 -lif lif1</code>
ISCSI: Authentication failed for initiator nodename	CHAP n'est pas configuré correctement pour l'initiateur spécifié.	Vous devez vérifier les paramètres CHAP ; vous ne pouvez pas utiliser le même nom d'utilisateur et mot de passe pour les paramètres entrant et sortant sur le système de stockage : <ul style="list-style-type: none"> • Les identifiants entrants du système de stockage doivent correspondre aux informations d'identification sortantes de l'initiateur. • Les identifiants sortants du système de stockage doivent correspondre aux informations d'identification entrantes de l'initiateur.

Activer ou désactiver le basculement automatique de LIF iSCSI

Après la mise à niveau vers ONTAP 9.11.1 ou une version ultérieure, vous devez activer manuellement le basculement automatique des LIF sur toutes les LIF iSCSI créées dans ONTAP 9.10.1 ou une version antérieure.

À partir de la version ONTAP 9.11.1, vous pouvez activer le basculement automatique des LIF iSCSI sur les plateformes SAN 100 % Flash. En cas de basculement du stockage, la LIF iSCSI est automatiquement migrée de son nœud ou port de rattachement vers son nœud ou port partenaire haute disponibilité, puis de nouveau une fois le basculement terminé. Ou, si le port de la LIF iSCSI devient défectueux, la LIF est automatiquement migrée vers un port sain de son nœud de rattachement actuel, puis de nouveau vers son port d'origine une fois le port refunctional. Permet aux charges de travail SAN exécutées sur iSCSI de reprendre plus rapidement le service d'E/S après un basculement.

Dans ONTAP 9.11.1 et versions ultérieures, par défaut, les LIF iSCSI nouvellement créées sont activées pour le basculement automatique des LIF, si l'une des conditions suivantes est vraie :

- Il n'y a pas de LIF iSCSI sur le SVM
- Toutes les LIFs iSCSI sur le SVM sont activées pour le basculement automatique des LIF

Activer le basculement automatique de LIF iSCSI

Par défaut, les LIF iSCSI créées dans ONTAP 9.10.1 et les versions antérieures ne sont pas activées pour le

basculement automatique des LIF. Si sur le SVM des LIF iSCSI ne sont pas activées pour le basculement automatique des LIF, vos nouvelles LIF ne seront pas non plus activées pour le basculement automatique des LIF. Si le basculement automatique de LIF n'est pas activé et qu'un événement de basculement se produit, vos LIFs iSCSI ne migrent pas.

En savoir plus sur ["Basculement et rétablissement de LIF"](#).

Étape

1. Activer le basculement automatique pour une LIF iSCSI :

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover  
-policy sfo-partner-only -auto-revert true
```

Pour mettre à jour toutes les LIFs iSCSI sur le SVM, utiliser `-lif*` au lieu de `lif`.

Désactivez le basculement automatique des LIF iSCSI

Si vous avez précédemment activé le basculement automatique de LIF iSCSI sur des LIF iSCSI créées dans ONTAP 9.10.1 ou une version antérieure, vous avez la possibilité de le désactiver.

Étape

1. Désactiver le basculement automatique pour une LIF iSCSI :

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover  
-policy disabled -auto-revert false
```

Pour mettre à jour toutes les LIFs iSCSI sur le SVM, utiliser `-lif*` au lieu de `lif`.

Informations associées

- ["Créer une LIF"](#)
- Manuellement ["Migrer une LIF"](#)
- Manuellement ["Restaure une LIF sur son port d'attache"](#)
- ["Configurer les paramètres de basculement sur une LIF"](#)

Gestion du protocole FC

Configuration d'un SVM pour FC

Pour configurer un SVM (Storage Virtual machine) pour FC, vous devez créer des LIFs pour le SVM et affecter le protocole FC à ces LIFs.

Avant de commencer

Vous devez disposer d'une licence FC (["Inclus avec ONTAP One"](#)) et il doit être activé. Si la licence FC n'est pas activée, les LIFs et les SVM semblent être en ligne, mais le statut opérationnel est `down`. Le service FC doit être activé pour que vos LIF et SVM soient opérationnels. Vous devez utiliser un zoning unique pour toutes les LIFs FC du SVM pour héberger les initiateurs.


Description de la tâche

NetApp prend en charge au moins une LIF FC par nœud pour chaque SVM assurant le service des données avec le protocole FC. Vous devez utiliser deux LIF par nœud et deux structures, avec une LIF par nœud attaché. Cela permet la redondance au niveau de la couche des nœuds et de la structure.

Exemple 13. Étapes

System Manager

Configurer une machine virtuelle de stockage pour iSCSI avec ONTAP System Manager (9.7 et versions ultérieures).

Pour configurer FC sur une nouvelle machine virtuelle de stockage	Pour configurer FC sur une machine virtuelle de stockage existante
<div>1. Dans System Manager, cliquez sur stockage > machines virtuelles de stockage, puis sur Ajouter.</div> <div>2. Entrez un nom pour la machine virtuelle de stockage.</div> <div>3. Sélectionnez FC pour Protocole d'accès.</div> <div>4. Cliquez sur Activer FC. + les ports FC sont attribués automatiquement.</div> <div>5. Cliquez sur Enregistrer.</div>	<div>1. Dans System Manager, cliquez sur stockage > machines virtuelles de stockage.</div> <div>2. Cliquez sur la VM de stockage que vous souhaitez configurer.</div> <div>3. Cliquez sur l'onglet Settings, puis cliquez sur  en regard du protocole FC.</div> <div>4. Cliquez sur Activer FC et entrez l'adresse IP et le masque de sous-réseau de l'interface réseau. + les ports FC sont attribués automatiquement.</div> <div>5. Cliquez sur Enregistrer.</div>

CLI

- 1. Activer le service FC sur le SVM :

```
vserver fcp create -vserver vserver_name -status-admin up
```

- 2. Créez deux LIF pour les SVM sur chaque nœud assurant le service FC :

- Pour ONTAP 9.6 et versions ultérieures :

```
network interface create -vserver vserver_name -lif lif_name -data -protocol fcp -service-policy default-data-fcp -home-node node_name -home-port port_name -address ip_address -netmask netmask -status-admin up
```

- Pour ONTAP 9.5 et versions antérieures :

```
network interface create -vserver vserver_name -lif lif_name -role data -data-protocol fcp -home-node node_name -home-port port
```

- 3. Vérifiez que vos LIF ont été créées et que leur statut opérationnel est online:

```
network interface show -vserver vserver_name lif_name
```

Informations associées

["Support NetApp"](#)

["Matrice d'interopérabilité NetApp"](#)

[Considérations relatives aux LIF dans les environnements cluster SAN](#)

Suppression d'un service FC pour une SVM

Vous pouvez supprimer un service FC pour une machine virtuelle de stockage (SVM) s'il n'est plus nécessaire.

Ce dont vous avez besoin

Le statut d'administration doit être « down » avant de supprimer un service FC pour une SVM. Vous pouvez définir l'état d'administration sur Down avec l'un ou l'autre `vserver fcp modify` commande ou le `vserver fcp stop` commande.

Étapes

1. Utilisez le `vserver fcp stop` Commande permettant d'arrêter les E/S vers la LUN.

```
vserver fcp stop -vserver vs_1
```

2. Utilisez le `vserver fcp delete` Commande permettant de supprimer le service du SVM.

```
vserver fcp delete -vserver vs_1
```

3. Utilisez le `vserver fcp show` Pour vérifier que vous avez supprimé le service FC de votre SVM :

```
vserver fcp show -vserver vs_1
```

Configurations MTU recommandées pour les trames jumbo FCoE

Pour la technologie Fibre Channel over Ethernet (FCoE), les trames jumbo pour la partie adaptateur Ethernet de la carte CNA doivent être configurées à 9000 MTU. Les trames Jumbo pour la partie adaptateur FCoE du CNA doivent être configurées à plus de 10 1500 MTU. Ne configurez les trames Jumbo que si l'initiateur, la cible et tous les commutateurs d'intervention prennent en charge et sont configurés pour les trames Jumbo.

Gérez le protocole NVMe

Démarrer le service NVMe pour un SVM

Avant de pouvoir utiliser le protocole NVMe sur votre SVM, vous devez démarrer le service NVMe sur la SVM.

Avant de commencer

NVMe doit être autorisé en tant que protocole sur votre système.

Les protocoles NVMe suivants sont pris en charge :

Protocole	À partir de ...	Autorisé par...
TCP	ONTAP 9.10.1	Valeur par défaut
FCP	ONTAP 9.4	Valeur par défaut

Étapes

1. Modifiez le paramètre de privilège sur avancé :

```
set -privilege advanced
```

2. Vérifiez que NVMe est autorisé en tant que protocole :

```
vserver nvme show
```

3. Créez le service de protocole NVMe :

```
vserver nvme create
```

4. Démarrer le service de protocole NVMe sur le SVM :

```
vserver nvme modify -status -admin up
```

Suppression du service NVMe d'un SVM

Si nécessaire, vous pouvez supprimer le service NVMe de votre SVM (Storage Virtual machine).

Étapes

1. Modifiez le paramètre de privilège sur avancé :

```
set -privilege advanced
```

2. Arrêter le service NVMe sur le SVM :

```
vserver nvme modify -status -admin down
```

3. Supprimez le service NVMe :


```
vserver nvme delete
```

Redimensionner un espace de noms

Depuis la version ONTAP 9.10.1, vous pouvez utiliser l'interface de ligne de commandes ONTAP pour augmenter ou réduire la taille d'un espace de noms NVMe. System Manager peut être utilisé pour augmenter la taille d'un namespace NVMe.

Augmenter la taille d'un namespace

System Manager

1. Cliquez sur **stockage > espaces de noms NVMe**.
2. Hoover sur l'espace de noms que vous voulez augmenter, cliquez sur , puis cliquez sur **Modifier**.
3. Sous **CAPACITY**, modifiez la taille de l'espace de noms.

CLI

1. Saisissez la commande suivante : `vserver nvme namespace modify -vserver SVM_name -path path -size new_size_of_namespace`

Réduire la taille d'un namespace

Vous devez utiliser l'interface de ligne de commandes de ONTAP pour réduire la taille d'un namespace NVMe.

1. Modifiez le paramètre de privilège sur avancé :

```
set -privilege advanced
```

2. Diminuer la taille du namespace :

```
vserver nvme namespace modify -vserver SVM_name -path namespace_path -size new_size_of_namespace
```

Convertir un namespace en LUN

Depuis la version ONTAP 9.11.1, vous pouvez utiliser l'interface de ligne de commandes ONTAP pour convertir un espace de noms NVMe existant en LUN sans déplacement.

Avant de commencer

- L'espace de noms NVMe spécifié ne doit pas disposer d'aucun mappage existant à un sous-système.
- L'espace de noms ne doit pas faire partie d'une copie Snapshot ni, du côté destination de la relation SnapMirror, en tant qu'espace de noms en lecture seule.
- Les espaces de noms NVMe ne sont pris en charge qu'avec des plates-formes spécifiques et des cartes réseau, cette fonctionnalité ne fonctionne qu'avec du matériel spécifique.

Étapes

1. Entrez la commande suivante pour convertir un namespace NVMe en LUN :

```
lun convert-from-namespace -vserver -namespace-path
```

Configuration de l'authentification intrabande sur NVMe

Depuis ONTAP 9.12.1, vous pouvez utiliser l'interface de ligne de commande ONTAP pour configurer l'authentification intrabande (sécurisée), bidirectionnelle et unidirectionnelle entre un hôte et un contrôleur NVMe via les protocoles NVMe/TCP et NVMe/FC à l'aide de l'authentification DH-HMAC-CHAP. À partir de ONTAP 9.14.1, l'authentification intrabande peut être configurée dans System Manager.

Pour configurer l'authentification intrabande, chaque hôte ou contrôleur doit être associé à une clé DH-HMAC-CHAP qui est une combinaison du NQN de l'hôte ou du contrôleur NVMe et d'un secret d'authentification configuré par l'administrateur. Pour qu'un hôte ou un contrôleur NVMe authentifie son homologue, il doit connaître la clé associée à celui-ci.

Dans l'authentification unidirectionnelle, une clé secrète est configurée pour l'hôte, mais pas pour le contrôleur. Dans le cas d'une authentification bidirectionnelle, une clé secrète est configurée pour l'hôte et le contrôleur.

SHA-256 est la fonction de hachage par défaut et 2048 bits est le groupe DH par défaut.

System Manager

Depuis ONTAP 9.14.1, vous pouvez utiliser System Manager pour configurer l'authentification intrabande lors de la création ou de la mise à jour d'un sous-système NVMe, de la création ou du clonage d'espaces de noms NVMe, ou de l'ajout de groupes de cohérence avec de nouveaux espaces de noms NVMe.

Étapes

1. Dans System Manager, cliquez sur **hosts > NVMe Subsystem**, puis sur **Add**.
2. Ajoutez le nom du sous-système NVMe, puis sélectionnez la VM de stockage et le système d'exploitation hôte.
3. Saisissez le NQN hôte.
4. Sélectionnez **utiliser l'authentification intrabande** en regard du NQN hôte.
5. Indiquez le secret de l'hôte et le secret du contrôleur.

La clé DH-HMAC-CHAP est une combinaison du NQN de l'hôte ou du contrôleur NVMe et d'un secret d'authentification configuré par l'administrateur.

6. Sélectionnez la fonction de hachage et le groupe DH de votre choix pour chaque hôte.

Si vous ne sélectionnez pas de fonction de hachage et de groupe DH, SHA-256 est affecté comme fonction de hachage par défaut et 2048 bits comme groupe DH par défaut.

7. Si vous le souhaitez, cliquez sur **Ajouter** et répétez les étapes nécessaires pour ajouter d'autres hôtes.
8. Cliquez sur **Enregistrer**.
9. Pour vérifier que l'authentification intrabande est activée, cliquez sur **System Manager > hosts > NVMe Subsystem > Grid > Peek View**.

Une icône de clé transparente en regard du nom d'hôte indique que le mode unidirectionnel est activé. Une clé opaque en regard du nom d'hôte indique que le mode bidirectionnel est activé.

CLI

Étapes

1. Ajoutez l'authentification DH-HMAC-CHAP à votre sous-système NVMe :

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -dhchap-host-secret
<authentication_host_secret> -dhchap-controller-secret
<authentication_controller_secret> -dhchap-hash-function <sha-
256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
bit|8192-bit>
```

2. Vérifiez que le protocole d'authentification CHAP DH-HMAC est ajouté à votre hôte :

```
vserver nvme subsystem host show
```

```

[ -dhchap-hash-function {sha-256|sha-512} ] Authentication Hash
Function
[ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
Diffie-Hellman
Group
[ -dhchap-mode {none|unidirectional|bidirectional} ]
Authentication Mode

```

3. Vérifier que l'authentification DH-HMAC CHAP a été effectuée lors de la création du contrôleur NVMe :

```
vserver nvme subsystem controller show
```

```

[ -dhchap-hash-function {sha-256|sha-512} ] Authentication Hash
Function
[ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
Diffie-Hellman
Group
[ -dhchap-mode {none|unidirectional|bidirectional} ]
Authentication Mode

```

Désactivez l'authentification intrabande sur NVMe

Si vous avez configuré l'authentification intrabande sur NVMe à l'aide de DH-HMAC-CHAP, vous pouvez choisir de la désactiver à tout moment.

Si vous revenez de ONTAP 9.12.1 ou version ultérieure à ONTAP 9.12.0 ou version antérieure, vous devez désactiver l'authentification intrabande avant de revenir à cette version. Si l'authentification intrabande à l'aide de DH-HMAC-CHAP n'est pas désactivée, le retour échoue.

Étapes

1. Supprimez l'hôte du sous-système pour désactiver l'authentification DH-HMAC-CHAP :

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Vérifiez que le protocole d'authentification DH-HMAC-CHAP est supprimé de l'hôte :

```
vserver nvme subsystem host show
```

3. Ajoutez l'hôte au sous-système sans authentification :

```
vserver nvme subsystem host add vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

Modification de la priorité d'hôte NVMe

À partir de ONTAP 9.14.1, vous pouvez configurer votre sous-système NVMe de manière à hiérarchiser l'allocation des ressources pour des hôtes spécifiques. Par défaut, lorsqu'un hôte est ajouté au sous-système, il se voit attribuer une priorité régulière. Les hôtes affectés à une priorité élevée reçoivent un nombre de files d'attente d'E/S et des profondeurs de files d'attente plus importants.

Vous pouvez utiliser l'interface de ligne de commandes ONTAP pour modifier manuellement la priorité par défaut, de normal à élevée. Pour modifier la priorité attribuée à un hôte, vous devez supprimer l'hôte du sous-système, puis l'ajouter à nouveau.

Étapes

1. Vérifiez que la priorité de l'hôte est définie sur Normal :

```
vserver nvme show-host-priority
```

2. Supprimez l'hôte du sous-système :

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

3. Vérifiez que l'hôte est supprimé du sous-système :

```
vserver nvme subsystem host show
```

4. Ajoutez de nouveau l'hôte au sous-système avec une priorité élevée :

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>  
-priority high
```

Gestion de la détection automatisée d'hôtes des contrôleurs NVMe/TCP

Depuis la version ONTAP 9.14.1, la détection des contrôleurs hôtes utilisant le protocole NVMe/TCP est automatisée par défaut dans les fabrics basés sur IP.

Activez la détection automatisée d'hôtes des contrôleurs NVMe/TCP

Si vous avez précédemment désactivé la découverte automatique d'hôtes, mais que vos besoins ont changé, vous pouvez la réactiver.

Étapes

1. Entrer en mode de privilège avancé :

```
set -privilege advanced
```

2. Activer la découverte automatisée :

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery  
-enabled true
```

3. Vérifiez que la détection automatisée des contrôleurs NVMe/TCP est activée.

```
vserver nvme show
```

Désactivation de la découverte automatique d'hôtes des contrôleurs NVMe/TCP

Si votre hôte n'a pas besoin de détecter automatiquement les contrôleurs NVMe/TCP et que vous détectez le trafic multidiffusion indésirable sur votre réseau, désactivez cette fonctionnalité.

Étapes

1. Entrer en mode de privilège avancé :

```
set -privilege advanced
```

2. Désactiver la découverte automatique :

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery  
-enabled false
```

3. Vérifiez que la détection automatisée des contrôleurs NVMe/TCP est désactivée.

```
vserver nvme show
```

Désactivez l'identificateur de machine virtuelle hôte NVMe

Depuis la version ONTAP 9.14.1, par défaut, ONTAP prend en charge la possibilité pour les hôtes NVMe/FC d'identifier les machines virtuelles à l'aide d'un identifiant unique, et pour les hôtes NVMe/FC de surveiller l'utilisation des ressources des machines virtuelles. Cela améliore le reporting et la résolution des problèmes côté hôte.

Vous pouvez utiliser le bootarg pour désactiver cette fonctionnalité.

Étape

1. Désactiver l'identifiant de la machine virtuelle :

```
bootargs set fct_sli_appid_off <port>, <port>
```

L'exemple suivant désactive le VMID sur le port 0g et le port 0i.

```
bootargs set fct_sli_appid_off 0g,0i  
  
fct_sli_appid_off == 0g,0i
```

Gestion des systèmes avec les adaptateurs FC

Gestion des systèmes avec les adaptateurs FC

Des commandes sont disponibles pour la gestion des adaptateurs FC intégrés et des cartes d'adaptateur FC. Ces commandes peuvent être utilisées pour configurer le mode adaptateur, afficher les informations relatives à l'adaptateur et modifier la vitesse.

La plupart des systèmes de stockage disposent d'adaptateurs FC intégrés pouvant être configurés en tant qu'initiateurs ou cibles. Vous pouvez également utiliser des cartes d'adaptateur FC configurées en tant qu'initiateurs ou cibles. Les initiateurs se connectent aux tiroirs disques internes, voire aux baies de stockage étrangères (FlexArray). Les cibles se connectent uniquement aux commutateurs FC. Les ports HBA FC cible et la vitesse du port du commutateur doivent être définis sur la même valeur et ne doivent pas être définis sur auto.

Informations associées

["Configuration SAN"](#)

Commandes de gestion des adaptateurs FC

Vous pouvez utiliser des commandes FC pour gérer les adaptateurs cibles FC, les adaptateurs initiateurs FC et les adaptateurs FC intégrés à votre contrôleur de stockage. Les mêmes commandes sont utilisées pour gérer les adaptateurs FC pour le protocole FC et le protocole FC-NVMe.

Les commandes de l'adaptateur initiateur FC fonctionnent uniquement au niveau du nœud. Vous devez utiliser le `run -node node_name` Commande avant de pouvoir utiliser les commandes de l'adaptateur FC initiator.

Commandes de gestion des adaptateurs cibles FC

Les fonctions que vous recherchez...	Utilisez cette commande...
Affiche les informations relatives à l'adaptateur FC sur un nœud	<code>network fcp adapter show</code>
Modifiez les paramètres de l'adaptateur cible FC	<code>network fcp adapter modify</code>
Affiche les informations de trafic du protocole FC	<code>run -node <i>node_name</i> sysstat -f</code>
Afficher la durée d'exécution du protocole FC	<code>run -node <i>node_name</i> uptime</code>
Affiche la configuration et l'état de la carte	<code>run -node <i>node_name</i> sysconfig -v <i>adapter</i></code>
Vérifiez quelles cartes d'extension sont installées et si des erreurs de configuration existent	<code>run -node <i>node_name</i> sysconfig -ac</code>
Affichez une page man pour une commande	<code>man <i>command_name</i></code>

Commandes de gestion des adaptateurs initiateurs FC

Les fonctions que vous recherchez...	Utilisez cette commande...
Affiche les informations relatives à la totalité des initiateurs et de leurs adaptateurs dans un nœud	<code>run -node <i>node_name</i> storage show adapter</code>
Affiche la configuration et l'état de la carte	<code>run -node <i>node_name</i> sysconfig -v <i>adapter</i></code>
Vérifiez quelles cartes d'extension sont installées et si des erreurs de configuration existent	<code>run -node <i>node_name</i> sysconfig -ac</code>

Commandes de gestion des adaptateurs FC intégrés

Les fonctions que vous recherchez...	Utilisez cette commande...
Affiche l'état des ports FC intégrés	<code>run -node <i>node_name</i> system hardware unified-connect show</code>

Configurez les adaptateurs FC

Chaque port FC intégré peut être configuré individuellement en tant qu'initiateur ou cible. Les ports de certains adaptateurs FC peuvent également être configurés individuellement en tant que port cible ou port initiateur, comme les ports FC intégrés. Une liste d'adaptateurs pouvant être configurés pour le mode cible est disponible dans le ["NetApp](#)

Hardware Universe".

Le mode cible est utilisé pour connecter les ports aux initiateurs FC. Ce mode permet de connecter les ports aux lecteurs de bande, aux bibliothèques de bandes ou aux systèmes de stockage tiers à l'aide de FlexArray Virtualization ou Foreign LUN Import (FLI).

La même procédure est utilisée lors de la configuration des adaptateurs FC pour le protocole FC et le protocole FC-NVMe. Cependant, seuls certains adaptateurs FC prennent en charge la connectivité FC-NVMe. Voir la "[NetApp Hardware Universe](#)" Par l'utilisation de la liste des adaptateurs prenant en charge le protocole FC-NVMe.

Configurer les adaptateurs FC pour le mode cible

Étapes

1. Mettez l'adaptateur hors ligne :

```
node run -node node_name storage disable adapter adapter_name
```

Si l'adaptateur ne passe pas hors ligne, vous pouvez également retirer le câble du port d'adaptateur approprié du système.

2. Modifiez l'adaptateur de l'initiateur sur la cible :

```
system hardware unified-connect modify -t target -node node_name adapter  
adapter_name
```

3. Redémarrez le nœud hébergeant l'adaptateur que vous avez changé.

4. Vérifiez que la configuration du port cible est correcte :

```
network fcp adapter show -node node_name
```

5. Mettez votre adaptateur en ligne :

```
network fcp adapter modify -node node_name -adapter adapter_port -state up
```

Configurer les adaptateurs FC pour le mode initiateur

Ce dont vous avez besoin

- Les LIF présentes sur l'adaptateur doivent être supprimées de n'importe quel ensemble de ports dont elles sont membres.
- Toutes les LIF de chaque machine virtuelle de stockage (SVM) utilisant le port physique à modifier doivent être migrées ou détruites avant de changer la personnalité du port physique de la cible à l'initiateur.



Le protocole NVMe/FC prend en charge le mode initiateur.

Étapes

1. Supprimer toutes les LIFs de l'adaptateur :

```
network interface delete -vserver SVM_name -lif LIF_name,LIF_name
```

2. Mettez votre adaptateur hors ligne :

```
network fcp adapter modify -node node_name -adapter adapter_port -status-admin  
down
```

Si l'adaptateur ne passe pas hors ligne, vous pouvez également retirer le câble du port d'adaptateur approprié du système.

3. Modifiez l'adaptateur de la cible à l'initiateur :

```
system hardware unified-connect modify -t initiator adapter_port
```

4. Redémarrez le nœud hébergeant l'adaptateur que vous avez changé.
5. Vérifier que les ports FC sont configurés dans l'état approprié pour votre configuration :

```
system hardware unified-connect show
```

6. Remettre la carte en ligne :

```
node run -node node_name storage enable adapter adapter_port
```

Afficher les paramètres de la carte

Vous pouvez utiliser des commandes spécifiques pour afficher des informations sur vos adaptateurs FC/UTA.

Adaptateur FC cible

Étape

1. Utilisez le `network fcp adapter show` commande permettant d'afficher les informations relatives à l'adaptateur : `network fcp adapter show -instance -node node1 -adapter 0a`

Le résultat de cette commande affiche des informations de configuration du système et des informations sur l'adaptateur pour chaque slot utilisé.

Adaptateur « Unified Target » (UTA) X1143A-R6

Étapes

1. Démarrez votre contrôleur sans les câbles connectés.
2. Exécutez le `system hardware unified-connect show` commande pour afficher la configuration des ports et les modules.
3. Afficher les informations relatives aux ports avant de configurer le CNA et les ports.

Remplacez le port UTA2 du mode CNA par le mode FC

Vous devez modifier le port UTA2 entre le mode CNA (Converged Network adapter) et le mode FC (Fibre Channel) pour prendre en charge l'initiateur FC et le mode cible FC. Vous devez modifier la personnalité du mode CNA en mode FC lorsque vous devez modifier le support physique qui connecte le port à son réseau.

Étapes

1. Mettez l'adaptateur hors ligne :


```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
down
```

2. Modifiez le mode des ports :

```
ucadmin modify -node node_name -adapter adapter_name -mode fcp
```

3. Redémarrez le nœud, puis mettez l'adaptateur en ligne :

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
up
```

4. Informez votre administrateur ou votre gestionnaire vif de supprimer ou de supprimer le port, le cas échéant :

- Si le port est utilisé en tant que port d'origine d'une LIF, est membre d'un groupe d'interface (ifgrp), ou des VLAN hôtes, un administrateur doit faire ce qui suit :
 - i. Déplacez les LIF, retirez le port du ifgrp ou supprimez les VLAN.
 - ii. Supprimez manuellement le port en exécutant le `network port delete` commande.

Si le `network port delete` échec de la commande, l'administrateur doit corriger les erreurs, puis exécuter de nouveau la commande.

- Si le port n'est pas utilisé comme port de base d'une LIF, n'est pas membre d'un ifgrp. Il ne héberge pas les VLAN, alors le vif Manager doit supprimer le port de ses enregistrements au moment du redémarrage.

Si le vif Manager ne supprime pas le port, l'administrateur doit le supprimer manuellement après le redémarrage à l'aide du `network port delete` commande.

```
net-f8040-34::> network port show
```

```
Node: net-f8040-34-01
```

Port	IPspace	Broadcast	Domain	Link	MTU	Speed (Mbps) Admin/Oper	Health Status
...							
e0i	Default	Default		down	1500	auto/10	-
e0f	Default	Default		down	1500	auto/10	-
...							

```
net-f8040-34::> ucadmin show
```

Admin	Current	Current	Pending	Pending
Node	Adapter	Mode	Type	Type
Status				
-----	-----	-----	-----	-----

```

net-f8040-34-01  0e      cna      target  -      -
offline
net-f8040-34-01  0f      cna      target  -      -
offline
...

net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0

net-f8040-34::> network interface show -fields home-port, curr-port

vserver lif                               home-port curr-port
-----
Cluster net-f8040-34-01_clus1 e0a          e0a
Cluster net-f8040-34-01_clus2 e0b          e0b
Cluster net-f8040-34-01_clus3 e0c          e0c
Cluster net-f8040-34-01_clus4 e0d          e0d
net-f8040-34
      cluster_mgmt          e0M          e0M
net-f8040-34
      m                      e0e          e0i
net-f8040-34
      net-f8040-34-01_mgmt1 e0M          e0M
7 entries were displayed.

net-f8040-34::> uadmin modify local 0e fc

Warning: Mode on adapter 0e and also adapter 0f will be changed to
fc.
Do you want to continue? {y|n}: y
Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

net-f8040-34::> reboot local
(system node reboot)

Warning: Are you sure you want to reboot node "net-f8040-34-01"?
{y|n}: y

```

5. Vérifiez que le SFP+ est installé correctement :

```
network fcp adapter show -instance -node -adapter
```

Pour le CNA, vous devez utiliser un SFP Ethernet 10 Gbit. Pour ce faire, vous devez utiliser un SFP 8 Gbit

ou un SFP 16 Gbit avant de modifier la configuration sur le nœud.

Modifiez les modules optiques des adaptateurs CNA/UTA2

Vous devez modifier les modules optiques de l'adaptateur cible unifié (CNA/UTA2) pour prendre en charge le mode de personnalisation sélectionné pour l'adaptateur.

Étapes

1. Vérifiez le SFP+ actuel utilisé dans la carte. Ensuite, remplacez le SFP+ actuel par le SFP+ approprié pour la personnalité préférée (FC ou CNA).
2. Retirez les modules optiques actuels de l'adaptateur X1143A-R6.
3. Insérez les modules appropriés pour l'optique de votre mode de personnalisation préféré (FC ou CNA).
4. Vérifiez que le SFP+ est installé correctement :

```
network fcp adapter show -instance -node -adapter
```

Les modules SFP+ et les câbles cuivre (Twinax) de marque Cisco sont répertoriés dans le *Hardware Universe*.

Informations associées

["NetApp Hardware Universe"](#)

Configurations de ports prises en charge pour les adaptateurs X1143A-R6

Le mode FC target est la configuration par défaut pour les ports d'adaptateur X1143A-R6. Cependant, les ports de cet adaptateur peuvent être configurés en tant que ports Ethernet 10 Gb et FCoE ou en tant que ports FC 16 Gb.

Lorsqu'ils sont configurés pour Ethernet et FCoE, les adaptateurs X1143A-R6 prennent en charge le trafic cible FCoE et les cartes réseau simultanés sur le même port 10 GBE. Lorsqu'elle est configurée pour FC, chaque paire à deux ports qui partage le même ASIC peut être configurée individuellement pour le mode FC cible ou initiateur FC. Cela signifie qu'un seul adaptateur X1143A-R6 peut prendre en charge le mode cible FC sur une paire à deux ports et le mode initiateur FC sur une autre paire à deux ports.

Informations associées

["NetApp Hardware Universe"](#)

["Configuration SAN"](#)

Configurez les ports

Pour configurer l'adaptateur cible unifié (X1143A-R6), vous devez configurer les deux ports adjacents sur la même puce dans le même mode de personnalisation.

Étapes

1. Configurez les ports selon vos besoins pour Fibre Channel (FC) ou CNA (Converged Network adapter) à l'aide du `system node hardware unified-connect modify` commande.
2. Connectez les câbles appropriés pour FC ou Ethernet 10 Gbit.
3. Vérifiez que le SFP+ est installé correctement :

```
network fcp adapter show -instance -node -adapter
```

Pour le CNA, vous devez utiliser un SFP Ethernet 10 Gbit. Pour ce faire, vous devez utiliser un SFP 8 Gbit ou un SFP 16 Gbit, selon la structure FC à laquelle vous êtes connecté.

Prévention des pertes de connectivité avec l'adaptateur X1133A-R6

Vous pouvez éviter la perte de connectivité lors d'une défaillance de port en configurant votre système avec des chemins redondants vers des HBA X1133A-R6 distincts.

La carte HBA X1133A-R6 est un adaptateur FC 16 Gbit à 4 ports composé de deux paires à 2 ports. L'adaptateur X1133A-R6 peut être configuré en mode cible ou initiateur. Chaque paire de 2 ports est prise en charge par un seul ASIC (par exemple, les ports 1 et 2 sur ASIC 1 et les ports 3 et 4 sur ASIC 2). Les deux ports d'un ASIC unique doivent être configurés pour fonctionner dans le même mode, soit en mode cible, soit en mode initiateur. En cas d'erreur sur l'ASIC prenant en charge une paire, les deux ports de la paire sont mis hors ligne.

Pour éviter ce risque de perte de connectivité, vous devez configurer votre système avec des chemins redondants vers des HBA X1133A-R6 distincts, ou avec des chemins redondants vers des ports pris en charge par différents ASIC sur le HBA.

Gérez les LIF de tous les protocoles SAN

Gérez les LIF de tous les protocoles SAN

Les initiateurs doivent utiliser les options MPIO (Multi Path I/O) et ALUA (Asymmetric Logical Unit Access) pour la capacité de basculement des clusters dans un environnement SAN. Si un nœud tombe en panne, les LIFs ne migrent pas et ne partent pas des adresses IP du nœud partenaire défaillant. À la place, le logiciel MPIO, avec ALUA sur l'hôte, est chargé de sélectionner les chemins d'accès appropriés pour les LUN via les LIF.

Vous devez créer un ou plusieurs chemins iSCSI depuis chaque nœud d'une paire haute disponibilité à l'aide des interfaces logiques (LIF) pour permettre l'accès aux LUN qui sont gérés par la paire haute disponibilité. Il est recommandé de configurer une LIF de gestion pour chaque SVM prenant en charge SAN.

La connexion directe ou l'utilisation de commutateurs Ethernet sont prises en charge pour la connectivité. Vous devez créer des LIF pour les deux types de connectivité.

- Il est recommandé de configurer une LIF de gestion pour chaque SVM prenant en charge SAN. Vous pouvez configurer deux LIF par nœud, un pour chaque structure utilisée avec FC et plusieurs réseaux Ethernet pour iSCSI.

Une fois les LIF créées, elles peuvent être supprimées des jeux de ports, déplacées vers différents nœuds d'une machine virtuelle de stockage (SVM), et supprimées.

Informations associées

- ["Configurer les LIFs erveiw"](#)
- ["Créer une LIF"](#)

Configurez une LIF NVMe

Lors de la configuration des LIFs NVMe, certaines exigences doivent être respectées.

Avant de commencer

NVMe doit être pris en charge par l'adaptateur FC sur lequel vous créez la LIF. Les cartes prises en charge sont répertoriées dans le "[Hardware Universe](#)".

Description de la tâche

À partir de ONTAP 9.12.1 et versions ultérieures, vous pouvez configurer deux LIF NVMe par nœud sur un maximum de 12 nœuds. Dans ONTAP 9.11.1 et les versions antérieures, vous pouvez configurer deux LIF NVMe par nœud sur un maximum de deux nœuds.

Les règles suivantes s'appliquent lors de la création d'une LIF NVMe :

- NVMe peut être le seul protocole de données sur les LIF de données.
- Vous devez configurer une LIF de gestion pour chaque SVM qui prend en charge SAN.
- Pour ONTAP 9.5 et versions ultérieures, vous devez configurer une LIF NVMe sur le nœud contenant le namespace et sur le partenaire HA du nœud.
- Pour ONTAP 9.4 uniquement :
 - Les LIFs et namespaces NVMe doivent être hébergés sur le même nœud.
 - Une seule LIF de données NVMe peut être configurée par SVM.

Étapes

1. Créer le LIF :

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role  
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>  
-home-port <home_port>
```



NVME/TCP est disponible à partir de ONTAP 9.10.1 et versions ultérieures.

2. Vérifier que le LIF a été créé :

```
network interface show -vserver <SVM_name>
```

Après sa création, les LIF NVMe/TCP écoutent la découverte sur le port 8009.

Que savoir avant de déplacer une LIF SAN

Vous n'avez besoin d'effectuer un déplacement de LIF que si vous modifiez le contenu du cluster, par exemple : ajout de nœuds au cluster ou suppression de nœuds. Si vous effectuez un déplacement LIF, vous n'avez pas besoin de remettre votre structure FC ou de créer de nouvelles sessions iSCSI entre les hôtes connectés de votre cluster et la nouvelle interface cible.

Vous ne pouvez pas déplacer une LIF SAN à l'aide de `network interface move` commande. Le déplacement de la LIF SAN doit être effectué en mettant la LIF hors ligne, en la déplaçant vers un autre nœud ou port de rattachement, puis en la remettant en ligne sur son nouvel emplacement. L'ALUA (Asymmetric Logical Unit Access) offre des chemins redondants et une sélection de chemin automatique dans le cadre de n'importe quelle solution SAN de ONTAP. Par conséquent, il n'y a pas d'interruption d'E/S lorsque la LIF est mise hors ligne pour le déplacement. L'hôte tente simplement de retraiter et déplace les E/S vers un autre LIF.

Grâce au déplacement de LIF, vous pouvez effectuer les opérations suivantes sans interruption :

- Remplacez une paire haute disponibilité d'un cluster par une paire haute disponibilité mise à niveau de manière transparente pour les hôtes qui accèdent aux données de la LUN
- Mettre à niveau une carte d'interface cible
- Transfert des ressources d'un serveur virtuel de stockage (SVM) d'un ensemble de nœuds d'un cluster vers un autre ensemble de nœuds du cluster

Supprimer une LIF SAN d'un port set

Si la LIF que vous souhaitez supprimer ou déplacer se trouve dans un port set, vous devez supprimer la LIF du port set avant de pouvoir supprimer ou déplacer la LIF.

Description de la tâche

Vous n'avez à effectuer l'étape 1 que si une LIF est dans le port set. Vous ne pouvez pas supprimer la dernière LIF d'un port défini si l'ensemble de ports est lié à un groupe initiateur. Sinon, vous pouvez commencer par l'étape 2 si plusieurs LIF se trouvent dans le port défini.

Étapes

1. Si un seul LIF est dans le port set, utilisez le `lun igroup unbind` commande permettant de dissocier le port défini sur le groupe initiateur.



Lorsque vous annulez la liaison d'un groupe initiateur à un ensemble de ports, tous les initiateurs du groupe initiateur ont accès à toutes les LUN cibles mappées sur le groupe initiateur sur toutes les interfaces réseau.

```
cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
```

2. Utilisez le `lun portset remove` Commande de supprimer le LIF du port set.

```
cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
```

Déplacer une LIF SAN

Si un nœud doit être mis hors ligne, vous pouvez déplacer une LIF SAN afin de préserver ses informations de configuration, telles que son WWPN, et éviter de resegmentation de la structure du commutateur. Comme une LIF SAN doit être mise hors ligne avant de pouvoir être déplacée, le trafic hôte doit utiliser un logiciel de chemins d'accès multiples sur l'hôte pour assurer un accès sans interruption à la LUN. Vous pouvez déplacer des LIF SAN vers n'importe quel nœud d'un cluster, mais vous ne pouvez pas déplacer ces LIF entre des SVM (Storage Virtual machine).

Ce dont vous avez besoin

Si le LIF est membre d'un port set, il faut que la LIF ait été supprimée du port set avant de pouvoir déplacer la LIF vers un autre nœud.

Description de la tâche

Le nœud de destination et le port physique d'une LIF que vous souhaitez déplacer doivent se trouver sur la même structure FC ou sur un même réseau Ethernet. Si vous déplacez une LIF vers une autre structure qui n'a pas été correctement zonée ou si vous déplacez la LIF vers un réseau Ethernet qui n'a pas de connectivité entre l'initiateur iSCSI et la cible, la LUN sera inaccessible lorsque vous la remettez en ligne.

Étapes

1. Afficher le statut administratif et opérationnel de la LIF :

```
network interface show -vserver vservice_name
```

2. Modifiez le statut de la LIF en down (hors ligne) :

```
network interface modify -vserver vservice_name -lif LIF_name -status-admin  
down
```

3. Assigner le LIF à un nouveau nœud et port :

```
network interface modify -vserver vservice_name -lif LIF_name -home-node  
node_name -home-port port_name
```

4. Modifiez le statut de la LIF en up (en ligne) :

```
network interface modify -vserver vservice_name -lif LIF_name -status-admin up
```

5. Vérifiez les modifications :

```
network interface show -vserver vservice_name
```

Supprimez une LIF dans un environnement SAN

Avant de supprimer une LIF, assurez-vous que l'hôte connecté à la LIF peut accéder aux LUN via un autre chemin.


Ce dont vous avez besoin

Si la LIF que vous souhaitez supprimer est membre d'un port set, vous devez d'abord supprimer cette LIF du port set avant de pouvoir supprimer la LIF.

System Manager

Supprimez une LIF avec ONTAP System Manager (9.7 et versions ultérieures).

Étapes

1. Dans System Manager, cliquez sur **réseau > Présentation**, puis sélectionnez **interfaces réseau**.
2. Sélectionnez la VM de stockage dont vous souhaitez supprimer la LIF.
3. Cliquez sur  et sélectionnez **Supprimer**.

CLI

Suppression d'une LIF via l'interface de ligne de commandes de ONTAP

Étapes

1. Vérifier le nom de la LIF et le port actuel à supprimer :

```
network interface show -vserver vs1
```

2. Supprimez le LIF :

```
network interface delete
```

```
network interface delete -vserver vs1 -lif lif1
```

3. Vérifier que vous avez supprimé la LIF :

```
network interface show
```

```
network interface show -vserver vs1
```

Logical Status	Network	Current	Current Is
Vserver Interface	Admin/Oper	Address/Mask	Node Port
Home			
-----	-----	-----	-----
vs1			
lif2	up/up	192.168.2.72/24	node-01 e0b
true			
lif3	up/up	192.168.2.73/24	node-01 e0b
true			

Conditions requises POUR l'ajout de nœuds à un cluster VIA SAN LIF

Lors de l'ajout de nœuds à un cluster, vous devez tenir compte de certaines considérations.

- Vous devez créer des LIF sur les nouveaux nœuds si nécessaire avant de créer des LUN sur ces nouveaux nœuds.

- Vous devez découvrir ces LIF depuis les hôtes, selon la pile hôte et le protocole.
- Vous devez créer des LIF sur les nouveaux nœuds afin que les mouvements de LUN et de volumes soient possibles sans utiliser le réseau d'interconnexion des clusters.

Configurer les LIF iSCSI pour renvoyer le FQDN à l'hôte iSCSI SendTargets Discovery Operation

Depuis ONTAP 9, les LIF iSCSI peuvent être configurées de façon à renvoyer un nom de domaine complet (FQDN) lorsqu'un OS hôte envoie une opération de découverte iSCSI SendTargets. Le retour d'un FQDN est utile lorsqu'il existe un périphérique NAT (Network Address Translation) entre le système d'exploitation hôte et le service de stockage.

Description de la tâche

Les adresses IP d'un côté du périphérique NAT n'ont aucun sens de l'autre côté, mais les FQDN peuvent avoir une signification des deux côtés.



La limite d'interopérabilité de la valeur FQDN est de 128 caractères sur tous les se hôtes.

Étapes

1. Modifiez le paramètre de privilège sur avancé :

```
set -privilege advanced
```

2. Configurer les LIF iSCSI pour renvoyer un FQDN :

```
vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name  
-sendtargets_fqdn FQDN
```

Dans l'exemple suivant, les LIFs iSCSI sont configurées de renvoyer storagehost-005.example.com en tant que FQDN.

```
vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn  
storagehost-005.example.com
```

3. Vérifiez que sendTargets est le FQDN :

```
vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
```

Dans cet exemple, storagehost-005.example.com s'affiche dans le champ de sortie sendTargets-fqdn.

```
cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields  
sendtargets-fqdn  
vserver lif          sendtargets-fqdn  
-----  
vs1      vs1_iscsi1  storagehost-005.example.com  
vs1      vs1_iscsi2  storagehost-006.example.com
```

Informations associées

["Référence de commande ONTAP"](#)

Combinaisons de configuration de volumes et de fichiers ou de LUN recommandées

Présentation des combinaisons de configuration de volumes et fichiers ou LUN recommandées

Il existe des combinaisons spécifiques de configurations de volumes et fichiers FlexVol ou LUN qui peuvent être utilisées, en fonction des exigences de l'application et de l'administration. Connaître les avantages et les coûts de ces combinaisons vous aidera à déterminer la combinaison volume-LUN qui convient à votre environnement.

Les combinaisons de configuration de volume et de LUN suivantes sont recommandées :

- Fichiers ou LUN réservés en espace avec provisionnement d'un volume lourd
- Fichiers ou LUN non réservés en espace avec le provisionnement fin du volume
- Fichiers ou LUN réservés en espace avec provisionnement de volumes semi-lourds

Vous pouvez utiliser le provisionnement fin SCSI sur vos LUN en association avec l'une de ces combinaisons de configuration.

Fichiers ou LUN réservés en espace avec provisionnement d'un volume lourd

Avantages :

- Toutes les opérations d'écriture dans les fichiers réservés à l'espace sont garanties ; elles ne échoueront pas en raison de l'espace insuffisant.
- Les technologies d'efficacité du stockage et de protection des données présentes sur le volume ne sont pas soumises à restrictions.

Coûts et limitations:

- L'espace doit être suffisant en dehors de l'agrégat pour prendre en charge le volume bénéficiant du provisionnement.
- Un espace égal à deux fois la taille de la LUN est alloué au volume au moment de sa création.

Fichiers ou LUN non réservés en espace avec le provisionnement fin du volume

Avantages :

- Les technologies d'efficacité du stockage et de protection des données présentes sur le volume ne sont pas soumises à restrictions.
- L'espace est alloué uniquement lorsqu'il est utilisé.

Coûts et restrictions:

- Les opérations d'écriture ne sont pas garanties ; elles peuvent échouer si le volume vient à manquer d'espace.
- Vous devez gérer efficacement l'espace libre dans l'agrégat pour empêcher ce dernier de manquer d'espace.

Avantages :

L'espace réservé est inférieur à celui du provisionnement d'un volume non lourd et la garantie d'écriture optimale est toujours fournie.

Coûts et restrictions:

- Cette option permet d'échouer les opérations d'écriture.

Vous pouvez réduire ce risque en équilibrant correctement l'espace libre du volume par rapport à la volatilité des données.

- Vous ne pouvez pas compter sur la conservation des objets de protection des données tels que les copies Snapshot, les fichiers FlexClone et les LUN.
- Vous ne pouvez pas utiliser les fonctionnalités ONTAP d'efficacité du stockage de partage de blocs qui ne peuvent pas être supprimées automatiquement, notamment la déduplication, la compression et ODX/déchargement des copies.

Déterminez la combinaison de configuration de volume et de LUN adaptée à votre environnement

En répondant à quelques questions de base sur votre environnement, vous pourrez déterminer la meilleure configuration de volumes FlexVol et de LUN pour votre environnement.

Description de la tâche

Vous pouvez optimiser les configurations des LUN et des volumes pour optimiser l'utilisation du stockage ou pour garantir la sécurité de l'écriture. En fonction de vos besoins en matière d'utilisation du stockage et de votre capacité à surveiller et à assurer la capacité des stocks disponibles rapidement, vous devez déterminer le volume FlexVol et les volumes LUN appropriés à votre installation.



Aucun volume n'est nécessaire pour chaque LUN.

Étape

1. Utilisez l'arbre de décision suivant pour déterminer la meilleure combinaison de configuration de volumes et de LUN pour votre environnement :



Calculer le taux de croissance des données pour les LUN

Vous devez connaître la vitesse de croissance de vos données LUN afin de déterminer si vous devez utiliser des LUN réservées à l'espace ou des LUN non réservées à l'espace.

Description de la tâche

Si vous taux de croissance des données régulièrement élevé, les LUN réservées à l'espace pourraient vous constituer une meilleure option. Si vous taux de croissance des données est faible, vous devez envisager des LUN non réservées aux espaces.

Vous pouvez utiliser des outils tels que OnCommand Insight pour calculer le taux de croissance de vos données ou le calculer manuellement. Les étapes suivantes concernent le calcul manuel.

Étapes

1. Configurez une LUN Space-Reserved.
2. Surveillez les données de la LUN pendant une période définie, par exemple une semaine.

Assurez-vous que votre période de surveillance est suffisamment longue pour former un échantillon représentatif des augmentations régulières de la croissance des données. Par exemple, vous pourriez avoir une forte croissance du volume des données de manière cohérente à la fin de chaque mois.

3. Chaque jour, enregistrez en Go la croissance de vos données.
4. À la fin de votre période de surveillance, additionnez les totaux pour chaque jour, puis divisez par le nombre de jours de votre période de surveillance.

Ce calcul produit votre taux de croissance moyen.

Exemple

Dans cet exemple, vous avez besoin d'une LUN de 200 Go. Vous décidez de contrôler le LUN pendant une semaine et d'enregistrer les modifications quotidiennes suivantes :

- Dimanche : 20 Go
- Lundi: 18 GB
- Mardi: 17 GB
- Mercredi: 20 GB
- Jeudi: 20 GB
- Vendredi : 23 GB
- Samedi: 22 GB

Dans cet exemple, votre taux de croissance est de $(20+18+17+20+20+23+22) / 7 = 20$ Go par jour.

Paramètres de configuration pour les fichiers réservés en espace ou les LUN avec des volumes à provisionnement lourd

La combinaison de configuration de volume et fichier FlexVol/LUN vous permet d'utiliser des technologies d'efficacité du stockage et ne vous demande pas de surveiller activement votre espace libre, car l'espace est alloué en amont.

Les paramètres suivants sont nécessaires pour configurer un fichier ou une LUN réservé à l'espace dans un volume à l'aide du provisionnement Thick :

Réglage du volume	Valeur
Résultats garantis	Volumétrie
Réserve fractionnaire	100
Réserve Snapshot	Toutes
Suppression automatique de l'instantané	Facultatif
Croissance automatique	Facultatif. Si cette option est activée, l'espace libre de l'agrégat doit être activement surveillé.

Paramètre fichier ou LUN	Valeur
Réservation d'espace	Activé

Paramètres de configuration pour les fichiers ou LUN non réservés en espace avec des volumes à provisionnement fin

Cette combinaison de configuration de volumes et de fichiers FlexVol ou de LUN requiert la réduction de la quantité de stockage allouée à l'avance, mais elle exige une gestion de l'espace libre actif pour éviter les erreurs liées au manque d'espace.

Les paramètres suivants sont requis pour configurer un LUN ou des fichiers non réservés en espace dans un volume à provisionnement fin :

Réglage du volume	Valeur
Résultats garantis	Aucune
Réserve fractionnaire	0
Réserve Snapshot	Toutes
Suppression automatique de l'instantané	Facultatif
Croissance automatique	Facultatif

Paramètre fichier ou LUN	Valeur
Réservation d'espace	Désactivé

Autres considérations

Lorsque l'espace est insuffisant pour le volume ou l'agrégat, les opérations d'écriture sur le fichier ou la LUN peuvent échouer.

Pour ne pas contrôler activement l'espace disponible pour le volume et l'agrégat, vous devez activer la croissance automatique du volume et définir la taille maximale du volume sur la taille de l'agrégat. Dans cette configuration, vous devez surveiller activement l'espace libre des agrégats, mais il n'est pas nécessaire de surveiller l'espace libre dans le volume.

Paramètres de configuration pour les fichiers réservés en espace ou les LUN avec provisionnement de volumes semi-lourds

Cette combinaison de configuration de volumes et de fichiers FlexVol ou de LUN requiert moins de stockage que la combinaison entièrement provisionnée, mais impose des restrictions sur les technologies d'efficacité que vous pouvez utiliser pour ce volume. Les écrasements sont effectués par le meilleur effort pour cette combinaison de configuration.

Les paramètres suivants sont nécessaires pour configurer une LUN Space-Reserved dans un volume à l'aide du provisionnement semi-thick :

Réglage du volume	Valeur
Résultats garantis	Volumétrie
Réserve fractionnaire	0
Réserve Snapshot	0

Réglage du volume	Valeur
Suppression automatique de l'instantané	On, avec un niveau d'engagement de destruction, une liste de destruction qui inclut tous les objets, le déclencheur défini sur volume, ainsi que toutes les LUN FlexClone et tous les fichiers FlexClone activés pour la suppression automatique.
Croissance automatique	Facultatif. Si cette option est activée, l'espace libre de l'agrégat doit être activement surveillé.

Paramètre fichier ou LUN	Valeur
Réservation d'espace	Activé

Restrictions technologiques

Pour cette combinaison de configuration, vous ne pouvez pas utiliser les technologies suivantes d'efficacité du stockage de volumes :

- Compression
- Déduplication
- ODX et allègement de la charge des copies FlexClone
- LUN FlexClone et fichiers FlexClone non marqués pour la suppression automatique (clones actifs)
- Sous-fichiers FlexClone
- ODX/allègement de la charge des copies

Autres considérations

Lors de l'utilisation de cette combinaison de configuration, vous devez tenir compte des éléments suivants :

- Lorsque le volume prenant en charge cette LUN fonctionne peu d'espace, les données de protection (LUN et fichiers FlexClone, copies Snapshot) sont détruites.
- Les opérations d'écriture peuvent entraîner un temps d'attente et l'échec lorsque l'espace disponible est insuffisant.

Par défaut, la compression est activée pour les plateformes AFF. Vous devez désactiver explicitement la compression pour tout volume pour lequel vous souhaitez utiliser un provisionnement semi-lourd sur une plateforme AFF.

Protection des données SAN

Présentation des méthodes de protection des données dans les environnements SAN

Vous pouvez protéger vos données en les faisant des copies afin qu'elles soient disponibles à des fins de restauration en cas de suppression accidentelle, de panne d'application, de corruption des données ou d'incident. Selon vos besoins en termes de

protection et de sauvegarde des données, ONTAP propose plusieurs méthodes pour protéger vos données.

Synchronisation active SnapMirror

Depuis la disponibilité générale de ONTAP 9.9.1, assure un délai de restauration nul ou un basculement transparent des applications (TAF) pour permettre le basculement automatique des applications stratégiques dans les environnements SAN. La synchronisation active SnapMirror nécessite l'installation du logiciel ONTAP Mediator 1.2 dans une configuration comprenant deux clusters AFF ou deux clusters ASA.

"Synchronisation active SnapMirror"

La copie Snapshot

Vous permet de créer, de planifier et de gérer plusieurs sauvegardes de vos LUN manuellement ou automatiquement. Les copies Snapshot n'utilisent qu'une quantité minimale d'espace supplémentaire sur le volume et ne présentent pas de coûts de performances. Si vos données de la LUN sont accidentellement modifiées ou supprimées, elles peuvent être restaurées facilement et rapidement à partir de l'une des dernières copies Snapshot.

LUN FlexClone (licence FlexClone requise)

Réalisation de copies inscriptibles instantanées d'une autre LUN dans un volume actif ou dans une copie Snapshot Un clone et son parent peuvent être modifiés de façon indépendante sans affecter les autres

SnapRestore (licence requise)

Permet de restaurer rapidement des données à la demande, sans utiliser d'espace et avec des copies Snapshot sur un volume entier. Vous pouvez utiliser SnapRestore pour restaurer une LUN à un état conservé antérieur sans redémarrer le système de stockage.

Copies miroir de protection des données (licence SnapMirror requise)

Offre une reprise après incident asynchrone en vous permettant de créer régulièrement des copies Snapshot des données sur votre volume, de les copier sur un réseau local ou étendu vers un volume partenaire, généralement sur un autre cluster, et de conserver ces copies Snapshot. La copie miroir du volume partenaire assure une disponibilité et une restauration rapides des données à partir de la dernière copie Snapshot, en cas de corruption ou de perte des données du volume source.

Sauvegardes SnapVault (licence SnapMirror requise)

Permet un stockage efficace et une conservation à long terme des sauvegardes. Les relations SnapVault vous permettent de sauvegarder des copies Snapshot de volumes sélectionnées sur un volume de destination et de conserver les sauvegardes.

Si vous réalisez des sauvegardes sur bande et des opérations d'archivage, vous pouvez les effectuer sur les données déjà sauvegardées sur le volume secondaire de SnapVault.

SnapDrive pour Windows ou UNIX (licence SnapDrive requise)

Configure l'accès aux LUN, gère les LUN et gère les copies Snapshot du système de stockage directement à partir d'hôtes Windows ou UNIX.

Sauvegarde et restauration natives sur bande

La prise en charge de la plupart des lecteurs de bandes existants est incluse dans ONTAP, ainsi qu'une méthode permettant aux fournisseurs de bandes d'ajouter dynamiquement la prise en charge des nouveaux périphériques. ONTAP prend également en charge le protocole RMT (Remote Magnetic Tape), permettant ainsi une sauvegarde et une restauration vers tout système capable.

Informations associées

["Documentation NetApp : SnapDrive pour UNIX"](#)

["Documentation NetApp : SnapDrive pour Windows \(versions actuelles\)"](#)

["Protection des données par sauvegarde sur bandes"](#)

Effet du déplacement ou de la copie d'une LUN sur des copies Snapshot

Effets du déplacement ou de la copie d'une LUN sur des copies Snapshot

Les copies Snapshot sont créées au niveau du volume. Si vous copiez ou déplacez une LUN vers un autre volume, la règle de copie Snapshot de la LUN de destination est appliquée au volume copié ou déplacé. Si les copies Snapshot ne sont pas établies pour le volume de destination, les copies Snapshot ne sont pas créées pour la LUN déplacée ou copiée.

Restaurez une LUN unique à partir d'une copie Snapshot

Vous pouvez restaurer une seule LUN à partir d'une copie Snapshot sans restaurer l'intégralité du volume qui contient la même LUN. Vous pouvez restaurer la LUN sur place ou sur un nouveau chemin d'accès dans le volume. L'opération restaure uniquement la LUN sans affecter les autres fichiers ou LUN du volume. Vous pouvez également restaurer des fichiers avec des flux.

Ce dont vous avez besoin

- Vous devez disposer d'espace suffisant sur votre volume pour mener à bien l'opération de restauration :
 - Si vous restaurez une LUN réservée à l'espace où la réserve fractionnaire est 0 %, vous devez avoir une fois la taille de la LUN restaurée.
 - Si vous restaurez une LUN réservée à l'espace où la réserve fractionnaire est de 100 %, vous avez besoin de deux fois la taille de la LUN restaurée.
 - Si vous restaurez une LUN non réservée à l'espace, seul l'espace utilisé pour la LUN restaurée est nécessaire.
- Une copie Snapshot de la LUN de destination doit avoir été créée.

Si l'opération de restauration échoue, la LUN de destination peut être tronquée. Dans ce cas, vous pouvez utiliser la copie Snapshot pour éviter la perte de données.

- Une copie Snapshot de la LUN source doit avoir été créée.

Dans de rares cas, la restauration de LUN peut échouer, ce qui laisse la LUN source inutilisable. Le cas échéant, vous pouvez utiliser la copie Snapshot pour rétablir l'état de la LUN juste avant la tentative de restauration.

- La LUN de destination et la LUN source doivent avoir le même type de système d'exploitation.

Si votre LUN de destination possède un type de système d'exploitation différent de votre LUN source, votre hôte peut perdre l'accès aux données à la LUN de destination après l'opération de restauration.

Étapes

1. Depuis l'hôte, arrêtez l'ensemble de l'accès des hôtes au LUN.
2. Démontez la LUN sur son hôte de manière à ce que l'hôte ne puisse pas accéder à la LUN.
3. Annulez le mappage de la LUN :

```
lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

4. Déterminez la copie Snapshot que vous souhaitez restaurer votre LUN sur :

```
volume snapshot show -vserver vserver_name -volume volume_name
```

5. Créer une copie Snapshot de la LUN avant de restaurer celle-ci :

```
volume snapshot create -vserver vserver_name -volume volume_name -snapshot  
snapshot_name
```

6. Restaurer la LUN spécifiée dans un volume :

```
volume snapshot restore-file -vserver vserver_name -volume volume_name  
-snapshot snapshot_name -path lun_path
```

7. Suivez les étapes à l'écran.
8. Si nécessaire, mettre la LUN en ligne :

```
lun modify -vserver vserver_name -path lun_path -state online
```

9. Si nécessaire, remappage la LUN :

```
lun mapping create -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

10. Depuis l'hôte, remontez la LUN.
11. Depuis l'hôte, redémarrez l'accès au LUN.

Restaurez toutes les LUN d'un volume à partir d'une copie Snapshot

Vous pouvez utiliser `volume snapshot restore` Commande permettant de restaurer toutes les LUN d'un volume spécifié à partir d'une copie Snapshot.

Étapes

1. Depuis l'hôte, arrêtez l'ensemble de l'accès des hôtes aux LUN.

L'utilisation de SnapRestore sans interrompre tout accès des hôtes aux LUN du volume peut entraîner une corruption des données et des erreurs système.

2. Démontez les LUN de cet hôte, de sorte que l'hôte ne puisse pas accéder aux LUN.

3. Annulez le mappage de vos LUN :

```
lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

4. Déterminez la copie Snapshot vers laquelle vous souhaitez restaurer votre volume :

```
volume snapshot show -vserver vserver_name -volume volume_name
```

5. Définissez votre paramètre de privilège sur Avancé :

```
set -privilege advanced
```

6. Restaurez vos données :

```
volume snapshot restore -vserver vserver_name -volume volume_name -snapshot  
snapshot_name
```

7. Suivez les instructions à l'écran.

8. Remappage de vos LUN :

```
lun mapping create -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

9. Vérifiez que vos LUN sont en ligne :

```
lun show -vserver vserver_name -path lun_path -fields state
```

10. Si vos LUN ne sont pas en ligne, mettez-les en ligne :

```
lun modify -vserver vserver_name -path lun_path -state online
```

11. Modifiez votre paramètre de privilège sur admin :

```
set -privilege admin
```

12. A partir de l'hôte, remontez vos LUN.

13. Depuis l'hôte, redémarrez l'accès à vos LUN.

Supprime une ou plusieurs copies Snapshot existantes d'un volume

Vous pouvez supprimer manuellement une ou plusieurs copies Snapshot du volume. Pour ce faire, il vous faudra peut-être plus d'espace sur le volume.

Étapes

1. Utilisez le `volume snapshot show` Commande pour vérifier les copies Snapshot que vous souhaitez supprimer.

```
cluster::> volume snapshot show -vserver vs3 -volume vol3
```

Vserver	Volume	Snapshot	Size	---Blocks---	
				Total%	Used%
-----	-----	-----	-----	-----	-----
vs3	vol3	snap1.2013-05-01_0015	100KB	0%	38%
		snap1.2013-05-08_0015	76KB	0%	32%
		snap2.2013-05-09_0010	76KB	0%	32%
		snap2.2013-05-10_0010	76KB	0%	32%
		snap3.2013-05-10_1005	72KB	0%	31%
		snap3.2013-05-10_1105	72KB	0%	31%
		snap3.2013-05-10_1205	72KB	0%	31%
		snap3.2013-05-10_1305	72KB	0%	31%
		snap3.2013-05-10_1405	72KB	0%	31%
		snap3.2013-05-10_1505	72KB	0%	31%

10 entries were displayed.

2. Utilisez le `volume snapshot delete` Commande permettant de supprimer les copies Snapshot.

Les fonctions que vous recherchez...	Entrez cette commande...
Supprimez une seule copie Snapshot	<code>volume snapshot delete -vserver svm_name -volume vol_name -snapshot snapshot_name</code>
Supprimez plusieurs copies Snapshot	<code>volume snapshot delete -vserver svm_name -volume vol_name -snapshot snapshot_name1[, snapshot_name2,...]</code>
Supprimez toutes les copies Snapshot	<code>volume snapshot delete -vserver svm_name -volume vol_name -snapshot *</code>

L'exemple suivant illustre la suppression de toutes les copies Snapshot du volume vol3.

```
cluster::> volume snapshot delete -vserver vs3 -volume vol3 *
```

10 entries were acted on.

Utilisez les LUN FlexClone pour protéger vos données

Utilisez les LUN FlexClone pour protéger vos données

Un LUN FlexClone est une copie inscriptible instantanée d'un autre LUN dans un volume

actif ou dans une copie Snapshot. Le clone et son parent peuvent être modifiés de façon indépendante sans affecter les uns les autres.

Une LUN FlexClone partage initialement de l'espace avec la LUN parent. Par défaut, la LUN FlexClone hérite de l'attribut réservé d'espace de la LUN parent. Par exemple, si la LUN parent est non-réservée à l'espace, la LUN FlexClone est également non réservée à l'espace par défaut. Cependant, vous pouvez créer une LUN FlexClone non réservée à l'espace à partir d'un parent qui est une LUN réservée à l'espace.

Lorsque vous clonez une LUN, le partage de blocs a lieu en arrière-plan et vous ne pouvez pas créer de copie Snapshot d'un volume tant que le partage de blocs n'est pas terminé.

Vous devez configurer le volume pour activer la fonction de suppression automatique de LUN FlexClone avec `volume snapshot autodelete modify` commande. Sinon, si vous souhaitez que les LUN FlexClone soient supprimées automatiquement, mais que le volume n'est pas configuré pour la suppression automatique FlexClone, aucune des LUN FlexClone n'est supprimée.

Lorsque vous créez une LUN FlexClone, la fonction de suppression automatique de LUN FlexClone est désactivée par défaut. Vous devez l'activer manuellement sur chaque LUN FlexClone avant de pouvoir supprimer automatiquement cette LUN. Si vous utilisez le provisionnement de volumes semi-lourds et que vous souhaitez la garantie d'écriture « meilleur effort » fournie par cette option, vous devez mettre des LUN All FlexClone à disposition pour la suppression automatique.



Lorsque vous créez une LUN FlexClone à partir d'une copie Snapshot, celle-ci est automatiquement répartie entre cette copie Snapshot à l'aide du processus d'arrière-plan compact. Ainsi, la LUN ne continue pas à dépendre de la copie Snapshot ni à consommer de l'espace supplémentaire. Si ce fractionnement en arrière-plan n'a pas été terminé et que cette copie Snapshot est automatiquement supprimée, cette LUN FlexClone est supprimée, même si vous avez désactivé la fonction de suppression automatique FlexClone pour cette LUN. Une fois le fractionnement en arrière-plan terminé, la LUN FlexClone n'est pas supprimée, même si cette copie Snapshot est supprimée.

Informations associées

["Gestion du stockage logique"](#)

Motifs d'utilisation des LUN FlexClone

Vous pouvez utiliser des LUN FlexClone pour créer plusieurs copies en lecture/écriture d'une LUN.

Vous pouvez vouloir le faire pour les raisons suivantes :

- Vous devez créer une copie temporaire d'une LUN afin d'y effectuer des tests.
- Vous devez mettre une copie de vos données à la disposition d'autres utilisateurs sans pour autant avoir accès aux données de production.
- Vous souhaitez créer un clone de base de données pour les opérations de manipulation et de projection, tout en préservant les données d'origine sous une forme non modifiée.
- Vous souhaitez accéder à un sous-ensemble spécifique des données d'une LUN (un volume logique ou un système de fichiers spécifique dans un groupe de volumes, Ou un fichier spécifique ou un ensemble de fichiers dans un système de fichiers) et copiez-le dans la LUN d'origine, sans restaurer le reste des données de la LUN d'origine. Ce fonctionnement fonctionne sur les systèmes d'exploitation qui prennent en charge le montage simultané d'une LUN et d'un clone de la LUN. SnapDrive pour UNIX en est capable avec le `snap connect` commande.

- Vous avez besoin de plusieurs hôtes de démarrage SAN avec le même système d'exploitation.

Comment un volume FlexVol peut récupérer de l'espace libre avec le paramètre de suppression automatique

Vous pouvez activer la suppression automatique d'un volume FlexVol pour supprimer automatiquement les fichiers FlexClone et les LUN FlexClone. En activant la suppression automatique, vous pouvez récupérer une quantité cible d'espace libre dans le volume lorsqu'un volume est presque plein.

Vous pouvez configurer un volume pour qu'il commence automatiquement la suppression des fichiers FlexClone et des LUN FlexClone lorsque l'espace libre du volume diminue en dessous d'un seuil particulier, et que l'espace disponible cible est récupéré lorsqu'une quantité d'espace libre dans le volume est arrêté automatiquement. Bien que vous ne puissiez pas spécifier la valeur de seuil au début de la suppression automatique de clones, vous pouvez spécifier si un clone peut être supprimé et vous pouvez spécifier la quantité cible d'espace libre d'un volume.

Un volume supprime automatiquement les fichiers FlexClone et les LUN FlexClone lorsque l'espace libre dans le volume diminue en dessous d'un seuil particulier et lorsque les *deux* des exigences suivantes sont remplies :

- La fonctionnalité de suppression automatique est activée pour le volume qui contient les fichiers FlexClone et les LUN FlexClone.

Vous pouvez activer la fonctionnalité de suppression automatique d'un volume FlexVol à l'aide du `volume snapshot autodelete modify` commande. Vous devez définir le `-trigger` paramètre à `volume` ou `snap_reserve` Pour qu'un volume supprime automatiquement les fichiers FlexClone et les LUN FlexClone.

- La fonctionnalité de suppression automatique est activée pour les fichiers FlexClone et les LUN FlexClone.

Vous pouvez activer la suppression automatique d'un fichier FlexClone ou d'une LUN FlexClone à l'aide du `file clone create` commande avec `-autodelete` paramètre. Par conséquent, vous pouvez préserver certains fichiers FlexClone et certaines LUN FlexClone en désactivant la suppression automatique des clones et en vous assurant que les autres paramètres de volume ne prévalent pas sur le paramètre de clonage.

Configurer un volume FlexVol pour supprimer automatiquement les fichiers FlexClone et les LUN FlexClone

Vous pouvez activer un volume FlexVol pour supprimer automatiquement les fichiers FlexClone et les LUN FlexClone avec la suppression automatique activée lorsque l'espace libre dans le volume diminue en dessous d'un seuil particulier.

Ce dont vous avez besoin

- Le volume FlexVol doit contenir des fichiers FlexClone et des LUN FlexClone, et doit être en ligne.
- Le volume FlexVol ne doit pas être un volume en lecture seule.

Étapes

1. Activez la suppression automatique des fichiers FlexClone et des LUN FlexClone dans le volume FlexVol à l'aide de la `volume snapshot autodelete modify` commande.

- Pour le `-trigger` vous pouvez spécifier un paramètre `volume` ou `snap_reserve`.
- Pour le `-destroy-list` paramètre, vous devez toujours spécifier `lun_clone`, `file_clone` que vous souhaitez supprimer un seul type de clone ou non.

L'exemple suivant montre comment activer la commande `volume vol1` pour déclencher la suppression automatique des fichiers FlexClone et des LUN FlexClone pour la récupération d'espace jusqu'à ce que 25 % du volume se compose d'espace libre :

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume
vol1 -enabled true -commitment disrupt -trigger volume -target-free
-space 25 -destroy-list lun_clone,file_clone
```

```
Volume modify successful on volume:vol1
```



Lors de l'activation des volumes FlexVol pour la suppression automatique, si vous définissez la valeur de `-commitment` paramètre à `destroy`, Tous les fichiers FlexClone et les LUN FlexClone avec `-autodelete` paramètre défini sur `true` il est possible de supprimer l'espace libre dans le volume lorsque la valeur de seuil spécifiée est inférieure à ce seuil. Mais, les fichiers FlexClone et les LUN FlexClone avec `-autodelete` paramètre défini sur `false` ne sera pas supprimé.

2. Vérifier que la suppression automatique des fichiers FlexClone et des LUN FlexClone est activée dans le volume FlexVol à l'aide de la `volume snapshot autodelete show` commande.

L'exemple suivant montre que le volume `vol1` est activé pour la suppression automatique des fichiers FlexClone et des LUN FlexClone :

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1
```

```
Vserver Name: vs1
Volume Name: vol1
Enabled: true
Commitment: disrupt
Defer Delete: user_created
Delete Order: oldest_first
Defer Delete Prefix: (not specified)*
Target Free Space: 25%
Trigger: volume
Destroy List: lun_clone,file_clone
Is Constituent Volume: false
```

3. Assurez-vous que la suppression automatique est activée pour les fichiers FlexClone et les LUN FlexClone dans le volume que vous souhaitez supprimer en effectuant les étapes suivantes :
 - a. Activez la suppression automatique d'un fichier FlexClone ou d'une LUN FlexClone spécifique à l'aide de `volume file clone autodelete` commande.

Vous pouvez forcer la suppression automatique d'un fichier FlexClone ou d'une LUN FlexClone spécifique à l'aide du `volume file clone autodelete` commande avec `-force` paramètre.

L'exemple suivant montre que la suppression automatique de la LUN FlexClone LUN1_clone contenue dans le volume vol1 est activée :

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path  
/vol/vol1/lun1_clone -enabled true
```

Vous pouvez activer la suppression automatique lors de la création de fichiers FlexClone et de LUN FlexClone.

- b. Vérifiez que le fichier FlexClone ou la LUN FlexClone est activé pour la suppression automatique à l'aide du `volume file clone show-autodelete` commande.

L'exemple suivant montre que la LUN FlexClone LUN1_clone est activée pour la suppression automatique :

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone  
-path vol/vol1/lun1_clone  
  
Name: vs1  
Path: vol/vol1/lun1_clone  
  
**Autodelete Enabled: true**
```

Pour plus d'informations sur l'utilisation des commandes, consultez les pages de manuels respectives.

Cloner des LUN à partir d'un volume actif

Vous pouvez créer des copies de vos LUN en clonant les LUN dans le volume actif. Ces LUN FlexClone sont des copies lisibles et inscriptibles des LUN d'origine dans le volume actif.

Ce dont vous avez besoin

Une licence FlexClone doit être installée. Cette licence est fournie avec ["ONTAP One"](#).

Description de la tâche

Une LUN FlexClone à espace réservé requiert autant d'espace que la LUN parent à espace réservé. Si la LUN FlexClone n'est pas réservée à l'espace, vous devez vous assurer que le volume dispose d'un espace suffisant pour les modifications apportées au LUN FlexClone.

Étapes

1. Vous devez avoir vérifié que les LUN ne sont pas mappées sur un groupe initiateur ou sont écrites sur avant de créer le clone.
2. Utilisez le `lun show` Commande pour vérifier que la LUN existe.


```
lun show -vserver vs1
```

Vserver	Path	State	Mapped	Type	Size
vs1	/vol/vol1/lun1	online	unmapped	windows	47.07MB

3. Utilisez le `volume file clone create` Commande permettant de créer la LUN FlexClone.

```
volume file clone create -vserver vs1 -volume vol1 -source-path lun1  
-destination-path/lun1_clone
```

Si le LUN FlexClone doit être disponible pour la suppression automatique, vous devez inclure `-autodelete true`. Si vous créez cette LUN FlexClone dans un volume avec provisionnement semi-lourd, vous devez activer la suppression automatique pour toutes les LUN FlexClone.

4. Utilisez le `lun show` Pour vérifier que vous avez créé une LUN.

```
lun show -vserver vs1
```

Vserver	Path	State	Mapped	Type	Size
vs1	/vol/volX/lun1	online	unmapped	windows	47.07MB
vs1	/vol/volX/lun1_clone	online	unmapped	windows	47.07MB

Créer des LUN FlexClone à partir d'une copie Snapshot d'un volume

Vous pouvez utiliser une copie Snapshot de votre volume pour créer des copies FlexClone de vos LUN. Les copies FlexClone des LUN sont à la fois lisibles et inscriptibles.

Ce dont vous avez besoin

Une licence FlexClone doit être installée. Cette licence est incluse avec ["ONTAP One"](#).

Description de la tâche

La LUN FlexClone hérite de l'attribut réservations d'espace de la LUN parent. Une LUN FlexClone à espace réservé requiert autant d'espace que la LUN parent à espace réservé. Si la LUN FlexClone n'est pas Space-Reserved, l'espace du volume doit être suffisant pour prendre en charge les modifications apportées au clone.

Étapes

1. Vérifiez que la LUN n'est pas mappée ou en cours d'écriture sur.
2. Créer une copie Snapshot du volume qui contient les LUN :

```
volume snapshot create -vserver vs1 -volume vol1 -snapshot  
snapshot_name
```

Vous devez créer une copie Snapshot (copie Snapshot de support) de la LUN à cloner.

3. Créer la LUN FlexClone à partir de la copie Snapshot :

```
file clone create -vserver vs1 -volume vol1 -source-path source_path -snapshot-name snapshot_name -destination-path destination_path
```

Si le LUN FlexClone doit être disponible pour la suppression automatique, vous devez inclure `-autodelete true`. Si vous créez cette LUN FlexClone dans un volume avec provisionnement semi-lourd, vous devez activer la suppression automatique pour toutes les LUN FlexClone.

4. Vérifiez que la LUN FlexClone est correcte :

```
lun show -vserver vs1
```

Vserver	Path	State	Mapped	Type	Size
vs1	/vol/vol1/lun1_clone	online	unmapped	windows	47.07MB
vs1	/vol/vol1/lun1_snap_clone	online	unmapped	windows	47.07MB

Empêchez la suppression automatique d'un fichier FlexClone ou d'une LUN FlexClone

Si vous configurez un volume FlexVol pour supprimer automatiquement les fichiers FlexClone et les LUN FlexClone, tout clone répondant aux critères spécifiés risque d'être supprimé. Si vous souhaitez préserver des fichiers FlexClone ou des LUN FlexClone spécifiques, vous pouvez les exclure du processus de suppression automatique de FlexClone.

Avant de commencer

Une licence FlexClone doit être installée. Cette licence est incluse avec ["ONTAP One"](#).

Description de la tâche

Lorsque vous créez un fichier FlexClone ou une LUN FlexClone, le paramètre de suppression automatique du clone est désactivé par défaut. Les fichiers FlexClone et les LUN FlexClone avec suppression automatique désactivée sont conservés lorsque vous configurez un volume FlexVol afin que vous puissiez supprimer automatiquement des clones pour récupérer de l'espace sur le volume.



Si vous définissez le `commitment` le niveau du volume vers `try` ou `disrupt`, Vous pouvez conserver individuellement des fichiers FlexClone ou des LUN FlexClone en désactivant la suppression automatique de ces clones. Cependant, si vous définissez le `commitment` le niveau du volume vers `destroy` et les listes de destruction incluent `lun_clone`, `file_clone`, Le paramètre de volume remplace le paramètre `clone`, et tous les fichiers FlexClone et LUN FlexClone peuvent être supprimés indépendamment du paramètre de suppression automatique des clones.

Étapes

1. Empêcher la suppression automatique d'un fichier FlexClone ou d'une LUN FlexClone spécifique à l'aide du système `volume file clone autodelete` commande.

L'exemple suivant montre comment désactiver la suppression automatique de la LUN FlexClone LUN1_clone contenue dans vol1 :

```
cluster1::> volume file clone autodelete -vserver vs1 -volume vol1  
-clone-path lun1_clone -enable false
```

Un fichier FlexClone ou une LUN FlexClone avec la suppression automatique désactivée ne peut pas être supprimé automatiquement pour récupérer de l'espace sur le volume.

2. Vérifiez que la suppression automatique est désactivée pour le fichier FlexClone ou le LUN FlexClone à l'aide du `volume file clone show-autodelete` commande.

L'exemple suivant montre que la suppression automatique est fausse pour la LUN FlexClone LUN1_clone :

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path  
vol/vol1/lun1_clone  
  
Name: vs1  
vol/vol1/lun1_clone  
Enabled: false  
  
Vserver  
Clone Path:  
Autodelete
```

Configuration et utilisation des sauvegardes SnapVault dans un environnement SAN

Configuration et utilisation des sauvegardes SnapVault dans un environnement SAN

La configuration et l'utilisation de SnapVault dans un environnement SAN sont très similaires à celles utilisées dans un environnement NAS. Toutefois, la restauration des LUN dans un environnement SAN nécessite des procédures spéciales.

Les sauvegardes SnapVault contiennent un ensemble de copies en lecture seule d'un volume source. Dans un environnement SAN, vous devez toujours sauvegarder des volumes entiers sur le volume secondaire SnapVault, et non sur des LUN individuelles.

La procédure de création et d'initialisation de la relation SnapVault entre un volume primaire contenant des LUN et un volume secondaire agissant comme sauvegarde SnapVault est identique à la procédure utilisée avec les volumes FlexVol utilisés pour les protocoles de fichiers. Cette procédure est décrite en détail dans ["La protection des données"](#).

Il est important de veiller à ce que les LUN sauvegardées soient dans un état cohérent avant de créer et de copier les copies Snapshot sur le volume secondaire SnapVault. Si la création de copie Snapshot est automatisée avec SnapCenter, les LUN sauvegardées sont complètes et utilisables par l'application d'origine.

Il existe trois options de base pour la restauration des LUN à partir d'un volume secondaire SnapVault :

- Vous pouvez mapper une LUN directement à partir du volume secondaire SnapVault et connecter un hôte au LUN pour accéder au contenu de la LUN.

La LUN est en lecture seule et vous ne pouvez mapper qu'à partir de la copie Snapshot la plus récente de

la sauvegarde SnapVault. Les réservations et autres métadonnées LUN sont perdues. Si vous le souhaitez, vous pouvez utiliser un programme de copie sur l'hôte pour copier le contenu de la LUN vers la LUN d'origine si celle-ci est toujours accessible.

Le numéro de série de la LUN source est différent de celui de la LUN source.

- Vous pouvez cloner n'importe quelle copie Snapshot du volume secondaire SnapVault sur un nouveau volume en lecture/écriture.

Vous pouvez ensuite mapper l'une des LUN du volume et connecter un hôte au LUN pour accéder au contenu de la LUN. Si vous le souhaitez, vous pouvez utiliser un programme de copie sur l'hôte pour copier le contenu de la LUN vers la LUN d'origine si celle-ci est toujours accessible.

- Vous pouvez restaurer la totalité du volume contenant la LUN à partir de n'importe quelle copie Snapshot du volume secondaire SnapVault.

La restauration du volume entier remplace toutes les LUN, ainsi que tous les fichiers, dans le volume. Toutes les nouvelles LUN créées depuis la création de la copie Snapshot sont perdues.

Les LUN conservent leur mappage, leur numéro de série, leurs UUID et leurs réservations permanentes.

Accédez à une copie LUN en lecture seule à partir d'une sauvegarde SnapVault

Vous pouvez accéder à une copie en lecture seule d'une LUN à partir de la dernière copie Snapshot d'une sauvegarde SnapVault. L'ID, le chemin et le numéro de série de la LUN source sont différents de celui-ci et doivent d'abord être mappés. Les réservations permanentes, les mappages de LUN et les groupes initiateurs ne sont pas répliqués sur le volume secondaire SnapVault.

Ce dont vous avez besoin

- La relation SnapVault doit être initialisée et la dernière copie Snapshot dans le volume secondaire SnapVault doit contenir la LUN souhaitée.
- Le serveur virtuel de stockage (SVM) contenant la sauvegarde SnapVault doit disposer d'une ou plusieurs LIF avec le protocole SAN souhaité accessible depuis l'hôte utilisé pour accéder à la copie LUN.
- Si vous prévoyez d'accéder directement aux copies de LUN à partir du volume secondaire SnapVault, vous devez créer vos groupes initiateurs sur la SVM SnapVault à l'avance.

Vous pouvez accéder à une LUN directement à partir du volume secondaire SnapVault sans avoir à effectuer au préalable la restauration ou le clonage du volume contenant la LUN.

Description de la tâche

Si une nouvelle copie Snapshot est ajoutée au volume secondaire de SnapVault alors que une LUN est mappée à partir d'une copie Snapshot précédente, le contenu de la LUN mappée change. La LUN est toujours mappée avec les mêmes identifiants, mais les données sont issues de la nouvelle copie Snapshot. Si la taille de LUN change, certains hôtes détectent automatiquement la modification de taille ; les hôtes Windows exigent une nouvelle analyse du disque pour identifier toute modification de taille.

Étapes

1. Exécutez le `lun show` Commande permettant de lister les LUN disponibles dans le volume secondaire SnapVault.

Dans cet exemple, vous pouvez voir les LUN d'origine dans le volume primaire srcvolA et les copies dans le volume secondaire SnapVault dstvolB :

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

6 entries were displayed.

2. Si le groupe initiateur pour l'hôte souhaité n'existe pas déjà sur la SVM contenant le volume secondaire SnapVault, exécutez la `igroup create` commande de création d'un groupe initiateur.

Cette commande crée un groupe initiateur pour un hôte Windows qui utilise le protocole iSCSI :

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup  
-protocol iscsi -ostype windows  
-initiator iqn.1991-05.com.microsoft:hostA
```

3. Exécutez le `lun mapping create` Commande permettant de mapper la copie de LUN souhaitée sur le groupe initiateur.

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A  
-igroup temp_igroup
```

4. Connectez l'hôte au LUN et accédez au contenu du LUN selon vos besoins.

Restaurez une LUN unique à partir d'une sauvegarde SnapVault

Vous pouvez restaurer une seule LUN à un nouvel emplacement ou à l'emplacement d'origine. Vous pouvez restaurer l'ensemble du volume secondaire SnapVault à partir de n'importe quelle copie Snapshot. Pour restaurer la LUN à l'emplacement d'origine, vous devez d'abord la restaurer à un nouvel emplacement, puis la copier.

Ce dont vous avez besoin

- La relation SnapVault doit être initialisée et le volume secondaire SnapVault doit contenir une copie Snapshot appropriée pour la restauration.
- La machine virtuelle de stockage (SVM) contenant le volume secondaire SnapVault doit disposer d'une ou plusieurs LIF avec le protocole SAN souhaité accessible depuis l'hôte utilisé pour accéder à la copie de

LUN.

- Les igroups doivent déjà exister sur le SVM SnapVault.

Description de la tâche

Le processus inclut la création d'un clone de volume de lecture/écriture à partir d'une copie Snapshot dans le volume secondaire SnapVault. Vous pouvez utiliser la LUN directement depuis le clone ou copier le contenu de la LUN vers l'emplacement d'origine.

Le chemin d'accès et le numéro de série de la LUN d'origine sont différents de ceux de la LUN d'origine. Les réservations permanentes ne sont pas conservées.

Étapes

1. Exécutez le `snapmirror show` Commande pour vérifier le volume secondaire contenant la sauvegarde SnapVault.

```
cluster::> snapmirror show
```

Source Path	Type	Dest Path	Mirror State	Relation Status	Total Progress	Healthy	Last Updated
vserverA:srcvolA	XDP	vserverB:dstvolB	Snapmirrored	Idle	-	true	-

2. Exécutez le `volume snapshot show` Commande permettant d'identifier la copie Snapshot à partir de laquelle vous souhaitez restaurer la LUN.

```
cluster::> volume snapshot show
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vserverB	dstvolB	snap2.2013-02-10_0010	valid	124KB	0%	0%
		snap1.2013-02-10_0015	valid	112KB	0%	0%
		snap2.2013-02-11_0010	valid	164KB	0%	0%

3. Exécutez le `volume clone create` Commande permettant de créer un clone de lecture/écriture à partir de la copie Snapshot souhaitée.

Le clone de volume est créé dans le même agrégat que la sauvegarde SnapVault. L'espace doit être suffisant dans l'agrégat pour stocker le clone.

```
cluster::> volume clone create -vserver vserverB
        -flexclone dstvolB_clone -type RW -parent-volume dstvolB
        -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. Exécutez le `lun show` Commande permettant d'afficher la liste des LUN dans le clone de volume.

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone
```

Vserver	Path	State	Mapped	Type
vserverB	/vol/dstvolB_clone/lun_A	online	unmapped	windows
vserverB	/vol/dstvolB_clone/lun_B	online	unmapped	windows
vserverB	/vol/dstvolB_clone/lun_C	online	unmapped	windows

3 entries were displayed.

5. Si le groupe initiateur pour l'hôte souhaité n'existe pas déjà sur la SVM contenant la sauvegarde SnapVault, exécutez la `igroup create` commande de création d'un groupe initiateur.

Cet exemple crée un groupe initiateur pour un hôte Windows qui utilise le protocole iSCSI :

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
        -protocol iscsi -ostype windows
        -initiator iqn.1991-05.com.microsoft:hostA
```

6. Exécutez le `lun mapping create` Commande permettant de mapper la copie de LUN souhaitée sur le groupe initiateur.

```
cluster::> lun mapping create -vserver vserverB
        -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

7. Connectez l'hôte au LUN et accédez au contenu du LUN, si nécessaire.

La LUN est en lecture/écriture et peut être utilisée à la place de la LUN d'origine. Le numéro de série de la LUN est différent, l'hôte l'interprète comme une LUN différente de l'original.

8. Utilisez un programme de copie sur l'hôte pour copier le contenu de la LUN vers la LUN d'origine.

Restaurez toutes les LUN d'un volume à partir d'une sauvegarde SnapVault

Si une ou plusieurs LUN d'un volume doivent être restaurées à partir d'une sauvegarde SnapVault, vous pouvez restaurer l'ensemble du volume. La restauration du volume affecte toutes les LUN du volume.

Ce dont vous avez besoin

La relation SnapVault doit être initialisée et le volume secondaire SnapVault doit contenir une copie Snapshot appropriée pour la restauration.

Description de la tâche

La restauration d'un volume complet renvoie l'état du volume à la date à laquelle il était créé. Si une LUN a été ajoutée au volume après la copie Snapshot, cette LUN est supprimée lors du processus de restauration.

Après la restauration du volume, les LUN restent mappées sur les groupes initiateurs auxquels ils ont été mappés avant la restauration. Le mappage de LUN peut être différent du mappage au moment de la copie Snapshot. Les réservations persistantes sur les LUN à partir des clusters hôtes sont conservées.

Étapes

1. Arrêtez les E/S à toutes les LUN du volume.
2. Exécutez le `snapmirror show` Commande pour vérifier le volume secondaire contenant le volume secondaire SnapVault.

```
cluster::> snapmirror show
```

Source Path	Type	Dest Path	Mirror State	Relation Status	Total Progress	Healthy	Last Updated
vserverA:srcvolA	XDP	vserverB:dstvolB	Snapmirrored	Idle	-	true	-

3. Exécutez le `volume snapshot show` Commande permettant d'identifier la copie Snapshot à partir de laquelle vous souhaitez restaurer.

```
cluster::> volume snapshot show
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vserverB	dstvolB	snap2.2013-02-10_0010	valid	124KB	0%	0%
		snap1.2013-02-10_0015	valid	112KB	0%	0%
		snap2.2013-02-11_0010	valid	164KB	0%	0%

4. Exécutez le `snapmirror restore` et spécifiez le `-source-snapshot` Option permettant de spécifier la copie Snapshot à utiliser.

La destination que vous spécifiez pour la restauration est le volume d'origine vers lequel vous restaurez.


```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
      -source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. Si vous partagez des LUN sur un cluster hôte, restaurez les réservations permanentes sur les LUN à partir des hôtes affectés.

Restauration d'un volume à partir d'une sauvegarde SnapVault

Dans l'exemple suivant, la LUN nommée lun_D a été ajoutée au volume après la création de la copie Snapshot. Après avoir restauré le volume entier à partir de la copie Snapshot, lun_D n'apparaît plus.

Dans le `lun show` Résultat de la commande, vous pouvez voir les LUN dans le volume primaire srcvolA et les copies en lecture seule de ces LUN dans le volume secondaire SnapVault dstvolB. Il n'y a pas de copie de lun_D dans la sauvegarde SnapVault.

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_D	online	mapped	windows	250.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

7 entries were displayed.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
-source-path vserverB:dstvolB
-source-snapshot daily.2013-02-10_0010
```

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on volume vserverA:src_volA will be deleted.

Do you want to continue? {y|n}: y

[Job 98] Job is queued: snapmirror restore from source "vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

6 entries were displayed.

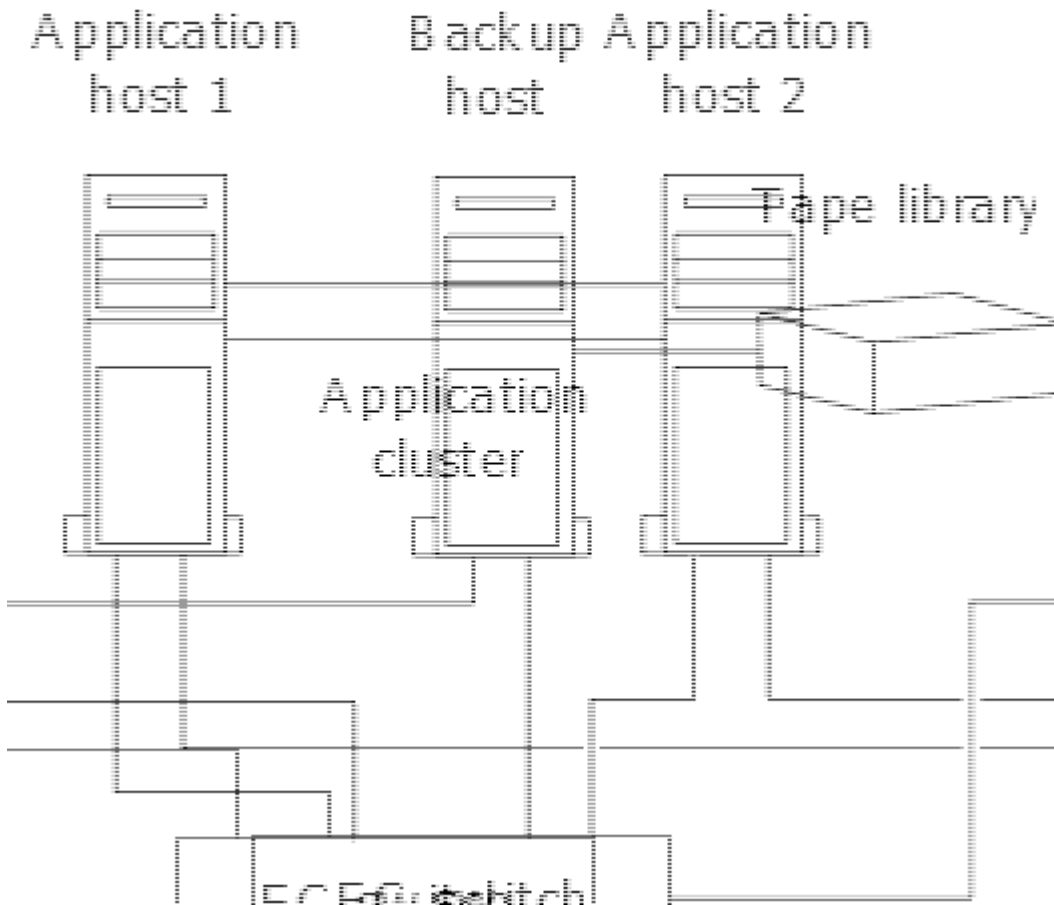
Une fois le volume restauré à partir du volume secondaire SnapVault, le volume source ne contient plus lun_D. Il n'est pas nécessaire de remapper les LUN du volume source une fois la restauration effectuée, car ces LUN restent mappées.

Comment connecter un système de sauvegarde hôte au système de stockage primaire

Vous pouvez sauvegarder les systèmes SAN sur bande via un hôte de sauvegarde distinct afin d'éviter une dégradation des performances de l'hôte applicatif.

Il est impératif de maintenir l séparation des données SAN et NAS à des fins de sauvegarde. La figure ci-

dessous présente la configuration physique recommandée pour un système de sauvegarde hôte sur le système de stockage primaire. Vous devez configurer des volumes en tant que SAN uniquement. Les LUN peuvent être limités à un seul volume ou être répartis sur plusieurs volumes ou systèmes de stockage.



Les volumes d'un hôte peuvent être constitués d'une seule LUN mappée à partir du système de stockage ou de plusieurs LUN à l'aide d'un gestionnaire de volumes, tel que VxVM sur des systèmes HP-UX.

Sauvegarder une LUN par le biais d'un système de sauvegarde hôte

Vous pouvez utiliser une LUN clonée à partir d'une copie Snapshot comme données source pour le système de sauvegarde hôte.

Ce dont vous avez besoin

Une LUN de production doit exister et être mappée sur un groupe initiateur qui inclut le WWPN ou le nom de nœud initiateur du serveur d'applications. La LUN doit également être formatée et accessible pour l'hôte

Étapes

1. Enregistrez le contenu des tampons du système de fichiers hôte sur le disque.

Vous pouvez utiliser la commande fournie par le système d'exploitation hôte ou utiliser SnapDrive pour Windows ou SnapDrive pour UNIX. Vous pouvez également choisir de faire de cette étape une partie de votre script de prétraitement de sauvegarde SAN.

2. Utilisez le volume `snapshot create` Commande pour créer une copie Snapshot de la LUN de production.

```
volume snapshot create -vserver vs0 -volume vol3 -snapshot vol3_snapshot  
-comment "Single snapshot" -foreground false
```

3. Utilisez le `volume file clone create` Commande permettant de créer un clone de la LUN de production.

```
volume file clone create -vserver vs3 -volume vol3 -source-path lun1 -snapshot  
-name snap_vol3 -destination-path lun1_backup
```

4. Utilisez le `lun igroup create` Commande permettant de créer un groupe initiateur incluant le WWPN du serveur de sauvegarde.

```
lun igroup create -vserver vs3 -igroup igroup3 -protocol fc -ostype windows  
-initiator 10:00:00:00:c9:73:5b:91
```

5. Utilisez le `lun mapping create` Commande pour mapper le clone de LUN que vous avez créé à l'étape 3 sur l'hôte de sauvegarde.

```
lun mapping create -vserver vs3 -volume vol3 -lun lun1_backup -igroup igroup3
```

Vous pouvez choisir de faire de cette étape une partie du script post-traitement de votre application de sauvegarde SAN.

6. Depuis l'hôte, découvrez le nouveau LUN et rendez le système de fichiers disponible pour l'hôte.

Vous pouvez choisir de faire de cette étape une partie du script post-traitement de votre application de sauvegarde SAN.

7. Sauvegardez les données du clone de LUN de l'hôte de sauvegarde sur bande à l'aide de votre application de sauvegarde SAN.

8. Utilisez le `lun modify` Commande permettant de mettre le clone de LUN hors ligne.

```
lun modify -vserver vs3 -path /vol/vol3/lun1_backup -state offline
```

9. Utilisez le `lun delete` Pour supprimer le clone de LUN.

```
lun delete -vserver vs3 -volume vol3 -lun lun1_backup
```

10. Utilisez le `volume snapshot delete` Commande permettant de supprimer la copie Snapshot.

```
volume snapshot delete -vserver vs3 -volume vol3 -snapshot vol3_snapshot
```

Référence de configuration SAN

Présentation de la configuration SAN

Un SAN (Storage Area Network) se compose d'une solution de stockage connectée à des hôtes via un protocole de transport SAN tel qu'iSCSI ou FC. Vous pouvez configurer votre SAN de sorte que votre solution de stockage se connecte à vos hôtes via un ou plusieurs commutateurs. Si vous utilisez iSCSI, vous pouvez également configurer votre SAN de sorte que votre solution de stockage se connecte directement à votre hôte sans

utiliser de commutateur.

Dans un SAN, plusieurs hôtes, utilisant différents systèmes d'exploitation, tels que Windows, Linux ou UNIX, peuvent accéder à la solution de stockage en même temps. Vous pouvez utiliser ["Mappage de LUN sélectif"](#) et ["ensembles de ports"](#) pour limiter l'accès aux données entre les hôtes et le stockage.

Pour iSCSI, la topologie réseau entre la solution de stockage et les hôtes est appelée réseau. Pour FC, FC/NVMe et FCoE, la topologie réseau entre la solution de stockage et les hôtes est appelée structure. Pour créer une redondance, ce qui vous protège contre la perte d'accès aux données, vous devez configurer votre SAN avec des paires haute disponibilité dans une configuration multi-réseau ou multi-structure. Les configurations utilisant des nœuds uniques ou des réseaux/structures uniques ne sont pas entièrement redondants et ne sont donc pas recommandées.

Une fois votre SAN configuré, vous pouvez le faire ["Provisionnez le stockage pour iSCSI ou FC"](#), ou vous pouvez ["Provisionnez le stockage pour FC/NVMe"](#). Vous pouvez ensuite vous connecter à vos hôtes pour commencer à assurer la maintenance des données.

La prise en charge du protocole SAN varie en fonction de votre version de ONTAP, de votre plateforme et de votre configuration. Pour plus de détails sur votre configuration spécifique, reportez-vous au ["Matrice d'interopérabilité NetApp"](#).

Informations associées

- ["Présentation de l'administration SAN"](#)
- ["Configuration, prise en charge et limitations de NVMe"](#)

Configurations iSCSI

Manières de configurer les hôtes SAN iSCSI

Vous devez configurer votre configuration iSCSI avec des paires haute disponibilité qui se connectent directement à vos hôtes SAN iSCSI ou qui se connectent à vos hôtes via un ou plusieurs commutateurs IP.

["Paires HA"](#) Sont définis comme nœuds de reporting pour les chemins Active/Optimized et Active/UnOptimized qui seront utilisés par les hôtes pour accéder aux LUN. Plusieurs hôtes, utilisant différents systèmes d'exploitation, tels que Windows, Linux ou UNIX, peuvent accéder au stockage en même temps. Les hôtes nécessitent qu'une solution de chemins d'accès multiples prise en charge qui prend en charge ALUA soit installée et configurée. Les systèmes d'exploitation et les solutions de chemins d'accès multiples pris en charge peuvent être vérifiés sur le ["Matrice d'interopérabilité NetApp"](#).

Dans une configuration multi-réseau, deux ou plusieurs commutateurs connectent les hôtes au système de stockage. Les configurations multi-réseau sont recommandées car elles sont entièrement redondantes. Dans une configuration à réseau unique, un commutateur connecte les hôtes au système de stockage. Les configurations à un seul réseau ne sont pas entièrement redondantes.



["Configurations à un seul nœud"](#) ne sont pas recommandées, car elles n'offrent pas la redondance nécessaire à la prise en charge de la tolérance aux pannes et de la continuité de l'activité.

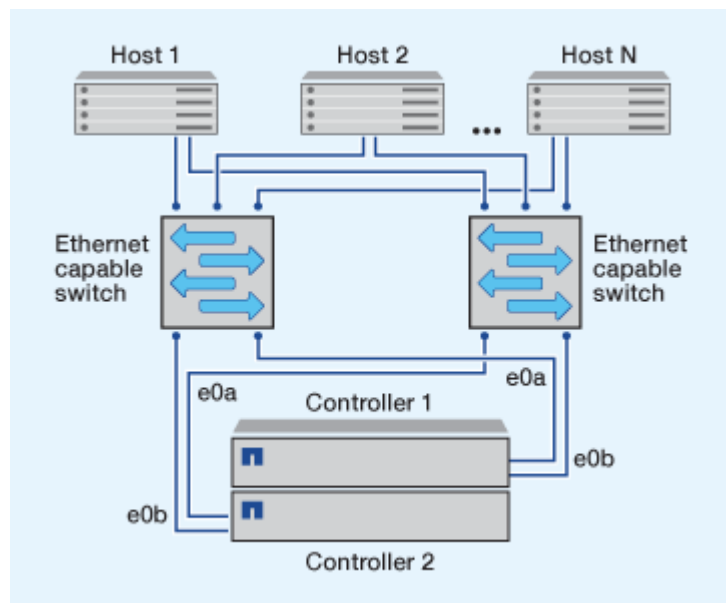
Informations associées

- Découvrez comment ["Mappage de LUN sélectif \(SLM\)"](#) Limite les chemins utilisés pour accéder aux LUN appartenant à une paire HA.

- Découvrez "[LIF SAN](#)".
- Découvrez le "[Avantages des VLAN dans iSCSI](#)".

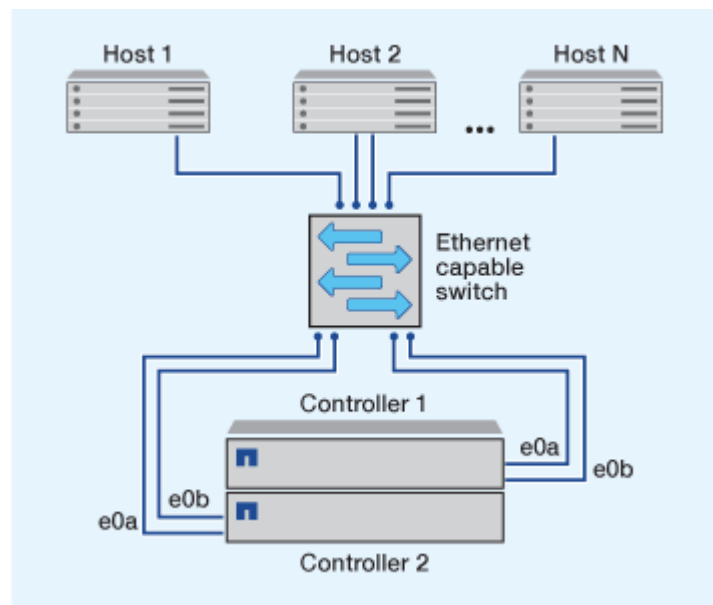
Configurations iSCSI multi-réseau

Dans les configurations de paires haute disponibilité à plusieurs réseaux, au moins deux commutateurs connectent la paire haute disponibilité à un ou plusieurs hôtes. Étant donné qu'il y a plusieurs commutateurs, cette configuration est totalement redondante.



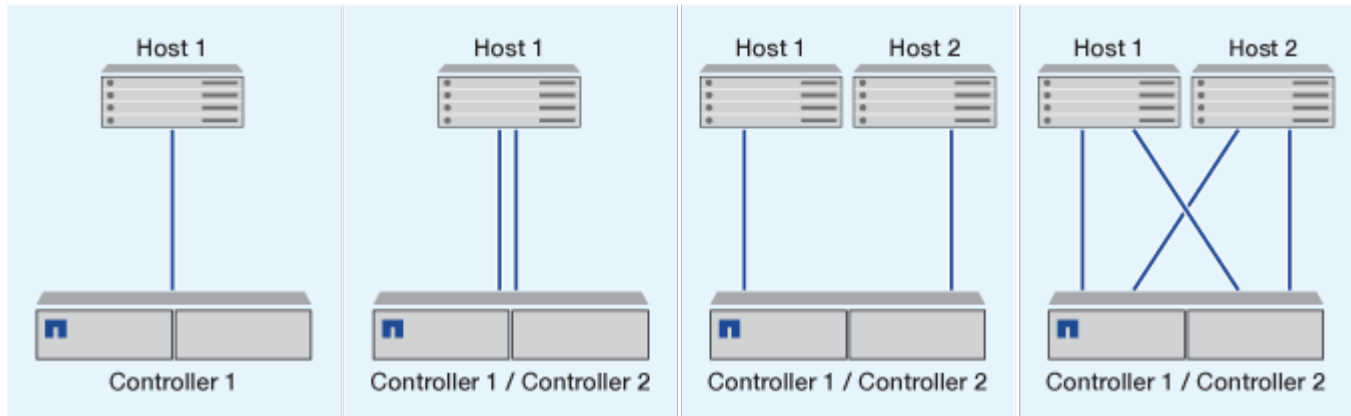
Configurations iSCSI à réseau unique

Dans les configurations de paires haute disponibilité à réseau unique, un switch connecte la paire haute disponibilité à un ou plusieurs hôtes. Comme il y a un seul commutateur, cette configuration n'est pas entièrement redondante.



Configuration iSCSI à connexion directe

Dans une configuration en attachement direct, un ou plusieurs hôtes sont directement connectés aux contrôleurs.



Avantages de l'utilisation des VLAN dans les configurations iSCSI

Un VLAN se compose d'un groupe de ports de commutateur regroupés dans un domaine de broadcast. Un VLAN peut se trouver sur un seul commutateur ou s'étendre sur plusieurs châssis de commutateur. Les VLAN statiques et dynamiques vous permettent d'accroître la sécurité, d'isoler les problèmes et de limiter les chemins disponibles au sein de votre infrastructure de réseau IP.

Lorsque vous implémentez des VLAN dans de grandes infrastructures de réseaux IP, vous bénéficiez des avantages suivants :

- Sécurité renforcée.

Les VLAN vous permettent d'exploiter l'infrastructure existante tout en améliorant la sécurité, car ils limitent l'accès entre différents nœuds d'un réseau Ethernet ou d'un SAN IP.

- Amélioration de la fiabilité du réseau Ethernet et du SAN IP en isolant les problèmes.
- Réduction du temps de résolution des problèmes en limitant l'espace dédié au problème
- Réduction du nombre de chemins disponibles vers un port cible iSCSI spécifique.
- Réduction du nombre maximal de chemins utilisés par un hôte.

Un trop grand nombre de chemins ralentit les temps de reconnexion. Si un hôte ne dispose pas d'une solution de chemins d'accès multiples, vous pouvez utiliser des VLAN pour n'autoriser qu'un seul chemin.

VLAN dynamiques

Les VLAN dynamiques sont basés sur une adresse MAC. Vous pouvez définir un VLAN en spécifiant l'adresse MAC des membres que vous souhaitez inclure.

Les VLAN dynamiques offrent une flexibilité accrue et ne nécessitent pas de mappage vers les ports physiques sur lesquels le périphérique est physiquement connecté au commutateur. Vous pouvez déplacer un câble d'un port à un autre sans reconfigurer le VLAN.

VLAN statiques

Les VLAN statiques sont basés sur des ports. Le commutateur et le port du commutateur sont utilisés pour définir le VLAN et ses membres.

Les VLAN statiques offrent une sécurité améliorée car il n'est pas possible d'enfreindre les VLAN à l'aide d'une usurpation MAC (Media Access Control). Cependant, si une personne a un accès physique au commutateur, le remplacement d'un câble et la reconfiguration de l'adresse réseau peuvent autoriser l'accès.

Dans certains environnements, il est plus facile de créer et de gérer des VLAN statiques que des VLAN dynamiques. En effet, les VLAN statiques nécessitent uniquement la spécification de l'identifiant du commutateur et du port, au lieu de l'adresse MAC 48 bits. En outre, vous pouvez étiqueter les plages de ports de commutateur avec l'identifiant VLAN.

Configurations FC

Manières de configurer les hôtes SAN FC et FC-NVMe

Il est recommandé de configurer vos hôtes SAN FC et FC-NVMe à l'aide de paires haute disponibilité et d'un minimum de deux commutateurs. Cela assure la redondance aux couches de la structure et du système de stockage pour prendre en charge la tolérance aux pannes et la continuité de l'activité. Vous ne pouvez pas connecter directement des hôtes SAN FC ou FC-NVMe à des paires haute disponibilité sans utiliser de commutateur.

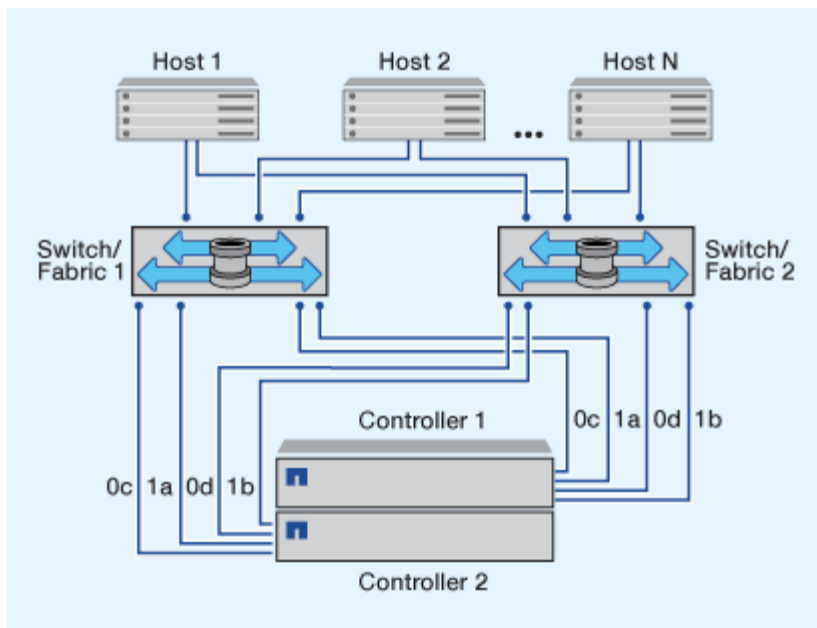
Les tissus en cascade, à maillage partiel, à maillage complet, à la périphérie du cœur et au directeur sont tous des méthodes standard de connexion des commutateurs FC à un tissu, et toutes sont prises en charge. L'utilisation de structures de commutateurs FC hétérogènes n'est pas prise en charge, sauf dans le cas de commutateurs lame intégrés. Des exceptions spécifiques sont répertoriées sur le ["Matrice d'interopérabilité"](#). Une structure peut comprendre un ou plusieurs commutateurs et les contrôleurs de stockage peuvent être connectés à plusieurs commutateurs.

Plusieurs hôtes, qui utilisent différents systèmes d'exploitation, tels que Windows, Linux ou UNIX, peuvent accéder aux contrôleurs de stockage en même temps. Les hôtes nécessitent l'installation et la configuration d'une solution de chemins d'accès multiples prise en charge. Les systèmes d'exploitation et les solutions de chemins d'accès multiples pris en charge peuvent être vérifiés à l'aide de l'outil Interoperability Matrix Tool.

Les configurations FC et FC-NVMe de Multifabric

Dans les configurations de paires haute disponibilité multistrukture, il existe au moins deux commutateurs qui connectent les paires haute disponibilité à un ou plusieurs hôtes. Pour plus de simplicité, la figure suivante de paire haute disponibilité multistrukture ne présente que deux fabrics, mais vous pouvez avoir au moins deux fabrics dans n'importe quelle configuration multistrukture.

Les numéros de port cible FC (0C, 0d, 1a, 1b) dans les illustrations sont des exemples. Les numéros de port réels varient selon le modèle de votre nœud de stockage et si vous utilisez des adaptateurs d'extension.

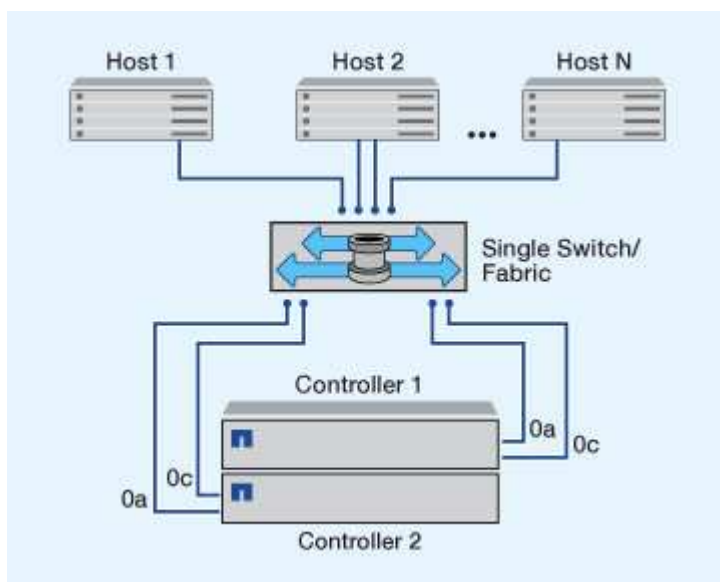


Les configurations FC et FC-NVMe à structure unique

Dans les configurations de paires haute disponibilité à structure unique, une structure relie les deux contrôleurs de la paire haute disponibilité à un ou plusieurs hôtes. Comme les hôtes et les contrôleurs sont connectés via un commutateur unique, les configurations de paires haute disponibilité à structure unique ne sont pas entièrement redondantes.

Les numéros de port FC cible (0a, 0C) dans les illustrations sont des exemples. Les numéros de port réels varient selon le modèle de votre nœud de stockage et si vous utilisez des adaptateurs d'extension.

Toutes les plateformes qui prennent en charge les configurations FC prennent en charge les paires haute disponibilité à structure unique.



"Configurations à un seul nœud" ne sont pas recommandées, car elles n'offrent pas la redondance nécessaire à la prise en charge de la tolérance aux pannes et de la continuité de l'activité.

Informations associées

- Découvrez comment "[Mappage de LUN sélectif \(SLM\)](#)" Limite les chemins utilisés pour accéder aux LUN appartenant à une paire HA.
- Découvrez "[LIF SAN](#)".

Meilleures pratiques en matière de configuration des commutateurs FC

Pour obtenir des performances optimales, vous devez tenir compte de certaines des meilleures pratiques lors de la configuration du commutateur FC.

Un paramètre de vitesse de liaison fixe est la meilleure pratique pour les configurations de commutateurs FC, en particulier pour les structures importantes, car il offre les meilleures performances pour les reconstructions de structures et peut gagner beaucoup de temps. Bien que la négociation automatique offre la plus grande flexibilité, la configuration des commutateurs FC ne fonctionne pas toujours comme prévu, et elle ajoute du temps à la séquence globale de création de la structure.

Tous les commutateurs connectés à la structure doivent prendre en charge la virtualisation NPIV (N_Port ID Virtualization) et doivent avoir NPIV activé. ONTAP utilise NPIV pour présenter les cibles FC à une structure.

Pour plus d'informations sur les environnements pris en charge, reportez-vous au "[Matrice d'interopérabilité NetApp](#)".

Pour connaître les meilleures pratiques relatives à FC et à l'iSCSI, reportez-vous à "[Rapport technique de NetApp 4080 : meilleures pratiques pour le SAN moderne](#)".

Nombre de sauts FC pris en charge

Le nombre maximal de sauts FC pris en charge entre un hôte et un système de stockage dépend du fournisseur du commutateur et de la prise en charge du système de stockage pour les configurations FC.

Le nombre de sauts est défini comme le nombre de commutateurs dans le chemin entre l'initiateur (hôte) et la cible (système de stockage). Cisco désigne également cette valeur par l'expression *diamètre de la structure SAN*.

Changer de fournisseur	Nombre de sauts pris en charge
Brocade	7 pour FC, 5 pour FCoE
Cisco	7 pour FC, jusqu'à 3 commutateurs peuvent être des commutateurs FCoE.

Informations associées

"[Téléchargements NetApp : documents Brocade relatifs à la matrice d'évolutivité](#)"

"[Téléchargements NetApp : documents Cisco scalabilité Matrix](#)"

Vitesses prises en charge par le port FC cible

Les ports cibles FC peuvent être configurés pour s'exécuter à différentes vitesses. Vous devez définir la vitesse du port cible en fonction de la vitesse du périphérique auquel il se

connecte. Tous les ports cibles utilisés par un hôte donné doivent être définis sur la même vitesse.

Les ports cibles FC peuvent être utilisés pour les configurations FC-NVMe de la même manière qu'ils sont utilisés pour les configurations FC.

Vous devez définir la vitesse du port cible afin qu'elle corresponde à la vitesse du périphérique auquel il se connecte au lieu d'utiliser la négociation automatique. Un port défini pour la négociation automatique peut prendre plus de temps pour se reconnecter après un basculement/rétablissement ou une autre interruption.

Vous pouvez configurer les ports intégrés et les adaptateurs d'extension pour qu'ils s'exécutent à la vitesse suivante. Chaque contrôleur et port d'adaptateur d'extension peuvent être configurés individuellement pour différentes vitesses, selon les besoins.

Ports 4 Go	Ports 8 Gb	Ports 16 Gb	Ports 32 Gb
<ul style="list-style-type: none">• 4 Go• 2 Go• 1 Go	<ul style="list-style-type: none">• 8 Go• 4 Go• 2 Go	<ul style="list-style-type: none">• 16 Go• 8 Go• 4 Go	<ul style="list-style-type: none">• 32 Go• 16 Go• 8 Go



Les ports UTA2 peuvent utiliser un adaptateur SFP+ de 8 Gb pour prendre en charge les vitesses de 8, 4 et 2 Go, si nécessaire.

Recommandations pour la configuration des ports FC cibles

Pour des performances optimales et une disponibilité optimale, vous devez utiliser la configuration de port cible FC recommandée.

Le tableau suivant indique l'ordre d'utilisation des ports préféré pour les ports intégrés FC et FC-NVMe cibles. Pour les adaptateurs d'extension, les ports FC doivent être répartis de manière à ne pas utiliser le même ASIC pour la connectivité. L'ordre de slot préféré est indiqué dans le "NetApp Hardware Universe" Pour la version du logiciel ONTAP utilisée par votre contrôleur.

La connectivité FC-NVMe est prise en charge sur les modèles suivants :

- AFF A300



Les ports intégrés des systèmes AFF A300 ne prennent pas en charge FC-NVMe.

- AFF A700
- AFF A700s
- AFF A800



Les systèmes FAS2520 ne disposent pas de ports FC intégrés et ne prennent pas en charge les adaptateurs add-on.

Contrôleur	Paires de ports avec ASIC partagé	Nombre de ports cibles : ports préférés
FAS9000, AFF A700, AFF A700S ET AFF A800	Aucune	Tous les ports de données se trouvent sur des adaptateurs d'extension. Voir " NetApp Hardware Universe " pour en savoir plus.
8080, 8060 et 8040	0e+0f 0g+0h	1 : 0e 2 : 0e, 0g 3 : 0e, 0g, 0h 4 : 0e, 0g, 0f, 0h
FAS8200 ET AFF A300	0g+0h	1: 0g 2: 0g, 0h
8020	0c+0d	1 : 0c 2 : 0c, 0d
62xx	0a+0b 0c+0d	1 : 0a 2 : 0a, 0c 3 : 0a, 0c, 0b 4 : 0a, 0c, 0b, 0d
32xx	0c+0d	1 : 0c 2 : 0c, 0d
FAS2554, FAS2552, FAS2600 SERIES, FAS2720, FAS2750, AFF A200 ET AFF A220	0c+0d 0e+0f	1 : 0c 2 : 0c, 0e 3 : 0c, 0e, 0d 4 : 0c, 0e, 0d, 0f

Gestion des systèmes avec les adaptateurs FC

Présentation de la gestion des systèmes avec des adaptateurs FC

Des commandes sont disponibles pour la gestion des adaptateurs FC intégrés et des cartes d'adaptateur FC. Ces commandes peuvent être utilisées pour configurer le mode

adaptateur, afficher les informations relatives à l'adaptateur et modifier la vitesse.

La plupart des systèmes de stockage disposent d'adaptateurs FC intégrés pouvant être configurés en tant qu'initiateurs ou cibles. Vous pouvez également utiliser des cartes d'adaptateur FC configurées en tant qu'initiateurs ou cibles. Les initiateurs se connectent aux tiroirs disques internes, voire aux baies de stockage étrangères (FlexArray). Les cibles se connectent uniquement aux commutateurs FC. Les ports HBA FC cible et la vitesse du port du commutateur doivent être définis sur la même valeur et ne doivent pas être définis sur auto.

Commandes de gestion des adaptateurs FC

Vous pouvez utiliser des commandes FC pour gérer les adaptateurs cibles FC, les adaptateurs initiateurs FC et les adaptateurs FC intégrés à votre contrôleur de stockage. Les mêmes commandes sont utilisées pour gérer les adaptateurs FC pour le protocole FC et le protocole FC-NVMe.

Les commandes de l'adaptateur initiateur FC fonctionnent uniquement au niveau du nœud. Vous devez utiliser le `run -node node_name` Commande avant de pouvoir utiliser les commandes de l'adaptateur FC initiator.

Commandes de gestion des adaptateurs cibles FC

Les fonctions que vous recherchez...	Utilisez cette commande...
Affiche les informations relatives à l'adaptateur FC sur un nœud	<code>network fcp adapter show</code>
Modifiez les paramètres de l'adaptateur cible FC	<code>network fcp adapter modify</code>
Affiche les informations de trafic du protocole FC	<code>run -node node_name sysstat -f</code>
Afficher la durée d'exécution du protocole FC	<code>run -node node_name uptime</code>
Affiche la configuration et l'état de la carte	<code>run -node node_name sysconfig -v adapter</code>
Vérifiez quelles cartes d'extension sont installées et si des erreurs de configuration existent	<code>run -node node_name sysconfig -ac</code>
Affichez une page man pour une commande	<code>man command_name</code>

Commandes de gestion des adaptateurs initiateurs FC

Les fonctions que vous recherchez...	Utilisez cette commande...
Affiche les informations relatives à la totalité des initiateurs et de leurs adaptateurs dans un nœud	<code>run -node node_name storage show adapter</code>

Les fonctions que vous recherchez...	Utilisez cette commande...
Affiche la configuration et l'état de la carte	<code>run -node <i>node_name</i> sysconfig -v <i>adapter</i></code>
Vérifiez quelles cartes d'extension sont installées et si des erreurs de configuration existent	<code>run -node <i>node_name</i> sysconfig -ac</code>

Commandes de gestion des adaptateurs FC intégrés

Les fonctions que vous recherchez...	Utilisez cette commande...
Affiche l'état des ports FC intégrés	<code>system node hardware unified-connect show</code>

Configurer les adaptateurs FC pour le mode initiateur

Vous pouvez configurer des ports FC individuels des adaptateurs intégrés et certaines cartes d'adaptateur FC pour le mode initiateur. Ce mode permet de connecter les ports aux lecteurs de bande, aux bibliothèques de bandes ou aux systèmes de stockage tiers à l'aide de FlexArray Virtualization ou Foreign LUN Import (FLI).

Ce dont vous avez besoin

- Les LIF présentes sur l'adaptateur doivent être supprimées de n'importe quel ensemble de ports dont elles sont membres.
- Toutes les LIF de chaque machine virtuelle de stockage (SVM) utilisant le port physique à modifier doivent être migrées ou détruites avant de changer la personnalité du port physique de la cible à l'initiateur.

Description de la tâche

Chaque port FC intégré peut être configuré individuellement en tant qu'initiateur ou cible. Les ports de certains adaptateurs FC peuvent également être configurés individuellement en tant que port cible ou port initiateur, comme les ports FC intégrés. Une liste des adaptateurs pouvant être configurés pour le mode cible est disponible dans ["NetApp Hardware Universe"](#).



Le protocole NVMe/FC prend en charge le mode initiateur.

Étapes

1. Supprimer toutes les LIFs de l'adaptateur :

```
network interface delete -vserver SVM_name -lif lif_name,lif_name
```

2. Mettez votre adaptateur hors ligne :

```
network fcp adapter modify -node node_name -adapter adapter_port -status-admin  
down
```

Si l'adaptateur ne passe pas hors ligne, vous pouvez également retirer le câble du port d'adaptateur approprié du système.

3. Modifiez l'adaptateur de la cible à l'initiateur :

```
system hardware unified-connect modify -t initiator adapter_port
```

4. Redémarrez le nœud hébergeant l'adaptateur que vous avez changé.

5. Vérifier que les ports FC sont configurés dans l'état approprié pour votre configuration :

```
system hardware unified-connect show
```

6. Remettre la carte en ligne :

```
node run -node node_name storage enable adapter adapter_port
```

Configurer les adaptateurs FC pour le mode cible

Vous pouvez configurer des ports FC individuels des adaptateurs intégrés et certaines cartes d'adaptateur FC pour le mode cible. Le mode cible est utilisé pour connecter les ports aux initiateurs FC.

Description de la tâche

Chaque port FC intégré peut être configuré individuellement en tant qu'initiateur ou cible. Les ports de certains adaptateurs FC peuvent également être configurés individuellement en tant que port cible ou port initiateur, comme les ports FC intégrés. Une liste d'adaptateurs pouvant être configurés pour le mode cible est disponible dans le ["NetApp Hardware Universe"](#).

La même procédure est utilisée lors de la configuration des adaptateurs FC pour le protocole FC et le protocole FC-NVMe. Cependant, seuls certains adaptateurs FC prennent en charge la connectivité FC-NVMe. Voir la ["NetApp Hardware Universe"](#) Par l'utilisation de la liste des adaptateurs prenant en charge le protocole FC-NVMe.

Étapes

1. Mettez l'adaptateur hors ligne :

```
node run -node node_name storage disable adapter adapter_name
```

Si l'adaptateur ne passe pas hors ligne, vous pouvez également retirer le câble du port d'adaptateur approprié du système.

2. Modifiez l'adaptateur de l'initiateur sur la cible :

```
system node hardware unified-connect modify -t target -node node_name adapter adapter_name
```

3. Redémarrez le nœud hébergeant l'adaptateur que vous avez changé.

4. Vérifiez que la configuration du port cible est correcte :

```
network fcp adapter show -node node_name
```

5. Mettez votre adaptateur en ligne :

```
network fcp adapter modify -node node_name -adapter adapter_port -state up
```

Affiche des informations relatives à un adaptateur cible FC

Vous pouvez utiliser le `network fcp adapter show` Commande permettant d'afficher les informations de configuration du système et d'adaptateur pour tout adaptateur FC dans le système.

Étape

1. Affiche des informations relatives à l'adaptateur FC en utilisant le `network fcp adapter show` commande.

Le résultat de cette commande affiche des informations de configuration du système et des informations sur l'adaptateur pour chaque slot utilisé.

```
network fcp adapter show -instance -node node1 -adapter 0a
```

Modifier la vitesse de l'adaptateur FC

Vous devez définir la vitesse du port cible de votre adaptateur afin qu'elle corresponde à la vitesse du périphérique auquel il se connecte, au lieu d'utiliser la négociation automatique. Un port défini pour la négociation automatique peut prendre plus de temps pour se reconnecter après un basculement/rétablissement ou une autre interruption.

Ce dont vous avez besoin

Toutes les LIFs qui utilisent cet adaptateur comme port de home port doivent être hors ligne.

Description de la tâche

Cette tâche englobant tous les SVM (Storage Virtual machine) et toutes les LIFs d'un cluster, vous devez utiliser le `-home-port` et `-home-lif` paramètres pour limiter la portée de cette opération. Si vous n'utilisez pas ces paramètres, l'opération s'applique à toutes les LIFs du cluster, ce qui peut ne pas être souhaitable.

Étapes

1. Mettre hors ligne toutes les LIFs sur cet adaptateur :

```
network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }  
-status-admin down
```

2. Mettez l'adaptateur hors ligne :

```
network fcp adapter modify -node node1 -adapter 0c -state down
```

Si l'adaptateur ne passe pas hors ligne, vous pouvez également retirer le câble du port d'adaptateur approprié du système.

3. Déterminez la vitesse maximale de l'adaptateur de port :

```
fcp adapter show -instance
```

Vous ne pouvez pas modifier la vitesse de l'adaptateur au-delà de la vitesse maximale.

4. Modifier la vitesse de l'adaptateur :

```
network fcp adapter modify -node node1 -adapter 0c -speed 16
```


5. Mettez la carte en ligne :

```
network fcp adapter modify -node node1 -adapter 0c -state up
```

6. Mettre en ligne toutes les LIFs sur l'adaptateur :

```
network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }  
-status-admin up
```

Ports FC pris en charge

Le nombre de ports FC intégrés et de ports CNA/UTA2 configurés pour FC varie en fonction du modèle du contrôleur. Les ports FC sont également disponibles par le biais d'adaptateurs d'extension FC cible pris en charge ou de cartes UTA2 supplémentaires configurées avec des adaptateurs FC SFP+.

Ports intégrés FC, UTA et UTA2

- Les ports intégrés peuvent être configurés individuellement en tant que ports FC cible ou initiateur.
- Le nombre de ports FC intégrés diffère selon le modèle de contrôleur.

Le "[NetApp Hardware Universe](#)" Contient la liste complète des ports FC intégrés sur chaque modèle de contrôleur.

- Les systèmes FAS2520 ne prennent pas en charge le protocole FC.

Ports FC des adaptateurs d'extension cibles

- Les adaptateurs d'extension cibles disponibles varient en fonction du modèle de contrôleur.

Le "[NetApp Hardware Universe](#)" contient une liste complète des adaptateurs d'extension cibles pour chaque modèle de contrôleur.

- Les ports de certains adaptateurs d'extension FC sont configurés en tant qu'initiateurs ou cibles en usine et ne peuvent pas être modifiés.

D'autres peuvent être configurés individuellement en tant que ports FC cible ou initiateur, comme les ports FC intégrés. Une liste complète est disponible dans "[NetApp Hardware Universe](#)".

Prévention des pertes de connectivité avec l'adaptateur X1133A-R6

Vous pouvez éviter la perte de connectivité lors d'une défaillance de port en configurant votre système avec des chemins redondants vers des HBA X1133A-R6 distincts.

La carte HBA X1133A-R6 est un adaptateur FC 16 Gbit à 4 ports composé de deux paires à 2 ports. L'adaptateur X1133A-R6 peut être configuré en mode cible ou initiateur. Chaque paire de 2 ports est prise en charge par un seul ASIC (par exemple, les ports 1 et 2 sur ASIC 1 et les ports 3 et 4 sur ASIC 2). Les deux ports d'un ASIC unique doivent être configurés pour fonctionner dans le même mode, soit en mode cible, soit en mode initiateur. En cas d'erreur sur l'ASIC prenant en charge une paire, les deux ports de la paire sont mis hors ligne.

Pour éviter ce risque de perte de connectivité, vous devez configurer votre système avec des chemins

redondants vers des HBA X1133A-R6 distincts, ou avec des chemins redondants vers des ports pris en charge par différents ASIC sur le HBA.

Gérez les adaptateurs X1143A-R6

Présentation des configurations de ports prises en charge pour les adaptateurs X1143A-R6

Par défaut, l'adaptateur X1143A-R6 est configuré en mode cible FC, mais vous pouvez configurer ses ports sous forme de ports Ethernet 10 Gb et FCoE (CNA) ou sous forme de ports d'initiateur FC 16 Gb ou cible. Cela nécessite différents adaptateurs SFP+.

Lorsqu'ils sont configurés pour Ethernet et FCoE, les adaptateurs X1143A-R6 prennent en charge le trafic cible FCoE et les cartes réseau simultanés sur le même port 10 GBE. Lorsqu'elle est configurée pour FC, chaque paire à deux ports qui partage le même ASIC peut être configurée individuellement pour le mode FC cible ou initiateur FC. Cela signifie qu'un seul adaptateur X1143A-R6 peut prendre en charge le mode cible FC sur une paire à deux ports et le mode initiateur FC sur une autre paire à deux ports. Les paires de ports connectées au même ASIC doivent être configurées dans le même mode.

En mode FC, l'adaptateur X1143A-R6 se comporte comme tout périphérique FC existant, avec des vitesses pouvant atteindre 16 Gbit/s. En mode CNA, vous pouvez utiliser l'adaptateur X1143A-R6 pour gérer simultanément le trafic NIC et FCoE et partager le même port 10 GbE. Le mode CNA ne prend en charge que le mode FC target pour la fonction FCoE.

Configurez les ports

Pour configurer l'adaptateur cible unifié (X1143A-R6), vous devez configurer les deux ports adjacents sur la même puce dans le même mode de personnalisation.

Étapes

1. Configurez les ports selon vos besoins pour Fibre Channel (FC) ou CNA (Converged Network adapter) à l'aide du `system node hardware unified-connect modify` commande.
2. Connectez les câbles appropriés pour FC ou Ethernet 10 Gbit.
3. Vérifiez que le SFP+ est installé correctement :

```
network fcp adapter show -instance -node -adapter
```

Pour le CNA, vous devez utiliser un SFP Ethernet 10 Gbit. Pour ce faire, vous devez utiliser un SFP 8 Gbit ou un SFP 16 Gbit, selon la structure FC à laquelle vous êtes connecté.

Remplacez le port UTA2 du mode CNA par le mode FC

Vous devez modifier le port UTA2 entre le mode CNA (Converged Network adapter) et le mode FC (Fibre Channel) pour prendre en charge l'initiateur FC et le mode cible FC. Vous devez modifier la personnalité du mode CNA en mode FC lorsque vous devez modifier le support physique qui connecte le port à son réseau.

Étapes

1. Mettez l'adaptateur hors ligne :

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
```

down

2. Modifiez le mode des ports :

```
ucadmin modify -node node_name -adapter adapter_name -mode fcp
```

3. Redémarrez le nœud, puis mettez l'adaptateur en ligne :

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin  
up
```

4. Informez votre administrateur ou votre gestionnaire vif de supprimer ou de supprimer le port, le cas échéant :

- Si le port est utilisé en tant que port d'origine d'une LIF, est membre d'un groupe d'interface (ifgrp), ou des VLAN hôtes, un administrateur doit faire ce qui suit :
 - i. Déplacez les LIF, retirez le port du ifgrp ou supprimez les VLAN.
 - ii. Supprimez manuellement le port en exécutant le `network port delete` commande.

Si le `network port delete` échec de la commande, l'administrateur doit corriger les erreurs, puis exécuter de nouveau la commande.

- Si le port n'est pas utilisé comme port de base d'une LIF, n'est pas membre d'un ifgrp. Il ne héberge pas les VLAN, alors le vif Manager doit supprimer le port de ses enregistrements au moment du redémarrage.

Si le vif Manager ne supprime pas le port, l'administrateur doit le supprimer manuellement après le redémarrage à l'aide du `network port delete` commande.

```
net-f8040-34::> network port show
```

```
Node: net-f8040-34-01
```

Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) Admin/Oper	Health Status
...						
e0i	Default	Default	down	1500	auto/10	-
e0f	Default	Default	down	1500	auto/10	-
...						

```
net-f8040-34::> ucadmin show
```

Node	Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin Status
net-f8040-34-01	0e	cna	target	-	-	

```

offline
  net-f8040-34-01
                                0f      cna      target      -      -
offline
  ...

  net-f8040-34::> network interface create -vs net-f8040-34 -lif m
                    -role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
                    -netmask 255.255.255.0

  net-f8040-34::> network interface show -fields home-port, curr-port

vserver lif                                home-port curr-port
-----
Cluster net-f8040-34-01_clus1 e0a          e0a
Cluster net-f8040-34-01_clus2 e0b          e0b
Cluster net-f8040-34-01_clus3 e0c          e0c
Cluster net-f8040-34-01_clus4 e0d          e0d
net-f8040-34
      cluster_mgmt          e0M          e0M
net-f8040-34
      m                      e0e          e0i
net-f8040-34
      net-f8040-34-01_mgmt1 e0M          e0M
7 entries were displayed.

net-f8040-34::> uadmin modify local 0e fc

Warning: Mode on adapter 0e and also adapter 0f will be changed to
fc.
Do you want to continue? {y|n}: y
Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

net-f8040-34::> reboot local
                    (system node reboot)

Warning: Are you sure you want to reboot node "net-f8040-34-01"?
{y|n}: y

```

5. Vérifiez que le SFP+ est installé correctement :

```
network fcp adapter show -instance -node -adapter
```

Pour le CNA, vous devez utiliser un SFP Ethernet 10 Gbit. Pour ce faire, vous devez utiliser un SFP 8 Gbit

ou un SFP 16 Gbit avant de modifier la configuration sur le nœud.

Modifiez les modules optiques des adaptateurs CNA/UTA2

Vous devez modifier les modules optiques de l'adaptateur cible unifié (CNA/UTA2) pour prendre en charge le mode de personnalisation sélectionné pour l'adaptateur.

Étapes

1. Vérifiez le SFP+ actuel utilisé dans la carte. Ensuite, remplacez le SFP+ actuel par le SFP+ approprié pour la personnalité préférée (FC ou CNA).
2. Retirez les modules optiques actuels de l'adaptateur X1143A-R6.
3. Insérez les modules appropriés pour l'optique de votre mode de personnalisation préféré (FC ou CNA).
4. Vérifiez que le SFP+ est installé correctement :

```
network fcp adapter show -instance -node -adapter
```

Les modules SFP+ pris en charge et les câbles Twinax (Cisco) sont répertoriés dans le ["NetApp Hardware Universe"](#).

Afficher les paramètres de la carte

Pour afficher les paramètres de votre adaptateur cible unifié (X1143A-R6), vous devez exécuter le `system hardware unified-connect show` commande permettant d'afficher tous les modules de votre contrôleur.

Étapes

1. Démarrez votre contrôleur sans les câbles connectés.
2. Exécutez le `system hardware unified-connect show` commande pour afficher la configuration des ports et les modules.
3. Afficher les informations relatives aux ports avant de configurer le CNA et les ports.

Configurations FCoE

Présentation des manières de configurer FCoE

FCoE peut être configuré de différentes manières avec les commutateurs FCoE. Les configurations à connexion directe ne sont pas prises en charge par la FCoE.

Toutes les configurations FCoE sont à double structure, entièrement redondantes et requièrent un logiciel de chemins d'accès multiples côté hôte. Dans toutes les configurations FCoE, vous pouvez avoir plusieurs commutateurs FCoE et FC dans le chemin entre l'initiateur et la cible, dans la limite maximale du nombre de sauts. Pour connecter les commutateurs les uns aux autres, les commutateurs doivent exécuter une version de firmware qui prend en charge les liens ISL Ethernet. Dans toutes les configurations FCoE, chaque hôte peut être configuré avec un système d'exploitation différent.

Les configurations FCoE requièrent des commutateurs Ethernet qui prennent explicitement en charge les fonctionnalités FCoE. Les configurations FCoE sont validées par le biais du même processus d'interopérabilité et d'assurance qualité que les commutateurs FC. Les configurations prises en charge sont répertoriées dans la matrice d'interopérabilité. Certains paramètres inclus dans ces configurations prises en charge sont le modèle

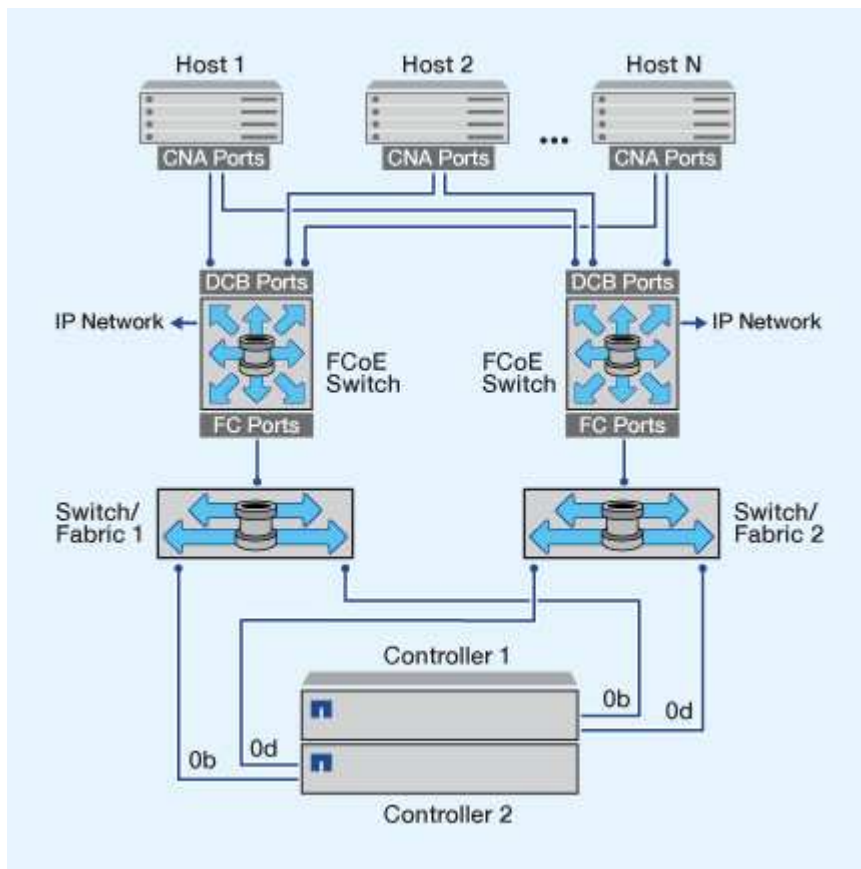
de commutateur, le nombre de commutateurs pouvant être déployés dans une structure unique et la version de micrologiciel du commutateur prise en charge.

Les numéros de ports des adaptateurs d'extension FC target de l'illustration sont à titre d'exemples. Les numéros réels des ports peuvent varier en fonction des connecteurs d'extension dans lesquels les adaptateurs d'extension de la cible FCoE sont installés.

Initiateur FCoE sur la cible FC

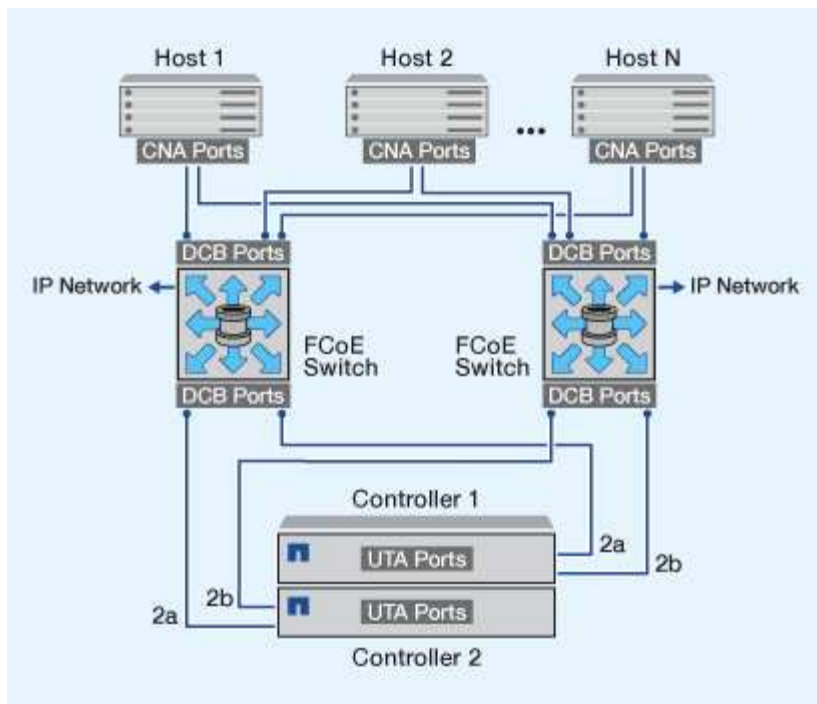
En utilisant les initiateurs FCoE (CNA), vous pouvez connecter des hôtes aux deux contrôleurs d'une paire haute disponibilité via des commutateurs FCoE vers les ports cible FC. Le commutateur FCoE doit également posséder des ports FC. L'initiateur FCoE hôte se connecte toujours au commutateur FCoE. Le commutateur FCoE peut se connecter directement à la cible FC ou se connecter à la cible FC via des commutateurs FC.

L'illustration suivante montre les CNA hôtes connectés à un commutateur FCoE, puis à un commutateur FC avant de se connecter à la paire haute disponibilité :



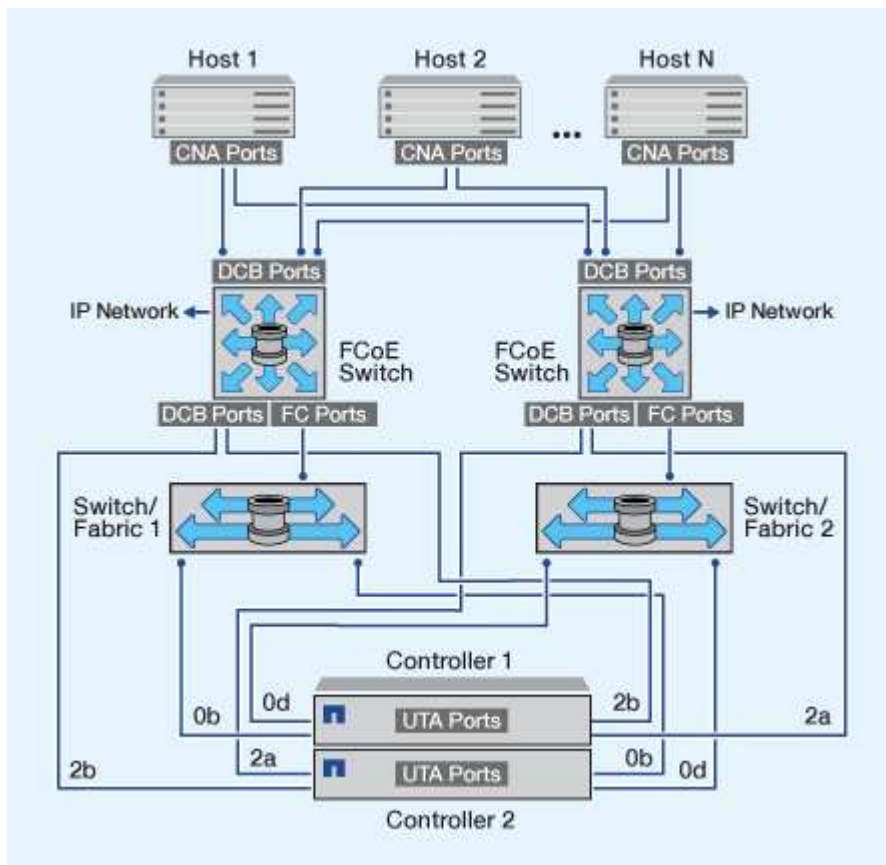
Initiateur FCoE vers la cible FCoE

En utilisant les initiateurs FCoE hôtes (CNA), vous pouvez connecter les hôtes aux deux contrôleurs d'une paire haute disponibilité aux ports cibles FCoE (également appelés UTAS ou UTA2) à l'aide des commutateurs FCoE.



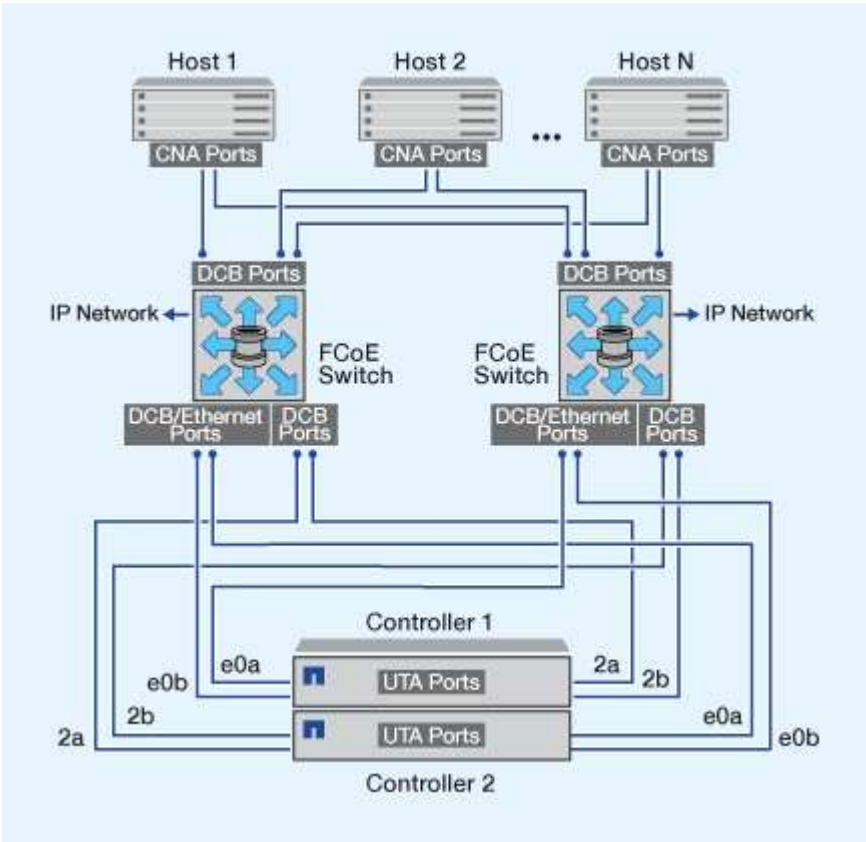
Initiateur FCoE sur les cibles FCoE et FC

En utilisant les initiateurs FCoE hôtes (CNA), vous pouvez connecter les hôtes aux deux contrôleurs d'une paire haute disponibilité aux ports cibles FCoE et FC (également appelés UTA ou UTA2) à l'aide des commutateurs FCoE.



FCoE combiné avec les protocoles de stockage IP

En utilisant les initiateurs FCoE hôtes (CNA), vous pouvez connecter les hôtes aux deux contrôleurs d'une paire haute disponibilité aux ports cibles FCoE (également appelés UTAS ou UTA2) à l'aide des commutateurs FCoE. Les ports FCoE ne peuvent pas utiliser l'agrégation de liens traditionnelle vers un commutateur unique. Les commutateurs Cisco prennent en charge un type spécial d'agrégation de liens (Virtual Port Channel) qui prend en charge le protocole FCoE. Un canal de port virtuel rassemble des liaisons individuelles vers deux commutateurs. Vous pouvez également utiliser les canaux de port virtuel pour d'autres trafics Ethernet. Les ports utilisés pour le trafic autre que FCoE, notamment les protocoles NFS, SMB, iSCSI et tout autre trafic Ethernet, peuvent utiliser des ports Ethernet classiques sur les switches FCoE.



Combinaisons d’initiateurs et de cibles FCoE

Certaines combinaisons d’initiateurs et de cibles FCoE et FC classiques sont prises en charge.

Initiateurs FCoE

Vous pouvez utiliser des initiateurs FCoE dans des ordinateurs hôtes avec des cibles FCoE et FC traditionnelles dans des contrôleurs de stockage. L’initiateur FCoE de l’hôte doit se connecter à un commutateur DCB (pontage du centre de données) FCoE ; la connexion directe à une cible n’est pas prise en charge.

Le tableau suivant répertorie les combinaisons prises en charge :

Initiateur	Cible	Pris en charge ?
FC	FC	Oui.

Initiateur	Cible	Pris en charge ?
FC	FCoE	Oui.
FCoE	FC	Oui.
FCoE	FCoE	Oui.

Cibles de la FCoE

Vous pouvez combiner les ports cibles FCoE avec des ports FC 4 Go, 8 Go ou 16 Go sur le contrôleur de stockage, que les ports FC soient des adaptateurs cibles supplémentaires ou des ports intégrés. Vous pouvez avoir des adaptateurs cibles FCoE et FC dans le même contrôleur de stockage.



Les règles relatives à l'association des ports FC intégrés et d'extension sont toujours applicables.

Nombre de sauts pris en charge par FCoE

Le nombre maximal de sauts Fibre Channel over Ethernet (FCoE) pris en charge entre un hôte et un système de stockage dépend du fournisseur du commutateur et de la prise en charge du système de stockage pour les configurations FCoE.

Le nombre de sauts est défini comme le nombre de commutateurs dans le chemin entre l'initiateur (hôte) et la cible (système de stockage). La documentation de Cisco Systems fait également référence à cette valeur comme le *diamètre de la structure SAN*.

Pour le protocole FCoE, vous pouvez avoir connecté les commutateurs FCoE aux commutateurs FC.

Pour les connexions FCoE de bout en bout, les commutateurs FCoE doivent exécuter une version de firmware qui prend en charge les liaisons ISL (Ethernet Inter-switch Links).

Le tableau suivant répertorie le nombre maximal de sauts pris en charge :

Changer de fournisseur	Nombre de sauts pris en charge
Brocade	7 pour FC 5 pour la FCoE
Cisco	7 Il est possible d'utiliser jusqu'à 3 commutateurs FCoE.

Segmentation Fibre Channel et FCoE

Présentation de la segmentation Fibre Channel et FCoE

Une zone FC, FC-NVMe ou FCoE est un regroupement logique d'un ou de plusieurs

ports au sein d'une structure. Pour que les périphériques puissent se voir, se connecter, créer des sessions entre eux et communiquer, les deux ports doivent avoir une zone commune. La segmentation à un seul initiateur est recommandée.

Motifs de la segmentation

- La segmentation réduit ou élimine la *diaphonie* entre les HBA initiateurs.

Cela se produit même dans les petits environnements et est l'un des meilleurs arguments pour la mise en œuvre du zonage. Les sous-ensembles logiques de structure créés par la segmentation éliminent les problèmes de diaphonie.

- La segmentation réduit le nombre de chemins disponibles vers un port FC, FC-NVMe ou FCoE spécifique. Elle diminue le nombre de chemins entre un hôte et une LUN précise visible.

Par exemple, certaines solutions de chemins d'accès multiples du système d'exploitation hôte ont une limite sur le nombre de chemins qu'elles peuvent gérer. La segmentation peut réduire le nombre de chemins qu'un pilote de chemins d'accès multiples du système d'exploitation voit. Si une solution de chemins d'accès multiples n'est pas installée sur un hôte, vérifiez qu'un seul chemin d'accès à une LUN est visible en utilisant le zoning dans la structure ou une combinaison de mappage de LUN sélectif (SLM) et de jeux de ports dans le SVM.

- Le zonage renforce la sécurité en limitant l'accès et la connectivité aux points de terminaison qui partagent une zone commune.

Les ports qui n'ont pas de zones en commun ne peuvent pas communiquer entre eux.

- La segmentation améliore la fiabilité du SAN en isolant les problèmes et réduit le temps de résolution des problèmes en limitant l'espace disponible.

Recommandations pour la segmentation

- Vous devez implémenter le zoning à tout moment si quatre hôtes ou plus sont connectés à un SAN ou si SLM n'est pas implémenté sur les nœuds vers un SAN.
- Bien que la segmentation WWNN (World Wide Node Name) soit possible avec certains fournisseurs de commutateurs, la segmentation WWPN (World Wide Port Name) est nécessaire pour définir correctement un port spécifique et pour utiliser NPIV efficacement.
- La taille de la zone doit être limitée tout en maintenant la facilité de gestion.

Pour limiter la taille, vous pouvez faire se chevaucher plusieurs zones. En principe, une zone est définie pour chaque hôte ou cluster hôte.

- Vous devez utiliser la segmentation à un seul initiateur pour éliminer la diaphonie entre les HBA initiateurs.

Segmentation basée sur le World Wide Name

La segmentation basée sur le World Wide Name (WWN) spécifie le WWN des membres à inclure dans la zone. Lors de la segmentation dans ONTAP, vous devez utiliser la segmentation WWPN (World Wide Port Name).

La segmentation WWPN apporte la flexibilité, car l'accès n'est pas déterminé par l'emplacement de connexion physique du dispositif à la structure. Vous pouvez déplacer un câble d'un port à un autre sans reconfigurer les zones.

Pour les chemins Fibre Channel vers les contrôleurs de stockage qui exécutent ONTAP, assurez-vous que les commutateurs FC sont zonés à l'aide des WWPN des interfaces logiques cibles (LIF), et non pas des WWPN des ports physiques du nœud. Pour plus d'informations sur les LIF, reportez-vous au *ONTAP Network Management Guide*.

"Gestion du réseau"

Zones individuelles

Dans la configuration de segmentation recommandée, il existe un initiateur hôte par zone. La zone se compose du port hôte et d'une ou plusieurs LIF cible sur les nœuds de stockage qui fournissent l'accès aux LUN jusqu'au nombre souhaité de chemins par cible. Cela signifie que les hôtes accédant aux mêmes nœuds ne peuvent pas voir les ports des autres hôtes, mais que l'initiateur peut accéder à tous les nœuds.

Vous devez ajouter toutes les LIF du serveur virtuel de stockage (SVM) dans la zone avec l'initiateur hôte. Cela vous permet de déplacer des volumes ou des LUN sans modifier vos zones existantes ni créer de nouvelles zones.

Pour les chemins Fibre Channel vers les nœuds qui exécutent ONTAP, assurez-vous que les commutateurs FC sont zonés à l'aide des WWPN des interfaces logiques cibles (LIF), et non pas des WWPN des ports physiques du nœud. Les WWPN des ports physiques commencent par « 50 » et les WWPN des LIF commencent par « 20 ».

Segmentation à structure unique

Dans une configuration à structure unique, vous pouvez toujours connecter chaque initiateur hôte à chaque nœud de stockage. Vous avez besoin d'un logiciel de chemins d'accès multiples sur l'hôte pour gérer les chemins multiples. Chaque hôte doit avoir deux initiateurs pour les chemins d'accès multiples pour fournir la résilience dans la solution.

Chaque initiateur doit disposer d'au moins une LIF à partir de chaque nœud auquel celui-ci peut accéder. Le zoning doit permettre à au moins un chemin entre l'initiateur hôte et la paire haute disponibilité de nœuds dans le cluster pour fournir un chemin d'accès à la connectivité LUN. Cela signifie que chaque initiateur sur l'hôte peut ne disposer que d'une seule LIF cible par nœud dans sa configuration de zone. Si des chemins d'accès multiples sont nécessaires vers le même nœud ou vers plusieurs nœuds du cluster, chaque nœud aura plusieurs LIF par nœud dans sa configuration de zone. Cela permet à l'hôte d'accéder toujours à ses LUN en cas de défaillance d'un nœud ou si un volume contenant la LUN est déplacé vers un autre nœud. Il est également nécessaire de définir correctement les nœuds de reporting.

Les configurations à structure unique sont prises en charge, mais ne sont pas considérées comme hautement disponibles. La défaillance d'un seul composant peut entraîner la perte de l'accès aux données.

Dans la figure suivante, l'hôte a deux initiateurs et exécute un logiciel de chemins d'accès multiples. Il y a deux zones :

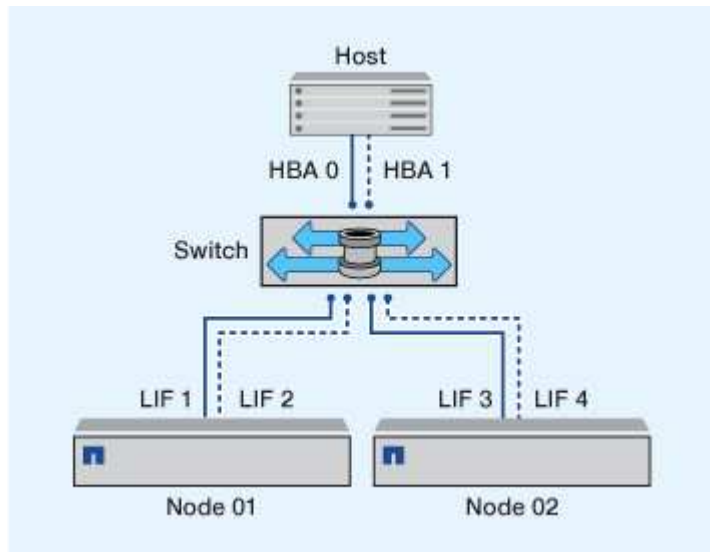


la convention de nom utilisée dans cette figure ne constitue qu'une recommandation d'une convention de nom possible que vous pouvez utiliser pour votre solution ONTAP.

- Zone 1 : HBA 0, LIF_1 et LIF_3

- Zone 2 : HBA 1, LIF_2 et LIF_4

Si la configuration incluait plus de nœuds, les LIF pour les nœuds supplémentaires seraient incluses dans ces zones.



Dans cet exemple, vous pouvez aussi avoir les quatre LIF dans chaque zone. Dans ce cas, les zones seraient les suivantes :

- Zone 1 : HBA 0, LIF_1, LIF_2, LIF_3 et LIF_4
- Zone 2 : HBA 1, LIF_1, LIF_2, LIF_3 et LIF_4



Le système d'exploitation hôte et le logiciel de chemins d'accès multiples doivent prendre en charge le nombre de chemins pris en charge qui sont utilisés pour accéder aux LUN sur les nœuds. Pour déterminer le nombre de chemins utilisés pour accéder aux LUN sur les nœuds, reportez-vous à la section limites de configuration SAN.

Informations associées

["NetApp Hardware Universe"](#)

Segmentation par paire haute disponibilité à double fabric

Dans les configurations à double structure, vous pouvez connecter chaque initiateur hôte à chaque nœud du cluster. Chaque initiateur hôte utilise un autre commutateur pour accéder aux nœuds du cluster. Vous avez besoin d'un logiciel de chemins d'accès multiples sur l'hôte pour gérer les chemins multiples.

Les configurations à double structure sont considérées comme haute disponibilité, car l'accès aux données est maintenu en cas de défaillance d'un composant.

Dans la figure suivante, l'hôte a deux initiateurs et exécute un logiciel de chemins d'accès multiples. Il y a deux zones. SLM est configuré de sorte que tous les nœuds soient considérés comme des nœuds de rapport.



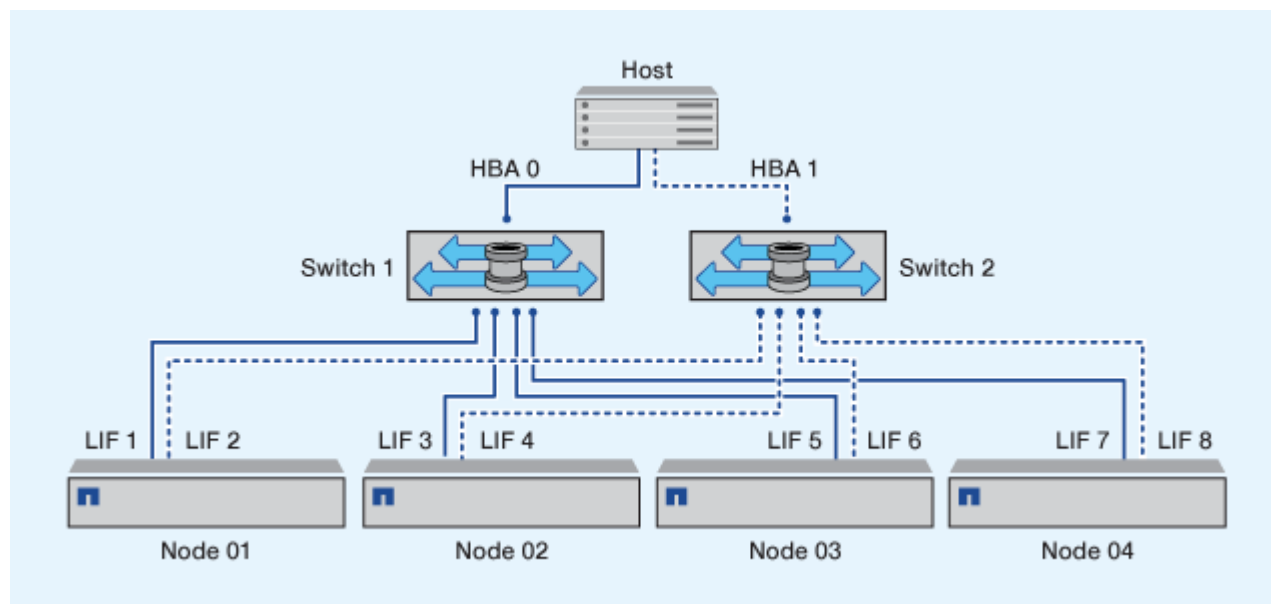
la convention de nom utilisée dans cette figure ne constitue qu'une recommandation d'une convention de nom possible que vous pouvez utiliser pour votre solution ONTAP.

- Zone 1 : HBA 0, LIF_1, LIF_3, LIF_5 et LIF_7
- Zone 2 : HBA 1, LIF_2, LIF_4, LIF_6 et LIF_8

Chaque initiateur hôte est zoné via un autre commutateur. La zone 1 est accessible via le commutateur 1. La zone 2 est accessible via le commutateur 2.

Chaque initiateur peut accéder à une LIF sur chaque nœud. Cela permet à l'hôte d'accéder toujours à ses LUN en cas de panne d'un nœud. Les SVM ont accès à toutes les LIF iSCSI et FC sur chaque nœud d'une solution en cluster, en fonction du paramètre SLM (Selective LUN Map) et de la configuration de nœud de reporting. Vous pouvez utiliser la segmentation de switch SLM, portsets ou FC pour réduire le nombre de chemins d'un SVM à l'hôte et le nombre de chemins d'un SVM vers une LUN.

Si la configuration incluait plus de nœuds, les LIF pour les nœuds supplémentaires seraient incluses dans ces zones.



Le système d'exploitation hôte et le logiciel de chemins d'accès multiples doivent prendre en charge le nombre de chemins d'accès utilisés pour accéder aux LUN sur les nœuds.

Informations associées

["NetApp Hardware Universe"](#)

Restrictions de segmentation pour les commutateurs Cisco FC et FCoE

Si vous utilisez des commutateurs Cisco FC et FCoE, une seule zone de structure ne doit pas contenir plus d'une LIF cible pour le même port physique. Si plusieurs LIF présentes sur le même port se trouvent dans la même zone, les ports LIF peuvent ne pas effectuer de restauration suite à une perte de connexion.

Le protocole FC-NVMe utilise régulièrement des switches FC de la même manière qu'ils sont utilisés pour le protocole FC.

- Plusieurs LIF pour les protocoles FC et FCoE peuvent partager des ports physiques sur un nœud tant qu'ils se trouvent dans des zones différentes.

- FC-NVMe et FCoE ne peuvent pas partager le même port physique.
- Les protocoles FC et FC-NVMe peuvent partager le même port physique de 32 Go.
- Les commutateurs FC et FCoE Cisco exigent que chaque LIF d'un port donné se trouve dans une zone distincte des autres LIF du port en question.
- Une seule zone peut avoir à la fois des LIF FC et FCoE. Une zone peut contenir une LIF à partir de chaque port cible du cluster, mais veillez à ne pas dépasser les limites de chemin de l'hôte et à vérifier la configuration SLM.
- Les LIF présentes sur différents ports physiques peuvent se trouver dans la même zone.
- Les commutateurs Cisco exigent la séparation des LIF.

Bien qu'elles ne soient pas requises, la séparation des LIF est recommandée pour tous les commutateurs

Conditions requises pour les configurations SAN partagées

Les configurations SAN partagées sont des hôtes connectés à la fois aux systèmes de stockage ONTAP et aux systèmes de stockage d'autres fournisseurs. L'accès aux systèmes de stockage ONTAP et aux systèmes de stockage d'autres fournisseurs à partir d'un hôte unique est pris en charge, dans la mesure où plusieurs conditions sont respectées.

Pour tous les systèmes d'exploitation hôtes, il est recommandé d'utiliser des adaptateurs distincts pour la connexion aux systèmes de stockage de chaque fournisseur. L'utilisation de cartes séparées réduit les risques de conflits entre les pilotes et les paramètres. Pour les connexions à un système de stockage ONTAP, le modèle d'adaptateur, le BIOS, le firmware et le pilote doivent être répertoriés comme pris en charge dans l'outil de matrice d'interopérabilité NetApp.

Vous devez définir les valeurs de temporisation requises ou recommandées et d'autres paramètres de stockage pour l'hôte. Vous devez toujours installer le logiciel NetApp ou appliquer les paramètres NetApp en dernier.

- Pour AIX, vous devez appliquer les valeurs de la version AIX Host Utilities répertoriée dans l'outil Interoperability Matrix Tool pour votre configuration.
- Pour ESX, vous devez appliquer les paramètres de l'hôte à l'aide de Virtual Storage Console pour VMware vSphere.
- Pour HP-UX, vous devez utiliser les paramètres de stockage par défaut HP-UX.
- Pour Linux, vous devez appliquer les valeurs de la version Linux Host Utilities répertoriée dans la matrice d'interopérabilité pour votre configuration.
- Pour Solaris, vous devez appliquer les valeurs de la version Solaris Host Utilities répertoriée dans la matrice d'interopérabilité pour votre configuration.
- Pour Windows, vous devez installer la version des utilitaires d'hôtes Windows répertoriée dans la matrice d'interopérabilité pour votre configuration.

Informations associées

["Matrice d'interopérabilité NetApp"](#)

Configurations SAN dans un environnement MetroCluster

Configurations SAN dans un environnement MetroCluster

Vous devez tenir compte de certaines considérations relatives à l'utilisation des configurations SAN dans un environnement MetroCluster.

- Les configurations MetroCluster ne prennent pas en charge les configurations VSAN « routées » de la structure FC front-end.
- À partir de ONTAP 9.15.1, les configurations IP MetroCluster à quatre nœuds sont prises en charge par le protocole NVMe/TCP.
- Depuis la version ONTAP 9.12.1, les configurations IP MetroCluster à quatre nœuds sont prises en charge sur NVMe/FC. Les configurations MetroCluster ne sont pas prises en charge pour les réseaux NVMe frontaux avant ONTAP 9.12.1.
- D'autres protocoles SAN, tels que iSCSI, FC et FCoE, sont pris en charge dans les configurations MetroCluster.
- Lors de l'utilisation de configurations client SAN, vous devez vérifier si des considérations spéciales sont incluses dans les configurations MetroCluster dans les notes fournies dans le ["Matrice d'interopérabilité NetApp" \(IMT\)](#).
- Les systèmes d'exploitation et les applications doivent offrir une résilience d'E/S de 120 secondes pour prendre en charge le basculement automatique non planifié et le basculement manuel d'utilisation (Tiebreaker) MetroCluster.
- Les configurations MetroCluster utilisent les mêmes WWN et WWPN des deux côtés de la structure FC frontale.

Informations associées

- ["Tout savoir sur la protection des données et la reprise après incident MetroCluster"](#)
- ["Article de la base de connaissances : que sont les considérations relatives à la prise en charge des hôtes AIX dans une configuration MetroCluster ?"](#)
- ["Article de la base de connaissances : considérations relatives au support des hôtes Solaris dans une configuration MetroCluster"](#)

Évitez le chevauchement des ports entre le basculement et le rétablissement

Dans un environnement SAN, vous pouvez configurer les commutateurs frontaux afin d'éviter tout chevauchement lorsque l'ancien port passe hors ligne et que le nouveau port est connecté.

Lors du basculement, le port FC du site survivant peut se connecter à la structure avant que la structure n'ait détecté que le port FC du site de reprise sur incident est hors ligne et que ce port a été supprimé du nom et des services d'annuaire.

Si le port FC de l'incident n'est pas encore supprimé, la tentative de connexion à la structure du port FC du site survivant peut être rejetée à cause d'un WWPN dupliqué. Ce comportement des commutateurs FC peut être modifié afin de respecter la connexion du périphérique précédent et non l'ancienne. Vous devez vérifier les effets de ce comportement sur d'autres périphériques de structure. Contactez le fournisseur du commutateur pour plus d'informations.

Choisissez la procédure correcte selon votre type de commutateur.

Exemple 14. Étapes

Commutateur Cisco

1. Connectez-vous au commutateur et connectez-vous.
2. Passer en mode configuration :

```
switch# config t  
switch(config)#
```

3. Remplacez la première entrée de périphérique dans la base de données du serveur de noms par le nouveau périphérique :

```
switch(config)# no fcns reject-duplicate-pwvn vsan 1
```

4. Dans les commutateurs exécutant NX-OS 8.x, vérifiez que le délai de mise en veille flogi est défini sur zéro :

- a. Afficher le délai de mise au repos :

```
switch(config)# show flogi interval info \ i quiesce
```

```
Stats:  fs flogi quiesce timerval:  0
```

- b. Si la sortie de l'étape précédente n'indique pas que le délai est égal à zéro, définissez-le sur zéro :

```
switch(config)# flogi scale enable
```

```
switch(config)$ flogi quiesce timeout 0
```

Commutateur Brocade

1. Connectez-vous au commutateur et connectez-vous.
2. Entrez le `switchDisable` commande.
3. Entrez le `configure` et appuyez sur `y` à l'invite.

```
F-Port login parameters (yes, y, no, n): [no] y
```

4. Choisir le paramètre 1 :


```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. Répondez aux autres invites ou appuyez sur **Ctrl + D**.

6. Entrez le `switchEnable` commande.

Informations associées

["Effectuer un basculement pour les tests ou la maintenance"](#)

Prise en charge des chemins d'accès multiples sur l'hôte

Prise en charge des hôtes pour la présentation des chemins d'accès multiples

ONTAP utilise toujours le protocole ALUA (Asymmetric Logical Unit Access) pour les chemins FC et iSCSI. Veillez à utiliser des configurations hôtes qui prennent en charge ALUA pour les protocoles FC et iSCSI.

Depuis la version ONTAP 9.5, le basculement/rétablissement de paire haute disponibilité multivoie est pris en charge dans les configurations NVMe utilisant un accès asynchrone à l'espace de noms (ANA). Dans ONTAP 9.4, NVMe ne prend en charge qu'un chemin d'accès de l'hôte à la cible. L'hôte applicatif doit gérer le basculement des chemins vers son partenaire haute disponibilité (HA).

Pour plus d'informations sur les configurations d'hôte spécifiques prenant en charge ALUA ou ANA, reportez-vous au ["Matrice d'interopérabilité NetApp"](#) et ["Configuration de l'hôte SAN ONTAP"](#) pour votre système d'exploitation hôte.

Lorsque le logiciel de chemins d'accès multiples de l'hôte est requis

Si il existe plusieurs chemins entre les interfaces logiques (LIF) du SVM et la structure, un logiciel de chemins d'accès multiples est nécessaire. Il est nécessaire de disposer de chemins d'accès multiples sur l'hôte chaque fois que l'hôte peut accéder à une LUN via plusieurs chemins.

Le logiciel de chemins d'accès multiples présente un seul disque au système d'exploitation pour tous les chemins d'accès à une LUN. Sans le logiciel de chemins d'accès multiples, le système d'exploitation pourrait traiter chaque chemin en tant que disque distinct, ce qui peut entraîner une corruption des données.

Votre solution est considérée comme ayant plusieurs chemins si vous avez l'un des suivants :

- Un port initiateur unique sur l'hôte reliant plusieurs LIF SAN au sein du SVM
- Plusieurs ports initiateurs se connectant à une seule LIF SAN dans le SVM
- Plusieurs ports initiateurs qui se fixent sur plusieurs LIF SAN au sein du SVM

Le logiciel de chemins d'accès multiples est recommandé dans les configurations haute disponibilité. Outre le mappage sélectif des LUN, il est recommandé d'utiliser des zoning switch FC ou des ensembles de ports pour limiter les chemins d'accès aux LUN.

Le logiciel de chemins d'accès multiples est également appelé le logiciel MPIO (chemins d'accès E/S multiples).

Nombre recommandé de chemins entre l'hôte et les nœuds dans le cluster

Vous ne devez pas dépasser huit chemins entre votre hôte et chaque nœud du cluster, en tenant compte du nombre total de chemins pouvant être pris en charge pour le système d'exploitation hôte et les chemins d'accès multiples utilisés sur cet hôte.

Au moins deux chemins par LUN doivent être connectés à chaque nœud de reporting via le mappage de LUN sélectif (SLM) utilisé par la machine virtuelle de stockage (SVM) dans votre cluster. Cela élimine les points de défaillance uniques et permet au système de résister aux défaillances des composants.

Si votre cluster contient quatre nœuds ou plus, ou plus de quatre ports cibles utilisés par les SVM sur l'un de vos nœuds, Vous pouvez utiliser les méthodes suivantes pour limiter le nombre de chemins pouvant être utilisés pour accéder aux LUN sur vos nœuds. De cette manière, vous ne devez pas dépasser le maximum recommandé de huit chemins.

- SLM

SLM réduit le nombre de chemins de l'hôte vers le LUN vers uniquement les chemins sur le nœud possédant le LUN et le partenaire HA du nœud propriétaire. SLM est activé par défaut.

- Ensembles de ports pour iSCSI
- Mappages de FC igroup depuis votre hôte
- Segmentation des commutateurs FC

Informations associées

["Administration SAN"](#)

Limites de configuration

Identification du nombre de nœuds pris en charge dans les configurations SAN

Le nombre de nœuds par cluster pris en charge par ONTAP varie en fonction de la version de ONTAP, des modèles de contrôleur de stockage dans le cluster et du protocole de vos nœuds de cluster.

Description de la tâche

Si un nœud du cluster est configuré pour les protocoles FC, FC-NVMe, FCoE ou iSCSI, ce cluster est limité aux limites du nœud SAN. Les limites de nœuds basées sur les contrôleurs de votre cluster sont répertoriées dans le *Hardware Universe*.

Étapes

1. Accédez à ["NetApp Hardware Universe"](#).
2. Cliquez sur **plates-formes** dans le coin supérieur gauche (en regard du bouton **Home**) et sélectionnez le type de plate-forme.
3. Cochez la case en regard de votre version de ONTAP.

Une nouvelle colonne s'affiche pour vous permettre de choisir vos plates-formes.

4. Cochez les cases en regard des plateformes utilisées dans votre solution.
5. Désélectionnez la case **Sélectionner tout** dans la colonne **Choisissez vos spécifications**.
6. Cochez la case **Max Nodes per Cluster (NAS/SAN)**.
7. Cliquez sur **Afficher les résultats**.

Informations associées

["NetApp Hardware Universe"](#)

Détermination du nombre d'hôtes pris en charge par cluster dans les configurations FC et FC-NVMe

Le nombre maximal d'hôtes SAN pouvant être connectés à un cluster varie considérablement en fonction de votre combinaison spécifique de plusieurs attributs de cluster, tels que le nombre d'hôtes connectés à chaque nœud de cluster, les initiateurs par hôte, les sessions par hôte et les nœuds du cluster.

Description de la tâche

Pour les configurations FC et FC-NVMe, vous devez utiliser le nombre de nases cibles (ITN) dans votre système pour déterminer si vous pouvez ajouter d'autres hôtes à votre cluster.

Un ITN représente un chemin entre l'initiateur de l'hôte et la cible du système de stockage. Le nombre maximum de N ITN par nœud dans les configurations FC et FC-NVMe est de 2,048. Tant que vous êtes en dessous du nombre maximum d'ITN, vous pouvez continuer à ajouter des hôtes à votre cluster.

Pour déterminer le nombre d'ITN utilisés dans votre cluster, effectuez les opérations suivantes pour chaque nœud du cluster.

Étapes

1. Identifier toutes les LIFs sur un certain nœud.
2. Lancer la commande suivante pour chaque LIF sur le nœud :

```
fcv initiator show -fields wwpn, lif
```

Le nombre d'entrées affichées au bas de la sortie de la commande représente votre nombre d'ITN pour cette LIF.

3. Notez le nombre de moustiquaires imprégnées d'insecticide affichées pour chaque LIF.
4. Ajoutez le nombre de moustiquaires imprégnées d'insecticide pour chaque LIF sur chaque nœud de votre cluster.

Ce total représente le nombre d'ITN dans votre cluster.

Identification du nombre d'hôtes pris en charge dans les configurations iSCSI

Le nombre maximal d'hôtes SAN pouvant être connectés dans des configurations iSCSI varie considérablement en fonction de votre combinaison spécifique de plusieurs attributs de cluster, tels que le nombre d'hôtes connectés à chaque nœud de cluster, les initiateurs par hôte, les connexions par hôte et les nœuds du cluster.

Description de la tâche

Le nombre d'hôtes pouvant être connectés directement à un nœud ou qui peuvent être connectés via un ou plusieurs commutateurs dépend du nombre de ports Ethernet disponibles. Le nombre de ports Ethernet disponibles est déterminé par le modèle du contrôleur et par le nombre et le type d'adaptateurs installés dans le contrôleur. Le nombre de ports Ethernet pris en charge pour les contrôleurs et les adaptateurs est disponible dans *Hardware Universe*.

Pour toutes les configurations de clusters à plusieurs nœuds, vous devez déterminer le nombre de sessions iSCSI par nœud pour savoir si vous pouvez ajouter d'autres hôtes à votre cluster. Tant que le cluster est inférieur au nombre maximal de sessions iSCSI par nœud, vous pouvez continuer à ajouter des hôtes au cluster. Le nombre maximal de sessions iSCSI par nœud varie en fonction des types de contrôleurs du cluster.

Étapes

1. Identifiez tous les groupes de portails cible sur le nœud.
2. Vérifier le nombre de sessions iSCSI pour chaque groupe de portails cible sur le nœud :

```
iscsi session show -tpgroup tpgroup
```

Le nombre d'entrées affichées au bas de la sortie de la commande représente le nombre de sessions iSCSI pour ce groupe de portails cible.

3. Notez le nombre de sessions iSCSI affichées pour chaque groupe de portails cible.
4. Ajoutez le nombre de sessions iSCSI pour chaque groupe de portails cible sur le nœud.

Le total représente le nombre de sessions iSCSI sur votre nœud.

Limites de configuration des commutateurs FC

Les commutateurs Fibre Channel ont des limites de configuration maximales, y compris le nombre de connexions prises en charge par port, groupe de ports, lame et commutateur. Les fournisseurs des commutateurs documentent leurs limites prises en charge.

Chaque interface logique FC (LIF) se connecte à un port de commutateur FC. Le nombre total de connexions à partir d'une seule cible sur le nœud est égal au nombre de LIF plus une connexion pour le port physique sous-jacent. Ne dépassez pas les limites de configuration du fournisseur du commutateur pour les connexions ou d'autres valeurs de configuration. Cela est également vrai pour les initiateurs utilisés côté hôte dans les environnements virtualisés avec NPIV activé. Ne dépassez pas les limites de configuration du fournisseur pour les connexions pour la cible ou les initiateurs utilisés dans la solution.

Limites des commutateurs Brocade

Les limites de configuration des commutateurs Brocade sont indiquées dans les *directives d'évolutivité Brocade*.

Limites du commutateur Cisco Systems

Les limites de configuration des commutateurs Cisco sont disponibles dans le "[Limites de configuration Cisco](#)" Guide de la version du logiciel du commutateur Cisco.

Calculer la profondeur de la file d'attente

Vous devrez peut-être ajuster la profondeur de votre file d'attente FC sur l'hôte pour

obtenir le maximum de valeurs pour les ITN par nœud et le « Fan-In » du port FC. Le nombre maximal de LUN et le nombre de HBA pouvant se connecter à un port FC sont limités par la profondeur de file d'attente disponible sur les ports FC target.

Description de la tâche

La longueur de la file d'attente correspond au nombre de demandes d'E/S (commandes SCSI) pouvant être mises en file d'attente simultanément sur un contrôleur de stockage. Chaque demande d'E/S provenant de l'adaptateur HBA initiateur de l'hôte vers l'adaptateur cible du contrôleur de stockage utilise une entrée de file d'attente. Généralement, une longueur de file d'attente plus élevée équivaut à des performances supérieures. Toutefois, si la profondeur maximale de file d'attente du contrôleur de stockage est atteinte, ce contrôleur de stockage rejette les commandes entrantes en leur renvoyant une réponse QFULL. Si un grand nombre d'hôtes accèdent à un contrôleur de stockage, prévoyez-vous d'éviter les conditions de QFULL qui dégradent considérablement les performances du système et peuvent entraîner des erreurs sur certains systèmes.

Dans une configuration avec plusieurs initiateurs (hôtes), tous les hôtes doivent avoir des profondeurs de file d'attente similaires. En raison des inégalités de profondeur de file d'attente entre les hôtes connectés au contrôleur de stockage via le même port cible, les hôtes dont la profondeur de file d'attente est réduite sont privés d'accès aux ressources par les hôtes dont la profondeur de file d'attente est supérieure.

Les recommandations générales suivantes peuvent être formulées sur les profondeurs de file d'attente « réglage » :

- Pour les systèmes de petite ou moyenne taille, utilisez une longueur de file d'attente HBA de 32.
- Pour les systèmes de grande taille, utilisez une profondeur de file d'attente HBA de 128.
- Pour les cas d'exception ou les tests de performances, utilisez une file d'attente de 256 afin d'éviter tout problème de mise en file d'attente.
- Toutes les profondeurs de file d'attente doivent être définies sur des valeurs similaires pour donner un accès égal à tous les hôtes.
- Pour éviter des pénalités ou des erreurs, la profondeur de la file d'attente du port FC cible du contrôleur de stockage ne doit pas être dépassée.

Étapes

1. Nombre total d'initiateurs FC dans tous les hôtes qui se connectent à un port FC cible.
2. Multiplier par 128.
 - Si le résultat est inférieur à 2,048, définissez la profondeur de la file d'attente pour tous les initiateurs sur 128.
Vous avez 15 hôtes avec un initiateur connecté à chacun des deux ports cibles du contrôleur de stockage. $15 \times 128 = 1,920$. Comme 1,920 est inférieur à la limite de profondeur totale de la file d'attente de 2,048, vous pouvez définir la profondeur de la file d'attente pour tous vos initiateurs sur 128.
 - Si le résultat est supérieur à 2,048, passer à l'étape 3.
Vous avez 30 hôtes avec un initiateur connecté à chacun des deux ports cibles du contrôleur de stockage. $30 \times 128 = 3,840$. Comme 3,840 est supérieur à la limite de profondeur totale de la file d'attente de 2,048, vous devez choisir l'une des options de l'étape 3 pour résoudre le problème.
3. Choisissez l'une des options suivantes pour ajouter d'autres hôtes au contrôleur de stockage.
 - Option 1 :
 - i. Ajoutez d'autres ports FC target.
 - ii. Redistribuez vos initiateurs FC.

iii. Répétez les étapes 1 et 2.

La profondeur de file d'attente souhaitée de 3,840 dépasse la profondeur de file d'attente disponible par port. Pour y remédier, vous pouvez ajouter un adaptateur cible FC à deux ports à chaque contrôleur puis resegmenter vos commutateurs FC de sorte que 15 de vos 30 hôtes se connectent à un ensemble de ports, et les 15 hôtes restants se connectent à un second ensemble de ports. La profondeur de file d'attente par port est alors réduite à $15 \times 128 = 1,920$.

◦ Option 2 :

- i. Désigner chaque hôte comme « grand » ou « centre commercial » en fonction de ses besoins d'E/S prévus.
- ii. Multiplier le nombre d'initiateurs volumineux par 128.
- iii. Multiplier le nombre de petits initiateurs par 32.
- iv. Additionnez les deux résultats.
- v. Si le résultat est inférieur à 2,048, définissez la profondeur de la file d'attente pour les hôtes volumineux sur 128 et la profondeur de la file d'attente pour les petits hôtes sur 32.
- vi. Si le résultat est toujours supérieur à 2,048 par port, réduisez la profondeur de file d'attente par initiateur jusqu'à ce que la profondeur totale de la file d'attente soit inférieure ou égale à 2,048.

Pour estimer la profondeur de file d'attente nécessaire pour obtenir un certain débit d'E/S par seconde, utilisez la formule suivante :



Profondeur de file d'attente nécessaire = (nombre d'E/S par seconde) × (temps de réponse)

Par exemple, si vous avez besoin de 40,000 E/S par seconde avec un temps de réponse de 3 millisecondes, la profondeur de file d'attente requise = $40,000 \times (.003) = 120$.

Le nombre maximal d'hôtes que vous pouvez connecter à un port cible est de 64, si vous décidez de limiter la profondeur de la file d'attente à la recommandation de base de 32. Cependant, si vous décidez d'avoir une profondeur de file d'attente de 128, vous pouvez avoir un maximum de 16 hôtes connectés à un port cible. Plus la longueur de la file d'attente est importante, plus le nombre d'hôtes qu'un seul port cible peut prendre en charge est élevé. Si vous avez besoin de telle sorte que vous ne puissiez pas compromettre la profondeur de la file d'attente, vous devriez obtenir plus de ports cibles.

La profondeur de file d'attente souhaitée de 3,840 dépasse la profondeur de file d'attente disponible par port. Vous disposez de 10 hôtes « grands » qui ont des besoins en E/S de stockage élevés, et de 20 hôtes « petits » qui ont des besoins en E/S faibles. Définissez la profondeur de la file d'attente d'initiateur sur les hôtes volumineux sur 128 et la profondeur de la file d'attente d'initiateur sur les petits hôtes sur 32.

La profondeur totale de file d'attente obtenue est de $(10 \times 128) + (20 \times 32) = 1,920$.

Vous pouvez répartir la profondeur de file d'attente disponible de manière égale sur chaque initiateur.

La profondeur de file d'attente par initiateur obtenue est de $2,048 \div 30 = 68$.

Définissez la profondeur de file d'attente sur les hôtes SAN

Vous devrez peut-être modifier la profondeur des files d'attente sur votre hôte pour atteindre les valeurs maximales pour les ITN par nœud et le Fan-In du port FC.

Hôtes AIX

Vous pouvez modifier la profondeur de la file d'attente sur les hôtes AIX à l'aide de l' `chdev` commande. Modifications effectuées à l'aide du `chdev` la commande persiste entre les redémarrages.

Exemples :

- Pour modifier la profondeur de la file d'attente pour le périphérique `hdisk7`, utilisez la commande suivante :

```
chdev -l hdisk7 -a queue_depth=32
```

- Pour modifier la profondeur de la file d'attente pour l'adaptateur HBA `fcs0`, utilisez la commande suivante :

```
chdev -l fcs0 -a num_cmd_elems=128
```

Valeur par défaut pour `num_cmd_elems` est 200. La valeur maximale est 2,048.



Il peut être nécessaire de mettre l'adaptateur HBA hors ligne pour le modifier `num_cmd_elems` puis le remettre en ligne à l'aide de `rmdev -l fcs0 -R` et `mkdev -l fcs0 -P` commandes.

Hôtes HP-UX

Vous pouvez modifier la profondeur de la file d'attente des LUN ou des périphériques sur les hôtes HP-UX à l'aide du paramètre noyau `scsi_max_qdepth`. Vous pouvez modifier la profondeur de la file d'attente HBA à l'aide du paramètre du noyau `max_fcp_reqs`.

- Valeur par défaut pour `scsi_max_qdepth` est 8. La valeur maximale est 255.

`scsi_max_qdepth` peut être modifié de manière dynamique sur un système en cours d'exécution à l'aide du `-u` sur le `kmtune` commande. Ce changement sera effectif pour tous les périphériques du système. Par exemple, utilisez la commande suivante pour augmenter la profondeur de la file d'attente de LUN à 64 :

```
kmtune -u -s scsi_max_qdepth=64
```

Il est possible de modifier la profondeur de la file d'attente pour les fichiers de périphériques individuels à l'aide de l' `scsictl` commande. Modifications à l'aide du `scsictl` les commandes ne sont pas conservées d'un redémarrage système à l'autre. Pour afficher et modifier la profondeur de la file d'attente d'un fichier de périphérique particulier, exécutez la commande suivante :

```
scsictl -a /dev/rdisk/c2t2d0
```

```
scsictl -m queue_depth=16 /dev/rdisk/c2t2d0
```

- Valeur par défaut pour `max_fcp_reqs` est 512. La valeur maximale est 1024.

Le noyau doit être reconstruit et le système doit être redémarré pour que les modifications soient apportées à `max_fcp_reqs` pour prendre effet. Pour modifier la profondeur de la file d'attente HBA sur 256, par exemple, utilisez la commande suivante :

```
kmtune -u -s max_fcp_reqs=256
```

Hôtes Solaris

Vous pouvez définir la profondeur de la file d'attente des LUN et HBA pour vos hôtes Solaris.

- Pour la profondeur de la file d'attente de LUN : le nombre de LUN utilisées sur un hôte multiplié par le papillon par LUN (`lun-queue-depth`) doit être inférieur ou égal à la valeur `tgt-queue-depth` sur l'hôte.
- Pour la profondeur de file d'attente dans une pile Sun : les pilotes natifs ne permettent pas pour chaque LUN ou par cible `max_throttle` Paramètres au niveau de la carte HBA. La méthode recommandée pour le réglage du `max_throttle` La valeur pour les pilotes natifs est sur un niveau par type de périphérique (VID_PID) dans l' `/kernel/drv/sd.conf` et `/kernel/drv/ssd.conf` fichiers. L'utilitaire hôte définit cette valeur sur 64 pour les configurations MPxIO et sur 8 pour les configurations Veritas DMP.

Étapes

1. `# cd /kernel/drv`
2. `# vi lpfc.conf`
3. Recherchez `/tft-queue (/tgt-queue)`

```
tgt-queue-depth=32
```



La valeur par défaut est 32 lors de l'installation.

4. Définissez la valeur souhaitée en fonction de la configuration de votre environnement.
5. Enregistrez le fichier.
6. Redémarrez l'hôte à l'aide de `sync; sync; sync; reboot -- -r` commande.

Hôtes VMware pour un HBA QLogic

Utilisez le `esxcfg-module` Commande permettant de modifier les paramètres de délai d'expiration de l'adaptateur HBA. Mise à jour manuelle du `esx.conf` le fichier n'est pas recommandé.

Étapes

1. Connectez-vous à la console de service en tant qu'utilisateur root.
2. Utilisez le `#vmkload_mod -l` Commande pour vérifier quel module HBA Qlogic est actuellement chargé.
3. Pour une seule instance d'un HBA Qlogic, exécutez la commande suivante :

```
#esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
```



Cet exemple utilise le module `qla2300_707`. Utilisez le module approprié en fonction de la sortie de `vmkload_mod -l`.

4. Enregistrez vos modifications à l'aide de la commande suivante :

```
#!/usr/sbin/esxcfg-boot -b
```

5. Redémarrez le serveur à l'aide de la commande suivante :

```
#reboot
```

6. Vérifiez les modifications à l'aide des commandes suivantes :

- a. `#esxcfg-module -g qla2300_707`
- b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

Hôtes VMware pour une carte HBA Emulex

Utilisez le `esxcfg-module` Commande permettant de modifier les paramètres de délai d'expiration de l'adaptateur HBA. Mise à jour manuelle du `esx.conf` le fichier n'est pas recommandé.

Étapes

1. Connectez-vous à la console de service en tant qu'utilisateur root.
2. Utilisez le `#vmkload_mod -l grep lpfc` Commande pour vérifier quelle carte HBA Emulex est actuellement chargée.
3. Pour une seule instance d'un HBA Emulex, entrez la commande suivante :

```
#esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```



Selon le modèle de l'adaptateur HBA, le module peut être `lpfcdd_7xx` ou `lpfcdd_732`. La commande ci-dessus utilise le module `lpfcdd_7xx`. Vous devez utiliser le module approprié en fonction des résultats de `vmkload_mod -l`.

L'exécution de cette commande permet de définir la profondeur de la file d'attente de LUN sur 16 pour l'adaptateur HBA représenté par `lpfc0`.

4. Pour plusieurs instances d'un HBA Emulex, exécutez la commande suivante :

```
a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
lpfcdd_7xx
```

La profondeur de la file d'attente LUN pour `lpfc0` et la profondeur de la file d'attente LUN pour `lpfc1` est définie sur 16.

5. Saisissez la commande suivante :

```
#esxcfg-boot -b
```

6. Redémarrez avec `#reboot`.

Hôtes Windows pour une carte HBA Emulex

Sur les hôtes Windows, vous pouvez utiliser `LPUTILNT` Utilitaire de mise à jour de la profondeur de la file d'attente pour les HBA Emulex.

Étapes

1. Exécutez le `LPUTILNT` utilitaire situé dans le `C:\WINNT\system32` répertoire.
2. Sélectionnez **Paramètres de conduite** dans le menu à droite.
3. Faites défiler vers le bas et double-cliquez sur **QueueDepth**.



Si vous définissez **QueueDepth** supérieur à 150, la valeur suivante du Registre Windows doit également être augmentée de façon appropriée :

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnids\Parameters\Device\NumberOfRequests

Hôtes Windows pour un HBA Qlogic

Sur les hôtes Windows, vous pouvez utiliser l' et l' SANsurfer Utilitaire HBA Manager pour mettre à jour les profondeurs de file d'attente pour les HBA Qlogic.

Étapes

1. Exécutez le SANsurfer Utilitaire HBA Manager.
2. Cliquez sur **Port HBA > Paramètres**.
3. Cliquez sur **Paramètres avancés du port HBA** dans la zone de liste.
4. Mettez à jour le `Execution Throttle` paramètre.

Hôtes Linux pour HBA Emulex

Vous pouvez mettre à jour les profondeurs de file d'attente d'une carte HBA Emulex sur un hôte Linux. Pour que les mises à jour soient conservées entre les redémarrages, vous devez ensuite créer une nouvelle image de disque RAM et redémarrer l'hôte.

Étapes

1. Identifiez les paramètres de profondeur de file d'attente à modifier :

```
modinfo lpfc|grep queue_depth
```

La liste des paramètres de profondeur de file d'attente avec leur description s'affiche. Selon la version de votre système d'exploitation, vous pouvez modifier un ou plusieurs des paramètres de profondeur de file d'attente suivants :

- ° `lpfc_lun_queue_depth`: Nombre maximal de commandes FC pouvant être mises en file d'attente vers une LUN spécifique (uint)
- ° `lpfc_hba_queue_depth`: Nombre maximal de commandes FC pouvant être mises en file d'attente dans un adaptateur Lpfc HBA (uint)
- ° `lpfc_tgt_queue_depth`: Nombre maximal de commandes FC pouvant être mises en file d'attente sur un port cible spécifique (uint)

Le `lpfc_tgt_queue_depth` Ce paramètre est uniquement applicable aux systèmes Red Hat Enterprise Linux 7.x, SUSE Linux Enterprise Server 11 SP4 et 12.x.

2. Mettez à jour les profondeurs de file d'attente en ajoutant les paramètres de profondeur de file d'attente au `/etc/modprobe.conf` Fichier pour un système Red Hat Enterprise Linux 5.x et vers `/etc/modprobe.d/scsi.conf` Fichier pour un système Red Hat Enterprise Linux 6.x ou 7.x, ou un système SUSE Linux Enterprise Server 11.x ou 12.x.

Selon la version de votre système d'exploitation, vous pouvez ajouter une ou plusieurs des commandes suivantes :

- `options lpfc lpfc_hba_queue_depth=new_queue_depth`
- `options lpfc lpfc_lun_queue_depth=new_queue_depth`
- `options lpfc tgt_queue_depth=new_queue_depth`

3. Créez une nouvelle image de disque RAM, puis redémarrez l'hôte pour que les mises à jour soient conservées entre les redémarrages.

Pour plus d'informations, reportez-vous à la section ["Administration du système"](#) Pour votre version du système d'exploitation Linux.

4. Vérifiez que les valeurs de profondeur de file d'attente sont mises à jour pour chaque paramètre de profondeur de file d'attente modifié :

```
root@localhost ~]# cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
30
```

La valeur actuelle de la profondeur de la file d'attente s'affiche.

Hôtes Linux pour QLogic HBA

Vous pouvez mettre à jour la longueur de la file d'attente d'un pilote QLogic sur un hôte Linux. Pour que les mises à jour soient conservées entre les redémarrages, vous devez ensuite créer une nouvelle image de disque RAM et redémarrer l'hôte. Vous pouvez utiliser l'interface graphique de gestion du HBA QLogic ou l'interface de ligne de commande pour modifier la profondeur de la file d'attente HBA QLogic.

Cette tâche montre comment utiliser la CLI QLogic HBA pour modifier la profondeur de la file d'attente HBA QLogic

Étapes

1. Identifiez le paramètre de profondeur de file d'attente de périphérique à modifier :

```
modinfo qla2xxx | grep ql2xmaxqdepth
```

Vous pouvez modifier uniquement le `ql2xmaxqdepth` Paramètre de profondeur de file d'attente, qui indique la profondeur maximale de file d'attente pouvant être définie pour chaque LUN. La valeur par défaut est 64 pour RHEL 7.5 et versions ultérieures. La valeur par défaut est 32 pour RHEL 7.4 et les versions antérieures.

```
root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
parm:          ql2xmaxqdepth:Maximum queue depth to set for each LUN.
Default is 64. (int)
```

2. Mettre à jour la valeur de profondeur de la file d'attente du périphérique :

- Pour que les modifications persistent, procédez comme suit :
 - i. Mettez à jour les profondeurs de file d'attente en ajoutant le paramètre de profondeur de file d'attente au `/etc/modprobe.conf` Fichier pour un système Red Hat Enterprise Linux 5.x et vers `/etc/modprobe.d/scsi.conf` Fichier pour un système Red Hat Enterprise Linux 6.x ou 7.x, ou

un système SUSE Linux Enterprise Server 11.x ou 12.x : options qla2xxx
ql2xmaxqdepth=new_queue_depth

- ii. Créez une nouvelle image de disque RAM, puis redémarrez l'hôte pour que les mises à jour soient conservées entre les redémarrages.

Pour plus d'informations, reportez-vous à la section "[Administration du système](#)" Pour votre version du système d'exploitation Linux.

- Si vous souhaitez modifier le paramètre uniquement pour la session en cours, exécutez la commande suivante :

```
echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

Dans l'exemple suivant, la profondeur de la file d'attente est définie sur 128.

```
echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

3. Vérifiez que les valeurs de profondeur de la file d'attente sont mises à jour :

```
cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

La valeur actuelle de la profondeur de la file d'attente s'affiche.

4. Modifiez la profondeur de la file d'attente HBA QLogic en mettant à jour le paramètre de micrologiciel Execution Throttle Du BIOS HBA QLogic.

- a. Connectez-vous à l'interface de ligne de commande de gestion QLogic HBA :

```
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli
```

- b. Dans le menu principal, sélectionnez Adapter Configuration option.

```

[root@localhost ~]#
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli
Using config file:
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli.cfg
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
Working dir: /root

QConvergeConsole

          CLI - Version 2.2.0 (Build 15)

Main Menu

1:  Adapter Information
**2:  Adapter Configuration**
3:  Adapter Updates
4:  Adapter Diagnostics
5:  Monitoring
6:  FabricCache CLI
7:  Refresh
8:  Help
9:  Exit

Please Enter Selection: 2

```

- c. Dans la liste des paramètres de configuration de l'adaptateur, sélectionner le HBA Parameters option.

```

1:  Adapter Alias
2:  Adapter Port Alias
**3:  HBA Parameters**
4:  Persistent Names (udev)
5:  Boot Devices Configuration
6:  Virtual Ports (NPIV)
7:  Target Link Speed (iidMA)
8:  Export (Save) Configuration
9:  Generate Reports
10:  Personality
11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
Please Enter Selection: 3

```

- d. Dans la liste des ports HBA, sélectionnez le port HBA requis.

Fibre Channel Adapter Configuration

HBA Model QLE2562 SN: BFD1524C78510

1: Port 1: WWPN: 21-00-00-24-FF-8D-98-E0 Online

2: Port 2: WWPN: 21-00-00-24-FF-8D-98-E1 Online

HBA Model QLE2672 SN: RFE1241G81915

3: Port 1: WWPN: 21-00-00-0E-1E-09-B7-62 Online

4: Port 2: WWPN: 21-00-00-0E-1E-09-B7-63 Online

(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)

Please Enter Selection: 1

Les détails du port HBA s'affichent.

- e. Dans le menu Paramètres HBA, sélectionner Display HBA Parameters option permettant d'afficher la valeur actuelle de l'Execution Throttle option.

La valeur par défaut du Execution Throttle option 65535.

HBA Parameters Menu

```
=====
HBA          : 2 Port: 1
SN           : BFD1524C78510
HBA Model    : QLE2562
HBA Desc.    : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version   : 8.01.02
WWPN         : 21-00-00-24-FF-8D-98-E0
WWNN         : 20-00-00-24-FF-8D-98-E0
Link         : Online
=====
```

- 1: Display HBA Parameters
- 2: Configure HBA Parameters
- 3: Restore Defaults

(p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)

Please Enter Selection: 1

```
-----
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
```

```

-----
Connection Options          : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                  : Auto
Frame Size                 : 2048
Hard Loop ID               : 0
Loop Reset Delay (seconds) : 5
Enable Host HBA BIOS      : Enabled
Enable Hard Loop ID       : Disabled
Enable FC Tape Support    : Enabled
Operation Mode            : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us) : 0
**Execution Throttle      : 65535**
Login Retry Count          : 8
Port Down Retry Count     : 30
Enable LIP Full Login     : Enabled
Link Down Timeout (seconds) : 30
Enable Target Reset       : Enabled
LUNs Per Target           : 128
Out Of Order Frame Assembly : Disabled
Enable LR Ext. Credits    : Disabled
Enable Fabric Assigned WWN : N/A

Press <Enter> to continue:

```

- a. Appuyez sur **entrée** pour continuer.
- b. Dans le menu Paramètres HBA, sélectionner Configure HBA Parameters Option permettant de modifier les paramètres HBA.
- c. Dans le menu configurer les paramètres, sélectionner Execute Throttle et mettez à jour la valeur de ce paramètre.

Configure Parameters Menu

```
=====
HBA          : 2 Port: 1
SN           : BFD1524C78510
HBA Model    : QLE2562
HBA Desc.    : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version   : 8.01.02
WWPN         : 21-00-00-24-FF-8D-98-E0
WWNN         : 20-00-00-24-FF-8D-98-E0
Link         : Online
=====
```

- 1: Connection Options
- 2: Data Rate
- 3: Frame Size
- 4: Enable HBA Hard Loop ID
- 5: Hard Loop ID
- 6: Loop Reset Delay (seconds)
- 7: Enable BIOS
- 8: Enable Fibre Channel Tape Support
- 9: Operation Mode
- 10: Interrupt Delay Timer (100 microseconds)
- 11: Execution Throttle
- 12: Login Retry Count
- 13: Port Down Retry Count
- 14: Enable LIP Full Login
- 15: Link Down Timeout (seconds)
- 16: Enable Target Reset
- 17: LUNs per Target
- 18: Enable Receive Out Of Order Frame
- 19: Enable LR Ext. Credits
- 20: Commit Changes
- 21: Abort Changes

(p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)

Please Enter Selection: 11

Enter Execution Throttle [1-65535] [65535]: 65500

- d. Appuyez sur **entrée** pour continuer.
- e. Dans le menu configurer les paramètres, sélectionner **Commit Changes** option pour enregistrer les modifications.
- f. Quitter le menu.

Gestion du stockage objet S3

Découvrez la prise en charge de S3 dans ONTAP 9

Présentation de la configuration S3

À partir de ONTAP 9.8, vous pouvez activer un serveur de stockage objet ONTAP simple Storage Service (S3) dans un cluster ONTAP à l'aide des outils de gestion familiers tels que ONTAP System Manager pour provisionner rapidement un stockage objet haute performance pour le développement et les opérations dans ONTAP, et profiter des fonctionnalités d'efficacité du stockage et de la sécurité d'ONTAP.

Configuration S3 avec System Manager et l'interface de ligne de commandes ONTAP

Vous pouvez configurer et gérer ONTAP S3 avec System Manager et l'interface de ligne de commandes d'ONTAP. Si vous activez S3 et créez des compartiments à l'aide de System Manager, ONTAP sélectionne les valeurs par défaut des meilleures pratiques pour une configuration simplifiée. Si vous devez spécifier des paramètres de configuration, vous pouvez utiliser l'interface de ligne de commandes de ONTAP. Si vous configurez le serveur S3 et les compartiments à partir de l'interface de ligne de commandes, vous pouvez toujours les gérer avec System Manager, le cas échéant, ou vice-versa.

Lorsque vous créez un compartiment S3 avec System Manager, ONTAP configure un niveau de service de performance par défaut qui est le plus élevé disponible sur votre système. Par exemple, sur un système AFF, le paramètre par défaut est **Extreme**. Les niveaux de service de performance sont des groupes de règles prédéfinies de qualité de service (QoS) adaptative. Au lieu d'un des niveaux de service par défaut, vous pouvez définir une « policy group » QoS personnalisée ou aucun « policy group ».

Les groupes de règles de QoS adaptatifs sont les suivants :

- **Extreme** : utilisé pour les applications qui exigent la plus faible latence et les meilleures performances.
- **Performance** : utilisé pour les applications avec des besoins de performances et une latence modestes.
- **Valeur** : utilisé pour les applications pour lesquelles le débit et la capacité sont plus importants que la latence.
- **Custom** : spécifiez une politique de QoS personnalisée ou aucune politique de QoS.

Si vous sélectionnez **utiliser pour le Tiering**, aucun niveau de service de performances n'est sélectionné et le système essaie de sélectionner un support à faible coût avec des performances optimales pour les données hiérarchisées.

Voir aussi : ["Utilisez les groupes de règles de QoS adaptatifs"](#).

ONTAP tente de provisionner ce compartiment sur les niveaux locaux qui comptent les disques les plus appropriés, en satisfaisant le niveau de service choisi. Toutefois, si vous devez spécifier les disques à inclure dans le compartiment, configurez le stockage objet S3 à partir de l'interface de ligne de commandes en spécifiant les niveaux locaux (agrégat). Si vous configurez le serveur S3 à partir de l'interface de ligne de commandes, vous pouvez toujours le gérer avec System Manager.

Si vous souhaitez spécifier les agrégats utilisés pour les compartiments, vous pouvez uniquement le faire via l'interface de ligne de commande.

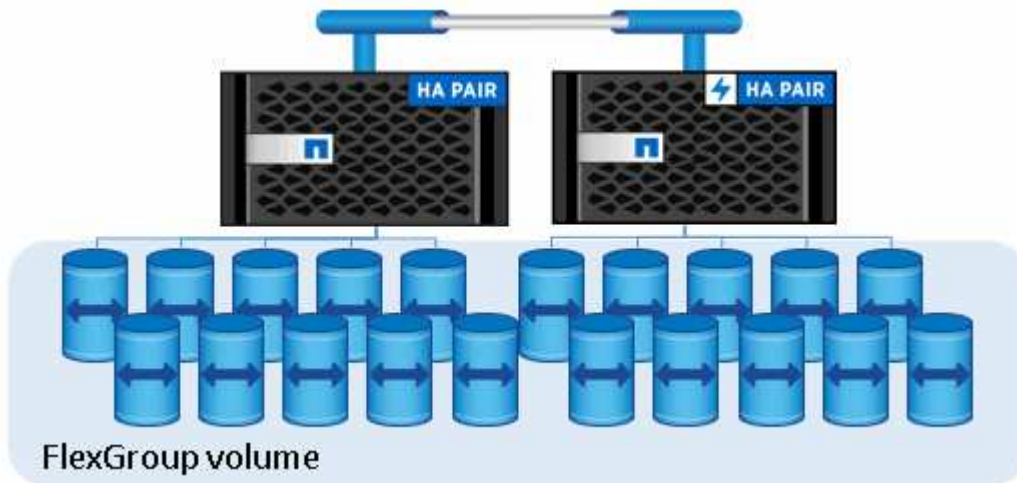
Configuration des compartiments S3 sur Cloud Volumes ONTAP

Pour fournir des compartiments à partir de Cloud Volumes ONTAP, il est fortement recommandé de sélectionner manuellement les agrégats sous-jacents pour vérifier qu'ils n'utilisent qu'un seul nœud. L'utilisation d'agrégats des deux nœuds peut avoir un impact sur les performances, car les nœuds se trouvent dans des zones de disponibilité séparées géographiquement et sont donc sujets aux problèmes de latence. Par conséquent, dans les environnements Cloud Volumes ONTAP, vous devriez le faire [Configuration des compartiments S3 à partir de l'interface de ligne de commandes](#).

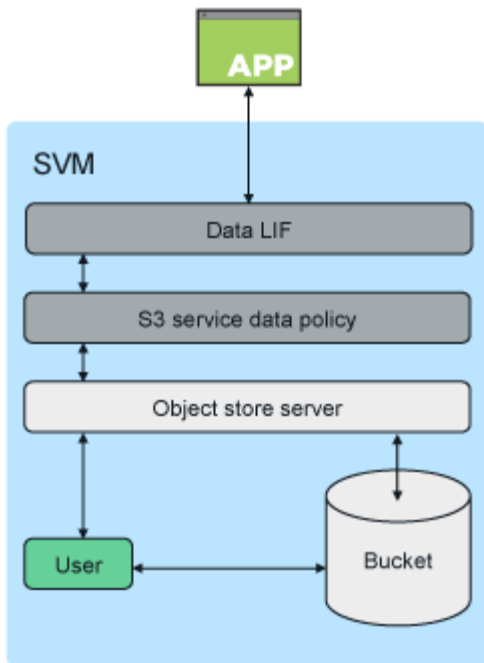
Sinon, les serveurs S3 sur Cloud Volumes ONTAP sont configurés et conservés dans Cloud Volumes ONTAP et dans des environnements sur site.

Architecture

Dans ONTAP, l'architecture sous-jacente d'un compartiment est un **"Volume FlexGroup"**, qui est un namespace unique composé de plusieurs volumes de membres constitutifs, mais qui est géré comme un seul volume.



L'accès au compartiment est fourni par le biais d'utilisateurs autorisés et d'applications client.



Lorsqu'un compartiment est utilisé exclusivement pour les applications S3, y compris en tant que terminal FabricPool, le volume FlexGroup sous-jacent ne prend en charge que le protocole S3.



À partir de ONTAP 9.12.1, le protocole S3 peut également être activé dans "[Volumes NAS multiprotocoles](#)" lequel il a été préconfiguré pour utiliser les protocoles NAS. Lorsque le protocole S3 est activé sur des volumes NAS multiprotocoles, les applications client peuvent lire et écrire des données à l'aide de NFS, SMB et S3.

Limites du godet

La taille minimale du godet est de 95 Go. + la taille maximale du godet est limitée à la taille maximale de FlexGroup de 60 po.

Il existe une limite de 1000 compartiments par volume FlexGroup, soit 12,000 compartiments par cluster (avec 12 volumes FlexGroup).

Dimensionnement automatique du FlexGroup avec ONTAP 9.14.1 et versions ultérieures

À partir de ONTAP 9.14.1, la taille de FlexGroup par défaut est basée sur la taille des compartiments sous-jacents. Le volume FlexGroup augmente ou diminue automatiquement à mesure que des compartiments sont ajoutés ou supprimés.

Par exemple, si un compartiment_A initial est provisionné sur 100 Go, le FlexGroup sera provisionné à l'aide de l'allocation dynamique de 100 Go. Si deux compartiments supplémentaires sont créés, Bucket_B à 300 Go et Bucket_C à 500 Go, le volume FlexGroup passera à 900 Go.

(Bucket_A à 100 Go + Bucket_B à 300 Go + Bucket_C à 500 Go = 900 Go.)

Si Bucket_A est supprimé, le volume FlexGroup sous-jacent passe à 800 Go.

Correction des tailles de FlexGroup par défaut dans ONTAP 9.13.1 et versions antérieures

Pour prendre en charge l'extension de compartiment, la capacité totale utilisée de tous les compartiments du volume FlexGroup doit être inférieure à 33 % de la capacité maximale du volume FlexGroup en fonction des agrégats de stockage disponibles dans le cluster. Si cela n'est pas possible, le nouveau compartiment créé est provisionné sur un nouveau volume FlexGroup créé automatiquement.

Avant ONTAP 9.14.1, la taille de la FlexGroup est définie sur une taille par défaut en fonction de son environnement :

- 1,6 po en ONTAP
- 100 To dans ONTAP Select

Si un cluster ne dispose pas de suffisamment de capacité pour provisionner un volume FlexGroup à sa taille par défaut, ONTAP réduit de moitié sa taille par défaut jusqu'à ce qu'il puisse être provisionné dans l'environnement existant.

Par exemple, dans un environnement de 300 To, un volume FlexGroup est automatiquement provisionné à 200 To (les volumes FlexGroup de 1,6 po, 800 To et 400 To étant trop volumineux pour l'environnement).

Cas d'utilisation

Les principales utilisations de S3 dans ONTAP sont les suivantes :

- Utilisation de FabricPool pour le Tiering des données inactives vers un compartiment dans ONTAP, permettant ainsi le Tiering ONTAP vers ONTAP. La hiérarchisation vers un compartiment dans —ou la hiérarchisation vers un compartiment dans "[cluster local](#)" un— "[cluster distant](#)" sont prises en charge. Le Tiering vers ONTAP S3 vous permet d'utiliser des systèmes ONTAP moins coûteux pour les données inactives et de réaliser des économies sur la nouvelle capacité Flash sans avoir à gérer de licences FabricPool supplémentaires ou de nouvelles technologies.
- À partir de ONTAP 9.12.1, le protocole S3 peut également être activé dans "[Volumes NAS multiprotocoles](#)" lequel il a été préconfiguré pour utiliser les protocoles NAS. Lorsque le protocole S3 est activé dans des volumes NAS multiprotocoles, les applications client peuvent lire et écrire des données à l'aide des protocoles S3, NFS et SMB. Cela ouvre la voie à de nombreux autres cas d'utilisation. L'une des utilisations les plus courantes est les clients NAS qui écrivent des données dans un volume et les clients S3 qui lisent les mêmes données, et qui effectuent des tâches spécialisées telles que l'analytique, la veille stratégique, le machine learning et la reconnaissance optique de caractères.



ONTAP S3 est approprié si vous souhaitez activer les fonctionnalités S3 sur des clusters ONTAP existants sans matériel ni gestion supplémentaires. NetApp StorageGRID est la solution phare de NetApp pour le stockage objet. StorageGRID est recommandé pour les applications S3 natives qui doivent exploiter la gamme complète d'actions S3, de fonctionnalités ILM avancées ou de capacités impossibles à atteindre dans les systèmes ONTAP. Pour plus d'informations, reportez-vous à la section "[Documentation StorageGRID](#)".

Informations associées

["Gestion des volumes FlexGroup"](#)

Planification

Prise en charge de la version ONTAP pour le stockage objet S3

Le stockage objet S3 est pris en charge sur toutes les plateformes AFF, FAS et ONTAP Select utilisant ONTAP 9.8 et versions ultérieures.

Comme avec d'autres protocoles tels que FC, iSCSI, NFS, NVMe_of et SMB, S3 requiert l'installation d'une licence avant de pouvoir être utilisée dans ONTAP. La licence S3 est une licence gratuite, mais elle doit être installée sur les systèmes effectuant une mise à niveau vers ONTAP 9.8. La licence S3 est téléchargeable depuis le site du ["Page clés de licence principale"](#) support NetApp.

La licence S3 est préinstallée sur les nouveaux systèmes ONTAP 9.8 et versions ultérieures.

Cloud Volumes ONTAP

ONTAP S3 est configuré et fonctionne de la même manière dans Cloud Volumes ONTAP que dans les environnements sur site, à l'exception des cas suivants :

- Lorsque vous créez des compartiments dans Cloud Volumes ONTAP, veillez à utiliser la procédure de l'interface de ligne de commandes pour vous assurer que le volume FlexGroup sous-jacent n'utilise que des agrégats à partir d'un seul nœud. L'utilisation d'agrégats provenant de plusieurs nœuds a un impact sur les performances, car les nœuds se trouvent dans des zones de disponibilité séparées par des emplacements géographiques et sont sensibles aux problèmes de latence.

Fournisseur cloud	Version ONTAP
Azure	ONTAP 9.9.1 et versions ultérieures
AWS	ONTAP 9.11.0 et versions ultérieures
Google Cloud	ONTAP 9.12.1 et versions ultérieures

Amazon FSX pour NetApp ONTAP

Le stockage objet S3 est pris en charge par les services Amazon FSX pour NetApp qui utilisent ONTAP 9.11 et versions ultérieures.

Prise en charge de S3 avec MetroCluster

À partir de ONTAP 9.14.1, vous pouvez activer un serveur de stockage objet S3 sur une SVM dans un agrégat en miroir dans des configurations MetroCluster IP et FC.

Depuis ONTAP 9.12.1, vous pouvez activer un serveur de stockage objet S3 sur un SVM dans un agrégat sans miroir dans une configuration MetroCluster IP. Pour plus d'informations sur les limites des agrégats non mis en miroir dans les configurations MetroCluster IP, reportez-vous à la section ["Considérations relatives aux agrégats non mis en miroir"](#).

Préversion publique de S3 dans ONTAP 9.7

Dans ONTAP 9.7, le stockage objet S3 a été introduit sous forme de préversion publique. Cette version n'était pas destinée aux environnements de production et ne sera plus mise à jour à partir de ONTAP 9.8. Seules les versions d'ONTAP 9.8 et ultérieures prennent en charge le stockage objet S3 dans les environnements de production.

Les compartiments S3 créés avec la version 9.7 de la préversion publique peuvent être utilisés dans ONTAP 9.8 et les versions ultérieures, mais ne peuvent pas tirer parti des améliorations des fonctionnalités. Si vous

avez créé des compartiments avec la prévisualisation publique 9.7, vous devez migrer le contenu de ces compartiments vers 9.8 compartiments pour une prise en charge des fonctionnalités, la sécurité et l'amélioration des performances.

Actions prises en charge par ONTAP S3

Les actions ONTAP S3 sont prises en charge par les API REST S3 standard, sauf comme indiqué ci-dessous. Pour plus d'informations, reportez-vous à la ["Référence de l'API Amazon S3"](#).

Opérations des compartiments

Les opérations suivantes sont prises en charge dans ONTAP à l'aide des API AWS S3 :

Utilisation du godet	Prise en charge de ONTAP commençant par
CreateBucket	ONTAP 9.11.1
DeleteBucket	ONTAP 9.11.1
DeleteBucketPolicy	ONTAP 9.12.1
GetBucketAcl	ONTAP 9.8
GetBucketLifecycleConfiguration	ONTAP 9.13.1 * seules les actions d'expiration sont prises en charge
GetBuckeLocation	ONTAP 9.10.1
GetBucketPolicy	ONTAP 9.12.1
Godet principal	ONTAP 9.8
Listseaux	ONTAP 9.8
ListBucketVersioning	ONTAP 9.11.1
ListObjectVersions	ONTAP 9.11.1
Seau de rangement	<ul style="list-style-type: none">• ONTAP 9.11.1• ONTAP 9.8 : pris en charge uniquement avec les API REST ONTAP
PutBucketLifecycleConfiguration	ONTAP 9.13.1 * seules les actions d'expiration sont prises en charge
PutBuckePolicy	ONTAP 9.12.1

Opérations sur l'objet

Depuis la version ONTAP 9.9.1, ONTAP S3 prend en charge le balisage et les métadonnées d'objet.

- PutObject et CreateMultipartUpload incluent des paires clé-valeur utilisant `x-amz-meta-<key>`.

Par exemple : `x-amz-meta-project: ontap_s3`.

- GetObject. Et HeadObject renvoient des métadonnées définies par l'utilisateur.

- Contrairement aux métadonnées, les balises peuvent être lues indépendamment des objets à l'aide de :
 - Marquage PutObject
 - GetObjectTagging
 - DeleteObjectTagging

Depuis ONTAP 9.11.1, ONTAP S3 prend en charge la gestion des versions d'objets et les actions associées avec les API ONTAP suivantes :

- GetBucketVersioning
- ListBuckeVersions
- PutBuckeVersioning

Opération d'objet	Prise en charge de ONTAP commençant par
AbortMultipartUpload	ONTAP 9.8
CompleteMultipartUpload	ONTAP 9.8
Objet de copie	ONTAP 9.12.1
CreateMultipartUpload	ONTAP 9.8
DeleteObject	ONTAP 9.8
DeleteObjects	ONTAP 9.11.1
DeleteObjectTagging	ONTAP 9.9.1
GetBucketVersioning	ONTAP 9.11.1
GetObject	ONTAP 9.8
GetObjectAcl	ONTAP 9.8
GetObjectRetention	ONTAP 9.14.1
GetObjectTagging	ONTAP 9.9.1
Objet principal	ONTAP 9.8
ListMultipartUpload	ONTAP 9.8
ListObjects	ONTAP 9.8
ListentsV2	ONTAP 9.8
ListBuckeVersions	ONTAP 9.11.1
ListParts	ONTAP 9.8
PutBuckeVersioning	ONTAP 9.11.1
PutObject	ONTAP 9.8
PutObjectLockConfiguration	ONTAP 9.14.1
PutObjectRetention	ONTAP 9.14.1
Marquage PutObject	ONTAP 9.9.1
UploadPart	ONTAP 9.8

Opération d'objet	Prise en charge de ONTAP commençant par
UploadPartCopy	ONTAP 9.12.1

Stratégies de groupe

Ces opérations ne sont pas spécifiques à S3 et sont généralement associées aux processus de gestion des identités et des données. ONTAP prend en charge ces commandes, mais n'utilise pas l'API REST IAM.

- Créer la règle
- Politique d'AttachGroup

Gestion des utilisateurs

Ces opérations ne sont pas spécifiques aux protocoles S3 et sont généralement associées aux processus IAM.

- CreateUser
- Supprimer un utilisateur
- CreateGroup
- DeleteGroup

Interopérabilité ONTAP S3

Le serveur ONTAP S3 interagit normalement avec d'autres fonctionnalités d'ONTAP, sauf comme indiqué dans ce tableau.

Zone de fonction	Pris en charge	Non pris en charge
Cloud Volumes ONTAP	<ul style="list-style-type: none"> • Clients Azure dans ONTAP 9.9.1 et versions ultérieures • Clients AWS dans ONTAP 9.11.0 et versions ultérieures • Clients Google Cloud dans ONTAP 9.12.1 et versions ultérieures 	<ul style="list-style-type: none"> • Cloud Volumes ONTAP pour tous les clients dans ONTAP 9.8 et versions antérieures

Zone de fonction	Pris en charge	Non pris en charge
Protection des données	<ul style="list-style-type: none"> • Cloud Sync • Verrouillage des objets, gouvernance et conformité (à partir de ONTAP 9.14.1) • "Gestion des versions d'objets" (À partir de ONTAP 9.11.1) • Agrégats MetroCluster sans miroir (à partir de ONTAP 9.12.1) • Agrégats MetroCluster en miroir (à partir de ONTAP 9.14.1) • "SnapMirror S3" (À partir de ONTAP 9.10.1) • SnapMirror (volumes NAS uniquement, à partir de ONTAP 9.12.1) • SnapLock (volumes NAS uniquement, à partir de ONTAP 9.14.1) 	<ul style="list-style-type: none"> • Le code d'effacement • NDMP • SMTape • SnapMirror • Cloud SnapMirror • Reprise d'activité de SVM • SyncMirror
Le cryptage	<ul style="list-style-type: none"> • Chiffrement d'agrégat NetApp (NAE) • NVE (NetApp Volume Encryption) • NetApp Storage Encryption (NSE) • TLS/SSL 	<ul style="list-style-type: none"> • SCORIES
Efficacité du stockage	<ul style="list-style-type: none"> • Déduplication • Compression • Compaction 	<ul style="list-style-type: none"> • Efficacité au niveau des agrégats • Clone de volume du volume FlexGroup contenant des compartiments ONTAP S3
Virtualisation du stockage	-	Virtualisation NetApp FlexArray
La qualité de service (QoS)	<ul style="list-style-type: none"> • Limites de QoS (plafonds) • Qualité de service minimale (au sol) 	-

Zone de fonction	Pris en charge	Non pris en charge
Ou des caractéristiques supplémentaires	<ul style="list-style-type: none"> • "Audit des événements S3" (À partir de ONTAP 9.10.1) • "Gestion du cycle de vie des compartiments" (À partir de ONTAP 9.13.1) 	<ul style="list-style-type: none"> • Volumes FlexCache • FPolicy • Qtrees • Quotas

Solutions tierces validées par ONTAP S3

NetApp a validé les solutions tierces suivantes pour une utilisation avec ONTAP S3. Si la solution que vous recherchez n'est pas répertoriée, contactez votre représentant de compte NetApp.

Solutions tierces validées sur ONTAP S3

NetApp a testé ces solutions en collaboration avec ses partenaires respectifs.

- Amazon SageMaker
- Client Apache Hadoop S3A
- Apache Kafka
- CommVault (V11)
- Kafka confluent
- Red Hat Quay
- Rubrik
- Flocon de neige
- Trino
- Veeam (V12)

Configurer

À propos du processus de configuration S3

Workflow de configuration S3

La configuration de S3 implique d'évaluer les exigences en matière de stockage physique et de réseau, puis de choisir un workflow spécifique à votre objectif : configurer l'accès S3 pour un SVM nouveau ou existant, ou ajouter un compartiment et des utilisateurs à une SVM existante déjà entièrement configurée pour l'accès S3.

Lorsque vous configurez l'accès S3 à une nouvelle machine virtuelle de stockage à l'aide de System Manager, vous êtes invité à saisir des informations de certificat et de mise en réseau, et la machine virtuelle de stockage et le serveur de stockage objet S3 sont créés en une seule opération.



Évaluer les besoins en matière de stockage physique

Avant de provisionner le stockage S3 pour les clients, vous devez vérifier que l'espace est suffisant dans les agrégats existants pour le nouveau magasin d'objets. Si ce n'est pas le cas, vous pouvez ajouter des disques à des agrégats existants ou créer de nouveaux agrégats du type et de l'emplacement souhaités.

Description de la tâche

Lorsque vous créez un compartiment S3 sur un SVM compatible avec S3, un volume FlexGroup **"créé automatiquement"** prend en charge le compartiment. Vous pouvez laisser ONTAP Select les agrégats sous-jacents et les composants FlexGroup automatiquement (par défaut) ou sélectionner les agrégats sous-jacents et les composants FlexGroup vous-même.

Si vous décidez de spécifier les agrégats et les composants FlexGroup, par exemple si vous avez des exigences de performances spécifiques pour les disques sous-jacents, vous devez vous assurer que la configuration de votre agrégat respecte les meilleures pratiques en matière de provisionnement d'un volume FlexGroup. En savoir plus :

- ["Gestion des volumes FlexGroup"](#)
- ["Rapport technique NetApp 4571-a : meilleures pratiques relatives au volume NetApp ONTAP FlexGroup"](#)

Si vous accédez aux compartiments à partir de Cloud Volumes ONTAP, il est fortement recommandé de sélectionner manuellement les agrégats sous-jacents pour vérifier qu'ils n'utilisent qu'un seul nœud. L'utilisation d'agrégats des deux nœuds peut avoir un impact sur les performances, car les nœuds se trouvent dans des zones de disponibilité séparées géographiquement et sont donc sujets aux problèmes de latence. Découvrez ["Création de compartiments pour Cloud Volumes ONTAP"](#).

Vous pouvez utiliser le serveur ONTAP S3 pour créer un Tier de capacité FabricPool local, à savoir dans le même cluster que le Tier de performance. Cela peut être utile, par exemple, si des disques SSD sont connectés à une paire haute disponibilité et que vous souhaitez hiérarchiser les données froide_ sur des disques HDD d'une autre paire haute disponibilité. Dans ce cas d'utilisation, le serveur S3 et le compartiment contenant le Tier de capacité locale doivent donc se trouver dans une paire HA différente de celle du Tier de performance. Le Tiering local n'est pas pris en charge sur les clusters à un ou deux nœuds.

Étapes

1. Afficher l'espace disponible dans les agrégats existants :

```
storage aggregate show
```

Si un agrégat dispose d'un espace suffisant ou si l'emplacement du nœud requis, enregistrez son nom pour votre configuration S3.

```
cluster-1::> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes  RAID Status
-----
aggr_0         239.0GB    11.13GB   95% online      1 node1  raid_dp, normal
aggr_1         239.0GB    11.13GB   95% online      1 node1  raid_dp, normal
aggr_2         239.0GB    11.13GB   95% online      1 node2  raid_dp, normal
aggr_3         239.0GB    11.13GB   95% online      1 node2  raid_dp, normal
aggr_4         239.0GB    238.9GB   95% online      5 node3  raid_dp, normal
aggr_5         239.0GB    239.0GB   95% online      4 node4  raid_dp, normal
6 entries were displayed.
```

2. En l'absence d'agrégats disposant d'espace suffisant ou d'emplacement de nœud requis, ajoutez des disques à un agrégat existant en utilisant le `storage aggregate add-disks` ou créez un nouvel agrégat à l'aide de `storage aggregate create` commande.

Évaluer les exigences de mise en réseau

Avant de fournir du stockage S3 aux clients, vous devez vérifier que le réseau est correctement configuré pour répondre aux exigences de provisionnement S3.

Avant de commencer

Les objets de réseau de cluster suivants doivent être configurés :

- Ports physiques et logiques
- Les domaines de diffusion
- Sous-réseaux (le cas échéant)
- IPspaces (selon les besoins, en plus de l'IPspace par défaut)
- Failover Groups (si nécessaire, en plus du groupe de basculement par défaut pour chaque broadcast domain)
- Pare-feu externes

Description de la tâche

Pour les tiers de capacité FabricPool distante (cloud) et les clients S3 distants, vous devez utiliser un SVM de données et configurer des LIF de données. Pour les niveaux cloud FabricPool, vous devez également configurer les LIF intercluster ; le peering de cluster n'est pas nécessaire.

Pour les niveaux de capacité FabricPool locaux, il est nécessaire d'utiliser la SVM système (appelée « Cluster »), mais il existe deux options de configuration de LIF :

- Vous pouvez utiliser les LIFs de cluster.

Avec cette option, aucune autre configuration LIF n'est requise, mais le trafic sur les LIFs du cluster sera augmenté. En outre, le niveau local ne sera pas accessible aux autres clusters.

- Vous pouvez utiliser des LIF data et intercluster.

Une configuration supplémentaire est nécessaire, notamment l'activation des LIF pour le protocole S3, mais le Tier local sera également accessible en tant que Tier cloud FabricPool distant vers d'autres clusters.

Étapes

1. Afficher les ports physiques et virtuels disponibles :

```
network port show
```

- Dans la mesure du possible, vous devez utiliser le port avec la vitesse la plus élevée pour le réseau de données.
- Tous les composants du réseau de données doivent avoir le même paramètre MTU pour optimiser les performances.

2. Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, vérifiez que le sous-réseau existe et dispose des adresses suffisantes :

```
network subnet show
```

Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche

3. Les sous-réseaux sont créés à l'aide du `network subnet create` commande.

3. Affichez les IPspaces disponibles :

```
network ipspace show
```

Vous pouvez utiliser l'IPspace par défaut ou un IPspace personnalisé.

4. Si vous souhaitez utiliser des adresses IPv6, vérifiez que l'IPv6 est activé sur le cluster :

```
network options ipv6 show
```

Si nécessaire, vous pouvez activer IPv6 en utilisant le `network options ipv6 modify` commande.

Choisissez où provisionner la capacité de stockage S3

Avant de créer un nouveau compartiment S3, vous devez décider de le placer dans un SVM nouveau ou existant. Cette décision détermine votre flux de travail.

Choix

- Si vous souhaitez provisionner un compartiment dans un nouveau SVM ou un SVM qui n'est pas activé pour S3, effectuez les étapes suivantes.

["Création d'un SVM pour S3"](#)

["Création d'un compartiment pour S3"](#)

Bien que S3 puisse coexister dans un SVM avec NFS et SMB, il est possible de créer un nouveau SVM si l'un des cas suivants est vrai :

- Vous activez S3 pour la première fois sur un cluster.
- Un cluster contient des SVM dans lesquels vous ne souhaitez pas activer la prise en charge de S3.
- Un ou plusieurs SVM compatibles S3 sont mis en cluster et un autre serveur S3 doit avoir des caractéristiques de performance différentes.

Après l'activation du protocole S3 sur le SVM, procéder au provisionnement d'un compartiment.

- Pour provisionner le compartiment initial ou un compartiment supplémentaire sur un SVM compatible S3, effectuez la procédure ci-dessous.

["Création d'un compartiment pour S3"](#)

Configurez l'accès S3 à un SVM

Création d'un SVM pour S3

Bien que S3 puisse coexister avec d'autres protocoles dans un SVM, il peut être nécessaire de créer un nouveau SVM afin d'isoler le namespace et les workloads.

Description de la tâche

Si vous fournit uniquement le stockage objet S3 à partir d'un SVM, le serveur S3 ne nécessite aucune configuration DNS. Toutefois, il peut être nécessaire de configurer le DNS sur le SVM si d'autres protocoles sont utilisés.

Lorsque vous configurez l'accès S3 à une nouvelle machine virtuelle de stockage à l'aide de System Manager, vous êtes invité à saisir des informations de certificat et de mise en réseau, et la machine virtuelle de stockage et le serveur de stockage objet S3 sont créés en une seule opération.

Exemple 15. Étapes

System Manager

Vous devez préparer à saisir le nom du serveur S3 en tant que nom de domaine complet (FQDN) que les clients utiliseront pour l'accès S3. Le FQDN du serveur S3 ne doit pas commencer par un nom de compartiment.


Vous devez être prêt à saisir des adresses IP pour les données de rôle d'interface.

Si vous utilisez un certificat signé par une autorité de certification externe, vous serez invité à le saisir au cours de cette procédure ; vous avez également la possibilité d'utiliser un certificat généré par le système.

1. Activez S3 sur une VM de stockage.

- a. Ajouter une nouvelle machine virtuelle de stockage : cliquez sur **stockage > machines virtuelles de stockage**, puis sur **Ajouter**.

S'il s'agit d'un nouveau système sans machines virtuelles de stockage existantes : cliquez sur **Tableau de bord > configurer les protocoles**.

Si vous ajoutez un serveur S3 à une machine virtuelle de stockage existante : cliquez sur **stockage > Storage VM**, sélectionnez une machine virtuelle de stockage, cliquez sur **Paramètres**, puis cliquez sous **S3** .

- a. Cliquez sur **Activer S3**, puis entrez le nom du serveur S3.
- b. Sélectionnez le type de certificat.

Que vous sélectionniez un certificat généré par le système ou l'un de vos propres certificats, il sera nécessaire d'accéder au client.

- c. Saisissez les interfaces réseau.

2. Si vous avez sélectionné le certificat généré par le système, les informations de certificat s'affichent lorsque la création de la nouvelle machine virtuelle de stockage est confirmée. Cliquez sur **Download** et enregistrez-le pour accéder au client.

- La clé secrète ne s'affiche plus.
- Si vous avez besoin de nouveau des informations de certificat : cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.

CLI

1. Vérifiez que la licence S3 est disponible sur votre cluster :

```
system license show -package s3
```

Si ce n'est pas le cas, contactez votre représentant commercial.

2. Création d'un SVM :


```
vserver create -vserver <svm_name> -subtype default -rootvolume  
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security  
-style unix -language C.UTF-8 -data-services <data-s3-server>  
-ipSPACE <ipSPACE_name>
```

- Utilisez le paramètre UNIX pour le `-rootvolume-security-style` option.
- Utilisez le paramètre par défaut C.UTF-8 `-language` option.
- Le `ipSPACE` le paramètre est facultatif.

3. Vérifier la configuration et le statut du nouveau SVM :

```
vserver show -vserver <svm_name>
```

Le `Vserver Operational State` le champ doit afficher `running` état. S'il affiche le `initializing` État, cela signifie qu'une opération intermédiaire telle que la création du volume root a échoué, et vous devez supprimer la SVM et la recréer.

Exemples

La commande suivante crée un SVM pour l'accès aux données dans l'IPspace `ipSPACEA` :

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume  
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language  
C.UTF-8 -data-services _data-s3-server_ -ipSPACE ipSPACEA
```

```
[Job 2059] Job succeeded:  
Vserver creation completed
```

La commande suivante montre qu'un SVM a été créé avec un volume root de 1 Go, il a été démarré automatiquement et qu'il est en `running` état. Le volume root dispose d'une export policy par défaut qui n'inclut aucune règle et qui ne précise donc pas l'exportation du volume root au moment de sa création. Par défaut, le compte utilisateur `vsadmin` est créé et est dans le `locked` état. Le rôle `vsadmin` est attribué au compte utilisateur par défaut `vsadmin`.

```

cluster-1::> vserver show -vserver svm1.example.com
Vserver: svm1.example.com
Vserver Type: data
Vserver Subtype: default
Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
Root Volume: root_svm1
Aggregate: aggr1
NIS Domain: -
Root Volume Security Style: unix
LDAP Client: -
Default Volume Language Code: C.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs
Disallowed Protocols: -
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspaceA

```

Créer et installer un certificat d'autorité de certification sur le SVM

Un certificat d'autorité de certification (CA) est nécessaire pour activer le trafic HTTPS des clients S3 vers le SVM compatible avec S3.

Description de la tâche

Bien qu'il soit possible de configurer un serveur S3 pour utiliser uniquement le protocole HTTP, et bien qu'il soit possible de configurer des clients sans exigence de certificat d'autorité de certification, il est recommandé de sécuriser le trafic HTTPS vers des serveurs ONTAP S3 avec un certificat d'autorité de certification.

Un certificat CA n'est pas nécessaire pour une utilisation de hiérarchisation locale, où le trafic IP transite uniquement par les LIFs de cluster.

Les instructions de cette procédure créent et installent un certificat auto-signé ONTAP. Les certificats CA de fournisseurs tiers sont également pris en charge ; consultez la documentation relative à l'authentification de l'administrateur pour plus d'informations.

"Authentification de l'administrateur et RBAC"

Voir la `security certificate` pages de manuel pour les options de configuration supplémentaires.

Étapes

1. Créer un certificat numérique auto-signé :

```
security certificate create -vserver svm_name -type root-ca -common-name  
ca_cert_name
```

Le `-type root-ca` Option crée et installe un certificat numérique auto-signé pour signer d'autres certificats en agissant comme autorité de certification (CA).

Le `-common-name` Option crée le nom de l'autorité de certification du SVM et sera utilisé lors de la génération du nom complet du certificat.

La taille du certificat par défaut est de 2048 bits.

Exemple

```
cluster-1::> security certificate create -vserver svm1.example.com -type  
root-ca -common-name svm1_ca
```

```
The certificate's generated name for reference:  
svm1_ca_159D1587CE21E9D4_svm1_ca
```

Lorsque le nom généré du certificat est affiché, veuillez à l'enregistrer pour les étapes ultérieures de cette procédure.

2. Générer une demande de signature de certificat :

```
security certificate generate-csr -common-name s3_server_name  
[additional_options]
```

Le `-common-name` Le paramètre de la demande de signature doit être le nom de serveur S3 (FQDN).

Vous pouvez fournir l'emplacement et d'autres informations détaillées sur la SVM si nécessaire.

Vous êtes invité à conserver une copie de votre demande de certificat et de votre clé privée pour référence ultérieure.

3. Signer la RSC à l'aide de SVM_CA pour générer le certificat du serveur S3 :

```
security certificate sign -vserver svm_name -ca ca_cert_name -ca-serial  
ca_cert_serial_number [additional_options]
```

Entrez les options de commande que vous avez utilisées aux étapes précédentes :

- `-ca` — le nom commun de l'autorité de certification que vous avez saisi à l'étape 1.
- `-ca-serial` — le numéro de série CA de l'étape 1. Par exemple, si le nom du certificat de l'autorité de certification est `svm1_CA_159D1587CE21E9D4_svm1_ca`, le numéro de série est `159D1587CE2E9D4`.

Par défaut, le certificat signé expirera dans 365 jours. Vous pouvez sélectionner une autre valeur et spécifier d'autres détails de signature.

Lorsque vous y êtes invité, copiez et entrez la chaîne de demande de certificat que vous avez enregistrée à l'étape 2.

Un certificat signé s'affiche ; enregistrez-le pour une utilisation ultérieure.

4. Installez le certificat signé sur le SVM compatible S3 :

```
security certificate install -type server -vserver svm_name
```

Lorsque vous y êtes invité, entrez le certificat et la clé privée.

Vous avez la possibilité de saisir des certificats intermédiaires si une chaîne de certificats est souhaitée.

Lorsque la clé privée et le certificat numérique signé par l'autorité de certification sont affichés, enregistrez-les pour référence ultérieure.

5. Obtenir le certificat de clé publique :

```
security certificate show -vserver svm_name -common-name ca_cert_name -type  
root-ca -instance
```

Enregistrez le certificat de clé publique pour une configuration client ultérieure.

Exemple

```

cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca -instance

                Name of Vserver: svm1.example.com
                FQDN or Custom Common Name: svm1_ca
                Serial Number of Certificate: 159D1587CE21E9D4
                Certificate Authority: svm1_ca
                Type of Certificate: root-ca
                (DEPRECATED)-Certificate Subtype: -
                Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
                Certificate Start Date: Thu May 09 10:58:39 2020
                Certificate Expiration Date: Fri May 08 10:58:39 2021
                Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----

                Country Name: US
                State or Province Name:
                Locality Name:
                Organization Name:
                Organization Unit:
Contact Administrator's Email Address:
                Protocol: SSL
                Hashing Function: SHA256
                Self-Signed Certificate: true
                Is System Internal Certificate: false

```

Création d'une règle de données de service S3

Vous pouvez créer des règles de service pour les données S3 et les services de gestion. Une règle de données de service S3 est nécessaire pour activer le trafic de données S3 sur les LIF.

Description de la tâche

Une politique de données de service S3 est requise si vous utilisez des LIF de données et des LIF intercluster. Il n'est pas nécessaire d'utiliser des LIF de cluster pour la hiérarchisation locale.

Lorsqu'une politique de services est spécifiée pour une LIF, cette règle est utilisée pour construire un rôle par défaut, une politique de basculement et une liste de protocoles de données pour la LIF.

Bien que plusieurs protocoles puissent être configurés pour les SVM et les LIF, il est recommandé de configurer S3 comme le seul protocole lors du service des données d'objet.

Étapes

1. Modifiez le paramètre de privilège sur avancé :

```
set -privilege advanced
```

2. Création d'une règle de données de service :

```
network interface service-policy create -vserver svm_name -policy policy_name
-services data-core,data-s3-server
```

Le `data-core` et `data-s3-server` Les services sont les seuls requis pour activer ONTAP S3, bien que d'autres services puissent être inclus si nécessaire.

Création de LIF de données

Si vous avez créé un nouveau SVM, les LIF dédiées que vous créez pour accéder à S3 doivent être des LIF de données.

Avant de commencer

- Le port réseau physique ou logique sous-jacent doit avoir été configuré sur l'administrateur `up` état.
- Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, le sous-réseau doit déjà exister.

Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche 3. Ils sont créés à l'aide du `network subnet create` commande.

- La politique de service LIF doit déjà exister.
- Dans le cadre de la bonne pratique, les LIF utilisées pour l'accès aux données (serveur-données-s3) et les LIF utilisées pour les opérations de gestion (management-https) doivent être séparées. Les deux services ne doivent pas être activés sur la même LIF.
- Les enregistrements DNS ne doivent contenir que des adresses IP des LIFs dont le serveur-s3-données est associé. Si les adresses IP des autres LIFs sont spécifiées dans l'enregistrement DNS, les requêtes ONTAP S3 peuvent être servies par d'autres serveurs ce qui provoque des réponses inattendues.

Description de la tâche

- Vous pouvez créer des LIF IPv4 et IPv6 sur le même port réseau.
- Si vous disposez d'un grand nombre de LIF dans le cluster, vous pouvez vérifier la capacité LIF prise en charge sur le cluster à l'aide de `network interface capacity show` Et la capacité LIF prise en charge sur chaque nœud à l'aide de `network interface capacity details show` commande (au niveau de privilège avancé).
- Si vous activez la hiérarchisation distante de la capacité FabricPool (cloud), vous devez également configurer les LIF intercluster.

Étapes

1. Créer une LIF :

```
network interface create -vserver svm_name -lif lif_name -service-policy
service_policy_names -home-node node_name -home-port port_name {-address
IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy
data -auto-revert {true|false}
```

- `-home-node` Est le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.

Vous pouvez également indiquer si la LIF doit revenir automatiquement au nœud home et au port

home-port avec le `-auto-revert` option.

- `-home-port` Est le port physique ou logique vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.
- Vous pouvez spécifier une adresse IP avec le `-address` et `-netmask` ou vous activez l'allocation à partir d'un sous-réseau avec le `-subnet_name` option.
- Lors de l'utilisation d'un sous-réseau pour fournir l'adresse IP et le masque de réseau, si le sous-réseau a été défini avec une passerelle, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau.
- Si vous attribuez des adresses IP manuellement (sans utiliser de sous-réseau), vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un autre sous-réseau IP. Le `network route create` La page man contient des informations sur la création d'une route statique au sein d'un SVM.
- Pour le `-firewall-policy` utilisez la même option par défaut `data` Comme le rôle LIF.

Vous pouvez créer et ajouter une stratégie de pare-feu personnalisée ultérieurement si vous le souhaitez.



Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir ["Configuration des politiques de pare-feu pour les LIF"](#).

- `-auto-revert` Vous permet de spécifier si une LIF de données est automatiquement rétablie sur le nœud de rattachement en cas de démarrage, de modifications du statut de la base de données de gestion ou lors de la connexion réseau. Le paramètre par défaut est `false`, mais vous pouvez le définir sur `false` selon les stratégies de gestion de réseau de votre environnement.
- Le `-service-policy` spécifie la stratégie de données et de services de gestion que vous avez créée ainsi que les autres règles dont vous avez besoin.

2. Si vous souhaitez attribuer une adresse IPv6 dans `-address` option :

- a. Utilisez le `network ndp prefix show` Commande permettant d'afficher la liste des préfixes de RA apprises sur diverses interfaces.

Le `network ndp prefix show` la commande est disponible au niveau de privilège avancé.

- b. Utiliser le format `prefix:id` Pour construire l'adresse IPv6 manuellement.

`prefix` est le préfixe utilisé sur les différentes interfaces.

Pour calculer le `id`, choisissez un nombre hexadécimal 64 bits aléatoire.

3. Vérifier que le LIF a été créé avec succès en utilisant le `network interface show` commande.

4. Vérifiez que l'adresse IP configurée est accessible :

Pour vérifier...	Utiliser...
Adresse IPv4	<code>network ping</code>

Pour vérifier...	Utiliser...
Adresse IPv6	<code>network ping6</code>

Exemples

La commande suivante montre comment créer une LIF de données S3 attribuée avec le `my-S3-policy` règle de service :

```
network interface create -vserver svml.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

La commande suivante affiche toutes les LIFs du cluster-1. Les LIF de données `datalif1` et `datalif3` sont configurées avec des adresses IPv4 et le `datalif4` est configuré avec une adresse IPv6 :


```
cluster-1::> network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
-----	-----	-----	-----	-----	-----	-----
cluster-1						
true	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a	
node-1						
true	clus1	up/up	192.0.2.12/24	node-1	e0a	
true	clus2	up/up	192.0.2.13/24	node-1	e0b	
true	mgmt1	up/up	192.0.2.68/24	node-1	e1a	
node-2						
true	clus1	up/up	192.0.2.14/24	node-2	e0a	
true	clus2	up/up	192.0.2.15/24	node-2	e0b	
true	mgmt1	up/up	192.0.2.69/24	node-2	e1a	
vs1.example.com						
true	datalif1	up/down	192.0.2.145/30	node-1	e1c	
vs3.example.com						
true	datalif3	up/up	192.0.2.146/30	node-2	e0c	
true	datalif4	up/up	2001::2/64	node-2	e0c	
5 entries were displayed.						

Création des LIFs intercluster pour le Tiering distant des FabricPool

Si vous activez le Tiering FabricPool à distance (cloud) à l'aide de ONTAP S3, vous devez configurer les LIF intercluster. Vous pouvez configurer les LIFs intercluster sur des ports partagés avec le réseau de données. Cela réduit le nombre de ports nécessaires pour la mise en réseau intercluster.

Avant de commencer

- Le port réseau physique ou logique sous-jacent doit avoir été configuré sur l'administrateur up état.
- La politique de service LIF doit déjà exister.

Description de la tâche

Les LIF intercluster ne sont pas nécessaires pour la hiérarchisation locale des pools de structure ni pour le traitement d'applications S3 externes.

Étapes

- 1. Lister les ports dans le cluster :

```
network port show
```

L'exemple suivant montre les ports réseau dans cluster01:

```
cluster01::> network port show
```

(Mbps)							Speed
Node	Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper

cluster01-01							
	e0a	Cluster	Cluster		up	1500	auto/1000
	e0b	Cluster	Cluster		up	1500	auto/1000
	e0c	Default	Default		up	1500	auto/1000
	e0d	Default	Default		up	1500	auto/1000
cluster01-02							
	e0a	Cluster	Cluster		up	1500	auto/1000
	e0b	Cluster	Cluster		up	1500	auto/1000
	e0c	Default	Default		up	1500	auto/1000
	e0d	Default	Default		up	1500	auto/1000

- 2. Création des LIFs intercluster sur le SVM système :

```
network interface create -vserver Cluster -lif LIF_name -service-policy
default-intercluster -home-node node -home-port port -address port_IP -netmask
netmask
```

L'exemple suivant illustre la création de LIFs intercluster cluster01_icl01 et cluster01_icl02:

```

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0

```

3. Vérifier que les LIFs intercluster ont été créés :

```
network interface show -service-policy default-intercluster
```

```

cluster01::> network interface show -service-policy default-intercluster

```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Home				Port
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
cluster01	cluster01_icl01	up/up	192.168.1.201/24	cluster01-01 e0c
true	cluster01_icl02	up/up	192.168.1.202/24	cluster01-02 e0c
true				

4. Vérifier que les LIFs intercluster sont redondants :

```
network interface show -service-policy default-intercluster -failover
```

L'exemple suivant indique que les LIFs intercluster cluster01_icl01 et cluster01_icl02 sur le e0c le port basculera vers le e0d port.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
cluster01	cluster01_icl01	cluster01-01:e0c	local-only	
192.168.1.201/24			Failover Targets: cluster01-01:e0c, cluster01-01:e0d	
	cluster01_icl02	cluster01-02:e0c	local-only	
192.168.1.201/24			Failover Targets: cluster01-02:e0c, cluster01-02:e0d	

Créez le serveur de magasin d'objets S3

Le serveur de magasin d'objets ONTAP gère les données sous forme d'objets S3 au lieu du stockage de fichiers ou de blocs fourni par les serveurs NAS et SAN ONTAP.

Avant de commencer

Vous devez préparer à saisir le nom du serveur S3 en tant que nom de domaine complet (FQDN) que les clients utiliseront pour l'accès S3. Le FQDN ne doit pas commencer par un nom de compartiment. Lorsque vous accédez à des compartiments à l'aide de style hébergement virtuel, le nom du serveur sera utilisé comme `mydomain.com`. Par exemple `bucketname.mydomain.com`, .

Vous devez disposer d'un certificat d'autorité de certification auto-signé (créé aux étapes précédentes) ou d'un certificat signé par un fournisseur d'autorité de certification externe. Un certificat CA n'est pas nécessaire pour une utilisation de hiérarchisation locale, où le trafic IP transite uniquement par les LIFs de cluster.

Description de la tâche

Lorsqu'un serveur de magasin d'objets est créé, un utilisateur root avec UID 0 est créé. Aucune clé d'accès ou clé secrète n'est générée pour cet utilisateur root. L'administrateur ONTAP doit exécuter le `object-store-server users regenerate-keys` commande permettant de définir la clé d'accès et la clé secrète pour cet utilisateur.



Dans le cadre de nos bonnes pratiques, ne pas utiliser cet utilisateur root. Toute application client qui utilise la clé d'accès ou la clé secrète de l'utilisateur root dispose d'un accès complet à tous les compartiments et objets du magasin d'objets.


Voir la `vserver object-store-server` pages de manuel pour des options de configuration et d'affichage supplémentaires.

Exemple 16. Étapes

System Manager

Suivez cette procédure si vous ajoutez un serveur S3 à une machine virtuelle de stockage existante. Pour ajouter un serveur S3 à une nouvelle machine virtuelle de stockage, voir ["Création d'un SVM de stockage pour S3"](#).

Vous devez être prêt à saisir des adresses IP pour les données de rôle d'interface.

1. Activez S3 sur une machine virtuelle de stockage existante.
 - a. Sélectionnez la machine virtuelle de stockage : cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez une machine virtuelle de stockage, cliquez sur **Paramètres**, puis cliquez  sous **S3**.
 - b. Cliquez sur **Activer S3**, puis entrez le nom du serveur S3.
 - c. Sélectionnez le type de certificat.

Que vous sélectionniez un certificat généré par le système ou l'un de vos propres certificats, il sera nécessaire d'accéder au client.
 - d. Saisissez les interfaces réseau.
2. Si vous avez sélectionné le certificat généré par le système, les informations de certificat s'affichent lorsque la création de la nouvelle machine virtuelle de stockage est confirmée. Cliquez sur **Download** et enregistrez-le pour accéder au client.
 - La clé secrète ne s'affiche plus.
 - Si vous avez besoin de nouveau des informations de certificat : cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.

CLI

1. Création du serveur S3 :

```
vserver object-store-server create -vserver svm_name -object-store-server  
s3_server_fqdn -certificate-name server_certificate_name -comment text  
[additional_options]
```

Vous pouvez spécifier des options supplémentaires lors de la création du serveur S3 ou à tout moment ultérieurement.

- Si vous configurez une hiérarchisation locale, le nom du SVM peut être un SVM de données ou un nom de SVM système (cluster).
- Le nom du certificat doit être le nom du certificat du serveur (certificat d'utilisateur final ou de serveur) et non le certificat de l'autorité de certification du serveur (certificat de l'autorité de certification intermédiaire ou racine).
- HTTPS est activé par défaut sur le port 443. Vous pouvez modifier le numéro de port à l'aide du `-secure-listener-port` option.

Lorsque HTTPS est activé, des certificats CA sont requis pour une intégration correcte avec SSL/TLS. À partir de ONTAP 9.15.1, TLS 1.3 est pris en charge avec le stockage objet S3.

- HTTP est désactivé par défaut. Lorsqu'il est activé, le serveur écoute sur le port 80. Vous pouvez

l'activer avec le `-is-http-enabled` ou modifiez le numéro de port avec le `-listener-port` option.

Lorsque HTTP est activé, la requête et les réponses sont envoyées sur le réseau en texte clair.

2. Vérifier que S3 est configuré :

```
vserver object-store-server show
```

Exemple

Cette commande vérifie les valeurs de configuration de tous les serveurs de stockage objet :

```
cluster1::> vserver object-store-server show

Vserver: vs1

Object Store Server Name: s3.example.com
Administrative State: up
Listener Port For HTTP: 80
Secure Listener Port For HTTPS: 443
HTTP Enabled: false
HTTPS Enabled: true
Certificate for HTTPS Connections: svml_ca
Comment: Server comment
```

Ajout de capacité de stockage à un SVM compatible S3

Créer un compartiment

Les objets S3 sont conservés dans *buckets*. Ils ne sont pas imbriqués en tant que fichiers dans un répertoire à l'intérieur d'autres répertoires.

Avant de commencer

Une VM de stockage contenant un serveur S3 doit déjà exister.

Description de la tâche

- Depuis la version ONTAP 9.14.1, le redimensionnement automatique a été activé sur les volumes FlexGroup S3 lorsque des compartiments sont créés. Cela élimine l'allocation excessive de capacité lors de la création du compartiment sur les volumes FlexGroup existants et nouveaux. Les volumes FlexGroup sont redimensionnés au minimum requis selon les instructions suivantes. La taille minimale requise correspond à la taille totale de tous les compartiments S3 d'un volume FlexGroup.
 - À partir de ONTAP 9.14.1, si un volume FlexGroup S3 est créé dans le cadre d'une nouvelle création de compartiment, le volume FlexGroup est créé avec la taille minimale requise.
 - Si un volume FlexGroup S3 a été créé avant ONTAP 9.14.1, le premier compartiment créé ou supprimé après ONTAP 9.14.1 redimensionne le volume FlexGroup à la taille minimale requise.
 - Si un volume FlexGroup S3 a été créé avant ONTAP 9.14.1 et disposait déjà de la taille minimale requise, la création ou la suppression d'un compartiment après ONTAP 9.14.1 conserve la taille du

volume FlexGroup S3.

- Les niveaux de service de stockage sont des groupes de règles prédéfinies de qualité de service (QoS) adaptative, avec des niveaux par défaut *Value*, *performance* et *Extreme*. Au lieu d'un des niveaux de service de stockage par défaut, vous pouvez également définir un groupe de règles de QoS personnalisé et le appliquer à un compartiment. Pour plus d'informations sur les définitions de service de stockage, reportez-vous à "[Définitions des services de stockage](#)" la section . Pour plus d'informations sur la gestion des performances, reportez-vous à la section "[Gestion des performances](#)". Depuis ONTAP 9.8, lorsque vous provisionnez le stockage, la QoS est activée par défaut. Vous pouvez désactiver QoS ou choisir une règle de QoS personnalisée lors du processus de provisionnement ou ultérieurement.
 - Si vous configurez la hiérarchisation de la capacité locale, vous créez des compartiments et des utilisateurs dans une VM de stockage des données, et non dans la VM de stockage du système où se trouve le serveur S3.
 - Pour l'accès client à distance, vous devez configurer des compartiments dans une VM de stockage compatible S3. Si vous créez un compartiment dans une machine virtuelle de stockage non compatible S3, il sera uniquement disponible pour le Tiering local.
 - À partir de ONTAP 9.14.1, vous pouvez "[Créer un compartiment sur un agrégat en miroir ou sans miroir dans une configuration MetroCluster](#)".
 - Pour l'interface de ligne de commandes, lorsque vous créez un compartiment, deux options de provisionnement sont disponibles :
 - Laissez ONTAP Select les agrégats sous-jacents et les composants FlexGroup (par défaut)
 - ONTAP crée et configure un volume FlexGroup pour le premier compartiment en sélectionnant automatiquement les agrégats. Il sélectionne automatiquement le niveau de service le plus élevé disponible pour votre plateforme, ou vous pouvez spécifier le niveau de service de stockage. Tout compartiment supplémentaire que vous ajoutez ultérieurement dans la VM de stockage aura le même volume FlexGroup sous-jacent.
 - Vous pouvez également indiquer si le compartiment sera utilisé pour le Tiering, dans ce cas, ONTAP tente de sélectionner un support économique avec des performances optimales pour les données hiérarchisées.
 - Vous sélectionnez les agrégats sous-jacents et les composants FlexGroup (nécessite des options de commande avec privilèges avancés) : vous pouvez sélectionner manuellement les agrégats sur lesquels le compartiment et le volume FlexGroup contenant doivent être créés, puis spécifier le nombre de composants sur chaque agrégat. Lors de l'ajout de compartiments supplémentaires :
 - Si vous spécifiez les agrégats et les composants pour un nouveau compartiment, un nouveau FlexGroup est créé pour ce nouveau compartiment.
 - Si vous ne spécifiez pas d'agrégats ni de composants pour un nouveau compartiment, le nouveau compartiment est ajouté à un FlexGroup existant.
Voir [Gestion des volumes FlexGroup](#) pour en savoir plus.
- Lorsque vous spécifiez des agrégats et des composants lors de la création d'un compartiment, aucun groupe de règles de QoS, n'est appliqué par défaut ou personnalisé. Vous pouvez le faire plus tard avec le `vserver object-store-server bucket modify` commande.

Voir pour en savoir plus.

Remarque : si vous utilisez des compartiments à partir de Cloud Volumes ONTAP, vous devez utiliser la procédure CLI. Il est fortement recommandé de sélectionner manuellement les agrégats sous-jacents pour s'assurer qu'ils n'utilisent qu'un seul nœud. L'utilisation d'agrégats des deux nœuds peut avoir un impact sur les performances, car les nœuds se trouvent dans des zones de disponibilité séparées géographiquement et sont donc sujets aux problèmes de latence.

Créez des compartiments S3 avec l'interface de ligne de commandes de ONTAP

1. Si vous prévoyez de sélectionner vous-même les agrégats et les composants FlexGroup, définissez le niveau de privilège sur Avancé (sinon, le niveau de privilège admin est suffisant) : `set -privilege advanced`
2. Création d'un compartiment :

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

Le nom de la VM de stockage peut être soit une VM de stockage de données, soit `Cluster` (Nom de la machine virtuelle de stockage du système) si vous configurez la hiérarchisation locale.

Si vous n'indiquez aucune option, ONTAP crée un compartiment de 800 Go avec un niveau de service défini sur le niveau le plus élevé disponible pour votre système.

Si vous souhaitez que ONTAP crée un compartiment en fonction de la performance ou de l'utilisation, choisissez l'une des options suivantes :

- niveau de service

Incluez le `-storage-service-level` option avec l'une des valeurs suivantes : `value`, `performance`, ou `extreme`.

- tiering

Incluez le `-used-as-capacity-tier true` option.

Pour spécifier les agrégats sur lesquels créer le volume FlexGroup sous-jacent, utilisez les options suivantes :

- Le `-aggr-list` Le paramètre spécifie la liste des agrégats à utiliser pour les composants de volume FlexGroup.

Chaque entrée de la liste crée un composant sur l'agrégat spécifié. Vous pouvez spécifier un agrégat plusieurs fois afin d'avoir plusieurs composants créés sur l'agrégat.

Pour assurer des performances prévisibles sur l'ensemble du volume FlexGroup, tous les agrégats doivent utiliser les mêmes configurations de type de disque et de groupe RAID.

- Le `-aggr-list-multiplier` le paramètre spécifie le nombre de fois pour effectuer l'itération sur les agrégats répertoriés avec le `-aggr-list` Paramètre lors de la création d'un volume FlexGroup.

La valeur par défaut du `-aggr-list-multiplier` le paramètre est 4.

3. Ajout d'une « policy group » QoS le cas échéant :

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy
-group qos_policy_group
```

4. Vérification de la création de compartiment :

```
vserver object-store-server bucket show [-instance]
```


Exemple

L'exemple suivant illustre la création d'un compartiment pour la machine virtuelle de stockage vs1 de taille 1TB et spécifier l'agrégat :

```
cluster-1::*> vserver object-store-server bucket create -vserver  
svml.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

Création de compartiments S3 avec System Manager

1. Ajoutez un nouveau compartiment à une machine virtuelle de stockage compatible S3.
 - a. Cliquez sur **stockage > compartiments**, puis sur **Ajouter**.
 - b. Entrez un nom, sélectionnez la machine virtuelle de stockage, puis entrez une taille.
 - Si vous cliquez sur **Enregistrer** à ce stade, un compartiment est créé avec les paramètres par défaut suivants :
 - L'accès au compartiment n'est accordé à aucun utilisateur, sauf si des règles de groupes sont déjà en vigueur.



Vous ne devez pas utiliser l'utilisateur root S3 pour gérer le stockage objet ONTAP et partager ses autorisations, car il dispose d'un accès illimité au magasin d'objets. Créez plutôt un utilisateur ou un groupe avec les privilèges d'administration que vous attribuez.

- Niveau de qualité de service (performance) le plus élevé disponible pour votre système
- Cliquez sur **Enregistrer** pour créer un compartiment avec ces valeurs par défaut.

Configurer des autorisations et restrictions supplémentaires

Vous pouvez cliquer sur **plus d'options** pour configurer les paramètres de verrouillage d'objet, les autorisations utilisateur et le niveau de performances lorsque vous configurez le compartiment, ou vous pouvez modifier ces paramètres ultérieurement.

Si vous prévoyez d'utiliser le stockage d'objets S3 pour le Tiering FabricPool, choisissez **use pour le Tiering** (utilisez des supports à faible coût avec des performances optimales pour les données hiérarchisées) plutôt que un niveau de service de performance.

Si vous souhaitez activer la gestion des versions de vos objets pour une récupération ultérieure, sélectionnez **Activer la gestion des versions**. La gestion des versions est activée par défaut si vous activez le verrouillage des objets sur le compartiment. Pour plus d'informations sur la gestion des versions d'objet, reportez-vous à la section "[Gestion des versions dans des compartiments S3 pour Amazon](#)".

À partir de la version 9.14.1, le verrouillage des objets est pris en charge par les compartiments S3. Le verrouillage des objets S3 nécessite une licence SnapLock standard. Cette licence est incluse avec "[ONTAP One](#)".

Avant ONTAP One, la licence SnapLock était incluse dans le bundle sécurité et conformité. Le bundle sécurité et conformité n'est plus proposé, mais reste valide. Bien qu'ils ne soient pas encore requis, les clients existants peuvent choisir de le faire "[Passez à ONTAP One](#)".

Si vous activez le verrouillage d'objet sur un compartiment, vous devez "[Vérifiez qu'une licence SnapLock est installée](#)". Si aucune licence SnapLock n'est installée, vous devez le faire "[installer](#)" avant de pouvoir activer le verrouillage des objets.

Une fois que vous avez vérifié que la licence SnapLock est installée, pour protéger les objets de votre compartiment contre la suppression ou l'écrasement, sélectionnez **Activer le verrouillage d'objet**. Le verrouillage peut être activé sur l'ensemble des versions d'objets ou sur des versions spécifiques, et uniquement lorsque l'horloge de conformité SnapLock est initialisée pour les nœuds de cluster. Voici la procédure à suivre :

1. Si l'horloge de conformité SnapLock n'est pas initialisée sur un nœud du cluster, le bouton **initialiser horloge de conformité SnapLock** apparaît. Cliquez sur **initialiser horloge de conformité SnapLock** pour initialiser l'horloge de conformité SnapLock sur les nœuds du cluster.
2. Sélectionnez le mode **Governance** pour activer un verrouillage basé sur le temps qui autorise les autorisations *Write Once, Read Many (WORM)* sur les objets. Même en mode *Governance*, les objets peuvent être supprimés par les utilisateurs administrateurs disposant d'autorisations spécifiques.
3. Sélectionnez le mode **conformité** si vous souhaitez affecter des règles plus strictes de suppression et de mise à jour des objets. Dans ce mode de verrouillage d'objet, les objets ne peuvent être expirés qu'à la fin de la période de conservation spécifiée. À moins qu'une période de conservation ne soit spécifiée, les objets restent verrouillés indéfiniment.
4. Spécifiez la durée de conservation du verrou en jours ou en années si vous souhaitez que le verrouillage soit effectif pendant une certaine période.



Le verrouillage s'applique aux compartiments S3 avec et sans version. Le verrouillage d'objet ne s'applique pas aux objets NAS.

Vous pouvez configurer les paramètres de protection et d'autorisation, ainsi que le niveau de service de performances du compartiment.



Vous devez avoir déjà créé un utilisateur et des groupes avant de configurer les autorisations.

Pour plus d'informations, voir "[Créer un miroir pour le nouveau godet](#)".

Vérifier l'accès au godet

Sur les applications client S3 (ONTAP S3 ou une application tierce externe), vous pouvez vérifier votre accès au nouveau compartiment en saisissant les informations suivantes :

- Certificat CA de serveur S3.
- La clé d'accès et la clé secrète de l'utilisateur.
- Nom de domaine complet du serveur S3 et nom de compartiment.


Gérer la taille du compartiment

Si nécessaire, vous pouvez augmenter ou diminuer la taille d'un godet existant.

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour gérer la taille de compartiment.

System Manager

1. Sélectionnez **stockage > compartiments** et localisez le godet que vous souhaitez modifier.
2. Cliquez sur  en regard du nom du compartiment et sélectionnez **Modifier**.
3. Dans la fenêtre **Edit bucket**, modifiez la capacité du compartiment.
4. **Enregistrer**.

CLI

1. Modifier la capacité du godet :

```
vserver object-store-server bucket modify -vserver <SVM_name>  
-bucket <bucket_name> -size {<integer>[KB|MB|GB|TB|PB]}
```

Créez un compartiment sur un agrégat en miroir ou sans miroir dans une configuration MetroCluster

À partir de ONTAP 9.14.1, vous pouvez provisionner un compartiment sur un agrégat en miroir ou sans miroir dans des configurations MetroCluster FC et IP.

Description de la tâche

- Par défaut, les compartiments sont provisionnés sur les agrégats en miroir.
- Les mêmes instructions de provisionnement que celles de la section "[Créer un compartiment](#)" S'applique à la création d'un compartiment dans un environnement MetroCluster.
- Les fonctionnalités de stockage objet S3 suivantes sont **non** prises en charge dans les environnements MetroCluster :
 - SnapMirror S3
 - Gestion du cycle de vie des compartiments S3
 - Verrouillage d'objet S3 en mode **Compliance**



Le verrouillage d'objet S3 en mode **gouvernance** est pris en charge.

- Tiering FabricPool local

Avant de commencer

Un SVM contenant un serveur S3 doit déjà exister.

Processus de création de compartiments

CLI

1. Si vous prévoyez de sélectionner vous-même les agrégats et les composants FlexGroup, définissez le niveau de privilège sur Avancé (sinon, le niveau de privilège admin est suffisant) : `set -privilege advanced`

2. Création d'un compartiment :

```
vserver object-store-server bucket create -vserver <svm_name> -bucket  
<bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates  
true/false]
```

Réglez le `-use-mirrored-aggregates` option à `true` ou `false` selon que vous souhaitez utiliser un agrégat en miroir ou sans miroir.



Par défaut, le `-use-mirrored-aggregates` l'option est définie sur `true`.

- Le nom du SVM doit être un SVM de données.
- Si vous n'indiquez aucune option, ONTAP crée un compartiment de 800 Go avec un niveau de service défini sur le niveau le plus élevé disponible pour votre système.
- Si vous souhaitez que ONTAP crée un compartiment en fonction de la performance ou de l'utilisation, choisissez l'une des options suivantes :
 - niveau de service

Incluez le `-storage-service-level` option avec l'une des valeurs suivantes : `value`, `performance`, ou `extreme`.
 - tiering

Incluez le `-used-as-capacity-tier true` option.
- Pour spécifier les agrégats sur lesquels créer le volume FlexGroup sous-jacent, utilisez les options suivantes :
 - Le `-aggr-list` Le paramètre spécifie la liste des agrégats à utiliser pour les composants de volume FlexGroup.

Chaque entrée de la liste crée un composant sur l'agrégat spécifié. Vous pouvez spécifier un agrégat plusieurs fois afin d'avoir plusieurs composants créés sur l'agrégat.

Pour assurer des performances prévisibles sur l'ensemble du volume FlexGroup, tous les agrégats doivent utiliser les mêmes configurations de type de disque et de groupe RAID.

- Le `-aggr-list-multiplier` le paramètre spécifie le nombre de fois pour effectuer l'itération sur les agrégats répertoriés avec le `-aggr-list` Paramètre lors de la création d'un volume FlexGroup.

La valeur par défaut du `-aggr-list-multiplier` le paramètre est 4.

3. Ajout d'une « policy group » QoS le cas échéant :

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy  
-group qos_policy_group
```

4. Vérification de la création de compartiment :

```
vserver object-store-server bucket show [-instance]
```

Exemple

L'exemple suivant illustre la création d'un compartiment pour le SVM vs1 de 1 To sur un agrégat en miroir :

```
cluster-1::*> vserver object-store-server bucket create -vserver  
svm1.example.com -bucket testbucket -size 1TB -use-mirrored-aggregates  
true
```

System Manager

1. Ajoutez un nouveau compartiment à une machine virtuelle de stockage compatible S3.

- a. Cliquez sur **stockage > compartiments**, puis sur **Ajouter**.
- b. Entrez un nom, sélectionnez la machine virtuelle de stockage, puis entrez une taille.

Par défaut, le compartiment est provisionné sur un agrégat en miroir. Si vous souhaitez créer un compartiment sur un agrégat sans miroir, sélectionnez **plus d'options** et décochez la case **utiliser le niveau SyncMirror** sous **protection**, comme illustré dans l'image suivante :

Add bucket

NAME

To use this bucket from a remote cluster, configure S3 service on storage VM "vs1".

FOLDER (OPTIONAL)

Specify the folder to map to this bucket. [Know more](#)

CAPACITY

Size

GB

☐ Use tiering
If you select this option, the system will try to select low-cost media with optimal performance for the tiered data.
☐ Enable versioning
Versioning-enabled buckets allow you to recover objects that were accidentally deleted or overwritten. After versioning is enabled, it can't be disabled. However, you can suspend versioning.

PERFORMANCE SERVICE LEVEL

Value

Not sure? [Get help selecting type](#)

Permissions

☐ Copy access permissions from an existing bucket

Principal	Effect	Actions	Resources	Conditions
All users of this stor...	allow	ListBucket	*	

+ Add

Object locking

☐ Enable object locking
Object locking utilizes the "Write Once, Read Many" (WORM) model in which objects or their versions are protected from being deleted or overwritten during the specified retention period.

Protection

☒ Use the S3x3lax protection

- Si vous cliquez sur **Enregistrer** à ce stade, un compartiment est créé avec les paramètres par défaut suivants :
 - L'accès au compartiment n'est accordé à aucun utilisateur, sauf si des règles de groupes sont déjà en vigueur.



Vous ne devez pas utiliser l'utilisateur root S3 pour gérer le stockage objet ONTAP et partager ses autorisations, car il dispose d'un accès illimité au magasin d'objets. Créez plutôt un utilisateur ou un groupe avec les privilèges d'administration que vous attribuez.

- Niveau de qualité de service (performance) le plus élevé disponible pour votre système
- Vous pouvez cliquer sur **plus d'options** pour configurer les autorisations utilisateur et le niveau de performances lorsque vous configurez le compartiment, ou vous pouvez modifier ces paramètres ultérieurement.

- Vous devez avoir déjà créé des utilisateurs et des groupes avant d'utiliser **plus d'options** pour configurer leurs autorisations.
 - Si vous prévoyez d'utiliser le stockage d'objets S3 pour le Tiering FabricPool, choisissez **use pour le Tiering** (utilisez des supports à faible coût avec des performances optimales pour les données hiérarchisées) plutôt que un niveau de service de performance.
2. Pour les applications client S3, un autre système ONTAP ou une application tierce externe, vérifiez l'accès au nouveau compartiment en saisissant les éléments suivants :
- Certificat CA de serveur S3.
 - Clé d'accès et clé secrète de l'utilisateur.
 - Nom de domaine complet du serveur S3 et nom de compartiment.

Créez une règle de gestion du cycle de vie des compartiments

À partir de ONTAP 9.13.1, vous pouvez créer des règles de gestion du cycle de vie pour gérer les cycles de vie des objets dans vos compartiments S3. Vous pouvez définir des règles de suppression pour des objets spécifiques d'un compartiment et, par le biais de ces règles, ces objets de compartiment expirent. Cela vous permet de respecter les exigences de conservation et de gérer efficacement l'ensemble du stockage objet S3.



Si le verrouillage des objets est activé pour vos objets de compartiment, les règles de gestion du cycle de vie pour l'expiration des objets ne seront pas appliquées aux objets verrouillés. Pour plus d'informations sur le verrouillage des objets, reportez-vous à la section "[Créer un compartiment](#)".

Avant de commencer

- Un SVM compatible S3 contenant un serveur S3 et un compartiment doivent déjà exister. Voir "[Création d'un SVM pour S3](#)" pour en savoir plus.
- Sachez que les règles de gestion du cycle de vie des compartiments ne sont pas prises en charge dans les configurations MetroCluster.

Description de la tâche

Lors de la création de vos règles de gestion du cycle de vie, vous pouvez appliquer les actions de suppression suivantes à vos objets de compartiment :

- Suppression des versions actuelles - cette action expire les objets identifiés par la règle. Si la gestion des versions est activée sur le compartiment, S3 rend tous les objets expirés indisponibles. Si la gestion des versions n'est pas activée, cette règle supprime définitivement les objets. L'action CLI est `Expiration`.
- Suppression de versions non actuelles - cette action indique quand S3 peut supprimer définitivement des objets non actuels. L'action CLI est `NoncurrentVersionExpiration`.
- Suppression des marqueurs de suppression expirés - cette action supprime les marqueurs de suppression d'objet expirés.
Dans les compartiments avec gestion des versions, les objets avec des marqueurs de suppression deviennent les versions actuelles des objets. Les objets ne sont pas supprimés et aucune action ne peut être effectuée sur eux. Ces objets deviennent expirés lorsqu'aucune version n'est associée à ces objets. L'action CLI est `Expiration`.
- Suppression des téléchargements partitionnés incomplets : cette action définit une durée maximale (en jours) pendant laquelle vous souhaitez autoriser les téléchargements partitionnés à rester en cours. Après

quoi, ils sont supprimés. L'action CLI est `AbortIncompleteMultipartUpload`.

La procédure à suivre dépend de l'interface que vous utilisez. Avec ONTAP 9.13.1, vous devez utiliser l'interface de ligne de commandes. Depuis ONTAP 9.14.1, vous pouvez également utiliser System Manager.

Gérez les règles de gestion du cycle de vie avec l'interface de ligne de commande

À partir de ONTAP 9.13.1, vous pouvez utiliser l'interface de ligne de commandes ONTAP pour créer des règles de gestion du cycle de vie et faire expirer les objets de vos compartiments S3.

Avant de commencer

Pour l'interface de ligne de commandes, vous devez définir les champs requis pour chaque type d'action d'expiration lors de la création d'une règle de gestion du cycle de vie des compartiments. Ces champs peuvent être modifiés après la création initiale. Le tableau suivant affiche les champs uniques pour chaque type d'action.

Type d'action	Champs uniques
NonCurrentVersionExpiation	<ul style="list-style-type: none">• <code>-non-curr-days</code> - Nombre de jours après lesquels les versions non actuelles seront supprimées• <code>-new-non-curr-versions</code> - Nombre de dernières versions non actuelles à conserver
Expiration	<ul style="list-style-type: none">• <code>-obj-age-days</code> - Nombre de jours depuis la création, après lesquels la version actuelle des objets peut être supprimée• <code>-obj-exp-date</code> - Date précise à laquelle les objets doivent expirer• <code>-expired-obj-del-markers</code> - Nettoyage des marqueurs de suppression d'objet
AbortIncompleteMultipartUpload	<ul style="list-style-type: none">• <code>-after-initiation-days</code> - Nombre de jours d'initiation, après quoi le téléchargement peut être abandonné

Pour que la règle de gestion du cycle de vie des compartiments ne s'applique qu'à un sous-ensemble d'objets spécifique, les administrateurs doivent définir chaque filtre lors de la création de la règle. Si ces filtres ne sont pas définis lors de la création de la règle, la règle s'applique à tous les objets du compartiment.

Tous les filtres peuvent être modifiés après la création initiale *sauf* pour les éléments suivants : +

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

Étapes

1. Utilisez le `vserver object-store-server bucket lifecycle-management-rule create` commande contenant les champs requis pour votre type d'action d'expiration pour créer votre règle de gestion du cycle de vie des compartiments.

Exemple

La commande suivante crée une règle de gestion du cycle de vie des compartiments
NonCurrentVersionExpiration :

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

Exemple

La commande suivante crée une règle de gestion du cycle de vie des compartiments d'expiration :

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

Exemple

La commande suivante crée une règle de gestion du cycle de vie des compartiments
AbortIncompleteMultipartUpload :


```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```


Gérez les règles de gestion du cycle de vie avec System Manager

Depuis ONTAP 9.14.1, vous pouvez faire expirer les objets S3 à l'aide de System Manager. Vous pouvez ajouter, modifier et supprimer des règles de gestion du cycle de vie pour vos objets S3. En outre, vous pouvez importer une règle de cycle de vie créée pour un compartiment et l'utiliser pour les objets d'un autre compartiment. Vous pouvez désactiver une règle active et l'activer ultérieurement.

Ajoutez une règle de gestion du cycle de vie

1. Cliquez sur **stockage > compartiments**.
2. Sélectionnez le compartiment pour lequel vous souhaitez spécifier la règle d'expiration.


3. Cliquez sur l'  icône et sélectionnez **gérer les règles de cycle de vie**.
4. Cliquez sur **Ajouter > règle de cycle de vie**.
5. Sur la page Ajouter une règle de cycle de vie, ajoutez le nom de la règle.
6. Définissez la portée de la règle, que vous souhaitiez qu'elle s'applique à tous les objets du compartiment ou à des objets spécifiques. Si vous souhaitez spécifier des objets, ajoutez au moins l'un des critères de filtre suivants :
 - a. **Préfixe** : spécifiez le préfixe des noms de clés d'objet auxquels la règle doit s'appliquer. Il s'agit généralement du chemin ou du dossier de l'objet. Vous pouvez entrer un préfixe par règle. À moins qu'un préfixe valide ne soit fourni, la règle s'applique à tous les objets d'un compartiment.
 - b. **Balises** : spécifiez jusqu'à trois paires de clés et de valeurs (balises) pour les objets auxquels la règle doit s'appliquer. Seules les clés valides sont utilisées pour le filtrage. La valeur est facultative. Cependant, si vous ajoutez des valeurs, assurez-vous d'ajouter uniquement des valeurs valides pour les clés correspondantes.
 - c. **Taille** : vous pouvez limiter la portée entre la taille minimale et la taille maximale des objets. Vous pouvez entrer l'une ou l'autre des valeurs ou les deux. L'unité par défaut est MIB.
7. Spécifiez l'action :
 - a. **Expire la version actuelle des objets** : définissez une règle pour rendre tous les objets actuels définitivement indisponibles après un nombre de jours spécifique depuis leur création ou à une date spécifique. Cette option n'est pas disponible si l'option **Supprimer les marqueurs de suppression d'objet expiré** est sélectionnée.
 - b. **Supprimer définitivement les versions non actuelles** : Indiquez le nombre de jours après lesquels la version devient non actuelle, puis peut être supprimée, et le nombre de versions à conserver.
 - c. **Supprimer les marqueurs de suppression d'objets expirés** : sélectionnez cette action pour supprimer des objets avec des marqueurs de suppression expirés, c'est-à-dire supprimer des marqueurs sans objet courant associé.



Cette option devient indisponible lorsque vous sélectionnez l'option **expire la version actuelle des objets** qui supprime automatiquement tous les objets après la période de rétention. Cette option devient également indisponible lorsque des balises d'objet sont utilisées pour le filtrage.

 - d. **Supprimer les téléchargements partiels incomplets** : définit le nombre de jours après lesquels les téléchargements partiels incomplets doivent être supprimés. Si les téléchargements partitionnés en cours échouent dans la période de conservation spécifiée, vous pouvez supprimer les téléchargements partitionnés incomplets. Cette option devient indisponible lorsque des balises d'objet sont utilisées pour le filtrage.
 - e. Cliquez sur **Enregistrer**.

Importer une règle de cycle de vie


1. Cliquez sur **stockage > compartiments**.
2. Sélectionnez le compartiment pour lequel vous souhaitez importer la règle d'expiration.
3. Cliquez sur l'  icône et sélectionnez **gérer les règles de cycle de vie**.
4. Cliquez sur **Ajouter > Importer une règle**.
5. Sélectionnez le compartiment à partir duquel vous souhaitez importer la règle. Les règles de gestion du cycle de vie définies pour le compartiment sélectionné s'affichent.

6. Sélectionnez la règle à importer. Vous avez la possibilité de sélectionner une règle à la fois, la sélection par défaut étant la première règle.
7. Cliquez sur **Importer**.

Modifier, supprimer ou désactiver une règle

Vous pouvez uniquement modifier les actions de gestion du cycle de vie associées à la règle. Si la règle a été filtrée avec des balises d'objet, les options **Supprimer les marqueurs de suppression d'objet expirés** et **Supprimer les téléchargements partitionnés incomplets** ne sont pas disponibles.

Lorsque vous supprimez une règle, celle-ci ne s'applique plus aux objets précédemment associés.

1. Cliquez sur **stockage > compartiments**.
2. Sélectionnez le compartiment pour lequel vous souhaitez modifier, supprimer ou désactiver la règle de gestion du cycle de vie.
3. Cliquez sur l'  icône et sélectionnez **gérer les règles de cycle de vie**.
4. Sélectionnez la règle requise. Vous pouvez modifier et désactiver une règle à la fois. Vous pouvez supprimer plusieurs règles à la fois.
5. Sélectionnez **Modifier**, **Supprimer** ou **Désactiver** et terminez la procédure.

Créez un utilisateur S3

Créez un utilisateur S3 avec des autorisations spécifiques. Une autorisation utilisateur est requise sur tous les magasins d'objets ONTAP pour limiter la connectivité aux clients autorisés.

Avant de commencer.

Une VM de stockage compatible avec S3 doit déjà exister.

Description de la tâche

Un utilisateur S3 peut se voir accorder l'accès à n'importe quel compartiment d'une VM de stockage. Lorsque vous créez un utilisateur S3, une clé d'accès et une clé secrète sont également générées pour l'utilisateur. Ils doivent être partagés avec l'utilisateur avec le nom de domaine complet du magasin d'objets et du nom du compartiment.

Pour plus de sécurité, à partir de ONTAP 9.15.1, les clés d'accès et les clés secrètes s'affichent uniquement au moment de la création de l'utilisateur S3 et ne peuvent pas être affichées à nouveau. Si les clés sont perdues, de nouvelles clés doivent être générées en recréant l'utilisateur.

Vous pouvez accorder des autorisations d'accès spécifiques aux utilisateurs S3 dans une stratégie de compartiment ou une stratégie de serveur d'objets.



Lorsque vous créez un nouveau serveur de magasin d'objets, ONTAP crée un utilisateur root (UID 0), qui est un utilisateur privilégié ayant accès à tous les compartiments. Au lieu d'administrer ONTAP S3 en tant qu'utilisateur root, NetApp recommande la création d'un rôle d'utilisateur admin avec des privilèges spécifiques.

CLI

1. Création d'un utilisateur S3 :

```
vserver object-store-server user create -vserver svm_name -user user_name  
-comment [-comment text] -key-time-to-live time
```


- L'ajout d'un commentaire est facultatif.
- À partir de ONTAP 9.14.1, vous pouvez définir la période pendant laquelle la clé sera valide dans le `-key-time-to-live` paramètre. Vous pouvez ajouter la période de conservation dans ce format pour indiquer la période après laquelle la clé d'accès expire :
`P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
Par exemple, si vous souhaitez entrer une période de conservation d'un jour, de deux heures, de trois minutes et de quatre secondes, entrez la valeur comme `P1DT2H3M4S`. Sauf indication contraire, la clé est valide pour une durée indéterminée.

L'exemple ci-dessous crée un utilisateur avec un nom `sm_user1` Sur la machine virtuelle de stockage `vs0`, avec une période de conservation des clés d'une semaine.

```
vserver object-store-server user create -vserver vs0 -user sm_user1  
-key-time-to-live P1W
```

2. Veillez à enregistrer la clé d'accès et la clé secrète. Elles seront requises pour l'accès à partir des clients S3.

System Manager

1. Cliquez sur **stockage > machines virtuelles de stockage**. Sélectionnez la machine virtuelle de stockage à laquelle vous devez ajouter un utilisateur, sélectionnez **Paramètres**, puis cliquez  sous S3.
2. Pour ajouter un utilisateur, cliquez sur **utilisateurs > Ajouter**.
3. Entrez un nom pour l'utilisateur.
4. À partir de ONTAP 9.14.1, vous pouvez spécifier la période de conservation des clés d'accès créées pour l'utilisateur. Vous pouvez spécifier la période de conservation en jours, heures, minutes ou secondes, après laquelle les clés expirent automatiquement. Par défaut, la valeur est définie sur 0 cela indique que la clé est indéfiniment valide.
5. Cliquez sur **Enregistrer**. L'utilisateur est créé et une clé d'accès et une clé secrète sont générées pour l'utilisateur.
6. Téléchargez ou enregistrez la clé d'accès et la clé secrète. Elles seront requises pour l'accès à partir des clients S3.

Étapes suivantes

- [Création ou modification de groupes S3](#)

Création ou modification de groupes S3

Vous pouvez simplifier l'accès au compartiment en créant des groupes d'utilisateurs avec les autorisations d'accès appropriées.

Avant de commencer

Les utilisateurs S3 d'un SVM compatible avec S3 doivent déjà exister.

Description de la tâche

Les utilisateurs d'un groupe S3 peuvent accéder à n'importe quel compartiment d'une SVM, mais pas dans plusieurs SVM. Les autorisations d'accès aux groupes peuvent être configurées de deux façons :


- Au niveau du godet

Une fois que vous avez créé un groupe d'utilisateurs S3, vous spécifiez les autorisations de groupe dans les instructions de règles de compartiment et elles ne s'appliquent qu'à ce compartiment.

- Au niveau de la SVM

Après la création d'un groupe d'utilisateurs S3, vous spécifiez les noms des règles de serveur d'objets dans la définition de groupe. Ces stratégies déterminent les compartiments et l'accès des membres du groupe.

System Manager

1. Modifiez la machine virtuelle de stockage : cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur la machine virtuelle de stockage, cliquez sur **Paramètres**, puis sur  sous S3.
2. Ajouter un groupe : sélectionnez **groupes**, puis **Ajouter**.
3. Entrez un nom de groupe et sélectionnez-le dans une liste d'utilisateurs.
4. Vous pouvez sélectionner une stratégie de groupe existante ou en ajouter une maintenant, ou vous pouvez ajouter une ultérieurement.

CLI

1. Création d'un groupe S3 :

```
vserver object-store-server group create -vserver svm_name -name group_name  
-users user_name\(s\) [-policies policy_names] [-comment text\]
```

Le `-policies` l'option peut être omise dans les configurations avec un seul compartiment dans un magasin d'objets ; le nom du groupe peut être ajouté à la politique de compartiment.

Le `-policies` vous pouvez l'ajouter ultérieurement avec le `vserver object-store-server group modify` commande après la création de règles de serveur de stockage objet

Régénérer les clés et modifier leur période de conservation

Les clés d'accès et les clés secrètes sont automatiquement générées lors de la création de l'utilisateur pour l'activation de l'accès client S3. Vous pouvez régénérer des clés pour un utilisateur si une clé est périmée ou compromise.

Pour plus d'informations sur la génération de clés d'accès, reportez-vous à la section "[Créez un utilisateur S3](#)".



CLI

1. Régénérer les clés d'accès et les clés secrètes pour un utilisateur en exécutant `vserver object-store-server user regenerate-keys` commande.
2. Par défaut, les clés générées sont valides indéfiniment. À partir de 9.14.1, vous pouvez modifier leur période de conservation, après laquelle les clés expirent automatiquement. Vous pouvez ajouter la période de conservation au format suivant :
`P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
Par exemple, si vous souhaitez entrer une période de conservation d'un jour, de deux heures, de trois minutes et de quatre secondes, entrez la valeur comme `P1DT2H3M4S`.

```
vserver object-store-server user regenerate-keys -vserver svm_name  
-user user -key-time-to-live 0
```

3. Enregistrez les clés d'accès et les clés secrètes. Elles seront requises pour l'accès à partir des clients S3.

System Manager

1. Cliquez sur **Storage > Storage VM**, puis sélectionnez la VM de stockage.
2. Dans l'onglet **Paramètres**, cliquez sur  la mosaïque **S3**.
3. Dans l'onglet **Users**, vérifiez qu'il n'y a pas de clé d'accès ou que la clé a expiré pour l'utilisateur.
4. Si vous devez régénérer la clé, cliquez sur  en regard de l'utilisateur, puis cliquez sur **régénérer la clé**.
5. Par défaut, les clés générées sont valides pour une durée indéterminée. À partir de 9.14.1, vous pouvez modifier leur période de conservation, après laquelle les clés expirent automatiquement. Entrez la période de conservation en jours, heures, minutes ou secondes.
6. Cliquez sur **Enregistrer**. La clé est régénérée. Toute modification de la période de conservation des clés prend effet immédiatement.
7. Téléchargez ou enregistrez la clé d'accès et la clé secrète. Elles seront requises pour l'accès à partir des clients S3.

Créer ou modifier des instructions de stratégie d'accès

À propos des règles des serveurs de compartiment et de magasin d'objets

L'accès des utilisateurs et des groupes aux ressources S3 est contrôlé par des règles de compartiment et de serveur de magasin d'objets. Si vous avez un petit nombre d'utilisateurs ou de groupes, le contrôle de l'accès au niveau du compartiment est probablement suffisant, mais si vous avez de nombreux utilisateurs et groupes, il est plus facile de contrôler l'accès au niveau du serveur du magasin d'objets.

Modifier une règle de compartiment

Vous pouvez ajouter des règles d'accès à la stratégie de compartiment par défaut. L'étendue de son contrôle d'accès est le godet contenant, il est donc le plus approprié

lorsqu'il y a un seul godet.

Avant de commencer

Une VM de stockage compatible avec S3 contenant un serveur S3 et un compartiment doit déjà exister.

Vous devez avoir déjà créé des utilisateurs ou des groupes avant d'accorder des autorisations.

Description de la tâche

Vous pouvez ajouter de nouvelles instructions pour les nouveaux utilisateurs et groupes ou modifier les attributs des instructions existantes. Pour plus d'options, reportez-vous à la section `vserver object-store-server bucket policy` pages de manuel.

Des autorisations d'utilisateur et de groupe peuvent être accordées lors de la création du compartiment ou lors de la création de ce dernier. Vous pouvez également modifier la capacité des compartiments et l'affectation des groupes de règles de QoS.

Depuis ONTAP 9.9.1, si vous prévoyez de prendre en charge la fonctionnalité de balisage d'objets du client AWS avec le serveur ONTAP S3, les actions sont les suivantes `GetObjectTagging`, `PutObjectTagging`, et `DeleteObjectTagging` doivent être autorisées à l'aide des règles de compartiment ou de groupe.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

Étapes

1. Modifiez le compartiment : cliquez sur **stockage > godets**, cliquez sur le compartiment souhaité, puis sur **Modifier**.

Lors de l'ajout ou de la modification d'autorisations, vous pouvez spécifier les paramètres suivants :

- **Principal** : l'utilisateur ou le groupe auquel l'accès est accordé.
- **Effet** : autorise ou refuse l'accès à un utilisateur ou à un groupe.
- **Actions** : actions autorisées dans le godet pour un utilisateur ou un groupe donné.
- **Ressources** : chemins et noms des objets dans le compartiment pour lesquels l'accès est accordé ou refusé.

Les valeurs par défaut **bucketname** et **bucketname/*** permettent d'accéder à tous les objets du compartiment. Vous pouvez également accorder l'accès à des objets uniques, par exemple **bucketname/*_readme.txt**.

- **Conditions** (facultatif) : expressions évaluées lors de la tentative d'accès. Par exemple, vous pouvez spécifier une liste d'adresses IP pour lesquelles l'accès sera autorisé ou refusé.



À partir de ONTAP 9.14.1, vous pouvez spécifier des variables pour la stratégie de compartiment dans le champ **Resources**. Ces variables sont des espaces réservés qui sont remplacés par des valeurs contextuelles lors de l'évaluation de la règle. Par exemple, si `${aws:username}` est spécifié comme variable pour une stratégie, puis cette variable est remplacée par le nom d'utilisateur du contexte de la demande et l'action de stratégie peut être exécutée comme configuré pour cet utilisateur.

CLI

Étapes

1. Ajouter une déclaration à une politique de compartiment :

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

Les paramètres suivants définissent les autorisations d'accès :

-effect	La déclaration peut autoriser ou refuser l'accès
-action	Vous pouvez spécifier * pour faire référence à toutes les actions ou à une liste d'une ou plusieurs des actions suivantes : GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, et ListMultipartUploadParts.

-principal	<p>Liste d'un ou plusieurs utilisateurs ou groupes S3.</p> <ul style="list-style-type: none"> • Vous pouvez spécifier un maximum de 10 utilisateurs ou groupes. • Si un groupe S3 est spécifié, il doit être dans le formulaire <code>group/group_name</code>. • * peut être spécifié pour signifier l'accès public, c'est-à-dire l'accès sans clé d'accès et clé secrète. • Si aucun principal n'est spécifié, l'accès est accordé à tous les utilisateurs S3 de la VM de stockage.
-resource	<p>Le compartiment et tout objet qu'il contient. Les caractères génériques * et ? peut être utilisé pour former une expression régulière pour spécifier une ressource. Pour une ressource, vous pouvez spécifier des variables dans une règle. Il s'agit de variables de stratégie qui sont remplacées par les valeurs contextuelles lors de l'évaluation de la règle.</p>

Vous pouvez éventuellement spécifier une chaîne de texte sous forme de commentaire avec l' `-sid` option.

Exemples

L'exemple suivant crée une instruction de stratégie de compartiment de serveur de magasin d'objets pour la machine virtuelle de stockage `svm1.example.com` et le `bucket1` qui spécifie l'accès autorisé à un dossier `readme` pour l'utilisateur du serveur de magasin d'objets `user1`.

```
cluster1::> vsserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

L'exemple suivant crée une instruction de stratégie de compartiment de serveur de magasin d'objets pour la VM de stockage `svm1.example.com` et `bucket1` qui spécifie l'accès autorisé à tous les objets pour le groupe de serveurs de magasin d'objets `groupe1`.

```
cluster1::> vsserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

Depuis ONTAP 9.14.1, vous pouvez spécifier des variables pour une règle de compartiment. L'exemple suivant crée une instruction de stratégie de compartiment de serveur pour la VM de stockage `svm1` et `bucket1`, et spécifie `${aws:username}` comme variable pour une ressource de stratégie. Lorsque la stratégie est évaluée, la variable de stratégie est remplacée par le nom d'utilisateur du contexte de demande et l'action de stratégie peut être exécutée comme configuré pour cet utilisateur. Par exemple, lorsque l'instruction de règle suivante est évaluée, `${aws:username}` Est remplacé par l'utilisateur effectuant l'opération S3. Si un utilisateur `user1` exécute l'opération, à laquelle l'utilisateur a accès

```
bucket1 comme bucket1/user1/*.
```

```
cluster1::> object-store-server bucket policy statement create -vserver  
svml -bucket bucket1 -effect allow -action * -principal - -resource  
bucket1,bucket1/${aws:username}/*##
```

Créer ou modifier une stratégie de serveur de magasin d'objets

Vous pouvez créer des règles qui s'appliquent à un ou plusieurs compartiments dans un magasin d'objets. Les stratégies de serveur de magasin d'objets peuvent être associées à des groupes d'utilisateurs, ce qui simplifie la gestion de l'accès aux ressources dans plusieurs compartiments.

Avant de commencer

Un SVM compatible S3 contenant un serveur S3 et un compartiment doivent déjà exister.

Description de la tâche

Vous pouvez activer les politiques d'accès au niveau du SVM en spécifiant une règle par défaut ou personnalisée dans un groupe de serveurs de stockage objet. Les stratégies ne prennent effet qu'après avoir été spécifiées dans la définition de groupe.



Lorsque vous utilisez des stratégies de serveur de stockage objet, vous spécifiez les entités (c'est-à-dire les utilisateurs et les groupes) dans la définition de groupe, et non dans la stratégie elle-même.

Il existe trois règles par défaut en lecture seule pour l'accès aux ressources ONTAP S3 :

- Accès complet
- Aucun accès
- ReadOnlyAccess

Vous pouvez également créer de nouvelles stratégies personnalisées, ajouter de nouvelles instructions pour les nouveaux utilisateurs et groupes, ou modifier les attributs des instructions existantes. Pour plus d'options, reportez-vous à la section `vserver object-store-server policy` "[référence de commande](#)".


Depuis ONTAP 9.9.1, si vous prévoyez de prendre en charge la fonctionnalité de balisage d'objets du client AWS avec le serveur ONTAP S3, les actions sont les suivantes `GetObjectTagging`, `PutObjectTagging`, et `DeleteObjectTagging` doivent être autorisées à l'aide des règles de compartiment ou de groupe.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

Utilisez System Manager pour créer ou modifier une stratégie de serveur de magasin d'objets

Étapes

1. Modifiez la machine virtuelle de stockage : cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur la machine virtuelle de stockage, cliquez sur **Paramètres**, puis sur  sous S3.
2. Ajouter un utilisateur : cliquez sur **Policies**, puis sur **Ajouter**.
 - a. Entrez un nom de stratégie et sélectionnez-le dans une liste de groupes.
 - b. Sélectionnez une stratégie par défaut existante ou ajoutez-en une nouvelle.

Lors de l'ajout ou de la modification d'une stratégie de groupe, vous pouvez spécifier les paramètres suivants :

- Groupe : groupes auxquels l'accès est accordé.
- Effet : autorise ou refuse l'accès à un ou plusieurs groupes.
- Actions : actions autorisées dans un ou plusieurs compartiments pour un groupe donné.
- Ressources : chemins et noms d'objets dans un ou plusieurs compartiments pour lesquels l'accès est accordé ou refusé.

Par exemple :

- * Permet l'accès à tous les compartiments de la machine virtuelle de stockage.
- **bucketname** et **bucketname/*** permettent d'accéder à tous les objets d'un compartiment spécifique.
- **bucketname/readme.txt** donne accès à un objet dans un compartiment spécifique.

- c. Si vous le souhaitez, ajoutez des instructions aux stratégies existantes.

CLI

Utilisez l'interface de ligne de commande pour créer ou modifier une stratégie de serveur de stockage d'objets

Étapes

1. Créer une stratégie de serveur de stockage objet :

```
vserver object-store-server policy create -vserver svm_name -policy policy_name [-comment text]
```

2. Créer une instruction pour la règle :

```
vserver object-store-server policy statement create -vserver svm_name -policy policy_name -effect {allow|deny} -action object_store_actions -resource object_store_resources [-sid text]
```

Les paramètres suivants définissent les autorisations d'accès :

-effect	La déclaration peut autoriser ou refuser l'accès
---------	--

<code>-action</code>	Vous pouvez spécifier * pour faire référence à toutes les actions ou à une liste d'une ou plusieurs des actions suivantes : <code>GetObject</code> , <code>PutObject</code> , <code>DeleteObject</code> , <code>ListBucket</code> , <code>GetBucketAcl</code> , <code>GetObjectAcl</code> , <code>ListAllMyBuckets</code> , <code>ListBucketMultipartUploads</code> , et <code>ListMultipartUploadParts</code> .
<code>-resource</code>	Le compartiment et tout objet qu'il contient. Les caractères génériques * et ? peut être utilisé pour former une expression régulière pour spécifier une ressource.

Vous pouvez éventuellement spécifier une chaîne de texte sous forme de commentaire avec l' `-sid` option.

Par défaut, de nouvelles instructions sont ajoutées à la fin de la liste des instructions, qui sont traitées dans l'ordre. Lorsque vous ajoutez ou modifiez des instructions ultérieurement, vous avez la possibilité de modifier les instructions `-index` paramètre permettant de modifier l'ordre de traitement.

Configurez l'accès S3 pour les services d'annuaire externes

Depuis ONTAP 9.14.1, les services pour les répertoires externes ont été intégrés au stockage objet ONTAP S3. Cette intégration simplifie la gestion des utilisateurs et des accès via des services d'annuaire externes.

Vous pouvez fournir des groupes d'utilisateurs appartenant à un service d'annuaire externe ayant accès à votre environnement de stockage objet ONTAP. Le protocole LDAP (Lightweight Directory Access Protocol) est une interface permettant de communiquer avec des services d'annuaire, tels qu'Active Directory, qui fournit une base de données et des services de gestion des identités et des accès (IAM). Pour y accéder, vous devez configurer les groupes LDAP dans votre environnement ONTAP S3. Une fois l'accès configuré, les membres du groupe disposent des autorisations nécessaires pour les compartiments ONTAP S3. Pour plus d'informations sur LDAP, reportez-vous à la section "[Présentation de l'utilisation de LDAP](#)".

Vous pouvez également configurer des groupes d'utilisateurs Active Directory en mode de liaison rapide, de sorte que les informations d'identification des utilisateurs puissent être validées et que les applications S3 tierces et open source puissent être authentifiées via des connexions LDAP.

Avant de commencer

Avant de configurer les groupes LDAP et d'activer le mode de liaison rapide pour l'accès aux groupes, vérifiez les points suivants :

1. Une VM de stockage compatible S3 contenant un serveur S3 a été créée. Voir "[Création d'un SVM pour S3](#)".
2. Un compartiment a été créé dans cette VM de stockage. Voir "[Créer un compartiment](#)".
3. DNS est configuré sur la machine virtuelle de stockage. Voir "[Configurez les services DNS](#)".
4. Un certificat d'autorité de certification racine (CA) auto-signé du serveur LDAP est installé sur la machine virtuelle de stockage. Voir "[Installer le certificat d'autorité de certification racine auto-signé sur le SVM](#)".

5. Un client LDAP est configuré avec TLS activé sur le SVM. Voir "[Créez une configuration client LDAP](#)" et "[Associez la configuration client LDAP aux SVM pour plus d'informations](#)".

Configurez l'accès S3 pour les services d'annuaire externes

1. Préciser LDAP comme *NAME service database* du SVM pour le groupe et password pour LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Pour plus d'informations sur cette commande, reportez-vous au "[vserver services name-service ns-switch modify](#)" commande.

2. Créez une instruction de stratégie de compartiment de magasin d'objets avec principal Sélectionnez le groupe LDAP auquel vous souhaitez accorder l'accès :

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

Exemple : l'exemple suivant crée une instruction de politique de compartiment pour buck1. La stratégie autorise l'accès au groupe LDAP group1 à la ressource (compartiment et ses objets) buck1.

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. Vérifiez qu'un utilisateur du groupe LDAP group1 Est capable d'effectuer des opérations S3 à partir du client S3.

Utilisez le mode de liaison rapide LDAP pour l'authentification

1. Préciser LDAP comme *NAME service database* du SVM pour le groupe et password pour LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Pour plus d'informations sur cette commande, reportez-vous au "[vserver services name-service ns-switch modify](#)" commande.

2. Assurez-vous qu'un utilisateur LDAP accédant au compartiment S3 dispose des autorisations définies dans les règles de compartiment. Pour plus d'informations, voir "[Modifier une règle de compartiment](#)".
3. Vérifiez qu'un utilisateur du groupe LDAP peut effectuer les opérations suivantes :
 - a. Configurez la clé d'accès sur le client S3 dans le format suivant :
`"NTAPFASTBIND" + base64-encode(user-name:password)`
Exemple : `"NTAPFASTBIND" + base64-encode(ldapuser:password)`, qui résulte en
`NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`



Le client S3 peut vous inviter à saisir une clé secrète. En l'absence d'une clé secrète, vous pouvez saisir un mot de passe d'au moins 16 caractères.

- b. Effectuez des opérations S3 de base à partir du client S3 pour lequel l'utilisateur dispose des autorisations nécessaires.

Authentification des ressources pour Active Directory pour les utilisateurs sans UID ni GID

Si le groupe nasgroup spécifié dans l'instruction bucket-policy ou si les utilisateurs qui font partie du groupe nasgroup n'ont pas d'UID et de GID définis, les recherches échoueront lorsque ces attributs ne sont pas trouvés.

Pour éviter les échecs de recherche, NetApp recommande d'utiliser des domaines approuvés pour l'autorisation des ressources au format UPN : nasgroup/group@trusted_domain.com

Pour générer les clés d'accès utilisateur pour les utilisateurs de domaine de confiance lorsque la liaison rapide LDAP n'est pas utilisée

Utilisez le `s3/services/<svm_uuid>/users` noeud final avec les utilisateurs spécifiés au format UPN.
Exemple :

```
$curl -siku FQDN\\user:<user_name> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn] (https://github.com/fqdn)>,"<key_time_to_live>":"PT6H3M"}'
```

Activez les utilisateurs LDAP ou du domaine pour générer leurs propres clés d'accès S3

À partir de ONTAP 9.14.1, en tant qu'administrateur ONTAP, vous pouvez créer des rôles personnalisés et les attribuer à des groupes locaux ou de domaine ou à des groupes LDAP (Lightweight Directory Access Protocol), de sorte que les utilisateurs appartenant à ces groupes puissent générer leur propre accès et leurs propres clés secrètes pour l'accès client S3.

Vous devez effectuer quelques étapes de configuration sur votre machine virtuelle de stockage, afin que le rôle personnalisé puisse être créé et attribué à l'utilisateur qui appelle l'API pour la génération de la clé d'accès.

Avant de commencer

Vérifiez les points suivants :

1. Une VM de stockage compatible S3 contenant un serveur S3 a été créée. Voir ["Création d'un SVM pour S3"](#).
2. Un compartiment a été créé dans cette VM de stockage. Voir ["Créer un compartiment"](#).
3. DNS est configuré sur la machine virtuelle de stockage. Voir ["Configurez les services DNS"](#).
4. Un certificat d'autorité de certification racine (CA) auto-signé du serveur LDAP est installé sur la machine virtuelle de stockage. Voir ["Installer le certificat d'autorité de certification racine auto-signé sur le SVM"](#).
5. Un client LDAP est configuré avec TLS activé sur la VM de stockage. Voir ["Créez une configuration client LDAP"](#) et .
6. Associer la configuration client au Vserver. Voir ["Associer la configuration client LDAP aux SVM"](#) et ["création du ldap nom-service des services vserver"](#).
7. Si vous utilisez une VM de stockage de données, créez une interface réseau de gestion (LIF) et sur la VM, ainsi qu'une politique de service pour la LIF. Voir la ["création d'interface réseau"](#) et ["création de la stratégie de service de l'interface réseau"](#) commandes.

Configurer les utilisateurs pour la génération de clés d'accès

1. Spécifiez LDAP comme *name service database* de la machine virtuelle de stockage pour le groupe et le mot de passe pour LDAP :

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Pour plus d'informations sur cette commande, reportez-vous au ["vserver services name-service ns-switch modify"](#) commande.

2. Créez un rôle personnalisé en accédant au terminal de l'API REST de l'utilisateur S3 :
`security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`
Dans cet exemple, le `s3-role` Le rôle est généré pour les utilisateurs de la VM de stockage `svm-1`, auquel tous les droits d'accès, lecture, création et mise à jour sont accordés.

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

Pour plus d'informations sur cette commande, reportez-vous au ["sécurité login rest-role créer"](#) commande.

3. Créez un groupe d'utilisateurs LDAP avec la commande Security login et ajoutez le nouveau rôle personnalisé pour accéder au point final de l'API REST de l'utilisateur S3. Pour plus d'informations sur cette commande, reportez-vous au ["création d'une connexion de sécurité"](#) commande.

```
security login create -user-or-group-name <ldap-group-name> -application  
http -authentication-method nsswitch -role <custom-role-name> -is-ns  
-switch-group yes
```

Dans cet exemple, le groupe LDAP `ldap-group-1` est créé dans `svm-1`, et le rôle personnalisé `s3role` est ajouté pour accéder au noeud final de l'API, ainsi que pour activer l'accès LDAP en mode de liaison rapide.

```
security login create -user-or-group-name ldap-group-1 -application http  
-authentication-method nsswitch -role s3role -is-ns-switch-group yes  
-second-authentication-method none -vserver svm-1 -is-ldap-fastbind yes
```

Pour plus d'informations, voir ["Utilisez LDAP FAST bind pour l'authentification nsswitch"](#).

L'ajout du rôle personnalisé au domaine ou au groupe LDAP permet aux utilisateurs de ce groupe d'avoir un accès limité à `ONTAP /api/protocols/s3/services/{svm.uuid}/users` point final. En appelant l'API, les utilisateurs du domaine ou du groupe LDAP peuvent générer leurs propres clés d'accès et secrètes pour accéder au client S3. Ils peuvent générer les clés pour eux-mêmes et non pour les autres utilisateurs.

En tant qu'utilisateur S3 ou LDAP, générez vos propres clés d'accès

À partir de ONTAP 9.14.1, vous pouvez générer vos propres clés d'accès et vos clés secrètes pour accéder aux clients S3, si votre administrateur vous a accordé le rôle de génération de vos propres clés. Vous ne pouvez générer les clés que vous-même à l'aide du terminal d'API REST ONTAP suivant.

Méthode HTTP et noeud final

Cet appel d'API REST utilise la méthode et le point de terminaison suivants. Pour plus d'informations sur les autres méthodes de ce noeud final, reportez-vous à la référence ["Documentation de l'API"](#).

Méthode HTTP	Chemin
POST	<code>/api/protocoles/s3/services/{svm.uuid}/utilisateurs</code>

Exemple de boucle

```
curl  
--request POST \  
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "  
\  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"  
--data '{"name": "_name_"}'
```


Exemple de sortie JSON

```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```

Activez l'accès client au stockage objet S3

Activation de l'accès ONTAP S3 pour le Tiering FabricPool distant

Pour qu'ONTAP S3 puisse être utilisé comme Tier de capacité FabricPool distante (cloud), l'administrateur ONTAP S3 doit fournir des informations sur la configuration du serveur S3 à l'administrateur du cluster ONTAP distant.

Description de la tâche

Pour configurer des tiers cloud FabricPool, vous devez disposer des informations suivantes sur le serveur S3 :

- Nom du serveur (FQDN)
- nom du compartiment
- Certificat CA
- touche d'accès
- mot de passe (clé d'accès secrète)

En outre, la configuration réseau suivante est requise :

- Il doit y avoir une entrée pour le nom d'hôte du serveur ONTAP S3 distant dans le serveur DNS configuré pour le SVM d'administration, notamment le nom de domaine complet du serveur S3 et les adresses IP sur les LIF.

- Les LIFs intercluster doivent être configurées sur le cluster local, bien que le peering de cluster n'est pas nécessaire.

Consultez la documentation d'FabricPool sur la configuration d'ONTAP S3 en tant que Tier cloud.

["Gestion des niveaux de stockage à l'aide de FabricPool"](#)

Activez l'accès ONTAP S3 pour le Tiering FabricPool local

Pour qu'ONTAP S3 puisse être utilisé comme Tier de capacité FabricPool locale, vous devez définir un magasin d'objets en fonction du compartiment que vous avez créé, puis relier le magasin d'objets à un agrégat de Tier de performance pour créer une FabricPool.

Avant de commencer

Vous devez disposer du nom du serveur ONTAP S3 et d'un nom de compartiment, et le serveur S3 doit avoir été créé à l'aide des LIFs de cluster (avec le `-vserver Cluster` paramètre).

Description de la tâche

La configuration du magasin d'objets contient des informations sur le Tier de capacité locale, notamment les noms de compartiment et de serveur S3 et les exigences d'authentification.

Une fois créée, une configuration de magasin d'objets ne doit pas être associée à un autre magasin d'objets ou compartiment. Vous pouvez créer plusieurs compartiments pour les tiers locaux, mais il n'est pas possible de créer plusieurs magasins d'objets dans un seul compartiment.

Aucune licence FabricPool n'est requise pour un niveau de capacité locale.

Étapes

1. Créez le magasin d'objets pour le Tier de capacité locale :

```
storage aggregate object-store config create -object-store-name store_name
-ipospace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
-name bucket_name -access-key access_key -secret-password password
```

- Le `-container-name` Est le compartiment S3 que vous avez créé.
- Le `-access-key` Paramètre autorise les requêtes vers le serveur ONTAP S3.
- Le `-secret-password` Le paramètre (clé d'accès secrète) authentifie les requêtes vers le serveur ONTAP S3.
- Vous pouvez définir le `-is-certificate-validation-enabled` paramètre à `false` Pour désactiver la vérification du certificat pour ONTAP S3.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyLocalObjStore -ipospace Cluster -provider-type
ONTAP_S3 -server s3.example.com
-container-name bucket1 -access-key myS3key -secret-password myS3pass
```

2. Afficher et vérifier les informations de configuration du magasin d'objets :

```
storage aggregate object-store config show
```

3. Facultatif : "Déterminez la quantité de données inactives d'un volume grâce au reporting des données inactives".

Vous savez combien de données inactives d'un volume peut vous aider à choisir l'agrégat à utiliser pour le Tiering FabricPool local.

4. Attacher le magasin d'objets à un agrégat :

```
storage aggregate object-store attach -aggregate aggr_name -object-store-name store_name
```

Vous pouvez utiliser le `allow-flexgroup true` Possibilité de connecter des agrégats contenant des composants de volume FlexGroup

```
cluster1::> storage aggregate object-store attach  
-aggregate aggr1 -object-store-name MyLocalObjStore
```

5. Afficher les informations du magasin d'objets et vérifier que le magasin d'objets attaché est disponible :

```
storage aggregate object-store show
```

```
cluster1::> storage aggregate object-store show
```

Aggregate	Object Store Name	Availability State
-----	-----	-----
aggr1	MyLocalObjStore	available

Activation de l'accès client à partir d'une application S3

Pour que les applications client S3 puissent accéder au serveur ONTAP S3, l'administrateur ONTAP S3 doit fournir des informations de configuration à l'utilisateur S3.

Avant de commencer

L'application client S3 doit être capable d'authentifier auprès du serveur ONTAP S3 à l'aide des versions de signature AWS suivantes :

- Signature version 4, ONTAP 9.8 et ultérieure
- Signature version 2, ONTAP 9.11.1 et ultérieure

Les autres versions de signatures ne sont pas prises en charge par ONTAP S3.

L'administrateur ONTAP S3 doit avoir créé des utilisateurs S3 et leur accorder des autorisations d'accès, en tant qu'utilisateurs individuels ou en tant que membre de groupe, dans la stratégie de compartiment ou la stratégie de serveur de stockage objet.

L'application du client S3 doit être capable de résoudre le nom du serveur ONTAP S3, ce qui requiert que l'administrateur ONTAP S3 fournisse le nom du serveur S3 (FQDN) et des adresses IP pour les LIF du serveur

S3.

Description de la tâche

Pour accéder à un compartiment ONTAP S3, un utilisateur de l'application client S3 saisit les informations fournies par l'administrateur ONTAP S3.

Depuis la version ONTAP 9.9.1, le serveur ONTAP S3 prend en charge les fonctionnalités de client AWS suivantes :

- métadonnées d'objet définies par l'utilisateur

Un ensemble de paires clé-valeur peut être attribué aux objets en tant que métadonnées lors de leur création à l'aide DE PUT (ou POST). Lorsqu'une opération GET/HEAD est exécutée sur l'objet, les métadonnées définies par l'utilisateur sont renvoyées avec les métadonnées du système.

- balisage d'objets

Un ensemble distinct de paires clé-valeur peut être attribué en tant que balises pour classer les objets. Contrairement aux métadonnées, les balises sont créées et lues avec les API REST indépendamment de l'objet. Elles sont implémentées lors de la création d'objets ou à tout moment après.



Pour permettre aux clients d'obtenir et de mettre des informations de marquage, les actions `GetObjectTagging`, `PutObjectTagging`, et `DeleteObjectTagging` doivent être autorisées à l'aide des règles de compartiment ou de groupe.

Pour plus d'informations, consultez la documentation AWS S3.

Étapes

1. Authentifiez l'application client S3 avec le serveur ONTAP S3 en saisissant le nom du serveur S3 et le certificat de l'autorité de certification.
2. Authentifier un utilisateur sur l'application client S3 en saisissant les informations suivantes :
 - Nom du serveur S3 (FQDN) et nom du compartiment
 - clé d'accès et clé secrète de l'utilisateur

Définitions des services de stockage

ONTAP inclut des services de stockage prédéfinis mappés sur les facteurs de performance minimaux correspondants.

L'ensemble réel de services de stockage disponibles dans un cluster ou un SVM est déterminé par le type de stockage qui constitue un agrégat dans la SVM.

Le tableau ci-dessous montre comment les facteurs de performance minimale sont mappés aux services de stockage prédéfinis :

Service de stockage	IOPS attendues (SLA)	IOPS en pic (SLO)	Nombre minimal d'IOPS pour le volume	Latence estimée	Les IOPS attendues sont-elles appliquées ?
valeur	128 par To	512 par To	75	17 ms.	Sur AFF: Oui Sinon : non
performances	2048 par To	4096 par To	500	2 ms.	Oui.
extrême	6144 par To	12288 par To	1000	1 ms.	Oui.

Le tableau ci-dessous définit le niveau de service de stockage disponible pour chaque type de support ou nœud :

Support ou nœud	Niveau de service du stockage disponible
Disque	valeur
Disque de machine virtuelle	valeur
LUN FlexArray	valeur
Hybride	valeur
Flash à capacité optimisée	valeur
Disque SSD (Solid-State Drive) - non AFF	valeur
Performance optimisée Flash - SSD (AFF)	extreme, performance, value

Protection des compartiments avec SnapMirror S3

Présentation de SnapMirror S3

Depuis ONTAP 9.10.1, vous pouvez protéger les compartiments dans des magasins d'objets ONTAP S3 à l'aide de la fonctionnalité de mise en miroir et de sauvegarde SnapMirror. À la différence d'SnapMirror standard, SnapMirror S3 permet la mise en miroir et les sauvegardes vers des destinations non-NetApp telles qu'AWS S3.

SnapMirror S3 prend en charge les miroirs actifs et les tiers de sauvegarde à partir de compartiments ONTAP S3 vers les destinations suivantes :

Cible	Prend en charge les miroirs actifs et le basculement ?	Prend en charge la sauvegarde et la restauration ?
ONTAP S3 <ul style="list-style-type: none"> • Compartiments dans le même SVM • Compartiments dans différents SVM sur le même cluster • Compartiments dans les SVM sur différents clusters 	Oui.	Oui.
StorageGRID	Non	Oui.
AWS S3	Non	Oui.
Cloud Volumes ONTAP pour Azure	Oui.	Oui.
Cloud Volumes ONTAP pour AWS	Oui.	Oui.
Cloud Volumes ONTAP pour Google Cloud	Oui.	Oui.

Vous pouvez protéger les compartiments existants sur les serveurs ONTAP S3 ou créer immédiatement des compartiments avec la protection des données activée.

Configuration requise pour SnapMirror S3

- Version ONTAP

ONTAP 9.10.1 ou version ultérieure doit s'exécuter sur les clusters source et cible.

- Licences

Les licences suivantes sont disponibles dans le ["ONTAP One"](#) Une suite logicielle est requise sur les systèmes source et de destination ONTAP pour permettre l'accès aux éléments suivants :

- Protocole et stockage ONTAP S3
- SnapMirror S3 pour cibler d'autres cibles de magasin d'objets NetApp (ONTAP S3, StorageGRID et Cloud Volumes ONTAP)
- SnapMirror S3 pour cibler des magasins d'objets tiers, y compris AWS S3 (disponible dans le ["Pack de compatibilité ONTAP One"](#))

- ONTAP S3

- Les serveurs ONTAP S3 doivent exécuter les SVM source et destination.
- Il est recommandé, mais pas nécessaire, que des certificats CA pour l'accès TLS soient installés sur des systèmes hébergeant des serveurs S3.
 - Les certificats d'autorité de certification utilisés pour signer les certificats des serveurs S3 doivent être installés sur la machine virtuelle de stockage d'administration des clusters qui hébergent des serveurs S3.
 - Vous pouvez utiliser un certificat d'autorité de certification auto-signé ou un certificat signé par un fournisseur d'autorité de certification externe.
 - Si les VM de stockage source ou cible ne sont pas à l'écoute via HTTPS, il n'est pas nécessaire

d'installer des certificats CA.

- Peering (pour les cibles ONTAP S3)
 - Les LIFs intercluster doivent être configurées (pour les cibles ONTAP distantes) et les LIFs intercluster du cluster source et destination peuvent se connecter aux LIFs de données du serveur S3 source et destination.
 - Les clusters source et de destination sont associés (pour les cibles ONTAP distantes).
 - Les machines virtuelles de stockage source et de destination sont peering (pour toutes les cibles ONTAP).
- Règle SnapMirror
 - Toutes les relations SnapMirror S3 requièrent une règle SnapMirror spécifique à S3, mais vous pouvez utiliser la même règle pour plusieurs relations.
 - Vous pouvez créer votre propre stratégie ou accepter la stratégie par défaut **continu**, qui comprend les valeurs suivantes :
 - Accélérateur (limite supérieure sur le débit/bande passante) - illimité.
 - Délai pour l'objectif de point de restauration : 1 heure (3600 secondes).



Notez que lorsque deux compartiments S3 se trouvent dans une relation SnapMirror, si des règles de cycle de vie sont configurées de façon à ce que la version actuelle d'un objet expire (est supprimée), la même action est répliquée dans le compartiment partenaire. C'est vrai même si le compartiment partenaire est en lecture seule ou passif.

- Clés d'utilisateur root les clés d'accès utilisateur root de Storage VM sont requises pour les relations SnapMirror S3 ; ONTAP ne les attribue pas par défaut. Lors de la première création d'une relation SnapMirror S3, vous devez vérifier que les clés existent sur les machines virtuelles de stockage source et de destination et les régénérer si ce n'est pas le cas. Si vous devez les régénérer, vous devez vous assurer que tous les clients et toutes les configurations du magasin d'objets SnapMirror utilisant la paire de clés Access et secret sont mis à jour avec les nouvelles clés.

Pour plus d'informations sur la configuration d'un serveur S3, consultez les rubriques suivantes :

- ["Activez un serveur S3 sur une machine virtuelle de stockage"](#)
- ["À propos du processus de configuration S3"](#)

Pour plus d'informations sur le cluster et le peering de machine virtuelle de stockage, consultez la rubrique suivante :

- ["Préparation à la mise en miroir et à l'archivage \(System Manager, étapes 1 à 6\)"](#)
- ["Cluster et SVM peering \(interface de ligne de commandes\)"](#)

Relations SnapMirror prises en charge

SnapMirror S3 prend en charge les relations « Fan-Out » et « Cascade ». Pour une vue d'ensemble, voir ["Déploiements de la protection des données en cascade et « Fan-Out »"](#).

SnapMirror S3 ne prend pas en charge les déploiements « Fan-In » (relations de protection des données entre plusieurs compartiments source et un compartiment de destination unique). SnapMirror S3 peut prendre en charge plusieurs miroirs de compartiments entre plusieurs clusters vers un seul cluster secondaire, mais chaque compartiment source doit avoir son propre compartiment de destination sur le cluster secondaire.

Contrôle de l'accès aux compartiments S3

Lorsque vous créez de nouveaux compartiments, vous pouvez contrôler l'accès en créant des utilisateurs et des groupes. Pour plus d'informations, consultez les rubriques suivantes :

- ["Ajout d'utilisateurs et de groupes S3 \(System Manager\)"](#)
- ["Création d'un utilisateur S3 \(interface de ligne de commandes\)"](#)
- ["Création ou modification de groupes S3 \(interface de ligne de commandes\)"](#)

Protection en miroir et sauvegarde sur un cluster distant

Création d'une relation de miroir pour un nouveau compartiment (cluster distant)

Lorsque vous créez de nouveaux compartiments S3, vous pouvez les protéger immédiatement vers une destination SnapMirror S3 sur un cluster distant.

Description de la tâche

Vous devez effectuer des tâches sur les systèmes source et de destination.

Avant de commencer


- Les exigences relatives aux versions ONTAP, aux licences et à la configuration des serveurs S3 sont terminées.
- Une relation de peering existe entre les clusters source et destination, et une relation de peering existe entre les machines virtuelles de stockage source et destination.
- Des certificats CA sont nécessaires pour les machines virtuelles source et cible. Vous pouvez utiliser des certificats d'autorité de certification auto-signés ou des certificats signés par un fournisseur d'autorité de certification externe.

System Manager

1. S'il s'agit de la première relation SnapMirror S3 pour cette VM de stockage, vérifiez qu'il existe des clés utilisateur root pour les machines virtuelles de stockage source et de destination, puis régénérez-les si ce n'est pas le cas :
 - a. Cliquez sur **Storage > Storage VM**, puis sélectionnez la VM de stockage.
 - b. Dans l'onglet **Paramètres**, cliquez sur  la mosaïque **S3**.
 - c. Dans l'onglet **Users**, vérifiez qu'il y a une clé d'accès pour l'utilisateur root.
 - d. Si ce n'est pas le cas, cliquez sur  en regard de **root**, puis cliquez sur **régénérer la clé**. Ne pas régénérer la clé si elle existe déjà.
2. Modifiez la machine virtuelle de stockage pour ajouter des utilisateurs, et ajoutez des utilisateurs à des groupes, sur les machines virtuelles de stockage source et cible :

Cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur la machine virtuelle de stockage, cliquez sur **Paramètres**, puis cliquez  sous S3.

Voir "[Ajoutez des utilisateurs et des groupes S3](#)" pour en savoir plus.

3. Sur le cluster source, créez une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :
 - a. Cliquez sur **protection > vue d'ensemble**, puis sur **Paramètres de stratégie locale**.
 - b. Cliquez sur  en regard de **politiques de protection**, puis cliquez sur **Ajouter**.
 - Entrez le nom et la description de la stratégie.
 - Sélectionner la « policy scope », le cluster ou le SVM
 - Sélectionnez **continu** pour les relations SnapMirror S3.
 - Saisissez les valeurs **accélérateur** et **objectif de point de récupération**.
4. Création d'un compartiment avec la protection SnapMirror :
 - a. Cliquez sur **stockage > compartiments**, puis sur **Ajouter**. La vérification des autorisations est facultative mais recommandée.
 - b. Entrez un nom, sélectionnez la VM de stockage, entrez une taille, puis cliquez sur **plus d'options**.
 - c. Sous **permissions**, cliquez sur **Ajouter**.
 - **Principal et effet** - sélectionnez les valeurs correspondant aux paramètres de votre groupe d'utilisateurs ou acceptez les valeurs par défaut.
 - **Actions**- Assurez-vous que les valeurs suivantes sont affichées :

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- **Ressources** - utilisez les valeurs par défaut (*bucketname*, *bucketname/**) ou d'autres valeurs dont vous avez besoin.

Voir "[Gérer l'accès des utilisateurs aux compartiments](#)" pour plus d'informations sur ces champs.

d. Sous **protection**, cochez **Activer SnapMirror (ONTAP ou Cloud)**. Saisissez ensuite les valeurs suivantes :

- Destination
 - **CIBLE : système ONTAP**
 - **CLUSTER** : sélectionnez le cluster distant.
 - **VM DE STOCKAGE** : sélectionnez une VM de stockage sur le cluster distant.
 - **CERTIFICAT d'autorité de certification DU SERVEUR S3** : copiez et collez le contenu du certificat *source*.
- Source
 - **CERTIFICAT CA DU SERVEUR S3** : copiez et collez le contenu du certificat *destination*.

5. Cochez **utilisez le même certificat sur la destination** si vous utilisez un certificat signé par un fournisseur de CA externe.

6. Si vous cliquez sur **Paramètres de destination**, vous pouvez également saisir vos propres valeurs à la place des valeurs par défaut pour le nom de compartiment, la capacité et le niveau de service de performances.

7. Cliquez sur **Enregistrer**. Un nouveau compartiment est créé dans la VM de stockage source, et il est mis en miroir dans un nouveau compartiment créé pour la VM de stockage de destination.

Recul des godets verrouillés

À partir de ONTAP 9.14.1, vous pouvez sauvegarder des compartiments S3 verrouillés et les restaurer selon vos besoins.

Lorsque vous définissez les paramètres de protection d'un compartiment nouveau ou existant, vous pouvez activer le verrouillage des objets dans les compartiments de destination, à condition que les clusters source et de destination exécutent ONTAP 9.14.1 ou version ultérieure et que le verrouillage des objets est activé dans le compartiment source. Le mode de verrouillage d'objet et la durée de conservation du verrou du compartiment source deviennent applicables aux objets répliqués sur le compartiment de destination. Vous pouvez également définir une période de rétention de verrouillage différente pour le compartiment de destination dans la section **Paramètres de destination**. Cette période de conservation s'applique également à tout objet non verrouillé répliqué à partir du compartiment source et des interfaces S3.

Pour plus d'informations sur l'activation du verrouillage d'objet sur un compartiment, reportez-vous à la section "[Créer un compartiment](#)".

CLI

1. S'il s'agit de la première relation SnapMirror S3 pour ce SVM, vérifiez que les clés utilisateur root existent pour les SVM source et de destination et les régénérer si ce n'est pas le cas :

```
vserver object-store-server user show
```

Vérifiez qu'il existe une clé d'accès pour l'utilisateur root. Si ce n'est pas le cas, entrez :

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

Ne pas régénérer la clé si elle existe déjà.

2. Création de compartiments dans les SVM source et destination :

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Ajout de règles d'accès aux règles de compartiment par défaut dans les SVM source et destination :

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

Exemple

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Sur le SVM source, créer une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Paramètres :

- **Type continuous** : seul type de règle pour les relations SnapMirror S3 (obligatoire).
- **-rpo** - spécifie le temps pour l'objectif de point de récupération, en secondes (facultatif).
- **-throttle** - spécifie la limite supérieure de débit/bande passante, en kilo-octets/seconde (facultatif).

Exemple

```
src_cluster::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Installez les certificats de serveur CA sur les SVM admin des clusters source et destination :

- a. Sur le cluster source, installez le certificat de l'autorité de certification qui a signé le certificat du serveur *destination* S3 :

```
security certificate install -type server-ca -vserver src_admin_svm
-cert-name dest_server_certificate
```

- b. Sur le cluster de destination, installez le certificat de l'autorité de certification qui a signé le certificat du serveur *source* S3 :

```
security certificate install -type server-ca -vserver dest_admin_svm
-cert-name src_server_certificate
```

Si vous utilisez un certificat signé par un fournisseur d'autorité de certification externe, installez le

même certificat sur le SVM d'administration source et de destination.

Voir la `security certificate install` page de manuel pour plus de détails.

6. Sur le SVM source, créer une relation SnapMirror S3 :

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]
```

Vous pouvez utiliser une stratégie que vous avez créée ou accepter la règle par défaut.

Exemple

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-  
bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy  
test-policy
```

7. Vérifiez que la mise en miroir est active :

```
snapmirror show -policy-type continuous -fields status
```

Création d'une relation de miroir pour un compartiment existant (cluster distant)

Vous pouvez commencer à protéger les compartiments S3 à tout moment. Par exemple, si vous avez mis à niveau une configuration S3 à partir d'une version antérieure à ONTAP 9.10.1.

Description de la tâche

Vous devez effectuer des tâches sur les clusters source et cible.

Avant de commencer

- Les exigences relatives aux versions ONTAP, aux licences et à la configuration des serveurs S3 sont terminées.
- Une relation de peering existe entre les clusters source et destination, et une relation de peering existe entre les machines virtuelles de stockage source et destination.
- Des certificats CA sont nécessaires pour les machines virtuelles source et cible. Vous pouvez utiliser des certificats d'autorité de certification auto-signés ou des certificats signés par un fournisseur d'autorité de certification externe.



Étapes

Vous pouvez créer une relation de miroir à l'aide de System Manager ou de l'interface de ligne de commandes de ONTAP.

System Manager

1. S'il s'agit de la première relation SnapMirror S3 pour cette VM de stockage, vérifiez qu'il existe des clés utilisateur root pour les machines virtuelles de stockage source et de destination, puis régénérez-les si ce n'est pas le cas :
 - a. Sélectionnez **stockage > Storage VM**, puis sélectionnez la VM de stockage.
 - b. Dans l'onglet **Paramètres**, cliquez sur  la mosaïque **S3**.
 - c. Dans l'onglet **Users**, vérifiez qu'il y a une clé d'accès pour l'utilisateur root.
 - d. Si ce n'est pas le cas, cliquez sur  en regard de **root**, puis cliquez sur **régénérer la clé**. Ne pas régénérer la clé si elle existe déjà.
2. Vérifiez que des utilisateurs et des groupes existants sont présents et disposent des droits d'accès appropriés dans les VM de stockage source et de destination : sélectionnez **stockage > VM de stockage**, puis sélectionnez la VM de stockage, puis l'onglet **Paramètres**. Enfin, localisez la mosaïque **S3**, sélectionnez , puis l'onglet **utilisateurs** et l'onglet **groupes** pour afficher les paramètres d'accès des utilisateurs et des groupes.

Voir "[Ajoutez des utilisateurs et des groupes S3](#)" pour en savoir plus.

3. Sur le cluster source, créez une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :
 - a. Sélectionnez **protection > vue d'ensemble**, puis cliquez sur **Paramètres de stratégie locale**.
 - b. Sélectionnez  en regard de **politiques de protection**, puis cliquez sur **Ajouter**.
 - c. Entrez le nom et la description de la stratégie.
 - d. Sélectionner la portée de la règle : cluster ou SVM
 - e. Sélectionnez **continu** pour les relations SnapMirror S3.
 - f. Saisissez les valeurs **accélérateur** et **objectif de point de récupération**.
4. Vérifiez que la politique d'accès au compartiment du compartiment existant répond toujours à vos besoins :
 - a. Cliquez sur **stockage > godets**, puis sélectionnez le compartiment à protéger.
 - b. Dans l'onglet **autorisations**, cliquez sur  **Modifier**, puis sur **Ajouter** sous **autorisations**.
 - **Principal et effet** : sélectionnez les valeurs correspondant aux paramètres de votre groupe d'utilisateurs ou acceptez les valeurs par défaut.
 - **Actions** : assurez-vous que les valeurs suivantes sont affichées :

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- **Ressources** : utilisez les valeurs par défaut (*bucketname*, *bucketname/**) ou d'autres valeurs dont vous avez besoin.

Voir "[Gérer l'accès des utilisateurs aux compartiments](#)" pour plus d'informations sur ces champs.

5. Protection d'un compartiment existant avec la protection SnapMirror S3 :

- a. Cliquez sur **stockage > godets**, puis sélectionnez le compartiment à protéger.
- b. Cliquez sur **Protect** et saisissez les valeurs suivantes :
 - Destination
 - **CIBLE** : système ONTAP
 - **CLUSTER** : sélectionnez le cluster distant.
 - **VM DE STOCKAGE** : sélectionnez une VM de stockage sur le cluster distant.
 - **CERTIFICAT d'autorité de certification DU SERVEUR S3** : copiez et collez le contenu du certificat *source*.
 - Source
 - **CERTIFICAT d'autorité de certification DU SERVEUR S3** : copiez et collez le contenu du certificat *destination*.
6. Cochez **utilisez le même certificat sur la destination** si vous utilisez un certificat signé par un fournisseur de CA externe.
7. Si vous cliquez sur **Paramètres de destination**, vous pouvez également saisir vos propres valeurs à la place des valeurs par défaut pour le nom de compartiment, la capacité et le niveau de service de performances.
8. Cliquez sur **Enregistrer**. Le compartiment existant est mis en miroir vers un nouveau compartiment dans la VM de stockage de destination.

Recul des godets verrouillés

À partir de ONTAP 9.14.1, vous pouvez sauvegarder des compartiments S3 verrouillés et les restaurer selon vos besoins.

Lorsque vous définissez les paramètres de protection d'un compartiment nouveau ou existant, vous pouvez activer le verrouillage des objets dans les compartiments de destination, à condition que les clusters source et de destination exécutent ONTAP 9.14.1 ou version ultérieure et que le verrouillage des objets est activé dans le compartiment source. Le mode de verrouillage d'objet et la durée de conservation du verrou du compartiment source deviennent applicables aux objets répliqués sur le compartiment de destination. Vous pouvez également définir une période de rétention de verrouillage différente pour le compartiment de destination dans la section **Paramètres de destination**. Cette période de conservation s'applique également à tout objet non verrouillé répliqué à partir du compartiment source et des interfaces S3.

Pour plus d'informations sur l'activation du verrouillage d'objet sur un compartiment, reportez-vous à la section "[Créer un compartiment](#)".

CLI

1. S'il s'agit de la première relation SnapMirror S3 pour ce SVM, vérifiez que des clés utilisateur root existent pour les SVM source et de destination et régénérez-les si ce n'est pas le cas :
`vserver object-store-server user show +` Vérifiez qu'il y a une clé d'accès pour l'utilisateur root. Si ce n'est pas le cas, entrez :
`vserver object-store-server user regenerate-keys -vserver svm_name -user root +` ne régénérez pas la clé si elle existe déjà.
2. Créer un compartiment sur le SVM de destination pour être la cible du miroir :

```
vserver object-store-server bucket create -vserver svm_name -bucket
dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Vérifier que les règles d'accès des politiques de compartiment par défaut sont correctes dans les SVM source et destination :

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

Exemple

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Sur le SVM source, créer une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Paramètres :

- *continuous* – Le seul type de règle pour les relations SnapMirror S3 (obligatoire).
- *-rpo* – indique le temps de l'objectif de point de récupération, en secondes (facultatif).
- *-throttle* – spécifie la limite supérieure sur le débit/bande passante, en kilo-octets/secondes (facultatif).

Exemple

```
src_cluster::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Installez les certificats CA sur les SVM admin des clusters source et destination :

- a. Sur le cluster source, installez le certificat de l'autorité de certification qui a signé le certificat du serveur *destination* S3 :

```
security certificate install -type server-ca -vserver src_admin_svm
-cert-name dest_server_certificate
```

- b. Sur le cluster de destination, installez le certificat de l'autorité de certification qui a signé le certificat du serveur *source* S3 :

```
security certificate install -type server-ca -vserver dest_admin_svm
-cert-name src_server_certificate
```

Si vous utilisez un certificat signé par un fournisseur d'autorité de certification externe, installez le même certificat sur le SVM d'administration source et de destination.

Voir la `security certificate install` page de manuel pour plus de détails.

6. Sur le SVM source, créer une relation SnapMirror S3 :

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]
```

Vous pouvez utiliser une stratégie que vous avez créée ou accepter la règle par défaut.

Exemple

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-  
bucket -destination-path vs1:/bucket/test-bucket-mirror -policy  
test-policy
```

7. Vérifiez que la mise en miroir est active :

```
snapmirror show -policy-type continuous -fields status
```

Basculement et accès aux données depuis le compartiment de destination (cluster distant)

Si les données d'un compartiment source ne sont plus disponibles, vous pouvez interrompre la relation SnapMirror pour rendre le compartiment de destination inscriptible et commencer à transférer les données.

Description de la tâche


Lorsqu'une opération de basculement est effectuée, le compartiment source est converti en lecture seule et le compartiment de destination d'origine est converti en lecture-écriture, inversant ainsi la relation SnapMirror S3.

Lorsque le compartiment source désactivé est de nouveau disponible, SnapMirror S3 resynchronise automatiquement le contenu des deux compartiments. Il n'est pas nécessaire de resynchroniser explicitement la relation, comme cela est requis pour les déploiements de SnapMirror volume.

L'opération de basculement doit être démarrée à partir du cluster distant.

System Manager

Le basculement depuis le compartiment non disponible et début du service des données :

1. Cliquez sur **protection > relations**, puis sélectionnez **SnapMirror S3**.
2. Cliquez sur , sélectionnez **basculement**, puis cliquez sur **basculement**.

CLI

1. Lancer une opération de basculement pour le compartiment de destination :
`snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. Vérifier l'état de l'opération de basculement :
`snapmirror show -fields status`

Exemple

```
dest_cluster::> snapmirror failover start -destination-path  
dest_svm1:/bucket/test-bucket-mirror
```

Restauration d'un compartiment à partir de la machine virtuelle de stockage de destination (cluster distant)

En cas de perte ou de corruption des données d'un compartiment source, vous pouvez restaurer les objets à partir d'un compartiment de destination.

Description de la tâche

Ce compartiment de destination peut être restauré vers un compartiment existant ou vers un nouveau compartiment. Le compartiment cible pour l'opération de restauration doit être supérieur à l'espace logique utilisé par le compartiment de destination.

Si vous utilisez un compartiment existant, celui-ci doit être vide au démarrage d'une opération de restauration. La restauration ne « restaure » pas un compartiment à la fois ; le contenu du compartiment est alors vide.

L'opération de restauration doit être démarrée à partir du cluster distant.

System Manager

Restaurez les données sauvegardées :

1. Cliquez sur **protection > relations**, puis sélectionnez **SnapMirror S3**.
2. Cliquez sur, puis sélectionnez **Restaurer**.
3. Sous **Source**, sélectionnez **Pot existant** (valeur par défaut) ou **Nouveau godet**.
 - Pour restaurer un **compartiment existant** (valeur par défaut), procédez comme suit :
 - Sélectionnez le cluster et la VM de stockage pour rechercher le compartiment existant.
 - Sélectionner le godet existant.
 - Copiez et collez le contenu du certificat CA du serveur *destination* S3.
 - Pour restaurer un **Nouveau godet**, entrez les valeurs suivantes :
 - Machine virtuelle de cluster et de stockage pour héberger le nouveau compartiment.
 - Nom du nouveau compartiment, niveau de service de capacité et de performance.
Voir "[Niveaux de services de stockage](#)" pour en savoir plus.
 - Contenu du certificat CA du serveur *destination* S3.
4. Sous **destination**, copiez et collez le contenu du certificat CA du serveur *source* S3.
5. Cliquez sur **protection > relations** pour contrôler la progression de la restauration.

Restaurer les compartiments verrouillés

À partir de ONTAP 9.14.1, vous pouvez sauvegarder les compartiments verrouillés et les restaurer si nécessaire.

Vous pouvez restaurer un compartiment verrouillé par objet vers un nouveau compartiment ou un compartiment existant. Vous pouvez sélectionner un compartiment verrouillé par objet comme destination dans les scénarios suivants :

- **Restaurer dans un nouveau compartiment** : lorsque le verrouillage d'objet est activé, un compartiment peut être restauré en créant un compartiment pour lequel le verrouillage d'objet est également activé. Lorsque vous restaurez un compartiment verrouillé, le mode de verrouillage des objets et la période de conservation du compartiment d'origine sont répliqués. Vous pouvez également définir une période de conservation de verrouillage différente pour le nouveau compartiment. Cette période de conservation est appliquée aux objets non verrouillés provenant d'autres sources.
- **Restaurer dans un compartiment existant** : un compartiment verrouillé par objet peut être restauré dans un compartiment existant, tant que la gestion des versions et un mode de verrouillage d'objet similaire sont activés sur le compartiment existant. La durée de conservation du godet d'origine est maintenue.
- **Restore non-locked bucket** : même si le verrouillage d'objet n'est pas activé sur un compartiment, vous pouvez le restaurer dans un compartiment dont le verrouillage d'objet est activé et qui se trouve sur le cluster source. Lorsque vous restaurez le compartiment, tous les objets non verrouillés sont verrouillés et le mode de conservation et la durée de conservation du compartiment de destination s'appliquent.

CLI

1. Créez le compartiment de destination à restaurer. Pour plus d'informations, voir "[Création d'une relation de sauvegarde pour un nouveau compartiment \(cible cloud\)](#)".

2. Lancer une opération de restauration pour le compartiment de destination :

```
snapmirror restore -source-path svm_name:/bucket/bucket_name -destination  
-path svm_name:/bucket/bucket_name
```

Exemple

```
dest_cluster::> snapmirror restore -source-path src_vs1:/bucket/test-  
bucket -destination-path dest_vs1:/bucket/test-bucket-mirror
```

Mise en miroir et protection des sauvegardes sur le cluster local




Création d'une relation de miroir pour un nouveau compartiment (cluster local)

Lorsque vous créez de nouveaux compartiments S3, vous pouvez les protéger immédiatement vers une destination SnapMirror S3 sur le même cluster. Il est possible de mettre en miroir les données sur un compartiment de machines virtuelles de stockage différentes ou sur la même machine virtuelle de stockage que la source.


Avant de commencer

- Les exigences relatives aux versions ONTAP, aux licences et à la configuration des serveurs S3 sont terminées.
- Une relation de peering existe entre les machines virtuelles de stockage source et de destination.
- Des certificats CA sont nécessaires pour les machines virtuelles source et cible. Vous pouvez utiliser des certificats d'autorité de certification auto-signés ou des certificats signés par un fournisseur d'autorité de certification externe.

System Manager

1. S'il s'agit de la première relation SnapMirror S3 pour cette VM de stockage, vérifiez qu'il existe des clés utilisateur root pour les machines virtuelles de stockage source et de destination, puis régénérez-les si ce n'est pas le cas :
 - a. Cliquez sur **Storage > Storage VM**, puis sélectionnez la VM de stockage.
 - b. Dans l'onglet **Paramètres**, cliquez sur  dans la mosaïque S3.
 - c. Dans l'onglet **Users**, vérifiez qu'il y a une clé d'accès pour l'utilisateur root
 - d. Si ce n'est pas le cas, cliquez sur  en regard de **root**, puis cliquez sur **régénérer la clé**. Ne pas régénérer la clé si elle existe déjà.
2. Modifiez la machine virtuelle de stockage pour ajouter des utilisateurs et ajouter des utilisateurs à des groupes, dans les machines virtuelles de stockage source et de destination : cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur la machine virtuelle de stockage, cliquez sur **Paramètres**, puis cliquez  sous S3.

Voir "[Ajoutez des utilisateurs et des groupes S3](#)" pour en savoir plus.

3. Créez une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :
 - a. Cliquez sur **protection > vue d'ensemble**, puis sur **Paramètres de stratégie locale**.
 - b. Cliquez sur  en regard de **politiques de protection**, puis cliquez sur **Ajouter**.
 - Entrez le nom et la description de la stratégie.
 - Sélectionner la « policy scope », le cluster ou le SVM
 - Sélectionnez **continu** pour les relations SnapMirror S3.
 - Saisissez les valeurs **accélérateur** et **objectif de point de récupération**.
4. Création d'un compartiment avec la protection SnapMirror :
 - a. Cliquez sur **stockage > compartiments**, puis sur **Ajouter**.
 - b. Entrez un nom, sélectionnez la VM de stockage, entrez une taille, puis cliquez sur **plus d'options**.
 - c. Sous **permissions**, cliquez sur **Ajouter**. La vérification des autorisations est facultative mais recommandée.
 - **Principal et effet** - sélectionnez les valeurs correspondant aux paramètres de votre groupe d'utilisateurs ou acceptez les valeurs par défaut.
 - **Actions** - Assurez-vous que les valeurs suivantes sont affichées :

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- **Ressources** - utilisez les valeurs par défaut (`bucketname`, `bucketname/*`) ou d'autres valeurs dont vous avez besoin

Voir "[Gérer l'accès des utilisateurs aux compartiments](#)" pour plus d'informations sur ces champs.

d. Sous **protection**, cochez **Activer SnapMirror (ONTAP ou Cloud)**. Saisissez ensuite les valeurs suivantes :

- Destination
 - **CIBLE** : système ONTAP
 - **CLUSTER** : sélectionnez le cluster local.
 - **VM de STOCKAGE** : sélectionnez une VM de stockage sur le cluster local.
 - **CERTIFICAT d'autorité de certification DU SERVEUR S3** : copiez et collez le contenu du certificat source.
- Source
 - **CERTIFICAT d'autorité de certification DU SERVEUR S3** : copiez et collez le contenu du certificat de destination.

5. Cochez **utilisez le même certificat sur la destination** si vous utilisez un certificat signé par un fournisseur de CA externe.
6. Si vous cliquez sur **Paramètres de destination**, vous pouvez également saisir vos propres valeurs à la place des valeurs par défaut pour le nom de compartiment, la capacité et le niveau de service de performances.
7. Cliquez sur **Enregistrer**. Un nouveau compartiment est créé dans la VM de stockage source, et il est mis en miroir dans un nouveau compartiment créé pour la VM de stockage de destination.

Recul des godets verrouillés

À partir de ONTAP 9.14.1, vous pouvez sauvegarder des compartiments S3 verrouillés et les restaurer selon vos besoins.

Lorsque vous définissez les paramètres de protection d'un compartiment nouveau ou existant, vous pouvez activer le verrouillage des objets dans les compartiments de destination, à condition que les clusters source et de destination exécutent ONTAP 9.14.1 ou version ultérieure et que le verrouillage des objets est activé dans le compartiment source. Le mode de verrouillage d'objet et la durée de conservation du verrou du compartiment source deviennent applicables aux objets répliqués sur le compartiment de destination. Vous pouvez également définir une période de rétention de verrouillage différente pour le compartiment de destination dans la section **Paramètres de destination**. Cette période de conservation s'applique également à tout objet non verrouillé répliqué à partir du compartiment source et des interfaces S3.

Pour plus d'informations sur l'activation du verrouillage d'objet sur un compartiment, reportez-vous à la section "[Créer un compartiment](#)".

CLI

1. S'il s'agit de la première relation SnapMirror S3 pour ce SVM, vérifiez que les clés utilisateur root existent pour les SVM source et de destination et les régénérer si ce n'est pas le cas :

```
vserver object-store-server user show
```

Vérifiez qu'il existe une clé d'accès pour l'utilisateur root. Si ce n'est pas le cas, entrez :

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

Ne pas régénérer la clé si elle existe déjà.

2. Création de compartiments dans les SVM source et destination :

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Ajout de règles d'accès aux règles de compartiment par défaut dans les SVM source et destination :

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Créez une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Paramètres :

- ° continuous – Le seul type de règle pour les relations SnapMirror S3 (obligatoire).
- ° -rpo – indique le temps de l'objectif de point de récupération, en secondes (facultatif).
- ° -throttle – spécifie la limite supérieure sur le débit/bande passante, en kilo-octets/seconde (facultatif).

Exemple

```
src_cluster::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Installer les certificats de serveur CA sur le SVM admin :

- a. Installez le certificat CA qui a signé le certificat du serveur *source* S3 sur le SVM admin :

```
security certificate install -type server-ca -vserver admin_svm -cert
-name src_server_certificate
```
- b. Installez le certificat CA qui a signé le certificat du serveur *destination* S3 sur le SVM admin :

```
security certificate install -type server-ca -vserver admin_svm -cert
-name dest_server_certificate
```

Si vous utilisez un certificat signé par un fournisseur de CA externe, il vous suffit d'installer ce certificat sur le SVM d'administration.

Voir la `security certificate install` page de manuel pour plus de détails.

6. Création d'une relation SnapMirror S3 :

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]`
```

Vous pouvez utiliser une stratégie que vous avez créée ou accepter la règle par défaut.

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-  
bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror  
-policy test-policy
```

7. Vérifiez que la mise en miroir est active :

```
snapmirror show -policy-type continuous -fields status
```

Création d'une relation de miroir pour un compartiment existant (cluster local)

Vous pouvez commencer à protéger à tout moment les compartiments S3 existants sur le même cluster. Par exemple, si vous mettez à niveau une configuration S3 à partir d'une version antérieure à ONTAP 9.10.1. Il est possible de mettre en miroir les données sur un compartiment de machines virtuelles de stockage différentes ou sur la même machine virtuelle de stockage que la source.



Avant de commencer

- Les exigences relatives aux versions ONTAP, aux licences et à la configuration des serveurs S3 sont terminées.
- Une relation de peering existe entre les machines virtuelles de stockage source et de destination.
- Des certificats CA sont nécessaires pour les machines virtuelles source et cible. Vous pouvez utiliser des certificats d'autorité de certification auto-signés ou des certificats signés par un fournisseur d'autorité de certification externe.

System Manager

1. S'il s'agit de la première relation SnapMirror S3 pour cette VM de stockage, vérifiez qu'il existe des clés utilisateur root pour les machines virtuelles de stockage source et de destination, puis régénérez-les si ce n'est pas le cas :
 - a. Cliquez sur **Storage > Storage VM**, puis sélectionnez la VM de stockage.
 - b. Dans l'onglet **Paramètres**, cliquez sur  la mosaïque **S3**.
 - c. Dans l'onglet **Users**, vérifiez qu'il y a une clé d'accès pour l'utilisateur root.
 - d. Si ce n'est pas le cas, cliquez sur  en regard de **root**, puis cliquez sur **régénérer la clé**. Ne pas régénérer la clé si elle existe déjà
2. Vérifiez que des utilisateurs et des groupes existants sont présents et disposent des droits d'accès appropriés dans les VM de stockage source et de destination : sélectionnez **stockage > VM de stockage**, puis sélectionnez la VM de stockage, puis l'onglet **Paramètres**. Enfin, localisez la mosaïque **S3**, sélectionnez , puis l'onglet **utilisateurs** et l'onglet **groupes** pour afficher les paramètres d'accès des utilisateurs et des groupes.

Voir "[Ajoutez des utilisateurs et des groupes S3](#)" pour en savoir plus.

3. Créez une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :
 - a. Cliquez sur **protection > vue d'ensemble**, puis sur **Paramètres de stratégie locale**.
 - b. Cliquez sur  en regard de **politiques de protection**, puis cliquez sur **Ajouter**.
 - Entrez le nom et la description de la stratégie.
 - Sélectionner la « policy scope », le cluster ou le SVM
 - Sélectionnez **continu** pour les relations SnapMirror S3.
 - Saisissez les valeurs **accélérateur** et **objectif de point de récupération**.
4. Vérifiez que la politique d'accès au compartiment du compartiment existant répond toujours à vos besoins :
 - a. Cliquez sur **stockage > godets**, puis sélectionnez le compartiment à protéger.
 - b. Dans l'onglet **autorisations**, cliquez sur  **Modifier**, puis sur **Ajouter** sous **autorisations**.
 - **Principal et effet** - sélectionnez les valeurs correspondant aux paramètres de votre groupe d'utilisateurs ou acceptez les valeurs par défaut.
 - **Actions** - Assurez-vous que les valeurs suivantes sont affichées :

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- **Ressources** - utilisez les valeurs par défaut (*bucketname*, *bucketname/**) ou d'autres valeurs dont vous avez besoin.

Voir "[Gérer l'accès des utilisateurs aux compartiments](#)" pour plus d'informations sur ces champs.

5. Protection d'un compartiment existant avec SnapMirror S3 :

- a. Cliquez sur **stockage > godets**, puis sélectionnez le compartiment à protéger.
- b. Cliquez sur **Protect** et saisissez les valeurs suivantes :
 - Destination
 - **CIBLE** : système ONTAP
 - **CLUSTER** : sélectionnez le cluster local.
 - **VM DE STOCKAGE** : sélectionnez la même machine virtuelle de stockage ou une autre.
 - **CERTIFICAT d'autorité de certification DU SERVEUR S3** : copiez et collez le contenu du certificat *source*.
 - Source
 - **CERTIFICAT d'autorité de certification DU SERVEUR S3** : copiez et collez le contenu du certificat *destination*.
6. Cochez **utilisez le même certificat sur la destination** si vous utilisez un certificat signé par un fournisseur de CA externe.
7. Si vous cliquez sur **Paramètres de destination**, vous pouvez également saisir vos propres valeurs à la place des valeurs par défaut pour le nom de compartiment, la capacité et le niveau de service de performances.
8. Cliquez sur **Enregistrer**. Le compartiment existant est mis en miroir vers un nouveau compartiment dans la VM de stockage de destination.

Recul des godets verrouillés

À partir de ONTAP 9.14.1, vous pouvez sauvegarder des compartiments S3 verrouillés et les restaurer selon vos besoins.

Lorsque vous définissez les paramètres de protection d'un compartiment nouveau ou existant, vous pouvez activer le verrouillage des objets dans les compartiments de destination, à condition que les clusters source et de destination exécutent ONTAP 9.14.1 ou version ultérieure et que le verrouillage des objets est activé dans le compartiment source. Le mode de verrouillage d'objet et la durée de conservation du verrou du compartiment source deviennent applicables aux objets répliqués sur le compartiment de destination. Vous pouvez également définir une période de rétention de verrouillage différente pour le compartiment de destination dans la section **Paramètres de destination**. Cette période de conservation s'applique également à tout objet non verrouillé répliqué à partir du compartiment source et des interfaces S3.

Pour plus d'informations sur l'activation du verrouillage d'objet sur un compartiment, reportez-vous à la section "[Créer un compartiment](#)".

CLI

1. S'il s'agit de la première relation SnapMirror S3 pour ce SVM, vérifiez que les clés utilisateur root existent pour les SVM source et de destination et les régénérer si ce n'est pas le cas :

```
vserver object-store-server user show
```

Vérifiez qu'il existe une clé d'accès pour l'utilisateur root. Si ce n'est pas le cas, entrez :

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

Ne pas régénérer la clé si elle existe déjà.

2. Créer un compartiment sur le SVM de destination pour être la cible du miroir :

```
vserver object-store-server bucket create -vserver svm_name -bucket
dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Vérifier que les règles d'accès aux règles de compartiment par défaut sont correctes dans les SVM source et destination :

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

Exemple

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Créez une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Paramètres :

- *continuous* – Le seul type de règle pour les relations SnapMirror S3 (obligatoire).
- *-rpo* – indique le temps de l'objectif de point de récupération, en secondes (facultatif).
- *-throttle* – spécifie la limite supérieure sur le débit/bande passante, en kilo-octets/secondes (facultatif).

Exemple

```
clusterA::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Installer les certificats de serveur CA sur le SVM admin :

- a. Installez le certificat CA qui a signé le certificat du serveur *source* S3 sur le SVM admin :

```
security certificate install -type server-ca -vserver admin_svm -cert
-name src_server_certificate
```
- b. Installez le certificat CA qui a signé le certificat du serveur *destination* S3 sur le SVM admin :

```
security certificate install -type server-ca -vserver admin_svm -cert
-name dest_server_certificate
```

Si vous utilisez un certificat signé par un fournisseur de CA externe, il vous suffit d'installer ce certificat sur le SVM d'administration.

Voir la `security certificate install` page de manuel pour plus de détails.

6. Création d'une relation SnapMirror S3 :

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]
```

Vous pouvez utiliser une stratégie que vous avez créée ou accepter la règle par défaut.

Exemple

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-  
bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy  
test-policy
```

7. Vérifiez que la mise en miroir est active :

```
snapmirror show -policy-type continuous -fields status
```

Basculement et accès aux données depuis le compartiment de destination (cluster local)

Si les données d'un compartiment source ne sont plus disponibles, vous pouvez interrompre la relation SnapMirror pour rendre le compartiment de destination inscriptible et commencer à transférer les données.

Description de la tâche


Lorsqu'une opération de basculement est effectuée, le compartiment source est converti en lecture seule et le compartiment de destination d'origine est converti en lecture-écriture, inversant ainsi la relation SnapMirror S3.

Lorsque le compartiment source désactivé est de nouveau disponible, SnapMirror S3 resynchronise automatiquement le contenu des deux compartiments. Vous n'avez pas besoin de resynchroniser explicitement la relation, comme cela est requis pour les déploiements de SnapMirror volume standard.

Si le compartiment de destination se trouve sur un cluster distant, l'opération de basculement doit être démarrée à partir du cluster distant.

System Manager

Le basculement depuis le compartiment non disponible et début du service des données :

1. Cliquez sur **protection > relations**, puis sélectionnez **SnapMirror S3**.
2. Cliquez sur , sélectionnez **basculement**, puis cliquez sur **basculement**.

CLI

1. Lancer une opération de basculement pour le compartiment de destination :
`snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. Vérifier l'état de l'opération de basculement :
`snapmirror show -fields status`

Exemple

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-  
bucket-mirror
```

Restaurer un compartiment depuis la VM de stockage de destination (cluster local)

En cas de perte ou de corruption des données d'un compartiment source, vous pouvez restaurer des objets à partir d'un compartiment de destination.

Description de la tâche

Ce compartiment de destination peut être restauré vers un compartiment existant ou vers un nouveau compartiment. Le compartiment cible pour l'opération de restauration doit être supérieur à l'espace logique utilisé par le compartiment de destination.

Si vous utilisez un compartiment existant, celui-ci doit être vide au démarrage d'une opération de restauration. La restauration ne « restaure » pas un compartiment à la fois ; le contenu du compartiment est alors vide.

L'opération de restauration doit être lancée à partir du cluster local.

System Manager

Restaurer les données de sauvegarde :

1. Cliquez sur **protection > relations**, puis sélectionnez le compartiment.
2. Cliquez sur, puis sélectionnez **Restaurer**.
3. Sous **Source**, sélectionnez **Pot existant** (valeur par défaut) ou **Nouveau godet**.
 - Pour restaurer un **compartiment existant** (valeur par défaut), procédez comme suit :
 - Sélectionnez le cluster et la VM de stockage pour rechercher le compartiment existant.
 - Sélectionner le godet existant.
4. Copiez et collez le contenu du certificat AC du serveur S3 de destination.
 - Pour restaurer un **Nouveau godet**, entrez les valeurs suivantes :
 - Machine virtuelle de cluster et de stockage pour héberger le nouveau compartiment.
 - Nom du nouveau compartiment, niveau de service de capacité et de performance.
Voir "[Niveaux de services de stockage](#)" pour en savoir plus.
 - Contenu du certificat d'autorité de certification du serveur S3 de destination.
5. Sous **destination**, copiez et collez le contenu du certificat d'autorité de certification du serveur S3 source.
6. Cliquez sur **protection > relations** pour contrôler la progression de la restauration.

Restaurer les compartiments verrouillés

À partir de ONTAP 9.14.1, vous pouvez sauvegarder les compartiments verrouillés et les restaurer si nécessaire.

Vous pouvez restaurer un compartiment verrouillé par objet vers un nouveau compartiment ou un compartiment existant. Vous pouvez sélectionner un compartiment verrouillé par objet comme destination dans les scénarios suivants :

- **Restaurer dans un nouveau compartiment** : lorsque le verrouillage d'objet est activé, un compartiment peut être restauré en créant un compartiment pour lequel le verrouillage d'objet est également activé. Lorsque vous restaurez un compartiment verrouillé, le mode de verrouillage des objets et la période de conservation du compartiment d'origine sont répliqués. Vous pouvez également définir une période de conservation de verrouillage différente pour le nouveau compartiment. Cette période de conservation est appliquée aux objets non verrouillés provenant d'autres sources.
- **Restaurer dans un compartiment existant** : un compartiment verrouillé par objet peut être restauré dans un compartiment existant, tant que la gestion des versions et un mode de verrouillage d'objet similaire sont activés sur le compartiment existant. La durée de conservation du godet d'origine est maintenue.
- **Restore non-locked bucket** : même si le verrouillage d'objet n'est pas activé sur un compartiment, vous pouvez le restaurer dans un compartiment dont le verrouillage d'objet est activé et qui se trouve sur le cluster source. Lorsque vous restaurez le compartiment, tous les objets non verrouillés sont verrouillés et le mode de conservation et la durée de conservation du compartiment de destination s'appliquent.

CLI

1. Si vous restaurez des objets dans un nouveau compartiment, créez le nouveau compartiment. Pour

plus d'informations, voir "[Création d'une relation de sauvegarde pour un nouveau compartiment \(cible cloud\)](#)".

2. Lancer une opération de restauration pour le compartiment de destination :

```
snapmirror restore -source-path svm_name:/bucket/bucket_name -destination  
-path svm_name:/bucket/bucket_name
```

Exemple

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket  
-destination-path vs1:/bucket/test-bucket-mirror
```

Protection des sauvegardes avec des cibles cloud

Exigences relatives aux relations cibles cloud

Assurez-vous que vos environnements source et cible respectent les exigences de protection de sauvegarde SnapMirror S3 sur des cibles cloud.

Pour accéder au compartiment de données, vous devez disposer d'identifiants de compte valides auprès du fournisseur de magasin d'objets.

Les interfaces réseau intercluster et un IPspace doivent être configurées sur le cluster avant que le cluster ne puisse se connecter à un magasin d'objets cloud. Vous devez créer des interfaces réseau du cluster sur chaque nœud pour transférer les données de manière transparente du stockage local vers le magasin d'objets cloud.

Pour les cibles StorageGRID, vous devez connaître les informations suivantes :

- Nom du serveur, exprimé sous forme de nom de domaine complet (FQDN) ou d'adresse IP
- nom de compartiment : ce compartiment doit déjà exister
- touche d'accès
- clé secrète

En outre, le certificat d'autorité de certification utilisé pour signer le certificat de serveur StorageGRID doit être installé sur la machine virtuelle de stockage d'administration du cluster ONTAP S3 à l'aide de `security certificate install` command. Pour plus d'informations, voir "[Installation d'un certificat CA](#)". Si vous utilisez StorageGRID.

Pour les cibles AWS S3, vous devez connaître les informations suivantes :

- Nom du serveur, exprimé sous forme de nom de domaine complet (FQDN) ou d'adresse IP
- nom de compartiment : ce compartiment doit déjà exister
- touche d'accès
- clé secrète

Le serveur DNS de la machine virtuelle de stockage admin du cluster ONTAP doit être capable de résoudre les FQDN (si utilisé) aux adresses IP.

Création d'une relation de sauvegarde pour un nouveau compartiment (cible cloud)


Lorsque vous créez des compartiments S3, vous pouvez les sauvegarder immédiatement dans un compartiment cible SnapMirror S3 sur un fournisseur de magasin d'objets, qui peut être un système StorageGRID ou un déploiement Amazon S3.

Avant de commencer

- Vous disposez d'informations d'identification de compte et de configuration valides pour le fournisseur de magasin d'objets.
- Les interfaces réseau intercluster et un IPspace ont été configurés sur le système source.
- • La configuration DNS de la machine virtuelle de stockage source doit pouvoir résoudre le nom de domaine complet de la cible.

System Manager

1. Modifiez la machine virtuelle de stockage pour ajouter des utilisateurs et ajouter des utilisateurs aux groupes :

- a. Cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur la machine virtuelle de stockage, cliquez sur **Paramètres**, puis cliquez sur  sous **S3**.


Voir "[Ajoutez des utilisateurs et des groupes S3](#)" pour en savoir plus.

2. Ajouter un magasin d'objets cloud sur le système source :

- a. Cliquez sur **protection > vue d'ensemble**, puis sélectionnez **magasins d'objets Cloud**.
- b. Cliquez sur **Ajouter**, puis sélectionnez **Amazon S3** ou **StorageGRID**.
- c. Saisissez les valeurs suivantes :

- Nom du magasin d'objets cloud
- Style d'URL (chemin d'accès ou hébergement virtuel)
- Machine virtuelle de stockage (activée pour S3)
- Nom du serveur de magasin d'objets (FQDN)
- Certificat de magasin d'objets
- Touche d'accès
- Clé secrète
- Nom du conteneur (compartiment)

3. Créez une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :

- a. Cliquez sur **protection > vue d'ensemble**, puis sur **Paramètres de stratégie locale**.
- b. Cliquez sur  en regard de **politiques de protection**, puis cliquez sur **Ajouter**.
 - Entrez le nom et la description de la stratégie.
 - Sélectionner la « policy scope », le cluster ou le SVM
 - Sélectionnez **continu** pour les relations SnapMirror S3.
 - Saisissez les valeurs **accélérateur** et **objectif de point de récupération**.

4. Création d'un compartiment avec la protection SnapMirror :

- a. Cliquez sur **stockage > compartiments**, puis sur **Ajouter**.
- b. Entrez un nom, sélectionnez la VM de stockage, entrez une taille, puis cliquez sur **plus d'options**.
- c. Sous **permissions**, cliquez sur **Ajouter**. La vérification des autorisations est facultative mais recommandée.
 - **Principal et effet** - sélectionnez les valeurs correspondant aux paramètres de votre groupe d'utilisateurs ou acceptez les valeurs par défaut.
 - **Actions** - Assurez-vous que les valeurs suivantes sont affichées :

```
`GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
```


- **Ressources** - utilisez les valeurs par défaut `_(bucketname, bucketname/*)` ou d'autres valeurs dont vous avez besoin.

Voir "[Gérer l'accès des utilisateurs aux compartiments](#)" pour plus d'informations sur ces champs.

- d. Sous **protection**, cochez **Activer SnapMirror (ONTAP ou Cloud)**, sélectionnez **stockage cloud**, puis sélectionnez **stockage objet cloud**.

Lorsque vous cliquez sur **Enregistrer**, un nouveau compartiment est créé dans la machine virtuelle de stockage source et il est sauvegardé dans le magasin d'objets cloud.

CLI

1. S'il s'agit de la première relation SnapMirror S3 pour ce SVM, vérifiez que les clés utilisateur root existent pour les SVM source et de destination et les régénérer si ce n'est pas le cas :

`vserver object-store-server user show` + Confirmez qu'il existe une clé d'accès pour l'utilisateur root. Si ce n'est pas le cas, entrez :

`vserver object-store-server user regenerate-keys -vserver svm_name -user root` + ne régénérez pas la clé si elle existe déjà.

2. Création d'un compartiment dans le SVM source :

`vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

3. Ajout de règles d'accès à la politique de compartiment par défaut :

`vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

Exemple

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Créez une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :

`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

Paramètres : * `type continuous` – seul type de règle pour les relations SnapMirror S3 (obligatoire). * `-rpo` – indique le temps de l'objectif de point de récupération, en secondes (facultatif). * `-throttle` – indique la limite supérieure de débit/bande passante, en kilo-octets/seconde (facultatif).

Exemple

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous  
-rpo 0 -policy test-policy
```

5. Si la cible est un système StorageGRID, installez le certificat du serveur StorageGRID CA sur le SVM admin du cluster source :

```
security certificate install -type server-ca -vserver src_admin_svm -cert  
-name storage_grid_server_certificate
```

Voir la `security certificate install` page de manuel pour plus de détails.

6. Définissez le magasin d'objets de destination SnapMirror S3 :

```
snapmirror object-store config create -vserver svm_name -object-store-name  
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server  
target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port  
port_number -access-key target_access_key -secret-password  
target_secret_key
```

Paramètres :

- * `-object-store-name` – Le nom de la cible de magasin d'objets sur le système ONTAP local.
- * `-usage` – utiliser `data` pour ce flux de travail.
- * `-provider-type` – `AWS_S3` et `SGWS` Les cibles (StorageGRID) sont prises en charge.
- * `-server` – Le FQDN ou l'adresse IP du serveur cible.
- * `-is-ssl-enabled` – L'activation de SSL est facultative mais recommandée.

Voir la `snapmirror object-store config create` page de manuel pour plus de détails.

Exemple

```
src_cluster::> snapmirror object-store config create -vserver vs0  
-object-store-name sgws-store -usage data -provider-type SGWS  
-server sgws.example.com -container-name target-test-bucket -is-ssl-  
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

7. Création d'une relation SnapMirror S3 :

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination  
-path object_store_name:/objstore -policy policy_name
```

Paramètres :

- * `-destination-path` - le nom du magasin d'objets que vous avez créé à l'étape précédente et la valeur fixe `objstore`.

Vous pouvez utiliser une stratégie que vous avez créée ou accepter la règle par défaut.

Exemple

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-  
bucket -destination-path sgws-store:/objstore -policy test-policy
```

8. Vérifiez que la mise en miroir est active :

```
snapmirror show -policy-type continuous -fields status
```


Création d'une relation de sauvegarde pour un compartiment existant (cible cloud)

Vous pouvez commencer à sauvegarder des compartiments S3 à tout moment. Par exemple, si vous avez mis à niveau une configuration S3 à partir d'une version antérieure à ONTAP 9.10.1.



Avant de commencer

- Vous disposez d'informations d'identification de compte et de configuration valides pour le fournisseur de magasin d'objets.
- Les interfaces réseau intercluster et un IPspace ont été configurés sur le système source.
- La configuration DNS de la machine virtuelle de stockage source doit pouvoir résoudre le FQDN de la cible.

System Manager

1. Vérifiez que les utilisateurs et les groupes sont correctement définis : cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur la machine virtuelle de stockage, cliquez sur **Paramètres**, puis sur  sous S3.

Voir "[Ajoutez des utilisateurs et des groupes S3](#)" pour en savoir plus.

2. Créez une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :
 - a. Cliquez sur **protection > vue d'ensemble**, puis sur **Paramètres de stratégie locale**.
 - b. Cliquez sur  en regard de **politiques de protection**, puis cliquez sur **Ajouter**.
 - c. Entrez le nom et la description de la stratégie.
 - d. Sélectionner la « policy scope », le cluster ou le SVM
 - e. Sélectionnez **continu** pour les relations SnapMirror S3.
 - f. Saisissez les valeurs **accélérateur** et **objectif de point de récupération**.
3. Ajouter un magasin d'objets cloud sur le système source :
 - a. Cliquez sur **protection > Présentation**, puis sélectionnez **Cloud Object Store**.
 - b. Cliquez sur **Ajouter**, puis sélectionnez **Amazon S3** ou **autres** pour StorageGRID Webscale.
 - c. Saisissez les valeurs suivantes :
 - Nom du magasin d'objets cloud
 - Style d'URL (chemin d'accès ou hébergement virtuel)
 - Machine virtuelle de stockage (activée pour S3)
 - Nom du serveur de magasin d'objets (FQDN)
 - Certificat de magasin d'objets
 - Touche d'accès
 - Clé secrète
 - Nom du conteneur (compartiment)
4. Vérifiez que la politique d'accès au compartiment du compartiment existant répond toujours à vos besoins :
 - a. Cliquez sur **stockage > godets**, puis sélectionnez le compartiment à protéger.
 - b. Dans l'onglet **autorisations**, cliquez sur  **Modifier**, puis sur **Ajouter** sous **autorisations**.
 - **Principal et effet** - sélectionnez les valeurs correspondant aux paramètres de votre groupe d'utilisateurs ou acceptez les valeurs par défaut.
 - **Actions** - Assurez-vous que les valeurs suivantes sont affichées :
`GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`
 - **Ressources** - utilisez les valeurs par défaut (`bucketname, bucketname/*`) ou d'autres valeurs dont vous avez besoin.

Voir "[Gérer l'accès des utilisateurs aux compartiments](#)" pour plus d'informations sur ces champs.

5. Sauvegarder le compartiment à l'aide de SnapMirror S3 :

- Cliquez sur **stockage > godets**, puis sélectionnez le compartiment à sauvegarder.
- Cliquez sur **protéger**, sélectionnez **Cloud Storage** sous **cible**, puis sélectionnez **Cloud Object Store**.

Lorsque vous cliquez sur **Enregistrer**, le compartiment existant est sauvegardé dans le magasin d'objets cloud.

CLI

1. Vérifiez que les règles d'accès dans la politique de compartiment par défaut sont correctes :

```
vserver object-store-server bucket policy add-statement -vserver svm_name  
-bucket bucket_name -effect {allow|deny} -action object_store_actions  
-principal user_and_group_names -resource object_store_resources [-sid  
text] [-index integer]
```

Exemple

```
clusterA::> vserver object-store-server bucket policy add-statement  
-bucket test-bucket -effect allow -action  
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,  
ListBucketMultipartUploads,ListMultipartUploadParts -principal -  
-resource test-bucket, test-bucket /*
```

2. Créez une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :

```
snapmirror policy create -vserver svm_name -policy policy_name -type  
continuous [-rpo integer] [-throttle throttle_type] [-comment text]  
[additional_options]
```

Paramètres : * type continuous – seul type de règle pour les relations SnapMirror S3 (obligatoire). * -rpo – indique le temps de l'objectif de point de récupération, en secondes (facultatif). * -throttle – indique la limite supérieure de débit/bande passante, en kilo-octets/secondes (facultatif).

Exemple

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous  
-rpo 0 -policy test-policy
```

3. Si la cible est un système StorageGRID, installez le certificat StorageGRID CA sur le SVM admin du cluster source :

```
security certificate install -type server-ca -vserver src_admin_svm -cert  
-name storage_grid_server_certificate
```

Voir la security certificate install page de manuel pour plus de détails.

4. Définissez le magasin d'objets de destination SnapMirror S3 :

```
snapmirror object-store config create -vserver svm_name -object-store-name  
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server
```

```
target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port
port_number -access-key target_access_key -secret-password
target_secret_key
```

Paramètres :

- * -object-store-name – Le nom de la cible de magasin d’objets sur le système ONTAP local.
- * -usage – utiliser data pour ce flux de travail.
- * -provider-type – AWS_S3 et SGWS Les cibles (StorageGRID) sont prises en charge.
- * -server – Le FQDN ou l’adresse IP du serveur cible.
- * -is-ssl-enabled –L’activation de SSL est facultative mais recommandée.

Voir la snapmirror object-store config create page de manuel pour plus de détails.

Exemple

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

5. Création d’une relation SnapMirror S3 :

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination
-path object_store_name:/objstore -policy policy_name
```

Paramètres :

- * -destination-path - le nom du magasin d’objets que vous avez créé à l’étape précédente et la valeur fixe objstore.

Vous pouvez utiliser une stratégie que vous avez créée ou accepter la règle par défaut.

```
src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
-destination-path sgws-store:/objstore -policy test-policy
```

6. Vérifiez que la mise en miroir est active :

```
snapmirror show -policy-type continuous -fields status
```

Restauration d’un compartiment à partir d’une cible cloud

En cas de perte ou de corruption des données d’un compartiment source, vous pouvez les remplir à nouveau en les restaurant à partir d’un compartiment de destination.

Description de la tâche

Ce compartiment de destination peut être restauré vers un compartiment existant ou vers un nouveau compartiment. Le compartiment cible pour l’opération de restauration doit être supérieur à l’espace logique utilisé du compartiment de destination.

Si vous utilisez un compartiment existant, celui-ci doit être vide au démarrage d’une opération de restauration. La restauration ne « restaure » pas un compartiment à la fois ; le contenu du compartiment est alors vide.

System Manager

Restaurer les données de sauvegarde :

1. Cliquez sur **protection > relations**, puis sélectionnez **SnapMirror S3**.
2. Cliquez sur, puis sélectionnez **Restaurer**.
3. Sous **Source**, sélectionnez **Pot existant** (valeur par défaut) ou **Nouveau godet**.
 - Pour restaurer un **compartiment existant** (valeur par défaut), procédez comme suit :
 - Sélectionnez le cluster et la VM de stockage pour rechercher le compartiment existant.
 - Sélectionner le godet existant.
 - Copiez et collez le contenu du certificat CA du serveur *destination* S3.
 - Pour restaurer un **Nouveau godet**, entrez les valeurs suivantes :
 - Machine virtuelle de cluster et de stockage pour héberger le nouveau compartiment.
 - Le nouveau compartiment : niveau de service du nom, de la capacité et des performances. Voir "[Niveaux de services de stockage](#)" pour en savoir plus.
 - Contenu du certificat d'autorité de certification du serveur S3 de destination.
4. Sous **destination**, copiez et collez le contenu du certificat CA du serveur *source* S3.
5. Cliquez sur **protection > relations** pour contrôler la progression de la restauration.

Procédure CLI

1. Créez le compartiment de destination à restaurer. Pour plus d'informations, voir "[Création d'une relation de sauvegarde pour un compartiment \(cible cloud\)](#)".
2. Lancer une opération de restauration pour le compartiment de destination :

```
snapmirror restore -source-path object_store_name:/objstore -destination  
-path svm_name:/bucket/bucket_name
```

Exemple

L'exemple suivant illustre la restauration d'un compartiment de destination vers un compartiment existant.


```
clusterA::> snapmirror restore -source-path sgws.store:/objstore  
-destination-path vs0:/bucket/test-bucket
```

Modifier une règle de miroir

Il peut être nécessaire de modifier une règle de miroir S3, par exemple pour ajuster les valeurs RPO et papillon.

System Manager

Si vous souhaitez modifier ces valeurs, vous pouvez modifier une stratégie de protection existante.

1. Cliquez sur **protection > relations**, puis sélectionnez la stratégie de protection pour la relation que vous souhaitez modifier.
2. Cliquez sur  en regard du nom de la stratégie, puis cliquez sur **Modifier**.

CLI

Modification d'une règle SnapMirror S3 :

```
snapmirror policy modify -vserver svm_name -policy policy_name [-rpo integer]
[-throttle throttle_type] [-comment text]
```

Paramètres :

- `-rpo` – spécifie le temps de l'objectif de point de récupération, en secondes.
- `-throttle` – spécifie la limite supérieure sur le débit/bande passante, en kilo-octets/seconde.

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

Audit des événements S3

Audit des événements S3

Depuis ONTAP 9.10.1, vous pouvez auditer les événements de gestion et de données dans des environnements ONTAP S3. La fonctionnalité d'audit S3 est similaire aux fonctionnalités d'audit NAS existantes, et l'audit S3 et NAS peut coexister dans un cluster.

Lorsque vous créez et activez une configuration d'audit S3 sur un SVM, les événements S3 sont enregistrés dans un fichier journal. Vous pouvez spécifier les événements suivants à enregistrer :

- Événements d'accès aux objets (données)

GetObject, PutObject et DeleteObject

- Les événements de gestion

PutBucket et DeleteBucket

Le format du journal est JavaScript Object notation (JSON).

La limite combinée des configurations d'audit S3 et NFS est de 50 SVM par cluster.

Le pack de licences suivant est requis :

- Bundle de base pour le protocole et le stockage ONTAP S3

Pour plus d'informations, voir ["Fonctionnement du processus d'audit ONTAP"](#).

Audit garanti

Par défaut, l'audit S3 et NAS est garanti. ONTAP garantit l'enregistrement de tous les événements d'accès au compartiment vérifiables, même si un nœud est indisponible. Une opération de compartiment demandée ne peut être effectuée qu'une fois l'enregistrement d'audit pour cette opération enregistré dans le volume intermédiaire du stockage persistant. Si les enregistrements d'audit ne peuvent pas être archivés dans les fichiers de transfert, soit en raison d'un espace insuffisant, soit en raison d'autres problèmes, les opérations du client sont refusées.

Besoins en espace pour l'audit

Dans le système d'audit ONTAP, les enregistrements d'audit sont initialement stockés dans des fichiers intermédiaires binaires sur des nœuds individuels. Ils sont régulièrement consolidés et convertis en journaux d'événements lisibles par l'utilisateur, qui sont stockés dans le répertoire du journal des événements d'audit de la SVM.

Les fichiers de sauvegarde sont stockés dans un volume de sauvegarde dédié, qui est créé par ONTAP lors de la création de la configuration d'audit. Il existe un volume intermédiaire par agrégat.

Vous devez prévoir suffisamment d'espace disponible dans la configuration d'audit :

- Pour les volumes intermédiaires dans des agrégats contenant des compartiments audités.
- Pour le volume contenant le répertoire dans lequel les journaux d'événements convertis sont stockés.

Vous pouvez contrôler le nombre de journaux d'événements et donc l'espace disponible dans le volume à l'aide de l'une des deux méthodes suivantes lors de la création de la configuration d'audit S3 :

- Une limite numérique ; le `-rotate-limit` paramètre contrôle le nombre minimal de fichiers d'audit qui doivent être conservés.
- Une limite de temps ; le `-retention-duration` paramètre contrôle la période maximale pendant laquelle les fichiers peuvent être conservés.

Dans les deux paramètres, une fois que la configuration est dépassée, les fichiers d'audit plus anciens peuvent être supprimés afin de faire place à des fichiers plus récents. Pour les deux paramètres, la valeur est 0, ce qui indique que tous les fichiers doivent être conservés. Afin de garantir un espace suffisant, il est donc recommandé de définir un des paramètres sur une valeur non nulle.

En raison de l'audit garanti, si l'espace disponible pour les données d'audit s'exécute avant la limite de rotation, des données d'audit plus récentes ne peuvent pas être créées, ce qui entraîne une incapacité des clients à accéder aux données. Par conséquent, le choix de cette valeur et de l'espace alloué à l'audit doit être soigneusement choisi, et vous devez répondre aux avertissements concernant l'espace disponible du système d'audit.

Pour plus d'informations, voir ["Concepts d'audit de base"](#).

Planification d'une configuration d'audit S3

Vous devez spécifier un certain nombre de paramètres pour la configuration d'audit S3 ou accepter les valeurs par défaut. En particulier, vous devez tenir compte des paramètres de rotation du journal qui vous aideront à garantir un espace libre adéquat.

Voir la **vserver object-store-server audit create** page man pour les détails de syntaxe.

Paramètres généraux

Vous devez spécifier deux paramètres requis lors de la création de la configuration d'audit. Vous pouvez également spécifier trois paramètres facultatifs.

Type d'information	Option	Obligatoire
<i>Nom du SVM</i> Nom du SVM sur lequel créer la configuration d'audit. Le SVM doit déjà exister et être activé pour S3.	<code>-vserver svm_name</code>	Oui.
<i>Chemin de destination du journal</i> Spécifie l'emplacement de stockage des journaux d'audit convertis. Le chemin doit déjà exister sur le SVM. Le chemin d'accès peut comporter jusqu'à 864 caractères et doit avoir des autorisations de lecture/écriture. Si le chemin n'est pas valide, la commande audit de configuration échoue.	<code>-destination text</code>	Oui.
<i>Catégories d'événements à auditer</i> Les catégories d'événements suivantes peuvent être auditées : <ul style="list-style-type: none">• les données Événements GetObject, PutObject et DeleteObject• gestion Événements PutBucket et DeleteBucket La valeur par défaut est d'auditer uniquement les événements de données.	<code>-events {data management}, ...</code>	Non

Vous pouvez entrer l'un des paramètres suivants pour contrôler le nombre de fichiers journaux d'audit. Si aucune valeur n'est saisie, tous les fichiers journaux sont conservés.

Type d'information	Option	Obligatoire
--------------------	--------	-------------

<p><i>Limite de rotation des fichiers journaux</i></p> <p>Détermine le nombre de fichiers journaux d'audit à conserver avant de faire pivoter le fichier journal le plus ancien vers l'extérieur. Par exemple, si vous saisissez une valeur de 5, les cinq derniers fichiers journaux sont conservés.</p> <p>Une valeur de 0 indique que tous les fichiers journaux sont conservés. La valeur par défaut est 0.</p>	<p><code>-rotate-limit integer</code></p>	<p>Non</p>
<p><i>Limite de durée des fichiers journaux</i></p> <p>Détermine la durée pendant laquelle un fichier journal peut être conservé avant d'être supprimé. Par exemple, si vous entrez une valeur de 5 portes 0h0m, les journaux de plus de 5 jours sont supprimés.</p> <p>Une valeur de 0 indique que tous les fichiers journaux sont conservés. La valeur par défaut est 0.</p>	<p><code>-retention duration integer_time</code></p>	<p>Non</p>

Paramètres de rotation du journal d'audit

Vous pouvez faire pivoter les journaux d'audit en fonction de la taille ou de la planification. La valeur par défaut consiste à faire pivoter les journaux d'audit en fonction de la taille.

Rotation des journaux en fonction de la taille du journal

Si vous souhaitez utiliser la méthode de rotation du journal par défaut et la taille du journal par défaut, vous n'avez pas besoin de configurer de paramètres spécifiques pour la rotation du journal. La taille du journal par défaut est de 100 Mo.

Si vous ne souhaitez pas utiliser la taille de journal par défaut, vous pouvez configurer le `-rotate-size` paramètre pour spécifier une taille de journal personnalisée.

Si vous souhaitez réinitialiser la rotation en fonction d'une taille de journal seule, utilisez la commande suivante pour annuler la sélection `-rotate-schedule-minute` paramètre :

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

Rotation des journaux en fonction d'un planning

Si vous choisissez de faire pivoter les journaux d'audit en fonction d'un planning, vous pouvez programmer la rotation du journal en utilisant les paramètres de rotation basés sur le temps dans n'importe quelle combinaison.

- Si vous utilisez une rotation basée sur le temps, le `-rotate-schedule-minute` paramètre obligatoire.
- Tous les autres paramètres de rotation basés sur le temps sont facultatifs.
 - `-rotate-schedule-month`
 - `-rotate-schedule-dayofweek`
 - `-rotate-schedule-day`

◦ `-rotate-schedule-hour`

- Le planning de rotation est calculé en utilisant toutes les valeurs liées au temps.
Par exemple, si vous spécifiez uniquement le `-rotate-schedule-minute` paramètre, les fichiers journaux d'audit sont pivotés en fonction des minutes spécifiées pour tous les jours de la semaine, pendant toutes les heures sur tous les mois de l'année.
- Si vous spécifiez uniquement un ou deux paramètres de rotation basés sur le temps (par exemple, `-rotate-schedule-month` et `-rotate-schedule-minutes`), les fichiers journaux pivotent en fonction des valeurs de minutes que vous avez spécifiées tous les jours de la semaine, pendant toutes les heures, mais seulement pendant les mois spécifiés.

Par exemple, vous pouvez préciser que le journal d'audit doit être tourné pendant les mois janvier, mars et août tous les lundis, mercredis et samedis à 10 h 30

- Si vous spécifiez des valeurs pour les deux `-rotate-schedule-dayofweek` et `-rotate-schedule-day`, ils sont considérés indépendamment.

Par exemple, si vous spécifiez `-rotate-schedule-dayofweek` Comme vendredi et `-rotate-schedule-day` Comme 13, les registres de vérification seront ensuite tournés tous les vendredis et les 13ème jours du mois spécifié, pas seulement tous les vendredis du 13ème.

- Si vous souhaitez réinitialiser la rotation en fonction d'une planification seule, utilisez la commande suivante pour annuler la définition du `-rotate-size` parameter:

```
vserver audit modify -vserver svm_name -destination / -rotate-size -
```

Rotation des journaux en fonction de la taille du journal et de la planification

Vous pouvez choisir de faire pivoter les fichiers journaux en fonction de la taille du journal et d'une planification en définissant à la fois le paramètre `-rotation-taille` et les paramètres de rotation basés sur le temps dans n'importe quelle combinaison. Par exemple : si `-rotate-size` Est défini sur 10 Mo et `-rotate-schedule-minute` Est défini sur 15, les fichiers journaux pivotent lorsque la taille du fichier journal atteint 10 Mo ou la 15e minute de chaque heure (selon la première éventualité).

Créez et activez une configuration d'audit S3

Pour implémenter l'audit S3, vous devez d'abord créer une configuration d'audit de magasin d'objets persistant sur un SVM compatible avec S3, puis activer la configuration.

Ce dont vous avez besoin

- SVM compatible S3.
- Espace suffisant pour les volumes intermédiaires dans l'agrégat.

Description de la tâche

Une configuration d'audit est requise pour chaque SVM contenant des compartiments S3 que vous souhaitez auditer. Vous pouvez activer l'audit S3 sur des serveurs S3 nouveaux ou existants. Les configurations d'audit restent conservées dans un environnement S3 jusqu'à ce qu'elles soient supprimées par la commande **vserver Object-store-Server audit delete**.

La configuration d'audit de S3 s'applique à toutes les compartiments du SVM que vous sélectionnez pour l'audit. Un SVM activé pour un audit peut contenir des compartiments audités et non audités.

Il est recommandé de configurer l'audit S3 pour une rotation automatique des journaux, déterminée par la taille du journal ou par une planification. Si vous ne configurez pas la rotation automatique des journaux, tous les fichiers journaux sont conservés par défaut. Vous pouvez également faire pivoter les fichiers journaux S3 manuellement à l'aide de la commande **vserver Object-store-Server audit rotate-log**.

Si le SVM est une source de reprise d'activité du SVM, le chemin de destination ne peut pas se trouver sur le volume root.

Procédure

- 1. Créez la configuration d'audit pour faire pivoter les journaux d'audit en fonction de la taille du journal ou d'une planification.

Si vous souhaitez faire pivoter les journaux d'audit en...	Entrer...
Taille du journal	<pre>vserver object-store-server audit create -vserver svm_name -destination path [[-events] {data management}, ...] [[-rotate-limit integer] [-retention-duration [integer_d] [_integer_h][_integer_m][_integers]]] [-rotate-size {integer[KB MB GB TB PB]}]</pre>
Un planning	<pre>vserver object-store-server audit create -vserver svm_name -destination path [[-events] {data management}, ...] [[-rotate-limit integer] [-retention-duration [integerd][integerh] [integerm][_integers]]] [-rotate-schedule-month chron_month] [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-day chron_dayofmonth] [-rotate-schedule-hour chron_hour] -rotate-schedule-minute chron_minute</pre> <p>Le -rotate-schedule-minute le paramètre est requis si vous configurez la rotation du journal d'audit basée sur le temps.</p>

- 2. Activation de l'audit S3 :

```
vserver object-store-server audit enable -vserver svm_name
```

Exemples

L'exemple suivant illustre une configuration d'audit qui audite tous les événements S3 (par défaut) à l'aide d'une rotation basée sur la taille. Les journaux sont stockés dans le répertoire /audit_log. La taille maximale du fichier journal est de 200 Mo. Les journaux pivotent lorsqu'ils atteignent 200 Mo de taille.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate -size 200MB
```

L'exemple suivant illustre une configuration d'audit qui audite tous les événements S3 (par défaut) à l'aide d'une rotation basée sur la taille. La taille maximale du fichier journal est de 100 Mo (valeur par défaut) et les journaux sont conservés pendant 5 jours avant leur suppression.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -retention
```

```
-duration 5d0h0m
```

L'exemple suivant crée une configuration d'audit qui audite les événements de gestion S3 et les événements d'activation de règles d'accès centrales à l'aide d'une rotation basée sur le temps. Les journaux d'audit sont pivotés tous les mois, à 12:30 tous les jours de la semaine. La limite de rotation du log est de 5.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events  
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate  
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

Sélectionnez des compartiments pour l'audit S3

Vous devez spécifier les compartiments à auditer dans une SVM activée par l'audit.

Ce dont vous avez besoin

- SVM activé pour l'audit S3.

Description de la tâche

Les configurations d'audit S3 sont activées par SVM, mais vous devez sélectionner les compartiments des SVM activés pour l'audit. Si vous ajoutez des compartiments au SVM et que vous souhaitez auditer les nouveaux compartiments, vous devez les sélectionner avec cette procédure. Vous pouvez également disposer de compartiments non audités dans une SVM activée pour l'audit de S3.

Les configurations d'audit restent conservées pour les compartiments jusqu'à ce qu'elles soient supprimées par le `vserver object-store-server audit object-select delete` commande.

Procédure

Sélectionner un compartiment pour l'audit S3 :

```
vserver object-store-server audit event-selector create -vserver svm_name -bucket  
bucket_name [[-access] {read-only|write-only|all}] [[-permission] {allow-  
only|deny-only|all}]
```

- `-access` - spécifie le type d'accès aux événements à auditer : `read-only`, `write-only` ou `all` (la valeur par défaut est `all`).
- `-permission` - spécifie le type d'autorisation d'événement à auditer : `allow-only`, `deny-only` ou `all` (la valeur par défaut est `all`).

Exemple

L'exemple suivant crée une configuration d'audit de compartiment qui connecte uniquement les événements autorisés avec un accès en lecture seule :

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1  
-bucket test-bucket -access read-only -permission allow-only
```

Modifiez une configuration d'audit S3

Vous pouvez modifier les paramètres d'audit de compartiments individuels ou la configuration d'audit de toutes les compartiments sélectionnés pour l'audit dans la SVM.

Si vous souhaitez modifier la configuration d'audit pour...	Entrer...
Seaux individuels	<code>vserver object-store-server audit event-selector modify -vserver <i>svm_name</i> [-bucket <i>bucket_name</i>] [<i>parameters to modify</i>]</code>
Tous les compartiments du SVM	<code>vserver object-store-server audit modify -vserver <i>svm_name</i> [<i>parameters to modify</i>]</code>

Exemples

L'exemple suivant modifie la configuration d'audit de compartiment individuel pour auditer uniquement les événements d'accès en écriture :

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

L'exemple suivant modifie la configuration d'audit de tous les buckets du SVM de manière à définir la taille limite des logs à 10 Mo et à conserver 3 fichiers journaux avant de faire pivoter.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

Affiche les configurations d'audit S3

Une fois la configuration d'audit terminée, vous pouvez vérifier que l'audit est correctement configuré et activé. Vous pouvez également afficher des informations sur toutes les configurations d'audit du magasin d'objets du cluster.

Description de la tâche

Vous pouvez afficher des informations sur les configurations d'audit de compartiment et SVM.

- **Godets** : utilisez le `vserver object-store-server audit event-selector show` commande

Sans aucun paramètre, la commande affiche les informations suivantes sur les compartiments de tous les SVM du cluster avec des configurations d'audit de magasin d'objets :

- Nom du SVM
- Nom du compartiment
- Valeurs d'accès et d'autorisation

- **SVM** : utilisez le `vserver object-store-server audit show` commande

Sans aucun paramètre, la commande affiche les informations suivantes sur tous les SVM du cluster avec des configurations d'audit du magasin d'objets :

- Nom du SVM

- État d'audit
- Répertoire cible

Vous pouvez spécifier le `-fields` paramètre pour spécifier les informations de configuration d'audit à afficher.

Procédure

Afficher des informations sur les configurations d'audit S3 :

Si vous souhaitez modifier la configuration pour...	Entrer...
Seaux	<code>vserver object-store-server audit event-selector show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code>
SVM	<code>vserver object-store-server audit show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code>

Exemples

L'exemple suivant affiche les informations pour un seul compartiment :

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
```

Vserver	Bucket	Access	Permission
-----	-----	-----	-----
vs1	bucket1	read-only	allow-only

L'exemple suivant affiche les informations pour toutes les compartiments d'un SVM :

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1
```

Vserver	:vs1
Bucket	:test-bucket
Access	:all
Permission	:all

L'exemple suivant affiche le nom, l'état d'audit, les types d'événements, le format du journal et le répertoire cible de tous les SVM.

```
cluster1::> vserver object-store-server audit show
```

Vserver	State	Event Types	Log Format	Target Directory
-----	-----	-----	-----	-----
vs1	false	data	json	/audit_log

L'exemple suivant affiche les noms des SVM et des détails sur le journal d'audit de tous les SVM.

```
cluster1::> vserver object-store-server audit show -log-save-details
```

Vserver	Rotation File Size	Rotation Schedule	Rotation Limit
vs1	100MB	-	0

L'exemple suivant s'affiche sous forme de liste toutes les informations de configuration d'audit relatives à tous les SVM.

```
cluster1::> vserver object-store-server audit show -instance
```

```

      Vserver: vs1
      Auditing state: true
      Log Destination Path: /audit_log
      Categories of Events to Audit: data
      Log Format: json
      Log File Size Limit: 100MB
      Log Rotation Schedule: Month: -
      Log Rotation Schedule: Day of Week: -
      Log Rotation Schedule: Day: -
      Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
      Rotation Schedules: -
      Log Files Rotation Limit: 0
      Log Retention Time: 0s
```

Authentification et contrôle d'accès

Présentation de l'authentification et du contrôle d'accès

Vous pouvez gérer l'authentification de cluster ONTAP et le contrôle d'accès aux services Web ONTAP.

À l'aide de System Manager ou de l'interface de ligne de commandes, vous pouvez contrôler et sécuriser l'accès des clients et des administrateurs au cluster et au stockage.

Si vous utilisez le Gestionnaire système classique (disponible uniquement dans ONTAP 9.7 et versions antérieures), reportez-vous à la section ["System Manager Classic \(ONTAP 9.0 à 9.7\)"](#)

Authentification et autorisation du client

ONTAP authentifie un ordinateur client et un utilisateur en vérifiant son identité avec une source de confiance. ONTAP autorise un utilisateur à accéder à un fichier ou à un répertoire en comparant les informations d'identification de l'utilisateur aux autorisations configurées sur le fichier ou le répertoire.

Authentification de l'administrateur et RBAC

Les administrateurs utilisent des comptes de connexion locaux ou distants pour s'authentifier auprès du cluster et de la machine virtuelle de stockage. Le contrôle d'accès basé sur des rôles (RBAC) détermine les commandes à laquelle un administrateur a accès.

Gestion de l'authentification administrateur et du RBAC

Authentification de l'administrateur et présentation du RBAC avec l'interface de ligne de commande

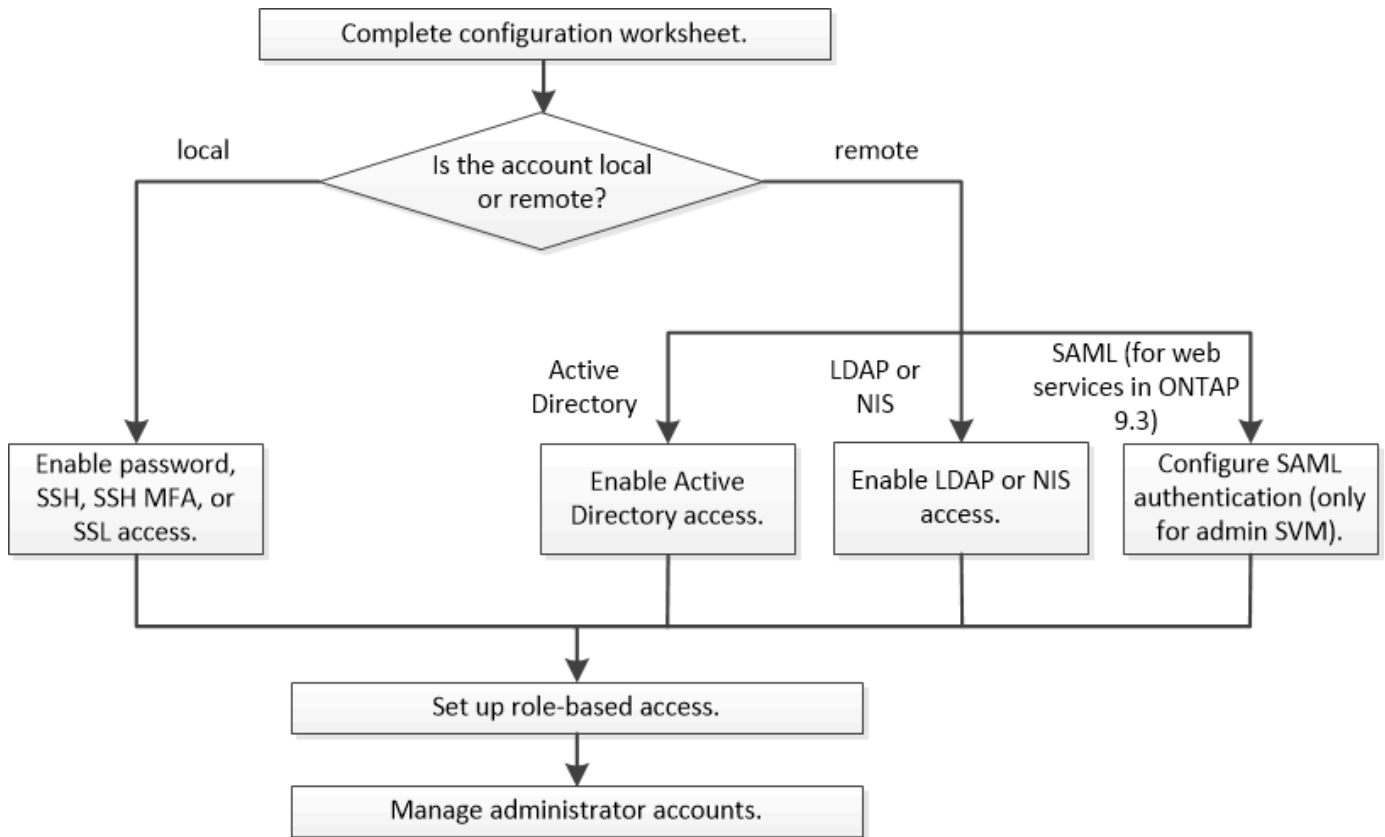
Vous pouvez activer des comptes de connexion pour les administrateurs du cluster ONTAP et des serveurs virtuels de stockage. Vous pouvez également utiliser le contrôle d'accès basé sur des rôles pour définir les fonctionnalités des administrateurs.

Vous activez les comptes de connexion et le RBAC de l'une des manières suivantes :

- Vous souhaitez utiliser l'interface de ligne de commandes ONTAP et non System Manager, ni un outil de création de scripts automatisé.
- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.
- Vous n'utilisez pas SNMP pour collecter des informations relatives au cluster.

Authentification de l'administrateur et flux de travail RBAC

Vous pouvez activer l'authentification pour les comptes d'administrateur local ou les comptes d'administrateur distant. Les informations de compte d'un compte local résident sur le système de stockage et les informations de compte d'un compte distant se trouvent ailleurs. Chaque compte peut avoir un rôle prédéfini ou un rôle personnalisé.



Vous pouvez activer les comptes d'administrateur local pour accéder à une machine virtuelle de stockage (SVM) d'administration ou à un SVM de données avec les types d'authentification suivants :

- Mot de passe
- Clé publique SSH
- Certificat SSL
- Authentification multifacteur SSH (MFA)

Depuis ONTAP 9.3, l'authentification avec mot de passe et clé publique est prise en charge.

Vous pouvez activer les comptes d'administrateur distant pour accéder à un SVM d'administration ou à un SVM de données avec les types d'authentification suivants :

- Active Directory
- Authentification SAML (uniquement pour le SVM d'administration)

Depuis ONTAP 9.3, l'authentification SAML permet d'accéder à la SVM d'administration à l'aide de l'un des services web suivants : service Processor Infrastructure, ONTAP API ou System Manager.

- Depuis la version ONTAP 9.4, l'authentification SSH MFA peut être utilisée pour les utilisateurs distants sur des serveurs LDAP ou NIS. L'authentification avec nsswitch et la clé publique est prise en charge.

Feuilles de calcul pour l'authentification de l'administrateur et la configuration du RBAC

Avant de créer des comptes de connexion et de configurer le contrôle d'accès basé sur

des rôles (RBAC), vous devez rassembler les informations de chaque élément des feuilles de configuration.

Créer ou modifier des comptes de connexion

Vous fournissez ces valeurs avec le `security login create` Lorsque vous activez les comptes de connexion pour accéder à une VM de stockage. Vous fournissez les mêmes valeurs avec le `security login modify` Lorsque vous modifiez la façon dont un compte accède à une VM de stockage.

Champ	Description	Votre valeur
<code>-vserver</code>	Nom de la VM de stockage auquel le compte accède. La valeur par défaut est le nom de la VM de stockage admin du cluster.	
<code>-user-or-group-name</code>	Nom d'utilisateur ou nom de groupe du compte. La définition d'un nom de groupe permet d'accéder à chaque utilisateur du groupe. Vous pouvez associer un nom d'utilisateur ou un nom de groupe à plusieurs applications.	
<code>-application</code>	L'application utilisée pour accéder à la VM de stockage : <ul style="list-style-type: none">• <code>http</code>• <code>ontapi</code>• <code>snmp</code>• <code>ssh</code>	

-authmethod	<p>Méthode utilisée pour authentifier le compte :</p> <ul style="list-style-type: none"> • <code>cert</code> Pour l'authentification par certificat SSL • <code>domain</code> Pour l'authentification Active Directory • <code>nsswitch</code> Pour l'authentification LDAP ou NIS • <code>password</code> pour l'authentification par mot de passe utilisateur • <code>publickey</code> pour l'authentification par clé publique • <code>community</code> Pour les chaînes de communauté SNMP • <code>usm</code> Pour le modèle de sécurité utilisateur SNMP • <code>saml</code> Pour l'authentification SAML (Security assertion Markup Language) 	
-remote-switch-ipaddress	<p>L'adresse IP du commutateur distant. Le commutateur distant peut être un commutateur de cluster surveillé par le moniteur d'état du commutateur du cluster (CSHM) ou un commutateur Fibre Channel (FC) surveillé par le moniteur d'état du MetroCluster (MCC-HM). Cette option n'est applicable que lorsque l'application est <code>snmp</code> et la méthode d'authentification est <code>usm</code>.</p>	
-role	<p>Rôle de contrôle d'accès attribué au compte :</p> <ul style="list-style-type: none"> • Pour le cluster (la VM de stockage admin), la valeur par défaut est <code>admin</code>. • Pour une VM de stockage de données, la valeur par défaut est <code>vsadmin</code>. 	

-comment	(Facultatif) texte descriptif pour le compte. Vous devez inclure le texte entre guillemets (").	
-is-ns-switch-group	Indique si le compte est un compte de groupe LDAP ou un compte de groupe NIS (yes ou no).	
-second-authentication-method	<p>Deuxième méthode d'authentification en cas d'authentification multifacteur :</p> <ul style="list-style-type: none"> • none si vous n'utilisez pas l'authentification multi-facteurs, valeur par défaut • publickey pour l'authentification par clé publique lorsque l'authmethod est un mot de passe ou un nsswitch • password pour l'authentification par mot de passe utilisateur lorsque authmethod est la clé publique • nsswitch pour l'authentification par mot de passe utilisateur lorsque la méthode d'authentification est publickey <p>L'ordre d'authentification est toujours la clé publique suivie du mot de passe.</p>	
-is-ldap-fastbind	À partir de ONTAP 9.11.1, lorsque la valeur est définie sur true, active la liaison rapide LDAP pour l'authentification nsswitch ; la valeur par défaut est false. Pour utiliser LDAP FAST bind, le -authentication-method la valeur doit être définie sur nsswitch. "Découvrez ldap fastbind pour l'authentification nsswitch."	

Configurer les informations de sécurité Cisco Duo

Vous fournissez ces valeurs avec le `security login duo create` Lorsque vous activez l'authentification à deux facteurs Cisco Duo avec des connexions SSH pour une machine virtuelle de stockage.

Champ	Description	Votre valeur
<code>-vserver</code>	La VM de stockage (appelée vServer dans l'interface de ligne de commandes ONTAP) à laquelle s'appliquent les paramètres d'authentification Duo.	
<code>-integration-key</code>	Votre clé d'intégration, obtenue lors de l'enregistrement de votre application SSH auprès de Duo.	
<code>-secret-key</code>	Votre clé secrète, obtenue lors de l'enregistrement de votre application SSH auprès de Duo.	
<code>-api-host</code>	<p>Le nom d'hôte de l'API, obtenu lors de l'enregistrement de votre application SSH auprès de Duo. Par exemple :</p> <div><pre>api- <HOSTNAME>.duosecurity.com</pre></div>	
<code>-fail-mode</code>	En cas d'erreurs de service ou de configuration qui empêchent l'authentification Duo, l'échec <code>safe</code> (autoriser l'accès) ou <code>secure</code> (refuser l'accès). La valeur par défaut est <code>safe</code> , Ce qui signifie que l'authentification Duo est ignorée si elle échoue en raison d'erreurs telles que le serveur d'API Duo inaccessible.	

-http-proxy	<p>Utilisez le proxy HTTP spécifié. Si le proxy HTTP nécessite une authentification, incluez les informations d'identification dans l'URL du proxy. Par exemple :</p> <pre>http- proxy=http://username :password@proxy.examp le.org:8080</pre>	
-autopush	<p>Soit <code>true</code> ou <code>false</code>. La valeur par défaut est <code>false</code>. Si <code>true</code>, Duo envoie automatiquement une demande de connexion Push au téléphone de l'utilisateur et revient à un appel téléphonique si Push n'est pas disponible. Notez que cela désactive efficacement l'authentification par mot de passe. Si <code>false</code>, l'utilisateur est invité à choisir une méthode d'authentification.</p> <p>Lorsqu'il est configuré avec <code>autopush = true</code>, nous recommandons le réglage <code>max-prompts = 1</code>.</p>	

<p><code>-max-prompts</code></p>	<p>Si un utilisateur ne parvient pas à s'authentifier avec un second facteur, Duo invite l'utilisateur à s'authentifier à nouveau. Cette option définit le nombre maximal d'invites affichées par Duo avant de refuser l'accès. Doit être de 1, 2, ou 3. La valeur par défaut est 1.</p> <p>Par exemple, quand <code>max-prompts = 1</code>, l'utilisateur doit s'authentifier avec succès à la première invite, tandis que si <code>max-prompts = 2</code>, si l'utilisateur saisit des informations incorrectes à l'invite initiale, il sera invité à s'authentifier à nouveau.</p> <p>Lorsqu'il est configuré avec <code>autopush = true</code>, nous recommandons le réglage <code>max-prompts = 1</code>.</p> <p>Pour la meilleure expérience, un utilisateur avec seulement l'authentification de clé publique aura toujours <code>max-prompts</code> réglé sur 1.</p>	
<p><code>-enabled</code></p>	<p>Activez l'authentification Duo à deux facteurs. Réglez sur <code>true</code> par défaut. Lorsqu'elle est activée, l'authentification Duo à deux facteurs est appliquée lors de la connexion SSH en fonction des paramètres configurés. Lorsque Duo est désactivé (défini sur <code>false</code>), l'authentification Duo est ignorée.</p>	
<p><code>-pushinfo</code></p>	<p>Cette option fournit des informations supplémentaires dans la notification Push, telles que le nom de l'application ou du service auquel vous accédez. Cela permet aux utilisateurs de vérifier qu'ils se connectent au service approprié et fournit une couche de sécurité supplémentaire.</p>	

Définissez des rôles personnalisés

Vous fournissez ces valeurs avec le `security login role create` commande lorsque vous définissez un rôle personnalisé.

Champ	Description	Votre valeur
<code>-vserver</code>	(Facultatif) nom de la VM de stockage (appelée vServer dans l'interface de ligne de commandes ONTAP) associée au rôle.	
<code>-role</code>	Nom du rôle.	
<code>-cmddirname</code>	Répertoire de la commande ou de la commande auquel le rôle donne accès. Vous devez inclure les noms des sous-répertoires de commandes entre guillemets ("). Par exemple : "volume snapshot". Vous devez entrer <code>DEFAULT</code> pour spécifier tous les répertoires de commandes.	

-access	<p>(Facultatif) le niveau d'accès du rôle. Pour les répertoires de commandes :</p> <ul style="list-style-type: none"> • <code>none</code> (la valeur par défaut pour les rôles personnalisés) refuse l'accès aux commandes dans le répertoire de commande • <code>readonly</code> permet l'accès au <code>show</code> commandes dans le répertoire de commande et ses sous-répertoires • <code>all</code> donne accès à toutes les commandes du répertoire de commande et de ses sous-répertoires <p>Pour <i>commandes non intrinsèques</i> (commandes qui ne se terminent pas dans <code>create</code>, <code>modify</code>, <code>delete</code>, ou <code>show</code>) :</p> <ul style="list-style-type: none"> • <code>none</code> (la valeur par défaut pour les rôles personnalisés) refuse l'accès à la commande • <code>readonly</code> n'est pas applicable • <code>all</code> accorde l'accès à la commande <p>Pour accorder ou refuser l'accès aux commandes intrinsèques, vous devez spécifier le répertoire de commande.</p>	
-query	<p>(Facultatif) l'objet de requête utilisé pour filtrer le niveau d'accès, qui est spécifié sous la forme d'une option valide pour la commande ou d'une commande dans le répertoire de commandes. Vous devez inclure l'objet de requête entre guillemets ("). Par exemple, si le répertoire de commande est <code>volume</code>, l'objet requête <code>"-aggr aggr0"</code> activation de l'accès pour le système <code>aggr0</code> agrégat uniquement.</p>	

Associer une clé publique à un compte d'utilisateur

Vous fournissez ces valeurs avec le `security login publickey create` Commande lorsque vous associez une clé publique SSH à un compte d'utilisateur.

Champ	Description	Votre valeur
<code>-vserver</code>	(Facultatif) Nom de la VM de stockage auquel le compte accède.	
<code>-username</code>	Nom d'utilisateur du compte. La valeur par défaut, <code>admin</code> , qui est le nom par défaut de l'administrateur du cluster.	
<code>-index</code>	Numéro d'index de la clé publique. La valeur par défaut est 0 si la clé est la première clé créée pour le compte ; sinon, la valeur par défaut est un plus que le numéro d'index existant le plus élevé pour le compte.	
<code>-publickey</code>	Clé publique OpenSSH. Vous devez inclure la clé entre guillemets (").	
<code>-role</code>	Rôle de contrôle d'accès attribué au compte.	
<code>-comment</code>	(Facultatif) texte descriptif pour la clé publique. Vous devez inclure le texte entre guillemets (").	

-x509-certificate	<p>(Facultatif) à partir de ONTAP 9.13.1, vous permet de gérer l'association de certificats X.509 avec la clé publique SSH.</p> <p>Lorsque vous associez un certificat X.509 à la clé publique SSH, ONTAP vérifie lors de la connexion SSH si ce certificat est valide. S'il a expiré ou a été révoqué, la connexion est interdite et la clé publique SSH associée est désactivée. Valeurs possibles :</p> <ul style="list-style-type: none"> • <code>install</code>: Installez le certificat X.509 codé PEM spécifié et associez-le à la clé publique SSH. Incluez le texte intégral du certificat que vous souhaitez installer. • <code>modify</code>: Mettez à jour le certificat X.509 codé PEM existant avec le certificat spécifié et associez-le à la clé publique SSH. Inclure le texte complet du nouveau certificat. • <code>delete</code>: Supprimez l'association de certificat X.509 existante avec la clé publique SSH. 	
-------------------	--	--

Configurer les paramètres globaux d'autorisation dynamique

À partir de ONTAP 9.15.1, vous fournissez ces valeurs avec `security dynamic-authorization modify` commande. Pour plus d'informations sur la configuration d'autorisation dynamique, reportez-vous à la section ["présentation de l'autorisation dynamique"](#).

Champ	Description	Votre valeur
-vserver	Nom de la machine virtuelle de stockage pour laquelle le paramètre de score de confiance doit être modifié. Si vous omettez ce paramètre, le paramètre de niveau du cluster est utilisé.	

-state	<p>Le mode d'autorisation dynamique. Valeurs possibles :</p> <ul style="list-style-type: none"> • disabled: (Par défaut) l'autorisation dynamique est désactivée. • visibility: Ce mode est utile pour tester l'autorisation dynamique. Dans ce mode, le score de confiance est vérifié avec chaque activité restreinte, mais pas appliqué. Cependant, toute activité qui aurait été refusée ou qui aurait fait l'objet de défis d'authentification supplémentaires est consignée. • enforced: Destiné à être utilisé après avoir terminé les tests avec visibility mode. Dans ce mode, le score de confiance est vérifié pour chaque activité restreinte et les restrictions d'activité sont appliquées si les conditions de restriction sont remplies. L'intervalle de suppression est également appliqué, ce qui évite des problèmes d'authentification supplémentaires dans l'intervalle spécifié. 	
-suppression-interval	<p>Empêche des problèmes d'authentification supplémentaires dans l'intervalle spécifié. L'intervalle est au format ISO-8601 et accepte des valeurs comprises entre 1 minute et 1 heure. Si la valeur est définie sur 0, l'intervalle de suppression est désactivé et l'utilisateur est toujours invité à effectuer une vérification d'authentification si nécessaire.</p>	
-lower-challenge-boundary	<p>Limite inférieure de pourcentage de défi pour l'authentification multifacteur (MFA). La plage valide est comprise entre 0 et 99. La valeur 100 n'est pas valide, car toutes les demandes sont refusées. La valeur par défaut est 0.</p>	

-upper-challenge-boundary	Limite supérieure de pourcentage de défi MFA. La plage valide est comprise entre 0 et 100. Cette valeur doit être égale ou supérieure à la valeur de la limite inférieure. Une valeur de 100 signifie que chaque demande sera refusée ou soumise à un défi d'authentification supplémentaire ; aucune demande n'est autorisée sans défi. La valeur par défaut est 90.	
---------------------------	---	--

Installez un certificat numérique de serveur signé par une autorité de certification

Vous fournissez ces valeurs avec le `security certificate generate-csr` Lorsque vous générez une requête de signature de certificat numérique (RSC) à utiliser pour authentifier une machine virtuelle de stockage en tant que serveur SSL.

Champ	Description	Votre valeur
-common-name	Nom du certificat, qui est soit un nom de domaine complet (FQDN) ou un nom commun personnalisé.	
-size	Nombre de bits dans la clé privée. Plus la valeur est élevée, plus la clé est sécurisée. La valeur par défaut est 2048. Les valeurs possibles sont 512, 1024, 1536, et 2048.	
-country	Pays de la machine virtuelle de stockage, sous un code à deux lettres. La valeur par défaut est US. Consultez les pages de manuel pour obtenir une liste de codes.	
-state	État ou province de la machine virtuelle de stockage.	
-locality	Localité de la VM de stockage.	
-organization	Organisation de la machine virtuelle de stockage.	
-unit	Unité dans l'organisation de la machine virtuelle de stockage.	

<code>-email-addr</code>	Adresse e-mail de l'administrateur du contact pour la machine virtuelle de stockage.	
<code>-hash-function</code>	Fonction de hachage cryptographique pour la signature du certificat. La valeur par défaut est SHA256. Les valeurs possibles sont SHA1, SHA256, et MD5.	

Vous fournissez ces valeurs avec le `security certificate install` Lorsque vous installez un certificat numérique signé par une autorité de certification pour l'authentification du cluster ou de la machine virtuelle de stockage en tant que serveur SSL. Seules les options pertinentes pour la configuration des comptes sont présentées dans le tableau suivant.

Champ	Description	Votre valeur
<code>-vserver</code>	Nom de la machine virtuelle de stockage sur laquelle le certificat doit être installé.	
<code>-type</code>	<p>Le type de certificat :</p> <ul style="list-style-type: none"> • <code>server</code> pour les certificats de serveur et les certificats intermédiaires • <code>client-ca</code> Pour le certificat de clé publique de l'autorité de certification racine du client SSL • <code>server-ca</code> Pour le certificat de clé publique de l'autorité de certification racine du serveur SSL dont ONTAP est un client • <code>client</code> Pour un certificat numérique et une clé privée auto-signés ou signés par une autorité de certification pour ONTAP en tant que client SSL 	

Configurez l'accès au contrôleur de domaine Active Directory

Vous fournissez ces valeurs avec le `security login domain-tunnel create` Commande lorsque vous avez déjà configuré un serveur SMB pour une machine virtuelle de stockage de données et que vous souhaitez configurer la machine virtuelle de stockage en tant que passerelle ou *tunnel* pour l'accès du contrôleur de domaine Active Directory au cluster.

Champ	Description	Votre valeur
-------	-------------	--------------

<code>-vserver</code>	Nom de la VM de stockage pour laquelle le serveur SMB a été configuré.	
-----------------------	--	--

Vous fournissez ces valeurs avec le `vserver active-directory create` Lorsque vous n'avez pas configuré de serveur SMB et que vous souhaitez créer un compte d'ordinateur de machine virtuelle de stockage sur le domaine Active Directory.


Champ	Description	Votre valeur
<code>-vserver</code>	Nom de la machine virtuelle de stockage pour laquelle vous souhaitez créer un compte d'ordinateur Active Directory.	
<code>-account-name</code>	Nom NetBIOS du compte ordinateur.	
<code>-domain</code>	Le nom de domaine complet (FQDN).	
<code>-ou</code>	Unité organisationnelle du domaine. La valeur par défaut est <code>CN=Computers</code> . ONTAP ajoute cette valeur au nom de domaine pour produire le nom distinctif d'Active Directory.	

Configurez l'accès aux serveurs LDAP ou NIS

Vous fournissez ces valeurs avec le `vserver services name-service ldap client create` Lorsque vous créez une configuration client LDAP pour la VM de stockage.

Seules les options pertinentes pour la configuration des comptes sont affichées dans le tableau suivant :

Champ	Description	Votre valeur
<code>-vserver</code>	Nom de la VM de stockage pour la configuration client.	
<code>-client-config</code>	Nom de la configuration client.	
<code>-ldap-servers</code>	Liste séparée par des virgules d'adresses IP et de noms d'hôte pour les serveurs LDAP auxquels le client se connecte.	

-schema	Schéma utilisé par le client pour effectuer des requêtes LDAP.	
-use-start-tls	<p>Si le client utilise Start TLS pour chiffrer la communication avec le serveur LDAP (<code>true</code> ou <code>false</code>).</p> <div>  <p>Le protocole Start TLS est pris en charge uniquement pour l'accès aux machines virtuelles de stockage de données. Elle n'est pas prise en charge pour l'accès aux machines virtuelles de stockage d'administration.</p> </div>	

Vous fournissez ces valeurs avec le `vserver services name-service ldap create` Lorsque vous associez une configuration client LDAP à la machine virtuelle de stockage.

Champ	Description	Votre valeur
-vserver	Nom de la machine virtuelle de stockage à laquelle la configuration client doit être associée.	
-client-config	Nom de la configuration client.	
-client-enabled	Indique si la VM de stockage peut utiliser la configuration client LDAP (<code>true</code> ou <code>false</code>).	

Vous fournissez ces valeurs avec le `vserver services name-service nis-domain create` Lorsque vous créez une configuration de domaine NIS sur une machine virtuelle de stockage.

Champ	Description	Votre valeur
-vserver	Nom de la machine virtuelle de stockage sur laquelle la configuration de domaine doit être créée.	
-domain	Le nom du domaine.	

-active	Indique si le domaine est actif (true ou false).	
-servers	ONTAP 9.0, 9.1 : liste séparée par des virgules d'adresses IP pour les serveurs NIS utilisés par la configuration de domaine.	
-nis-servers	Liste séparée par des virgules d'adresses IP et de noms d'hôte pour les serveurs NIS utilisés par la configuration de domaine.	

Vous fournissez ces valeurs avec le `vserver services name-service ns-switch create` commande lorsque vous spécifiez l'ordre de recherche des sources de service de noms.

Champ	Description	Votre valeur
-vserver	Nom de la machine virtuelle de stockage sur laquelle l'ordre de recherche de service de noms doit être configuré.	
-database	La base de données du service de noms : <ul style="list-style-type: none"> • <code>hosts</code> Pour les services de noms DNS et de fichiers • <code>group</code> Pour les fichiers, LDAP et services de noms NIS • <code>passwd</code> Pour les fichiers, LDAP et services de noms NIS • <code>netgroup</code> Pour les fichiers, LDAP et services de noms NIS • <code>namemap</code> Pour les fichiers et les services de noms LDAP 	
-sources	Ordre dans lequel rechercher les sources de service de noms (dans une liste séparée par des virgules) : <ul style="list-style-type: none"> • <code>files</code> • <code>dns</code> • <code>ldap</code> • <code>nis</code> 	

Configurez l'accès SAML

À partir de ONTAP 9.3, vous fournissez ces valeurs à `security saml-sp create` Commande pour configurer l'authentification SAML.

Champ	Description	Votre valeur
<code>-idp-uri</code>	Adresse FTP ou adresse HTTP de l'hôte IDP (Identity Provider) à partir duquel les métadonnées IDP peuvent être téléchargées.	
<code>-sp-host</code>	Nom d'hôte ou adresse IP de l'hôte SAML Service Provider (système ONTAP). Par défaut, l'adresse IP de la LIF de cluster-management est utilisée.	
<code>-cert-ca</code> et <code>-cert-serial</code> , ou <code>-cert-common-name</code>	Détails du certificat de serveur de l'hôte du fournisseur de services (système ONTAP). Vous pouvez saisir soit le certificat du fournisseur de services émettant l'autorité de certification (CA) et le numéro de série du certificat, soit le nom commun du certificat de serveur.	
<code>-verify-metadata-server</code>	Indique si l'identité du serveur de métadonnées IDP doit être validée (<code>true</code> ou <code>false</code>). Il est recommandé de toujours définir cette valeur sur <code>true</code> .	

Créer des comptes de connexion

Présentation de la création de comptes de connexion

Vous pouvez activer les comptes d'administrateur des clusters et des SVM locaux ou distants. Un compte local est un compte dans lequel les informations de compte, la clé publique ou le certificat de sécurité résident sur le système de stockage. Les informations de compte AD sont stockées sur un contrôleur de domaine. Les comptes LDAP et NIS résident sur des serveurs LDAP et NIS.

Administrateurs Cluster et SVM

Un *cluster Administrator* accède au SVM d'admin pour le cluster. La SVM d'admin et un administrateur du cluster avec le nom réservé `admin` sont automatiquement créées lorsque le cluster est configuré.

Un administrateur de cluster avec la valeur par défaut `admin` le rôle peut administrer l'ensemble du cluster et ses ressources. L'administrateur du cluster peut créer d'autres administrateurs de cluster disposant de

différents rôles selon les besoins.

Un *administrateur SVM* accède à un SVM de données. L'administrateur du cluster crée des SVM de données et des administrateurs SVM si nécessaire.

Les administrateurs du SVM sont affectés à `vsadmin` rôle par défaut. L'administrateur du cluster peut attribuer différents rôles aux administrateurs du SVM si nécessaire.

Respecter les conventions de nom

Les noms génériques suivants ne peuvent pas être utilisés pour les comptes d'administrateur du cluster distant et du SVM :

- « adm »
- « bac »
- « cli »
- « démon »
- « ftp »
- « jeux »
- « arrêter »
- « lp »
- « courrier »
- « homme »
- « naroot »
- « NetApp »
- « actualités »
- « personne »
- « opérateur »
- « racine »
- « arrêt »
- « sshd »
- « sync »
- « sys »
- « uuucp »
- « www »

Rôles fusionnés

Si vous activez plusieurs comptes distants pour le même utilisateur, l'utilisateur est affecté à l'Union de tous les rôles spécifiés pour les comptes. C'est-à-dire, si un compte LDAP ou NIS est affecté à `vsadmin` Et le compte de groupe AD pour le même utilisateur est affecté à `vsadmin-volume` Rôle, l'utilisateur AD se connecte avec les fonctions plus inclusives `vsadmin` capacités. Les rôles sont définis comme *fusionnés*.

Activez l'accès au compte local

Activer la présentation de l'accès au compte local

Un compte local est un compte dans lequel les informations de compte, la clé publique ou le certificat de sécurité résident sur le système de stockage. Vous pouvez utiliser le `security login create` Commande pour permettre aux comptes locaux d'accéder à un admin ou un SVM de données.

Activer l'accès au compte par mot de passe

Vous pouvez utiliser le `security login create` Commande permettant aux comptes d'administrateur d'accéder à un admin ou un SVM de données avec un mot de passe. Après avoir saisi la commande, vous êtes invité à saisir le mot de passe.

Description de la tâche

Si vous n'êtes pas certain du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser le `security login modify` commande permettant d'ajouter le rôle ultérieurement.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étape

1. Activer les comptes d'administrateur local pour accéder à un SVM via un mot de passe :

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

La commande suivante active le compte d'administrateur du cluster admin1 avec le prédéfini backup Rôle d'accès à la SVM d'adminengCluster à l'aide d'un mot de passe. Après avoir saisi la commande, vous êtes invité à saisir le mot de passe.

```
cluster1::>security login create -vserver engCluster -user-or-group-name  
admin1 -application ssh -authmethod password -role backup
```

Activez les comptes de clé publique SSH

Vous pouvez utiliser le `security login create` Commande permettant aux comptes d'administrateur d'accéder à un SVM de données ou admin avec une clé publique SSH.

Description de la tâche

- Vous devez associer la clé publique au compte avant que le compte puisse accéder à la SVM.

[Association d'une clé publique à un compte d'utilisateur](#)

Vous pouvez effectuer cette tâche avant ou après avoir activé l'accès au compte.

- Si vous n'êtes pas certain du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser le `security login modify` commande permettant d'ajouter le rôle ultérieurement.

Si vous souhaitez activer le mode FIPS sur votre cluster, vous devez reconfigurer les comptes de clés publiques SSH existants sans les algorithmes de clé pris en charge avec un type de clé pris en charge. Les comptes doivent être reconfigurés avant l'activation de FIPS, sinon l'authentification de l'administrateur échouera.

Le tableau suivant indique les algorithmes de type de clé hôte pris en charge pour les connexions ONTAP SSH. Ces types de clés ne s'appliquent pas à la configuration de l'authentification publique SSH.

Version de ONTAP	Types de clés pris en charge en mode FIPS	Types de clés pris en charge en mode non FIPS
9.11.1 et versions ultérieures	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 et versions antérieures	ecdsa-sha2-nistp256 ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss ssh-rsa



La prise en charge de l'algorithme de clé hôte ssh-ed25519 a été supprimée à partir de ONTAP 9.11.1.

Pour plus d'informations, voir ["Configurez la sécurité réseau à l'aide de FIPS"](#).

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étape

1. Activer les comptes d'administrateur local pour accéder à un SVM à l'aide d'une clé publique SSH :

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role role -comment
comment
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

La commande suivante active le compte d'administrateur du SVM `svmadmin1` avec le prédéfini `vsadmin-volume` Rôle d'accès à la `SVMengData1` Utilisation d'une clé publique SSH :

```
cluster1::>security login create -vserver engData1 -user-or-group-name
svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
```

Une fois que vous avez terminé

Si vous n'avez pas associé de clé publique au compte administrateur, vous devez le faire avant que le compte puisse accéder à la SVM.

[Association d'une clé publique à un compte d'utilisateur](#)

Activez les comptes d'authentification multifacteur (MFA)

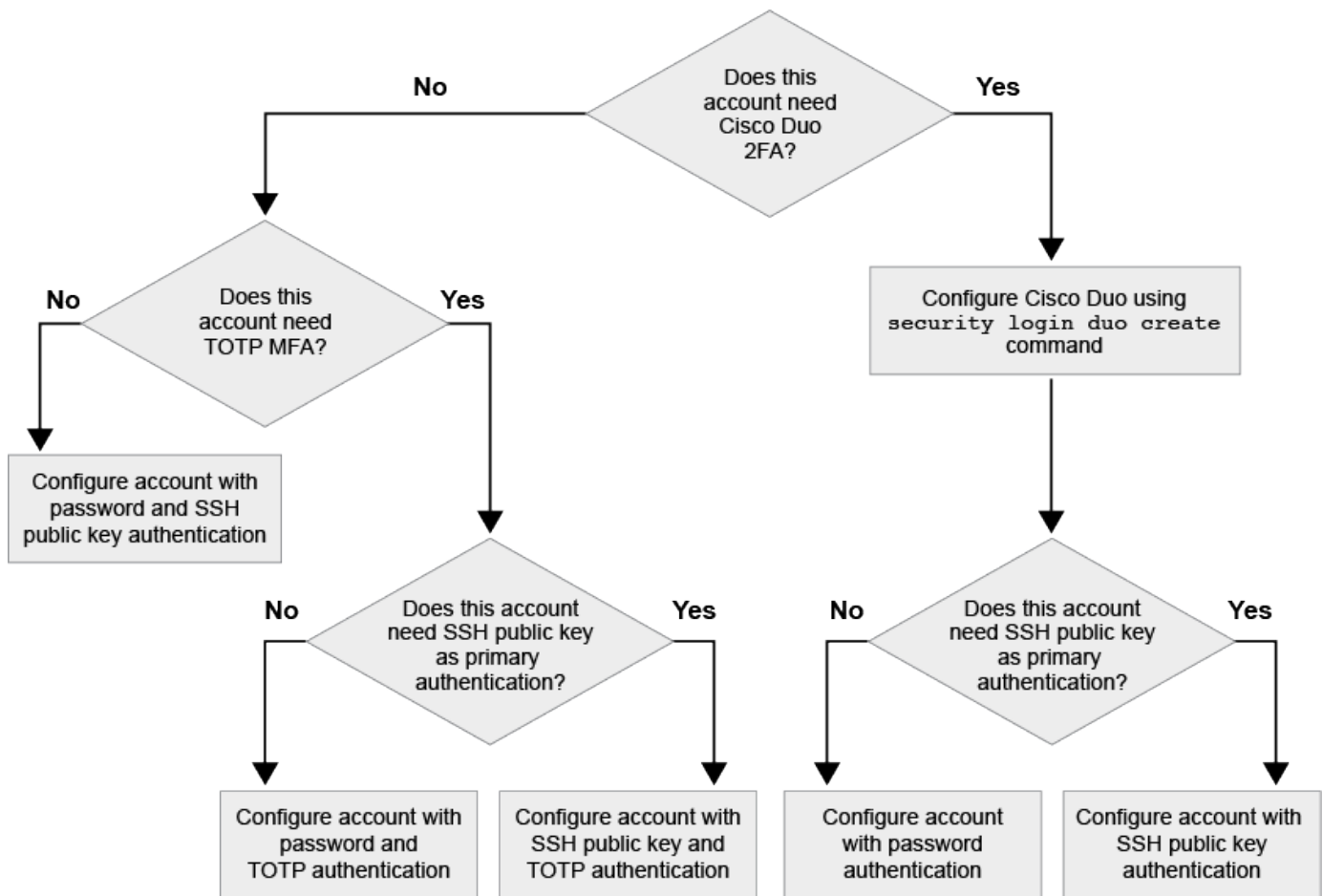
Présentation de l'authentification multifacteur

L'authentification multifacteur (MFA) vous permet d'améliorer la sécurité en exigeant que les utilisateurs fournissent deux méthodes d'authentification pour se connecter à un administrateur ou à une VM de stockage des données.

Selon votre version de ONTAP, vous pouvez utiliser une clé publique SSH, un mot de passe utilisateur et un mot de passe à usage unique (TOTP) pour l'authentification multifacteur. Lorsque vous activez et configurez Cisco Duo (ONTAP 9.14.1 et versions ultérieures), il sert de méthode d'authentification supplémentaire, en complément des méthodes existantes pour tous les utilisateurs.

Disponible à partir de...	Première méthode d'authentification	Deuxième méthode d'authentification
ONTAP 9.14.1	Clé publique SSH	TOTP
	Mot de passe utilisateur	TOTP
	Clé publique SSH	Duo Cisco
	Mot de passe utilisateur	Duo Cisco
ONTAP 9.13.1	Clé publique SSH	TOTP
	Mot de passe utilisateur	TOTP
ONTAP 9.3	Clé publique SSH	Mot de passe utilisateur

Si l'authentification multifacteur est configurée, l'administrateur du cluster doit d'abord activer le compte utilisateur local. Le compte doit alors être configuré par l'utilisateur local.



Activez l'authentification multifacteur

L'authentification multifacteur (MFA) vous permet d'améliorer la sécurité en exigeant que les utilisateurs fournissent deux méthodes d'authentification pour se connecter à un administrateur ou à un SVM de données.

Description de la tâche

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Si vous n'êtes pas certain du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser le `security login modify` commande permettant d'ajouter le rôle ultérieurement.

"Modification du rôle attribué à un administrateur"

- Si vous utilisez une clé publique pour l'authentification, vous devez associer la clé publique au compte avant que le compte puisse accéder à la SVM.

"Associer une clé publique à un compte d'utilisateur"

Vous pouvez effectuer cette tâche avant ou après avoir activé l'accès au compte.

- À partir de ONTAP 9.12.1, vous pouvez utiliser les périphériques d'authentification matérielle Yubikey pour le client SSH MFA en utilisant les normes d'authentification FIDO2 (Fast Identity Online) ou PIV (Personal Identity Verification).

Activez MFA avec la clé publique SSH et le mot de passe utilisateur

Depuis la version ONTAP 9.3, l'administrateur du cluster peut configurer des comptes utilisateurs locaux pour se connecter à MFA à l'aide d'une clé publique SSH et d'un mot de passe utilisateur.

1. Activer MFA sur le compte utilisateur local avec la clé publique SSH et le mot de passe utilisateur :

```
security login create -vserver <svm_name> -user-or-group-name  
<user_name> -application ssh -authentication-method <password|publickey>  
-role admin -second-authentication-method <password|publickey>
```

La commande suivante nécessite un compte d'administrateur du SVM admin2 avec le prédéfini admin Rôle de connexion à la SVMengData1 Avec une clé publique SSH et un mot de passe utilisateur :

```
cluster-1::> security login create -vserver engData1 -user-or-group-name  
admin2 -application ssh -authentication-method publickey -role admin  
-second-authentication-method password
```

Please enter a password for user 'admin2':

Please enter it again:

Warning: To use public-key authentication, you must create a public key
for user "admin2".

Activez MFA avec TOTP

À partir de ONTAP 9.13.1, vous pouvez améliorer la sécurité en exigeant des utilisateurs locaux qu'ils se connectent à un administrateur ou à un SVM de données à l'aide d'une clé publique SSH ou d'un mot de passe utilisateur et d'un mot de passe à usage unique (TOTP) basé sur le temps. Une fois le compte activé pour MFA avec TOTP, l'utilisateur local doit se connecter à [terminez la configuration](#).

TOTP est un algorithme informatique qui utilise l'heure actuelle pour générer un mot de passe à usage unique. Si TOTP est utilisé, il s'agit toujours de la deuxième forme d'authentification après la clé publique SSH ou le mot de passe utilisateur.

Avant de commencer

Vous devez être administrateur du stockage pour effectuer ces tâches.

Étapes

Vous pouvez configurer MFA avec un mot de passe utilisateur ou une clé publique SSH comme première méthode d'authentification et TOTP comme deuxième méthode d'authentification.

Activer MFA avec mot de passe utilisateur et TOTP

1. Activez un compte utilisateur pour l'authentification multifacteur avec un mot de passe utilisateur et un TOTP.

Pour les nouveaux comptes utilisateur

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

Pour les comptes utilisateur existants

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

2. Vérifier que MFA avec TOTP est activé :

```
security login show
```

Activez MFA avec clé publique SSH et TOTP

1. Activez un compte utilisateur pour l'authentification multifacteur avec une clé publique SSH et un TOTP.

Pour les nouveaux comptes utilisateur

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

Pour les comptes utilisateur existants

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

2. Vérifier que MFA avec TOTP est activé :

```
security login show
```

Une fois que vous avez terminé

- Si vous n'avez pas associé de clé publique au compte administrateur, vous devez le faire avant que le compte puisse accéder à la SVM.

["Association d'une clé publique à un compte d'utilisateur"](#)

- L'utilisateur local doit se connecter pour terminer la configuration MFA avec TOTP.

["Configurer le compte utilisateur local pour MFA avec TOTP"](#)

Informations associées

En savoir plus sur ["Authentification multifactorielle dans ONTAP 9 \(TR-4647\)"](#).

Configurer le compte utilisateur local pour MFA avec TOTP

À partir de la ONTAP 9.13.1, les comptes utilisateur peuvent être configurés avec l'authentification multifacteur (MFA) avec un mot de passe à usage unique (TOTP).

Avant de commencer

- L'administrateur du stockage doit ["Activez MFA avec TOTP"](#) comme deuxième méthode d'authentification pour votre compte utilisateur.
- La méthode d'authentification de votre compte utilisateur principal doit être un mot de passe utilisateur ou une clé SSH publique.
- Vous devez configurer votre application TOTP pour qu'elle fonctionne avec votre smartphone et créer votre clé secrète TOTP.

TOTP est pris en charge par diverses applications d'authentificateur telles que Google Authenticator.

Étapes

1. Connectez-vous à votre compte utilisateur avec votre méthode d'authentification actuelle.

Votre méthode d'authentification actuelle doit être un mot de passe utilisateur ou une clé publique SSH.

2. Créez la configuration TOTP sur votre compte :

```
security login totp create -vserver "<svm_name>" -username  
"<account_username >"
```

3. Vérifiez que la configuration TOTP est activée sur votre compte :

```
security login totp show -vserver "<svm_name>" -username  
"<account_username>"
```

Réinitialiser la clé secrète TOTP

Pour protéger la sécurité de votre compte, si votre clé secrète TOTP est compromise ou perdue, vous devez la désactiver et en créer une nouvelle.

Réinitialisez le TOTP si votre clé est compromise

Si votre clé secrète TOTP est compromise, mais que vous y avez toujours accès, vous pouvez supprimer la clé compromise et en créer une nouvelle.

1. Connectez-vous à votre compte utilisateur avec votre mot de passe utilisateur ou votre clé publique SSH et votre clé secrète TOTP compromise.
2. Supprimez la clé secrète TOTP compromise :

```
security login totp delete -vserver <svm_name> -username  
<account_username>
```

3. Créez une nouvelle clé secrète TOTP :

```
security login totp create -vserver <svm_name> -username  
<account_username>
```

4. Vérifiez que la configuration TOTP est activée sur votre compte :

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

Réinitialisez le TOTP en cas de perte de votre clé

Si votre clé secrète TOTP est perdue, contactez votre administrateur de stockage à l'adresse ["faites désactiver la clé"](#). Une fois votre clé désactivée, vous pouvez utiliser votre première méthode d'authentification pour vous connecter et configurer un nouveau TOTP.

Avant de commencer

La clé secrète TOTP doit être désactivée par un administrateur de stockage.

Si vous ne possédez pas de compte d'administrateur de stockage, contactez votre administrateur de stockage pour que la clé soit désactivée.

Étapes

1. Une fois le secret TOTP désactivé par un administrateur de stockage, utilisez votre méthode d'authentification principale pour vous connecter à votre compte local.
2. Créez une nouvelle clé secrète TOTP :

```
security login totp create -vserver <svm_name> -username  
<account_username >
```

3. Vérifiez que la configuration TOTP est activée sur votre compte :

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

Désactiver la clé secrète TOTP pour le compte local

Si la clé secrète TOTP (Time-based password) d'un utilisateur local est perdue, la clé perdue doit être désactivée par un administrateur de stockage avant que l'utilisateur puisse créer une nouvelle clé secrète TOTP.

Description de la tâche

Cette tâche ne peut être effectuée qu'à partir d'un compte d'administrateur de cluster.

Étape

1. Désactiver la clé secrète TOTP :

```
security login totp delete -vserver "<svm_name>" -username  
"<account_username>"
```

Activez les comptes de certificat SSL

Vous pouvez utiliser le `security login create` Commande pour permettre aux comptes d'administrateur d'accéder à un SVM d'administration ou de données avec un certificat SSL.

Description de la tâche

- Vous devez installer un certificat numérique de serveur signé par une autorité de certification pour que le compte puisse accéder à la SVM.

[Génération et installation d'un certificat de serveur signé par une autorité de certification](#)

Vous pouvez effectuer cette tâche avant ou après avoir activé l'accès au compte.

- Si vous n'êtes pas certain du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez ajouter le rôle ultérieurement avec le `security login modify` commande.

[Modification du rôle attribué à un administrateur](#)



Pour les comptes d'administrateur de cluster, l'authentification par certificat est prise en charge avec `http`, `ontapi`, et `rest` en termes de latence. Pour les comptes d'administrateur SVM, l'authentification par certificat est prise en charge uniquement avec `ontapi` et `rest` en termes de latence.

Étape

1. Activer les comptes d'administrateur local pour accéder à un SVM à l'aide d'un certificat SSL :

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

Pour obtenir la syntaxe complète de la commande, reportez-vous à la ["Pages de manuel ONTAP par version"](#).

La commande suivante active le compte d'administrateur du SVM `svmadmin2` avec la valeur par défaut `vsadmin` Rôle d'accès à la SVM `engData2` Utilisation d'un certificat numérique SSL.

```
cluster1::>security login create -vserver engData2 -user-or-group-name  
svmadmin2 -application ontapi -authmethod cert
```

Une fois que vous avez terminé

Si vous n'avez pas installé de certificat numérique serveur signé par une autorité de certification, vous devez le faire avant que le compte puisse accéder à la SVM.

Génération et installation d'un certificat de serveur signé par une autorité de certification

Activez l'accès au compte Active Directory

Vous pouvez utiliser le `security login create` Commande pour permettre aux utilisateurs ou groupes Active Directory (AD) d'accéder à un SVM d'administration ou de données. Tout utilisateur du groupe AD peut accéder à la SVM avec le rôle attribué au groupe.

Description de la tâche

- Vous devez configurer l'accès du contrôleur AD domain au cluster ou au SVM avant que le compte ne puisse accéder au SVM.

Configuration de l'accès au contrôleur de domaine Active Directory

Vous pouvez effectuer cette tâche avant ou après avoir activé l'accès au compte.

- À partir de ONTAP 9.13.1, vous pouvez utiliser une clé publique SSH comme méthode d'authentification principale ou secondaire avec un mot de passe utilisateur AD.

Si vous choisissez d'utiliser une clé publique SSH comme authentification principale, aucune authentification AD n'a lieu.

- Vous pouvez utiliser ONTAP 9.11.1 depuis ["LDAP Fast bind pour l'authentification nsswitch"](#) S'il est pris en charge par le serveur LDAP AD.

- Si vous n'êtes pas certain du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser le `security login modify` commande permettant d'ajouter le rôle ultérieurement.

Modification du rôle attribué à un administrateur



L'accès au compte du groupe D'ANNONCES est pris en charge uniquement avec le `SSH`, `ontapi`, et `rest` en termes de latence. Les groupes AD ne sont pas pris en charge avec l'authentification de clé publique `SSH`, qui est couramment utilisée pour l'authentification multifacteur.

Avant de commencer

- L'heure du cluster doit être synchronisée sur dans les cinq minutes qui suivent l'heure sur le contrôleur de domaine AD.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étape

1. Activer les comptes d'utilisateur ou d'administrateur de groupe AD pour accéder à un SVM :

Pour les utilisateurs AD :

Version ONTAP	Authentification principale	Authentification secondaire	Commande
9.13.1 et versions ultérieures	Clé publique	Aucune	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role></pre>

Version ONTAP	Authentification principale	Authentification secondaire	Commande
9.13.1 et versions ultérieures	Domaine	Clé publique	<p>Pour un nouvel utilisateur</p> <pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre> <p>Pour un utilisateur existant</p> <pre>security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre>
9.0 et versions ultérieures	Domaine	Aucune	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap- fastbind true]</pre>

Pour les groupes AD :

Version ONTAP	Authentification principale	Authentification secondaire	Commande
9.0 et versions ultérieures	Domaine	Aucune	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap- fastbind true]</pre>

Pour connaître la syntaxe complète des commandes, voir ["Feuilles de travail pour l'authentification administrateur et la configuration RBAC"](#)

Une fois que vous avez terminé

Si vous n'avez pas configuré l'accès au contrôleur AD domain au cluster ou au SVM, vous devez le faire avant que le compte puisse accéder au SVM.

Configuration de l'accès au contrôleur de domaine Active Directory

Activez l'accès aux comptes LDAP ou NIS

Vous pouvez utiliser le `security login create` Commande pour activer les comptes utilisateur LDAP ou NIS pour accéder à un SVM de données ou admin Si vous n'avez pas configuré l'accès au serveur LDAP ou NIS au SVM, vous devez le faire avant que le compte puisse accéder à la SVM.

Description de la tâche

- Les comptes de groupe ne sont pas pris en charge.
- Vous devez configurer l'accès des serveurs LDAP ou NIS au SVM avant que le compte ne puisse accéder au SVM.

Configuration de l'accès aux serveurs LDAP ou NIS

Vous pouvez effectuer cette tâche avant ou après avoir activé l'accès au compte.

- Si vous n'êtes pas certain du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser le `security login modify` commande permettant d'ajouter le rôle ultérieurement.

Modification du rôle attribué à un administrateur

- Depuis la version ONTAP 9.4, l'authentification multifacteur (MFA) est prise en charge pour les utilisateurs distants sur des serveurs LDAP ou NIS.
- Vous pouvez utiliser ONTAP 9.11.1 depuis ["LDAP Fast bind pour l'authentification nsswitch"](#) S'il est pris en charge par le serveur LDAP.
- En raison d'un problème LDAP connu, vous ne devez pas utiliser le ' : ' (Deux-points) dans n'importe quel champ d'informations de compte d'utilisateur LDAP (par exemple, `gecos`, `userPassword`, etc.). Dans le cas contraire, l'opération de recherche échoue pour cet utilisateur.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étapes

1. Activer les comptes utilisateurs ou groupes LDAP ou NIS pour accéder à un SVM :

```
security login create -vserver SVM_name -user-or-group-name user_name
-application application -authmethod nsswitch -role role -comment comment -is
-ns-switch-group yes|no [-is-ldap-fastbind true]
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

"Création ou modification de comptes de connexion"

La commande suivante active le compte d'administrateur de cluster LDAP ou NIS `guest2` avec le prédéfini `backup` Rôle d'accès à la SVM d'`adminengCluster`.

```
cluster1::>security login create -vserver engCluster -user-or-group-name
guest2 -application ssh -authmethod nsswitch -role backup
```

2. Activer la connexion MFA pour les utilisateurs LDAP ou NIS :

```
security login modify -user-or-group-name rem_usr1 -application ssh
-authentication-method nsswitch -role admin -is-ns-switch-group no -second
-authentication-method publickey
```

La méthode d'authentification peut être spécifiée comme `publickey` et deuxième méthode d'authentification en tant que `nsswitch`.

L'exemple suivant montre que l'authentification MFA est activée :

```
cluster-1::*> security login modify -user-or-group-name rem_usr2
-application ssh -authentication-method nsswitch -vserver
cluster-1 -second-authentication-method publickey"
```

Une fois que vous avez terminé

Si vous n'avez pas configuré l'accès au serveur LDAP ou NIS au SVM, vous devez le faire avant que le compte puisse accéder à la SVM.

Configuration de l'accès aux serveurs LDAP ou NIS

Gestion des rôles de contrôle d'accès

Gérer la présentation des rôles de contrôle d'accès

Le rôle attribué à un administrateur détermine les commandes auxquelles l'administrateur a accès. Vous attribuez le rôle lorsque vous créez le compte pour l'administrateur. Vous pouvez attribuer un autre rôle ou définir des rôles personnalisés selon vos besoins.

Modifiez le rôle attribué à un administrateur

Vous pouvez utiliser le `security login modify` Commande pour modifier le rôle d'un compte d'administrateur de cluster ou de SVM. Vous pouvez affecter un rôle prédéfini ou personnalisé.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étape

1. Modifier le rôle d'un administrateur de cluster ou de SVM :

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

"Création ou modification de comptes de connexion"

La commande suivante permet de changer le rôle du compte d'administrateur du cluster AD
DOMAIN1\guest1 au prédéfini readonly rôle.

```
cluster1::>security login modify -vserver engCluster -user-or-group-name  
DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
```

La commande suivante permet de changer le rôle des comptes administrateur du SVM dans le compte AD
group DOMAIN1\adgroup au personnalisé vol_role rôle.

```
cluster1::>security login modify -vserver engData -user-or-group-name  
DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
```

Définissez des rôles personnalisés

Vous pouvez utiliser le `security login role create` commande pour définir un rôle personnalisé. Vous pouvez exécuter la commande autant de fois que nécessaire pour obtenir la combinaison exacte de fonctions que vous souhaitez associer au rôle.

Description de la tâche

- Un rôle, qu'il soit prédéfini ou personnalisé, accorde ou refuse l'accès aux commandes ou aux répertoires de commandes ONTAP.

Un répertoire de commande (`volume`, par exemple) est un groupe de commandes et de sous-répertoires de commandes associés. Sauf comme décrit dans cette procédure, l'octroi ou le refus de l'accès à un répertoire de commandes accorde ou refuse l'accès à chaque commande du répertoire et de ses sous-répertoires.

- L'accès aux commandes ou aux sous-répertoires spécifiques remplace l'accès au répertoire parent.

Si un rôle est défini à l'aide d'un répertoire de commandes, puis qu'il est défini à nouveau avec un niveau d'accès différent pour une commande spécifique ou pour un sous-répertoire du répertoire parent, le niveau d'accès spécifié pour la commande ou le sous-répertoire remplace celui du parent.



Vous ne pouvez pas attribuer un administrateur SVM un rôle qui donne accès à une commande ou au répertoire de commande disponible uniquement pour le `admin` administrateur du cluster --par exemple, le `security` répertoire de commande.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étape

1. Définissez un rôle personnalisé :

```
security login role create -vserver SVM_name -role role -cmddirname
command_or_directory_name -access access_level -query query
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

Les commandes suivantes permettent d'accorder le `vol_role` rôle accès complet aux commandes dans `volume` le répertoire de commande et l'accès en lecture seule aux commandes de l'`volume snapshot` sous-répertoire.

```
cluster1::>security login role create -role vol_role -cmddirname
"volume" -access all

cluster1::>security login role create -role vol_role -cmddirname "volume
snapshot" -access readonly
```

Les commandes suivantes permettent d'accorder le `SVM_storage` accès en lecture seule du rôle aux commandes dans `storage` répertoire de commandes, pas d'accès aux commandes dans le `storage encryption` sous-répertoire et accès complet au `storage aggregate plex offline` commande non intrinsèque.

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

Rôles prédéfinis pour les administrateurs du cluster

Les rôles prédéfinis des administrateurs du cluster doivent répondre à la plupart des besoins. Vous pouvez créer des rôles personnalisés selon vos besoins. Par défaut un administrateur de cluster se voit attribuer le paramétrage prédéfini `admin` rôle.

Le tableau suivant répertorie les rôles prédéfinis pour les administrateurs du cluster :

Ce rôle...	Dispose de ce niveau d'accès...	Aux commandes ou répertoires de commandes suivants
------------	---------------------------------	--

admin	tous	Tous les répertoires de commandes (DEFAULT)
admin-no-fsa (disponible à partir de ONTAP 9.12.1)	Lecture/écriture	<ul style="list-style-type: none"> • Tous les répertoires de commandes (DEFAULT) • security login rest-role • security login role
Lecture seule	<ul style="list-style-type: none"> • security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics 	Aucune
volume file show-disk-usage	AutoSupport	tous
<ul style="list-style-type: none"> • set • system node autosupport 	Aucune	Tous les autres répertoires de commandes (DEFAULT)
sauvegarde	tous	vserver services ndmp
lecture seule	volume	Aucune

Tous les autres répertoires de commandes (DEFAULT)	lecture seule	tous
<ul style="list-style-type: none"> • security login password <p>Pour la gestion du mot de passe local et des informations clés du compte utilisateur</p> <ul style="list-style-type: none"> • set 	Aucune	security
lecture seule	Tous les autres répertoires de commandes (DEFAULT)	SnapLock
tous	<ul style="list-style-type: none"> • set • volume create • volume modify • volume move • volume show 	Aucune
<ul style="list-style-type: none"> • volume move governor • volume move recommend 	Aucune	Tous les autres répertoires de commandes (DEFAULT)
Aucune	Aucune	Tous les répertoires de commandes (DEFAULT)



Le autosupport le rôle est affecté au prédéfini autosupport Compte, utilisé par AutoSupport OnDemand. ONTAP vous empêche de modifier ou de supprimer le autosupport compte. ONTAP vous empêche également d'attribuer le autosupport rôle vers d'autres comptes utilisateur.

Rôles prédéfinis pour les administrateurs des SVM

Les rôles prédéfinis des administrateurs des SVM devraient répondre à la plupart des besoins. Vous pouvez créer des rôles personnalisés selon vos besoins. Par défaut un administrateur SVM est affecté au prédéfini `vsadmin` rôle.

Le tableau suivant répertorie les rôles prédéfinis pour les administrateurs du SVM :

Nom du rôle	Capacités
-------------	-----------

vsadmin	<ul style="list-style-type: none"> • Gestion du mot de passe local et des informations clés du compte utilisateur • Gestion des volumes, à l'exception des déplacements de volumes • Gestion des quotas, des qtrees, des copies Snapshot et des fichiers • Gestion des LUN • Exécution d'opérations SnapLock, sauf suppression privilégiée • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Surveillance des tâches • Surveillance des connexions réseau et de l'interface réseau • Contrôle de l'état de santé de la SVM
volume vsadmin	<ul style="list-style-type: none"> • Gestion du mot de passe local et des informations clés du compte utilisateur • Gestion des volumes, y compris les déplacements de volumes • Gestion des quotas, des qtrees, des copies Snapshot et des fichiers • Gestion des LUN • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Surveillance de l'interface réseau • Contrôle de l'état de santé de la SVM
protocole vsadmin	<ul style="list-style-type: none"> • Gestion du mot de passe local et des informations clés du compte utilisateur • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Gestion des LUN • Surveillance de l'interface réseau • Contrôle de l'état de santé de la SVM

sauvegarde vsadmin	<ul style="list-style-type: none"> • Gestion du mot de passe local et des informations clés du compte utilisateur • Gestion des opérations NDMP • Opérations de lecture/écriture d'un volume restauré • Gestion des relations SnapMirror et des copies Snapshot • Affichage des volumes et des informations réseau
vsadmin-snaplock	<ul style="list-style-type: none"> • Gestion du mot de passe local et des informations clés du compte utilisateur • Gestion des volumes, à l'exception des déplacements de volumes • Gestion des quotas, des qtrees, des copies Snapshot et des fichiers • Exécution d'opérations SnapLock, y compris la suppression privilégiée • Configuration des protocoles : NFS et SMB • Configuration des services : DNS, LDAP et NIS • Surveillance des tâches • Surveillance des connexions réseau et de l'interface réseau
vsadmin-readdisponible	<ul style="list-style-type: none"> • Gestion du mot de passe local et des informations clés du compte utilisateur • Contrôle de l'état de santé de la SVM • Surveillance de l'interface réseau • Affichage des volumes et des LUN • Affichage des services et protocoles

Contrôlez l'accès administrateur

Le rôle attribué à un administrateur détermine les fonctions que l'administrateur peut exécuter avec System Manager. Les rôles prédéfinis pour les administrateurs du cluster et des VM de stockage sont fournis par System Manager. Vous attribuez le rôle lorsque vous créez le compte de l'administrateur ou vous pouvez lui attribuer un autre rôle ultérieurement.

En fonction de la manière dont vous avez activé l'accès au compte, vous devrez peut-être effectuer l'une des opérations suivantes :

- Associer une clé publique à un compte local.
- Installez un certificat numérique de serveur signé par une autorité de certification.

- Configuration de l'accès AD, LDAP ou NIS.

Vous pouvez effectuer ces tâches avant ou après l'activation de l'accès au compte.

Attribution d'un rôle à un administrateur

Attribuez un rôle à un administrateur, comme suit :

Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Sélectionnez → en regard de **utilisateurs et rôles**.
3. Sélectionnez **+ Add** sous **utilisateurs**.
4. Spécifiez un nom d'utilisateur et sélectionnez un rôle dans le menu déroulant pour **role**.
5. Spécifiez une méthode de connexion et un mot de passe pour l'utilisateur.

Modification du rôle d'un administrateur

Modifiez le rôle d'un administrateur comme suit :

Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Sélectionnez le nom de l'utilisateur dont vous souhaitez modifier le rôle, puis cliquez sur le ⋮ qui s'affiche en regard du nom d'utilisateur.
3. Cliquez sur **Modifier**.
4. Sélectionnez un rôle dans le menu déroulant pour **role**.

Gérez les comptes d'administrateur

Gérer la présentation des comptes d'administrateur

Selon la manière dont vous avez activé l'accès au compte, vous devrez peut-être associer une clé publique à un compte local, installer un certificat numérique de serveur signé par une autorité de certification ou configurer l'accès AD, LDAP ou NIS. Vous pouvez effectuer toutes ces tâches avant ou après l'activation de l'accès au compte.

Associer une clé publique à un compte d'administrateur

Pour l'authentification de clé publique SSH, vous devez associer la clé publique à un compte d'administrateur avant que le compte puisse accéder à la SVM. Vous pouvez utiliser le `security login publickey create` commande permettant d'associer une clé à un compte d'administrateur.

Description de la tâche

Si vous authentifiez un compte via SSH avec un mot de passe et une clé publique SSH, le compte est authentifié d'abord par la clé publique.

Avant de commencer

- Vous devez avoir généré la clé SSH.

- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Associer une clé publique à un compte d'administrateur :

```
security login publickey create -vserver SVM_name -username user_name -index
index -publickey certificate -comment comment
```

Pour obtenir la syntaxe complète de la commande, reportez-vous à la fiche de référence de ["Association d'une clé publique à un compte d'utilisateur"](#).

2. Vérifiez la modification en affichant la clé publique :

```
security login publickey show -vserver SVM_name -username user_name -index
index
```

Exemple

La commande suivante associe une clé publique au compte d'administrateur du SVM `svmadmin1` Pour la SVM `engData1`. La clé publique est affectée à l'index numéro 5.

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

Gérer les clés publiques SSH et les certificats X.509 pour un compte d'administrateur

Pour une sécurité accrue de l'authentification SSH avec des comptes d'administrateur, vous pouvez utiliser `security login publickey` Ensemble de commandes pour gérer la clé publique SSH et son association avec les certificats X.509.

Associer une clé publique et un certificat X.509 à un compte d'administrateur

À partir de ONTAP 9.13.1, vous pouvez associer un certificat X.509 à la clé publique que vous associez au compte d'administrateur. Cela vous donne la sécurité supplémentaire des vérifications d'expiration ou de révocation des certificats lors de la connexion SSH à ce compte.

Description de la tâche

Si vous authentifiez un compte via SSH avec une clé publique SSH et un certificat X.509, ONTAP vérifie la validité du certificat X.509 avant de s'authentifier avec la clé publique SSH. La connexion SSH sera refusée si le certificat a expiré ou a été révoqué et la clé publique sera automatiquement désactivée.

Avant de commencer

- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Vous devez avoir généré la clé SSH.
- Si vous n'avez besoin que de vérifier l'expiration du certificat X.509, vous pouvez utiliser un certificat auto-signé.
- Si vous avez besoin de vérifier l'expiration et la révocation du certificat X.509 :
 - Vous devez avoir reçu le certificat d'une autorité de certification (CA).

- Vous devez installer la chaîne de certificats (certificats CA intermédiaire et racine) à l'aide de `security certificate install` commandes.
- Vous devez activer OCSP pour SSH. Reportez-vous à la section "[Vérifiez que les certificats numériques sont valides à l'aide du protocole OCSP](#)" pour obtenir des instructions.

Étapes

1. Associer une clé publique et un certificat X.509 à un compte d'administrateur :

```
security login publickey create -vserver SVM_name -username user_name -index
index -publickey certificate -x509-certificate install
```

Pour obtenir la syntaxe complète de la commande, reportez-vous à la fiche de référence de "[Association d'une clé publique à un compte d'utilisateur](#)".

2. Vérifiez la modification en affichant la clé publique :

```
security login publickey show -vserver SVM_name -username user_name -index
index
```

Exemple

La commande suivante associe une clé publique et un certificat X.509 au compte d'administrateur du SVM svmadmin2 Pour la SVM engData2. Le numéro d'index 6 est attribué à la clé publique.

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

Supprimez l'association de certificat de la clé publique SSH d'un compte d'administrateur

Vous pouvez supprimer l'association de certificat actuelle de la clé publique SSH du compte, tout en conservant la clé publique.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Supprimez l'association de certificat X.509 d'un compte d'administrateur et conservez la clé publique SSH existante :

```
security login publickey modify -vserver SVM_name -username user_name -index
index -x509-certificate delete
```

2. Vérifiez la modification en affichant la clé publique :

```
security login publickey show -vserver SVM_name -username user_name -index
index
```

Exemple

La commande suivante supprime l'association de certificat X.509 du compte d'administrateur du SVM svmadmin2 Pour la SVM engData2 au numéro d'index 6.

```
cluster1::> security login publickey modify -vserver engData2 -username  
svmadmin2 -index 6 -x509-certificate delete
```

Supprimez la clé publique et l'association de certificat d'un compte d'administrateur

Vous pouvez supprimer la clé publique actuelle et la configuration de certificat d'un compte.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Supprimez la clé publique et une association de certificat X.509 d'un compte d'administrateur :

```
security login publickey delete -vserver SVM_name -username user_name -index  
index
```

2. Vérifiez la modification en affichant la clé publique :

```
security login publickey show -vserver SVM_name -username user_name -index  
index
```

Exemple

La commande suivante supprime une clé publique et un certificat X.509 du compte d'administrateur du SVM svmadmin3 Pour la SVM engData3 au numéro d'index 7.

```
cluster1::> security login publickey delete -vserver engData3 -username  
svmadmin3 -index 7
```

Configurez Cisco Duo 2FA pour les connexions SSH

À partir de ONTAP 9.14.1, vous pouvez configurer ONTAP pour qu'il utilise Cisco Duo pour l'authentification à deux facteurs (2FA) pendant les connexions SSH. Vous configurez Duo au niveau du cluster et il s'applique par défaut à tous les comptes utilisateur. Vous pouvez également configurer Duo au niveau de la machine virtuelle de stockage (anciennement vServer), auquel cas il s'applique uniquement aux utilisateurs de cette machine virtuelle de stockage. Si vous activez et configurez Duo, il sert de méthode d'authentification supplémentaire, en complément des méthodes existantes pour tous les utilisateurs.

Si vous activez l'authentification Duo pour les connexions SSH, les utilisateurs devront inscrire un périphérique lors de leur prochaine connexion à l'aide de SSH. Pour plus d'informations sur l'inscription, reportez-vous au Cisco Duo ["documentation d'inscription"](#).

Vous pouvez utiliser l'interface de ligne de commande ONTAP pour effectuer les tâches suivantes avec Cisco Duo :

- [Configurez Cisco Duo](#)
- [Modifier la configuration Cisco Duo](#)
- [Supprimez la configuration Cisco Duo](#)
- [Afficher la configuration Cisco Duo](#)
- [Supprimer un groupe Duo](#)
- [Afficher les groupes Duo](#)
- [Contourner l'authentification Duo pour les utilisateurs](#)

Configurez Cisco Duo

Vous pouvez créer une configuration Cisco Duo pour l'ensemble du cluster ou pour une VM de stockage spécifique (appelée vServer dans l'interface de ligne de commande ONTAP) à l'aide de `security login duo create` commande. Dans ce cas, Cisco Duo est activé pour les connexions SSH pour ce cluster ou cette machine virtuelle de stockage.

Étapes

1. Connectez-vous au panneau d'administration Cisco Duo.
2. Accédez à **applications > application UNIX**.
3. Enregistrez votre clé d'intégration, votre clé secrète et le nom d'hôte de l'API.
4. Connectez-vous à votre compte ONTAP à l'aide de SSH.
5. Activez l'authentification Cisco Duo pour cette machine virtuelle de stockage, en remplaçant les informations de votre environnement par les valeurs entre parenthèses :

```
security login duo create \  
-vserver <STORAGE_VM_NAME> \  
-integration-key <INTEGRATION_KEY> \  
-secret-key <SECRET_KEY> \  
-apihost <API_HOSTNAME>
```

Pour plus d'informations sur les paramètres requis et facultatifs pour cette commande, reportez-vous à la section "[Feuilles de calcul pour l'authentification de l'administrateur et la configuration du RBAC](#)".

Modifier la configuration Cisco Duo

Vous pouvez modifier la façon dont Cisco Duo authentifie les utilisateurs (par exemple, le nombre d'invites d'authentification données ou le proxy HTTP utilisé). Si vous devez modifier la configuration Cisco Duo pour une machine virtuelle de stockage (appelée vServer dans l'interface de ligne de commande ONTAP), vous pouvez utiliser `security login duo modify` commande.

Étapes

1. Connectez-vous au panneau d'administration Cisco Duo.
2. Accédez à **applications > application UNIX**.

3. Enregistrez votre clé d'intégration, votre clé secrète et le nom d'hôte de l'API.
4. Connectez-vous à votre compte ONTAP à l'aide de SSH.
5. Modifiez la configuration Cisco Duo pour cette machine virtuelle de stockage en remplaçant les informations mises à jour de votre environnement par les valeurs entre parenthèses :

```
security login duo modify \  
-vserver <STORAGE_VM_NAME> \  
-integration-key <INTEGRATION_KEY> \  
-secret-key <SECRET_KEY> \  
-apihost <API_HOSTNAME> \  
-pushinfo true|false \  
-http-proxy <HTTP_PROXY_URL> \  
-autopush true|false \  
-prompts 1|2|3 \  
-max-unenrolled-logins <NUM_LOGINS> \  
-is-enabled true|false \  
-fail-mode safe|secure
```

Supprimez la configuration Cisco Duo

Vous pouvez supprimer la configuration Cisco Duo, ce qui supprime la nécessité pour les utilisateurs SSH de s'authentifier à l'aide de Duo lors de la connexion. Pour supprimer la configuration Cisco Duo d'une machine virtuelle de stockage (appelée vServer dans l'interface de ligne de commande ONTAP), vous pouvez utiliser `security login duo delete` commande.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Supprimez la configuration Cisco Duo pour cette machine virtuelle de stockage, en remplaçant le nom de votre machine virtuelle de stockage par `<STORAGE_VM_NAME>`:

```
security login duo delete -vserver <STORAGE_VM_NAME>
```

Cette opération supprime définitivement la configuration Cisco Duo pour cette machine virtuelle de stockage.

Afficher la configuration Cisco Duo

Vous pouvez afficher la configuration Cisco Duo existante pour une machine virtuelle de stockage (appelée vServer dans l'interface de ligne de commande ONTAP) à l'aide de `security login duo show` commande.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Affiche la configuration Cisco Duo pour cette machine virtuelle de stockage. Si vous le souhaitez, vous pouvez utiliser le `vserver` Paramètre permettant de spécifier une machine virtuelle de stockage, en

remplaçant le nom de la machine virtuelle de stockage par <STORAGE_VM_NAME>:

```
security login duo show -vserver <STORAGE_VM_NAME>
```

Vous devez voir les résultats similaires à ce qui suit :

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

Créez un groupe Duo

Vous pouvez demander à Cisco Duo d'inclure uniquement les utilisateurs d'un certain groupe d'utilisateurs Active Directory, LDAP ou local dans le processus d'authentification Duo. Si vous créez un groupe Duo, seuls les utilisateurs de ce groupe sont invités à s'authentifier Duo. Vous pouvez créer un groupe Duo à l'aide du `security login duo group create` commande. Lorsque vous créez un groupe, vous pouvez exclure certains utilisateurs de ce groupe du processus d'authentification Duo.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Créez le groupe Duo en remplaçant les informations de votre environnement par les valeurs entre parenthèses. Si vous omettez le `-vserver` le groupe est créé au niveau du cluster :

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -exclude-users <USER1, USER2>
```

Le nom du groupe Duo doit correspondre à un groupe Active Directory, LDAP ou local. Utilisateurs que vous spécifiez avec le facultatif `-exclude-users` Le paramètre ne sera pas inclus dans le processus d'authentification Duo.

Afficher les groupes Duo

Vous pouvez afficher les entrées de groupe Cisco Duo existantes à l'aide du `security login duo group show` commande.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Affichez les entrées du groupe Duo, en remplaçant les informations de votre environnement par les valeurs entre parenthèses. Si vous omettez le `-vserver` paramètre, le groupe s'affiche au niveau du cluster :

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME> -exclude-users <USER1, USER2>
```

Le nom du groupe Duo doit correspondre à un groupe Active Directory, LDAP ou local. Utilisateurs que vous spécifiez avec le facultatif `-exclude-users` le paramètre ne s'affiche pas.

Supprimer un groupe Duo

Vous pouvez supprimer une entrée de groupe Duo à l'aide du `security login duo group delete` commande. Si vous supprimez un groupe, les utilisateurs de ce groupe ne sont plus inclus dans le processus d'authentification Duo.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Supprimez l'entrée de groupe Duo, en remplaçant les informations de votre environnement par les valeurs entre parenthèses. Si vous omettez le `-vserver` paramètre, le groupe est supprimé au niveau du cluster :

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME>
```

Le nom du groupe Duo doit correspondre à un groupe Active Directory, LDAP ou local.

Contourner l'authentification Duo pour les utilisateurs

Vous pouvez exclure tous les utilisateurs ou des utilisateurs spécifiques du processus d'authentification Duo SSH.

Exclure tous les utilisateurs Duo

Vous pouvez désactiver l'authentification SSH Cisco Duo pour tous les utilisateurs.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Désactivez l'authentification Cisco Duo pour les utilisateurs SSH en remplaçant le nom du vServer par `<STORAGE_VM_NAME>`:

```
security login duo -vserver <STORAGE_VM_NAME> -is-duo-enabled-false
```

Exclure les utilisateurs du groupe Duo

Vous pouvez exclure certains utilisateurs faisant partie d'un groupe Duo du processus d'authentification Duo SSH.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Désactivez l'authentification Cisco Duo pour des utilisateurs spécifiques d'un groupe. Remplacez le nom du groupe et la liste des utilisateurs à exclure par les valeurs entre parenthèses :

```
security login group modify -group-name <GROUP_NAME> -exclude-users  
<USER1, USER2>
```

Le nom du groupe Duo doit correspondre à un groupe Active Directory, LDAP ou local. Utilisateurs que vous spécifiez avec `-exclude-users` Le paramètre ne sera pas inclus dans le processus d'authentification Duo.

Exclure les utilisateurs Duo locaux

Vous pouvez exclure certains utilisateurs locaux de l'authentification Duo à l'aide du panneau d'administration Cisco Duo. Pour obtenir des instructions, reportez-vous au ["Documentation Cisco Duo"](#).

Générer et installer un certificat de serveur signé par une autorité de certification

Sur les systèmes de production, il est recommandé d'installer un certificat numérique signé par une autorité de certification pour l'authentification du cluster ou d'un SVM en tant que serveur SSL. Vous pouvez utiliser le `security certificate generate-csr` Commande pour générer une requête de signature de certificat (CSR) et le `security certificate install` commande permettant d'installer le certificat que vous recevez de l'autorité de certification.

Générer une demande de signature de certificat

Vous pouvez utiliser le `security certificate generate-csr` Commande pour générer une requête de signature de certificat (CSR). Après le traitement de votre demande, l'autorité de certification vous envoie le certificat numérique signé.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Générer une RSC :

```
security certificate generate-csr -common-name FQDN_or_common_name -size  
512|1024|1536|2048 -country country -state state -locality locality  
-organization organization -unit unit -email-addr email_of_contact -hash  
-function SHA1|SHA256|MD5
```

La commande suivante crée une CSR avec une clé privée 2048 bits générée par la fonction de hachage «

'S ra256' » à l'usage du groupe « logiciels » dans le département « IT » d'une entreprise dont le nom commun personnalisé est « `erver1.companyname.com`" », situé à Sunnyvale, en Californie, aux États-Unis. L'adresse e-mail de l'administrateur du contact du SVM est « web@example.com ». Le système affiche la RSC et la clé privée dans la sortie.

Exemple de création d'une RSC

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
```

Certificate Signing Request :

-----BEGIN CERTIFICATE REQUEST-----

```
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTElMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADAEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAStADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApt1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJbmXuj6U3alwoUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

Private Key :

-----BEGIN RSA PRIVATE KEY-----

```
MIIBOwIBAAJBAPXFanNoJApt1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJb
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
```

Note: Please keep a copy of your certificate request and private key for future reference.

2. Copiez la demande de certificat à partir de la sortie CSR et envoyez-la sous forme électronique (par exemple un courriel) à une autorité de certification tierce approuvée pour signature.

Après le traitement de votre demande, l'AC vous envoie le certificat numérique signé. Vous devez conserver une copie de la clé privée et du certificat numérique signé par l'autorité de certification.

Installez un certificat de serveur signé par une autorité de certification

Vous pouvez utiliser le `security certificate install` Commande permettant d'installer un certificat de

serveur signé par une autorité de certification sur un SVM. ONTAP vous invite à entrer les certificats racine et intermédiaire de l'autorité de certification (CA) qui forment la chaîne de certificats du certificat du serveur.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étape

1. Installer un certificat de serveur signé par une autorité de certification :

```
security certificate install -vserver SVM_name -type certificate_type
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).



ONTAP vous invite à entrer les certificats racine et intermédiaire de l'autorité de certification qui constituent la chaîne de certificats du certificat du serveur. La chaîne commence par le certificat de l'autorité de certification qui a émis le certificat du serveur et peut atteindre le certificat racine de l'autorité de certification. Tout certificat intermédiaire manquant entraîne l'échec de l'installation du certificat du serveur.

La commande suivante installe le certificat de serveur signé par l'autorité de certification et les certificats intermédiaires sur SVM « engData2 ».

Exemple d'installation de certificats intermédiaires de certificat de serveur signés par une autorité de certification

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCA ZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADAJMAcGA1UECXMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADAJMAcGA1UECXMAM
Q8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIaKEAyXrK2sry
-----END CERTIFICATE-----
```

```
Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLyCsUdXA7hXhumHNpvF
C6lX2G32Sx8VEalth94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM70tbUsgPKw+QCCh9dF1jmuQKeDr+wUMWkn1DeGrfhILpzfJGHRlJ
z7UCIQDr8d3gOG7lUyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEArlmnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAZt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----
```

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

```
Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSGAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwwgsxJDAiBgNVBACGTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTTFZhbGlDZXJ0IENsYXNzIDIGUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFROZSBHbyBE
YWRkeSBHcm9lcCwgSW5jLjExMC8GA1UECXMOR28gRGFkZkhkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBACGTG1ZhbG1DZXJ0
IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIgUG9saWN5IFZhbG1kYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDEzhodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTE5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBACGTG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENs
YXNzIDIgUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEzhodHRw
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital certificate for future reference.

Gérer les certificats avec System Manager

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour gérer les autorités de certification de confiance, les certificats client/serveur et les autorités de certification locales (intégrées).

Avec System Manager, vous pouvez gérer les certificats reçus d'autres applications afin de pouvoir authentifier les communications de ces applications. Vous pouvez également gérer vos propres certificats qui identifient votre système à d'autres applications.

Afficher les informations sur le certificat

System Manager vous permet d'afficher les autorités de certification approuvées, les certificats client/serveur et les autorités de certification locales stockées sur le cluster.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Faites défiler jusqu'à la zone **sécurité**.
Dans la section **certificats**, les détails suivants sont affichés :
 - Le nombre d'autorités de certification stockées approuvées.
 - Nombre de certificats client/serveur stockés.
 - Le nombre d'autorités de certification locales stockées.
3. Sélectionnez n'importe quel nombre pour afficher les détails d'une catégorie de certificats, ou sélectionnez  pour ouvrir la page **certificats**, qui contient des informations sur toutes les catégories. La liste affiche les informations relatives à l'ensemble du cluster. Pour afficher les informations relatives à une seule machine virtuelle de stockage spécifique, effectuez les opérations suivantes :
 - a. Sélectionnez **stockage > machines virtuelles de stockage**.

- b. Sélectionnez la VM de stockage.
- c. Passez à l'onglet **Paramètres**.
- d. Sélectionnez un numéro affiché dans la section **certificat**.

Que faire ensuite

- À partir de la page **certificats**, vous pouvez [Générer une demande de signature de certificat](#).
- Les informations de certificat sont séparées en trois onglets, un pour chaque catégorie. Vous pouvez effectuer les tâches suivantes à partir de chaque onglet :

Dans cet onglet...	Vous pouvez effectuer ces procédures...
Autorités de certification approuvées	<ul style="list-style-type: none"> • [install-trusted-cert] • Supprimer une autorité de certification approuvée • Renouvelez une autorité de certification approuvée
Certificats client/serveur	<ul style="list-style-type: none"> • [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
Autorités locales de certification	<ul style="list-style-type: none"> • Créez une autorité de certification locale • Signer un certificat à l'aide d'une autorité de certification locale • Supprimer une autorité de certification locale • Renouvelez une autorité de certification locale

Générer une demande de signature de certificat

Vous pouvez générer une demande de signature de certificat (CSR) avec System Manager à partir de n'importe quel onglet de la page **certificats**. Une clé privée et une RSC correspondante sont générées, qui peuvent être signées à l'aide d'une autorité de certification pour générer un certificat public.

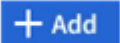
Étapes

1. Consultez la page **certificats**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez **+Generate CSR**.
3. Renseignez les informations relatives au nom du sujet :
 - a. Saisissez un **nom commun**.
 - b. Sélectionnez un **pays**.
 - c. Saisissez une **organisation**.
 - d. Entrez une **unité d'organisation**.
4. Si vous souhaitez remplacer les valeurs par défaut, sélectionnez **plus d'options** et fournissez des informations supplémentaires.

Installez (ajoutez) une autorité de certification approuvée

Vous pouvez installer des autorités de certification approuvées supplémentaires dans System Manager.

Étapes

1. Affichez l'onglet **autorités de certification approuvées**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez .
3. Dans le panneau **Ajouter une autorité de certification approuvée**, effectuez les opérations suivantes :
 - Saisissez un **nom**.
 - Pour le **scope**, sélectionnez une VM de stockage.
 - Saisissez un **nom commun**.
 - Sélectionnez un **type**.
 - Entrez ou importez **détails du certificat**.


Supprimer une autorité de certification approuvée

Avec System Manager, vous pouvez supprimer une autorité de certification approuvée.



Vous ne pouvez pas supprimer les autorités de certification approuvées préinstallées avec ONTAP.


Étapes

1. Affichez l'onglet **autorités de certification approuvées**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez le nom de l'autorité de certification approuvée.
3. Sélectionnez  en regard du nom, puis sélectionnez **Supprimer**.

Renouvelez une autorité de certification approuvée

Avec System Manager, vous pouvez renouveler une autorité de certification de confiance qui a expiré ou est sur le point d'expirer.

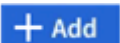
Étapes

1. Affichez l'onglet **autorités de certification approuvées**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez le nom de l'autorité de certification approuvée.
3. Sélectionnez  en regard du nom du certificat, puis **Renew**.

Installez (ajoutez) un certificat client/serveur

System Manager vous permet d'installer des certificats client/serveur supplémentaires.

Étapes

1. Affichez l'onglet **certificats client/serveur**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez .
3. Sur le panneau **Ajouter un certificat client/serveur**, effectuez les opérations suivantes :
 - Saisissez un **nom de certificat**.

- Pour le **scope**, sélectionnez une VM de stockage.
- Saisissez un **nom commun**.
- Sélectionnez un **type**.
- Entrez ou importez **détails du certificat**.
Vous pouvez écrire ou copier et coller les détails du certificat à partir d'un fichier texte ou importer le texte d'un fichier de certificat en cliquant sur **Importer**.
- Entrez la **clé privée**.
Vous pouvez écrire ou copier et coller la clé privée à partir d'un fichier texte ou importer le texte d'un fichier de clé privée en cliquant sur **Importer**.

Générer (ajouter) un certificat client/serveur auto-signé

System Manager vous permet de générer des certificats client/serveur autosignés supplémentaires.


Étapes

1. Afficher l'onglet **certificats client/serveur**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez **+générer un certificat auto-signé**.
3. Dans le panneau **générer un certificat auto-signé**, effectuez les opérations suivantes :
 - Saisissez un **nom de certificat**.
 - Pour le **scope**, sélectionnez une VM de stockage.
 - Saisissez un **nom commun**.
 - Sélectionnez un **type**.
 - Sélectionnez une fonction **hachage**.
 - Sélectionnez un **taille de clé**.
 - Sélectionnez une **VM de stockage**.

Supprimer un certificat client/serveur

Avec System Manager, vous pouvez supprimer les certificats client/serveur.


Étapes

1. Afficher l'onglet **certificats client/serveur**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez le nom du certificat client/serveur.
3. Sélectionnez  en regard du nom, puis cliquez sur **Supprimer**.

Renouveler un certificat client/serveur

Avec System Manager, vous pouvez renouveler un certificat client/serveur qui a expiré ou est sur le point d'expirer.

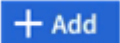
Étapes

1. Afficher l'onglet **certificats client/serveur**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez le nom du certificat client/serveur.
3. Sélectionnez  en regard du nom, puis cliquez sur **Renew**.

Créer une autorité de certification locale

Avec System Manager, vous pouvez créer une nouvelle autorité de certification locale.

Étapes

1. Affichez l'onglet **autorités locales de certification**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez  **Add**.
3. Dans le panneau **Ajouter une autorité de certification locale**, effectuez les opérations suivantes :
 - Saisissez un **nom**.
 - Pour le **scope**, sélectionnez une VM de stockage.
 - Saisissez un **nom commun**.
4. Si vous souhaitez remplacer les valeurs par défaut, sélectionnez **plus d'options** et fournissez des informations supplémentaires.

Signer un certificat à l'aide d'une autorité de certification locale

Dans System Manager, vous pouvez signer un certificat à l'aide d'une autorité de certification locale.


Étapes

1. Affichez l'onglet **autorités locales de certification**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez le nom de l'autorité de certification locale.
3. Sélectionnez  en regard du nom, puis **signer un certificat**.
4. Remplissez le formulaire **signer une demande de signature de certificat**.
 - Vous pouvez coller le contenu de la signature de certificat ou importer un fichier de demande de signature de certificat en cliquant sur **Importer**.
 - Indiquez le nombre de jours pendant lesquels le certificat sera valide.

Supprimer une autorité de certification locale

Avec System Manager, vous pouvez supprimer une autorité de certification locale.


Étapes

1. Affichez l'onglet **local Certificate Authority**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez le nom de l'autorité de certification locale.
3. Sélectionnez  en regard du nom, puis **Supprimer**.

Renouvelez une autorité de certification locale

Avec System Manager, vous pouvez renouveler une autorité de certification locale qui a expiré ou est sur le point d'expirer.

Étapes

1. Affichez l'onglet **local Certificate Authority**. Voir [Afficher les informations sur le certificat](#).
2. Sélectionnez le nom de l'autorité de certification locale.
3. Sélectionnez  en regard du nom, puis cliquez sur **Renew**.

Présentation de la configuration de l'accès au contrôleur de domaine Active Directory

Vous devez configurer l'accès du contrôleur AD domain au cluster ou au SVM avant qu'un compte AD ne puisse accéder au SVM. Si vous avez déjà configuré un serveur SMB pour un SVM de données, vous pouvez configurer le SVM en tant que passerelle, ou *tunnel*, pour l'accès AD au cluster. Si vous n'avez pas configuré de serveur SMB, vous pouvez créer un compte ordinateur pour le SVM sur le domaine AD.

ONTAP prend en charge les services d'authentification de contrôleur de domaine suivants :

- Kerberos
- LDAP
- NETLOGON
- Autorité de sécurité locale (LSA)

ONTAP prend en charge les algorithmes de clé de session suivants pour les connexions Netlogon sécurisées :

Algorithme de clé de session	Disponible à partir de...
HMAC-SHA256, basé sur la norme AES (Advanced Encryption Standard) Si votre cluster exécute ONTAP 9.9.1 ou une version antérieure et que votre contrôleur de domaine applique AES pour des services Netlogon sécurisés, la connexion échoue. Dans ce cas, vous devez reconfigurer votre contrôleur de domaine pour accepter les connexions par clé forte avec ONTAP.	ONTAP 9.10.1
DES et HMAC-MD5 (lorsque la clé est réglée)	Toutes les versions d'ONTAP 9

Si vous souhaitez utiliser les clés de session AES lors de l'établissement d'un canal sécurisé Netlogon, vous devez vérifier que AES est activé sur votre SVM.

- Depuis ONTAP 9.14.1, AES est activé par défaut lorsque vous créez un SVM, et vous n'avez pas besoin de modifier les paramètres de sécurité de votre SVM pour utiliser des clés de session AES lors de l'établissement de canaux sécurisés Netlogon.
- Dans ONTAP 9.10.1 à 9.13.1, AES est désactivé par défaut lors de la création d'un SVM. Vous devez activer AES à l'aide de la commande suivante :

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```



Lorsque vous effectuez une mise à niveau vers ONTAP 9.14.1 ou une version ultérieure, le paramètre AES des SVM existants créés avec les anciennes versions de ONTAP ne changera pas automatiquement. Vous devez toujours mettre à jour la valeur de ce paramètre pour activer les AES sur ces SVM.

Configurer un tunnel d'authentification

Si vous avez déjà configuré un serveur SMB pour un SVM de données, vous pouvez utiliser le `security login domain-tunnel create` Commande permettant de configurer le SVM en tant que passerelle ou *tunnel*, pour l'accès AD au cluster.

Avant de commencer

- Un serveur SMB doit être configuré pour un SVM de données.
- Vous devez avoir activé un compte utilisateur AD domain pour accéder au SVM admin pour le cluster.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.

Depuis ONTAP 9.10.1, si vous disposez d'une passerelle SVM (tunnel du domaine) pour l'accès AD, vous pouvez utiliser Kerberos pour l'authentification admin si vous avez désactivé NTLM dans votre domaine AD. Dans les versions précédentes, Kerberos n'était pas pris en charge par l'authentification admin pour les passerelles SVM. Cette fonctionnalité est disponible par défaut ; aucune configuration n'est requise.



L'authentification Kerberos a toujours été tentée en premier. En cas d'échec, l'authentification NTLM est alors tentée.

Étape

1. Configurer un SVM de données compatible SMB en tant que tunnel d'authentification pour l'accès au contrôleur de domaine AD au cluster :

```
security login domain-tunnel create -vserver svm_name
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).



Le SVM doit être exécuté pour que l'utilisateur puisse être authentifié.

La commande suivante configure le SVM de données SMB « engData » comme un tunnel d'authentification.

```
cluster1::>security login domain-tunnel create -vserver engData
```

Créer un compte SVM Computer sur le domaine

Si vous n'avez pas configuré de serveur SMB pour un SVM de données, vous pouvez utiliser le `vserver active-directory create` Commande pour créer un compte ordinateur pour le SVM sur le domaine.

Description de la tâche

Une fois que vous avez saisi le `vserver active-directory create` Vous êtes invité à fournir les informations d'identification d'un compte utilisateur AD avec suffisamment de privilèges pour ajouter des ordinateurs à l'unité organisationnelle spécifiée dans le domaine. Le mot de passe du compte ne peut pas être vide.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étape

1. Créer un compte ordinateur pour un SVM sur le domaine AD :

```
vserver active-directory create -vserver SVM_name -account-name  
NetBIOS_account_name -domain domain -ou organizational_unit
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

La commande suivante crée un compte ordinateur nommé « ADSERVER1 » sur le domaine « example.com » pour SVM « engData ». Une fois la commande saisie, vous êtes invité à saisir les informations d'identification du compte utilisateur AD.

```
cluster1::>vserver active-directory create -vserver engData -account  
-name ADSERVER1 -domain example.com
```

```
In order to create an Active Directory machine account, you must supply  
the name and password of a Windows account with sufficient privileges to  
add computers to the "CN=Computers" container within the "example.com"  
domain.
```

```
Enter the user name: Administrator
```

```
Enter the password:
```

Configuration de la présentation de l'accès aux serveurs LDAP ou NIS

Vous devez configurer l'accès des serveurs LDAP ou NIS à un SVM pour que les comptes LDAP ou NIS puissent accéder au SVM. La fonction de commutation vous permet d'utiliser LDAP ou NIS comme sources de service de noms alternatifs.

Configurez l'accès au serveur LDAP

Vous devez configurer l'accès des serveurs LDAP à une SVM avant que les comptes LDAP ne puissent accéder à la SVM. Vous pouvez utiliser le `vserver services name-service ldap client create` Commande permettant de créer une configuration client LDAP sur le SVM. Vous pouvez ensuite utiliser le `vserver services name-service ldap create` Commande permettant d'associer la configuration client LDAP à la SVM.

Description de la tâche

La plupart des serveurs LDAP peuvent utiliser les schémas par défaut fournis par ONTAP :

- MS-AD-BIS (schéma préféré pour la plupart des serveurs AD Windows 2012 et versions ultérieures)
- AD-IDMU (serveurs AD Windows 2008, Windows 2016 et versions ultérieures)
- AD-SFU (serveurs AD Windows 2003 et versions antérieures)
- RFC-2307 (SERVEURS LDAP UNIX)

Il est préférable d'utiliser les schémas par défaut à moins qu'il n'y ait une obligation de faire autrement. Si c'est le cas, vous pouvez créer votre propre schéma en copiant un schéma par défaut et en modifiant la copie. Pour plus d'informations, voir :

- ["Configuration NFS"](#)
- ["Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP"](#)

Avant de commencer

- Vous devez avoir installé un ["Certificat numérique de serveur signé CA"](#) Sur le SVM.
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Créer une configuration client LDAP sur un SVM :

```
vserver services name-service ldap client create -vserver SVM_name -client
-config client_configuration -servers LDAP_server_IPs -schema schema -use
-start-tls true|false
```



Le démarrage de TLS est pris en charge uniquement pour l'accès aux SVM de données. Il n'est pas pris en charge pour l'accès aux SVM d'administration.

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

La commande suivante crée une configuration client LDAP nommée « corp » sur le SVM « engData ». Le client établit des liaisons anonymes vers les serveurs LDAP avec les adresses IP 172.160.0.100 et 172.16.0.101. Le client utilise le schéma RFC-2307 pour effectuer des requêtes LDAP. La communication entre le client et le serveur est cryptée à l'aide de Start TLS.

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```



À partir de ONTAP 9.2, le champ `-ldap-servers` remplace le champ `-servers`. Ce nouveau champ peut prendre un nom d'hôte ou une adresse IP pour le serveur LDAP.

2. Associer la configuration client LDAP au SVM :

```
vserver services name-service ldap create
-vserver SVM_name -client-config client_configuration -client-enabled
true|false
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

La commande suivante associe la configuration du client LDAP corp Avec la SVM engData, Et active le client LDAP sur la SVM.

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```



À partir de ONTAP 9.2, le `vserver services name-service ldap create` Commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP n'est pas en mesure de contacter le serveur de noms.

3. Valider le statut des serveurs name en utilisant la commande `vserver services name-service ldap check`.

La commande suivante valide les serveurs LDAP sur le SVM vs 0.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                     |
| Client Configuration Name: c1                     |
| LDAP Status: up                                   |
| LDAP Status Details: Successfully connected to LDAP server |
| "10.11.12.13".                                   |
```

La commande `name service check` est disponible à partir de ONTAP 9.2.

Configurer l'accès au serveur NIS

Vous devez configurer l'accès du serveur NIS à un SVM pour que les comptes NIS puissent accéder au SVM. Vous pouvez utiliser le `vserver services name-service nis-domain create` Commande permettant de créer une configuration de domaine NIS sur un SVM

Description de la tâche

Vous pouvez créer plusieurs domaines NIS. Un seul domaine NIS peut être défini sur `active` à la fois.

Avant de commencer

- Tous les serveurs configurés doivent être disponibles et accessibles avant de configurer le domaine NIS sur le SVM.
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étape

1. Créer une configuration de domaine NIS sur un SVM :

```
vserver services name-service nis-domain create -vserver SVM_name -domain
client_configuration -active true|false -nis-servers NIS_server_IPs
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).



À partir de ONTAP 9.2, le champ `-nis-servers` remplace le champ `-servers`. Ce nouveau champ peut prendre un nom d'hôte ou une adresse IP pour le serveur NIS.

La commande suivante crée une configuration de domaine NIS sur SVM « engData ». Domaine NIS `nisdomain` Est actif lors de la création et communique avec un serveur NIS avec l'adresse IP `192.0.2.180`.

```
cluster1::>vserver services name-service nis-domain create
-vserver engData -domain nisdomain -active true -nis-servers 192.0.2.180
```

Créer un commutateur de service de nom

La fonction de changement de service de noms vous permet d'utiliser LDAP ou NIS comme sources de service de noms alternatifs. Vous pouvez utiliser le `vserver services name-service ns-switch modify` commande permettant de spécifier l'ordre de recherche des sources de service de noms.

Avant de commencer

- Vous devez avoir configuré l'accès aux serveurs LDAP et NIS.
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou un administrateur SVM.

Étape

1. Spécifiez l'ordre de recherche des sources de service de noms :

```
vserver services name-service ns-switch modify -vserver SVM_name -database  
name_service_switch_database -sources name_service_source_order
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["feuille de calcul"](#).

La commande suivante spécifie l'ordre de recherche des sources de service de noms LDAP et NIS pour la base de données « passwd » sur SVM « engData ».

```
cluster1::>vserver services name-service ns-switch  
modify -vserver engData -database passwd -source files ldap,nis
```

Modifier un mot de passe administrateur

Vous devez modifier votre mot de passe initial immédiatement après la première connexion au système. Si vous êtes un administrateur de SVM, vous pouvez utiliser `security login password` commande permettant de modifier votre propre mot de passe. Si vous êtes administrateur de cluster, vous pouvez utiliser `security login password` pour modifier le mot de passe d'un administrateur.

Description de la tâche

Le nouveau mot de passe doit respecter les règles suivantes :

- Il ne peut pas contenir le nom d'utilisateur
- Elle doit comporter au moins huit caractères
- Il doit contenir au moins une lettre et un chiffre
- Il ne peut pas être le même que les six derniers mots de passe



Vous pouvez utiliser le `security login role config modify` commande permettant de modifier les règles de mot de passe des comptes associés à un rôle donné. Pour plus d'informations, reportez-vous à la section ["référence de commande"](#).

Avant de commencer

- Vous devez être un administrateur de cluster ou de SVM pour modifier votre propre mot de passe.
- Vous devez être un administrateur de cluster pour modifier le mot de passe d'un autre administrateur.

Étape

1. Modifier un mot de passe d'administrateur : `security login password -vserver svm_name -username user_name`

La commande suivante permet de modifier le mot de passe de l'administrateur `admin1` Pour la SVM `vs1.example.com`. Vous êtes invité à saisir le mot de passe actuel, puis à saisir de nouveau le nouveau mot de passe.

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

Verrouiller et déverrouiller un compte administrateur

Vous pouvez utiliser le `security login lock` commande permettant de verrouiller un compte d'administrateur, et le `security login unlock` commande pour déverrouiller le compte.

Avant de commencer

Pour effectuer ces tâches, vous devez être un administrateur de cluster.

Étapes

1. Verrouiller un compte administrateur :

```
security login lock -vserver SVM_name -username user_name
```

La commande suivante verrouille le compte administrateur `admin1` Pour la SVM `vs1.example.com`:

```
cluster1::>security login lock -vserver engData -username admin1
```

2. Déverrouiller un compte administrateur :

```
security login unlock -vserver SVM_name -username user_name
```

La commande suivante déverrouille le compte administrateur `admin1` Pour la SVM `vs1.example.com`:

```
cluster1::>security login unlock -vserver engData -username admin1
```

La gestion des tentatives de connexion a échoué

Les tentatives répétées de connexion échouées indiquent parfois qu'un intrus tente d'accéder au système de stockage. Vous pouvez prendre plusieurs mesures pour vous assurer qu'une intrusion n'a pas lieu.

Comment savoir que les tentatives de connexion ont échoué

Le système de gestion des événements (EMS) vous informe de l'échec des tentatives de connexion toutes les heures. Vous pouvez trouver un enregistrement des tentatives de connexion échouées dans le `audit.log` fichier.

Que faire en cas d'échec des tentatives de connexion répétées

À court terme, vous pouvez prendre plusieurs mesures pour éviter une intrusion :

- Exiger que les mots de passe soient composés d'un nombre minimum de caractères majuscules, de minuscules, de caractères spéciaux et/ou de chiffres
- Imposer un délai après une tentative de connexion échouée
- Limitez le nombre de tentatives de connexion ayant échoué autorisées et verrouillez les utilisateurs après le nombre spécifié de tentatives ayant échoué
- Expire et verrouille les comptes inactifs pendant un nombre de jours spécifié

Vous pouvez utiliser le `security login role config modify` pour effectuer ces tâches.

Sur le long terme, vous pouvez prendre les mesures suivantes :

- Utilisez le `security ssh modify` Commande pour limiter le nombre de tentatives de connexion ayant échoué pour tous les SVM nouvellement créés.
- Migrez les comptes d'algorithme MD5 existants vers l'algorithme SHA-512 plus sécurisé en exigeant des utilisateurs de modifier leurs mots de passe.

Appliquer SHA-2 sur les mots de passe du compte d'administrateur

Les comptes d'administrateur créés avant ONTAP 9.0 continuent d'utiliser des mots de passe MD5 après la mise à niveau, jusqu'à ce que les mots de passe soient changés manuellement. MD5 est moins sécurisé que SHA-2. Par conséquent, après la mise à niveau, vous devez inviter les utilisateurs de comptes MD5 à modifier leurs mots de passe pour utiliser la fonction de hachage SHA-512 par défaut.

Description de la tâche

La fonctionnalité de hachage du mot de passe vous permet d'effectuer les opérations suivantes :

- Affiche les comptes utilisateur correspondant à la fonction de hachage spécifiée.
- Expire les comptes qui utilisent une fonction de hachage spécifiée (par exemple MD5), forçant les utilisateurs à modifier leurs mots de passe lors de leur prochaine connexion.
- Verrouiller les comptes dont les mots de passe utilisent la fonction de hachage spécifiée.
- Pour revenir à une version antérieure à ONTAP 9, réinitialisez le mot de passe de l'administrateur du cluster afin qu'il soit compatible avec la fonction de hachage (MD5) prise en charge par la version précédente.

ONTAP n'accepte que les mots de passe SHA-2 pré-hachés à l'aide du SDK de gestion NetApp (`security-login-create` et `security-login-modify-password`).

Étapes

1. Migrez les comptes administrateur MD5 vers la fonction de hachage SHA-512 :

- a. Expire tous les comptes administrateur MD5 : `security login expire-password -vserver * -username * -hash-function md5`

Cela oblige les utilisateurs de compte MD5 à changer leurs mots de passe lors de la prochaine connexion.

- b. Demandez aux utilisateurs de comptes MD5 de se connecter par le biais d'une console ou d'une session SSH.

Le système détecte que les comptes ont expiré et invite les utilisateurs à modifier leur mot de passe. SHA-512 est utilisé par défaut pour les mots de passe modifiés.

2. Pour les comptes MD5 dont les utilisateurs ne se connectent pas pour modifier leurs mots de passe dans un délai donné, forcez la migration du compte :

- a. Verrouiller les comptes qui utilisent toujours la fonction de hachage MD5 (niveau de privilège avancé) :
`security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`


Après le nombre de jours spécifié par `-lock-after`, Les utilisateurs ne peuvent pas accéder à leurs comptes MD5.

- b. Déverrouillez les comptes lorsque les utilisateurs sont prêts à modifier leur mot de passe : `security login unlock -vserver svm_name -username user_name`


- c. Demandez aux utilisateurs de se connecter à leurs comptes via une console ou une session SSH et de modifier leur mot de passe lorsque le système les invite à le faire.

Diagnostiquer et corriger les problèmes d'accès aux fichiers

Étapes

1. Dans System Manager, sélectionnez **stockage > machines virtuelles de stockage**.
2. Sélectionnez la VM de stockage sur laquelle vous souhaitez effectuer un suivi.
3. Cliquez sur  **plus**.
4. Cliquez sur **Trace File Access**.
5. Indiquez le nom d'utilisateur et l'adresse IP du client, puis cliquez sur **Start Tracing**.

Les résultats de la trace s'affichent dans un tableau. La colonne **motifs** indique la raison pour laquelle un fichier n'a pas pu être accédé.

6. Cliquez sur  dans la colonne de gauche du tableau de résultats pour afficher les autorisations d'accès aux fichiers.

Gestion de la vérification multi-administrateurs

Présentation de la vérification multi-administrateur

Depuis ONTAP 9.11.1, vous pouvez utiliser la vérification multi-administration (MAV) pour vous assurer que certaines opérations, telles que la suppression de volumes ou de copies Snapshot, ne peuvent être exécutées qu'après approbation d'administrateurs désignés. Cela empêche les administrateurs compromis, malveillants ou peu expérimentés d'effectuer des modifications ou de supprimer des données indésirables.

La configuration de la vérification multi-administrateurs comprend :

- ["Création d'un ou plusieurs groupes d'approbation administrateur."](#)
- ["Activation de la fonctionnalité de vérification multi-administrateurs."](#)
- ["Ajout ou modification de règles."](#)

Après la configuration initiale, ces éléments ne peuvent être modifiés que par les administrateurs d'un groupe d'approbation MAV (administrateurs MAV).

Lorsque la vérification multiadministrateur est activée, la réalisation de chaque opération protégée nécessite les étapes suivantes :

1. Lorsqu'un utilisateur lance l'opération, un ["la demande a été générée."](#)
2. Avant de pouvoir être exécuté, au moins un ["L'administrateur MAV doit approuver."](#)
3. Après approbation, l'utilisateur termine l'opération.



Si vous avez besoin de désactiver la fonctionnalité de vérification multi-administrateurs sans l'approbation de l'administrateur MAV, contactez le support NetApp et mentionnez l'article suivant de la base de connaissances : ["Comment désactiver la vérification multi-administrateur si MAV admin n'est pas disponible"](#).

La vérification multi-administrateurs n'est pas destinée aux volumes ou aux flux de travail nécessitant une automatisation élevée, car chaque tâche automatisée nécessite une approbation avant que l'opération ne puisse être terminée. Si vous souhaitez utiliser l'automatisation et MAV ensemble, il est recommandé d'utiliser des requêtes pour des opérations MAV spécifiques. Vous pouvez, par exemple, appliquer `volume delete` MAV ne règle que les volumes où l'automatisation n'est pas impliquée et vous pouvez désigner ces volumes avec un schéma de nommage particulier.



La vérification multiadministrateur n'est pas disponible avec Cloud Volumes ONTAP.

Fonctionnement de la vérification multi-administration

La vérification multi-administrateurs comprend les éléments suivants :

- Groupe d'un ou plusieurs administrateurs ayant des pouvoirs d'approbation et de veto.
- Un ensemble d'opérations ou de commandes protégées dans une table *rules*.
- Un *moteur de règles* pour identifier et contrôler l'exécution des opérations protégées.

Les règles MAV sont évaluées après les règles de contrôle d'accès basé sur des rôles (RBAC). Par conséquent, les administrateurs qui exécutent ou approuvent les opérations protégées doivent déjà posséder le minimum de privilèges RBAC pour ces opérations. ["En savoir plus sur le RBAC"](#).

Règles définies par le système

Lorsque la vérification multi-admin est activée, les règles définies par le système (également appelées règles *Guard-rail*) établissent un ensemble d'opérations MAV pour contenir le risque de contournement du processus MAV lui-même. Ces opérations ne peuvent pas être supprimées de la table des règles. Une fois MAV activé, les opérations désignées par un astérisque (*) nécessitent l'approbation d'un ou de plusieurs administrateurs avant l'exécution, à l'exception des commandes `* show*`.

- `security multi-admin-verify modify fonctionnement *`

Contrôle la configuration de la fonctionnalité de vérification multi-administrateur.

- `security multi-admin-verify approval-group` exploitation *

Contrôlez l'appartenance à un ensemble d'administrateurs avec des informations d'identification de vérification multi-administrateur.

- `security multi-admin-verify rule` exploitation *

Contrôler le jeu de commandes qui nécessitent une vérification multi-administrateur.

- `security multi-admin-verify request` exploitation

Contrôler le processus d'approbation.

Commandes protégées par des règles

Outre les opérations définies par le système, les commandes suivantes sont protégées par défaut lorsque la vérification multiadministrateur est activée, mais vous pouvez modifier les règles pour supprimer la protection de ces commandes.

- `security login password`
- `security login unlock`
- `set`

Chaque version de ONTAP fournit plus de commandes que vous pouvez choisir de protéger avec des règles de vérification multi-admin. Choisissez votre version ONTAP pour obtenir la liste complète des commandes disponibles pour la protection.

9.15.1

- cluster date modify³
- cluster log-forwarding create³
- cluster log-forwarding delete³
- cluster log-forwarding modify³
- cluster peer delete
- cluster time-service ntp server create³
- cluster time-service ntp server delete³
- cluster time-service ntp server key create³
- cluster time-service ntp server key delete³
- cluster time-service ntp server key modify³
- cluster time-service ntp server modify³
- event config modify
- lun delete³
- security anti-ransomware volume attack clear-suspect¹
- security anti-ransomware volume disable¹
- security anti-ransomware volume event-log modify²
- security anti-ransomware volume pause¹
- security anti-ransomware vserver event-log modify²
- security audit modify³
- security ipsec config modify³
- security ipsec policy create³
- security ipsec policy delete³
- security ipsec policy modify³
- security login create
- security login delete
- security login modify
- security key-manager onboard update-passphrase³
- security saml-sp create³
- security saml-sp delete³
- security saml-sp modify³
- snaplock legal-hold end³
- storage aggregate delete³

- storage encryption disk destroy³
- storage encryption disk modify³
- storage encryption disk revert-to-original-state³
- storage encryption disk sanitize³
- system bridge run-cli³
- system controller flash-cache secure-erase run³
- system controller service-event delete³
- system health alert delete³
- system health alert modify³
- system health policy definition modify³
- system node autosupport modify³
- system node autosupport trigger modify³
- system node coredump delete³
- system node coredump delete-all³
- system node hardware nvram-encryption modify³
- system node run
- system node systemshell
- system script delete³
- system service-processor ssh add-allowed-addresses³
- system service-processor ssh remove-allowed-addresses³
- system smtape restore³
- system switch ethernet log disable-collection³
- system switch ethernet log modify³
- timezone³
- volume create³
- volume delete
- volume file privileged-delete³
- volume flexcache delete
- volume modify³
- volume recovery-queue modify²
- volume recovery-queue purge²
- volume recovery-queue purge-all²
- volume snaplock modify¹
- volume snapshot autodelete modify

- volume snapshot create³
- volume snapshot delete
- volume snapshot modify³
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename³
- volume snapshot restore
- vservers audit create³
- vservers audit delete³
- vservers audit disable³
- vservers audit modify³
- vservers audit rotate-log³
- vservers create²
- vservers delete³
- vservers modify²
- vservers object-store-server audit create³
- vservers object-store-server audit delete³
- vservers object-store-server audit disable³
- vservers object-store-server audit modify³
- vservers object-store-server audit rotate-log³
- vservers options³
- vservers peer delete
- vservers security file-directory apply³
- vservers security file-directory remove-slag³
- vservers vscan disable³
- vservers vscan on-access-policy create³
- vservers vscan on-access-policy delete³
- vservers vscan on-access-policy disable³
- vservers vscan on-access-policy modify³
- vservers vscan scanner-pool create³

- vserver vscan scanner-pool delete³

- vserver vscan scanner-pool modify³

9.14.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect¹
- security anti-ransomware volume disable¹
- security anti-ransomware volume event-log modify²
- security anti-ransomware volume pause¹
- security anti-ransomware vserver event-log modify²
- security login create
- security login delete
- security login modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume recovery-queue modify²
- volume recovery-queue purge²
- volume recovery-queue purge-all²
- volume snaplock modify¹
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete^{*}
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver create²
- vserver modify²
- vserver peer delete

9.13.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect¹
- security anti-ransomware volume disable¹
- security anti-ransomware volume pause¹
- security login create
- security login delete
- security login modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snaplock modify¹
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete*
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vservice peer delete

9.12.1/9.11.1

- cluster peer delete
- event config modify
- security login create
- security login delete
- security login modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete

- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vservers peer delete

1. Nouvelle commande protégée par des règles pour 9.13.1
2. Nouvelle commande protégée par des règles pour 9.14.1
3. Nouvelle commande protégée par des règles pour 9.15.1

*Cette commande n'est disponible qu'avec l'interface de ligne de commande et n'est pas disponible pour System Manager.

Fonctionnement de l'approbation multi-admin

Chaque fois qu'une opération protégée est saisie sur un cluster protégé par MAV, une demande d'exécution d'opération est envoyée au groupe d'administrateurs MAV désigné.

Vous pouvez configurer :

- Les noms, les coordonnées et le nombre d'administrateurs du groupe MAV.
Un administrateur MAV doit avoir un rôle RBAC avec des privilèges d'administrateur de cluster.
- Nombre de groupes d'administrateurs MAV.
 - Un groupe MAV est attribué pour chaque règle d'opération protégée.
 - Pour plusieurs groupes MAV, vous pouvez configurer quel groupe MAV approuve une règle donnée.
- Nombre d'approbations MAV nécessaires à l'exécution d'une opération protégée.
- Période_d'expiration_ de l'approbation au cours de laquelle un administrateur MAV doit répondre à une demande d'approbation.
- Période_d'expiration_ de l'exécution pendant laquelle l'administrateur demandeur doit effectuer l'opération.

Une fois ces paramètres configurés, l'approbation MAV est requise pour les modifier.

Les administrateurs MAV ne peuvent pas approuver leurs propres demandes d'exécution d'opérations protégées. Par conséquent :

- MAV ne doit pas être activé sur les clusters avec un seul administrateur.
- S'il n'y a qu'une seule personne dans le groupe MAV, cet administrateur MAV ne peut pas lancer des opérations protégées ; les administrateurs réguliers doivent lancer des opérations protégées et

l'administrateur MAV peut uniquement approuver.

- Si vous souhaitez que les administrateurs MAV puissent exécuter des opérations protégées, le nombre d'administrateurs MAV doit être supérieur d'un au nombre d'approbations requises.
Par exemple, si deux approbations sont requises pour une opération protégée et que vous voulez que les administrateurs MAV les exécutent, il doit y avoir trois personnes dans le groupe administrateurs MAV.

Les administrateurs MAV peuvent recevoir des demandes d'approbation dans des alertes par e-mail (à l'aide d'EMS) ou interroger la file d'attente des requêtes. Lorsqu'ils reçoivent une demande, ils peuvent effectuer l'une des trois actions suivantes :

- Approuver
- Rejet (veto)
- Ignorer (aucune action)

Les notifications par e-mail sont envoyées à tous les approbateurs associés à une règle MAV lorsque :

- Une demande est créée.
- Une demande est approuvée ou vetotée.
- Une requête approuvée est exécutée.

Si le demandeur se trouve dans le même groupe d'approbation pour l'opération, il recevra un e-mail lorsque sa demande est approuvée.



Un demandeur ne peut pas approuver ses propres demandes, même s'il fait partie du groupe d'approbation. Ils peuvent recevoir des notifications par e-mail. Les demandeurs qui ne sont pas dans les groupes d'approbation (c'est-à-dire qui ne sont pas des administrateurs MAV) ne reçoivent pas de notifications par e-mail.

Fonctionnement de l'exécution des opérations protégées

Si l'exécution est approuvée pour une opération protégée, l'utilisateur demandeur continue avec l'opération à l'invite. Si l'opération est mise au veto, l'utilisateur requérant doit supprimer la demande avant de continuer.

Les règles MAV sont évaluées après les autorisations RBAC. Par conséquent, un utilisateur sans autorisations RBAC suffisantes pour l'exécution de l'opération ne peut pas lancer le processus de requête MAV.

Gérer les groupes d'approbation des administrateurs

Avant d'activer la vérification multi-administrateur (MAV), vous devez créer un groupe d'approbation administrateur contenant un ou plusieurs administrateurs à accorder ou à accorder une autorité d'approbation ou de veto. Une fois que vous avez activé la vérification multi-administrateur, toute modification de l'appartenance au groupe d'approbation nécessite l'approbation de l'un des administrateurs qualifiés existants.

Description de la tâche

Vous pouvez ajouter des administrateurs existants à un groupe MAV ou créer de nouveaux administrateurs.

La fonctionnalité MAV permet de définir les paramètres existants de contrôle d'accès basé sur des rôles (RBAC). Les administrateurs MAV potentiels doivent disposer de privilèges suffisants pour exécuter des opérations protégées avant d'être ajoutés aux groupes d'administrateurs MAV. ["En savoir plus sur le RBAC."](#)



Vous pouvez configurer MAV pour avertir les administrateurs MAV que les demandes d'approbation sont en attente. Pour ce faire, vous devez configurer les notifications par e-mail, en particulier, le `Mail From` et `Mail Server` paramètres—ou vous pouvez effacer ces paramètres pour désactiver la notification. Sans alertes par e-mail, les administrateurs MAV doivent vérifier manuellement la file d'attente d'approbation.

Procédure de System Manager

Si vous souhaitez créer un groupe d'approbation MAV pour la première fois, reportez-vous à la procédure System Manager à "[activation de la vérification multi-administrateurs](#)"



Pour modifier un groupe d'approbation existant ou créer un groupe d'approbation supplémentaire :

1. Identifiez les administrateurs pour qu'ils reçoivent une vérification multi-administrateur.

- a. Cliquez sur **Cluster > Paramètres**.
- b. Cliquez sur  en regard de **utilisateurs et rôles**.
- c. Cliquez sur  **Add** sous **utilisateurs**.
- d. Modifiez la liste si nécessaire.

Pour plus d'informations, voir "[Contrôlez l'accès administrateur](#)."

2. Créer ou modifier le groupe d'approbation MAV :

- a. Cliquez sur **Cluster > Paramètres**.
- b. Cliquez sur  en regard de **Multi-Admin Approval** dans la section **sécurité**. (Vous verrez l'  icône si MAV n'est pas encore configuré.)
 - Nom : entrez un nom de groupe.
 - Approbateurs : sélectionnez des approbateurs dans une liste d'utilisateurs.
 - Adresse e-mail : saisissez une ou plusieurs adresses e-mail.
 - Groupe par défaut : sélectionnez un groupe.

Une approbation MAV est requise pour modifier une configuration existante une fois que MAV est activé.

Procédure CLI

1. Vérifier que les valeurs ont été définies pour le `Mail From` et `Mail Server` paramètres. Entrez :

```
event config show
```

L'affichage doit être similaire à ce qui suit :

```
cluster01::> event config show
                        Mail From:  admin@localhost
                        Mail Server: localhost
                        Proxy URL:   -
                        Proxy User:  -
                        Publish/Subscribe Messaging Enabled: true
```

Pour configurer ces paramètres, entrez :

```
event config modify -mail-from email_address -mail-server server_name
```

2. Identifiez les administrateurs pour qu'ils reçoivent une vérification multi-administrateur

Si vous voulez...	Saisissez cette commande
Afficher les administrateurs actuels	<code>security login show</code>
Modifier les informations d'identification des administrateurs actuels	<code>security login modify <parameters></code>
Créer de nouveaux comptes d'administrateur	<code>security login create -user-or-group -name <i>admin_name</i> -application ssh -authentication-method password</code>

3. Créer le groupe d'approbation MAV :

```
security multi-admin-verify approval-group create [ -vserver svm_name] -name  
group_name -approvers approver1[,approver2...] [[-email address1], address1...]
```

- `-vserver` - Seul le SVM d'admin est pris en charge dans cette version.
- `-name` - Le nom du groupe MAV, jusqu'à 64 caractères.
- `-approvers` - La liste d'un ou plusieurs approbateurs.
- `-email` - Une ou plusieurs adresses e-mail qui sont notifiées lors de la création, de l'approbation, du veto ou de l'exécution d'une demande.

Exemple : la commande suivante crée un groupe MAV avec deux membres et des adresses e-mail associées.

```
cluster-1::> security multi-admin-verify approval-group create -name  
mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. Vérifier la création et l'appartenance de groupe :

```
security multi-admin-verify approval-group show
```

Exemple:

```
cluster-1::> security multi-admin-verify approval-group show  
Vserver   Name           Approvers      Email  
-----  
svm-1     mav-grp1      pavan,julia    email  
pavan@myfirm.com,julia@myfirm.com
```

Utilisez ces commandes pour modifier votre configuration initiale du groupe MAV.

Remarque : tous exigent l'approbation de l'administrateur MAV avant l'exécution.

Si vous voulez...	Saisissez cette commande
Modifier les caractéristiques du groupe ou modifier les informations du membre existant	<code>security multi-admin-verify approval-group modify [parameters]</code>
Ajouter ou supprimer des membres	<code>security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[, approver2...]] [-approvers-to-remove approver1[, approver2...]]</code>
Supprimer un groupe	<code>security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name</code>

Activez et désactivez la vérification multi-administration

La vérification multi-administrateur (MAV) doit être activée explicitement. Une fois que vous avez activé la vérification multi-administrateur, l'approbation par les administrateurs d'un groupe d'approbation MAV (administrateurs MAV) est requise pour la supprimer.

Description de la tâche

Une fois MAV activé, la modification ou la désactivation de MAV nécessite l'approbation de l'administrateur MAV.



Si vous avez besoin de désactiver la fonctionnalité de vérification multi-administrateurs sans l'approbation de l'administrateur MAV, contactez le support NetApp et mentionnez l'article suivant de la base de connaissances : "[Comment désactiver la vérification multi-administrateur si MAV admin n'est pas disponible](#)".

Lorsque vous activez MAV, vous pouvez spécifier globalement les paramètres suivants.

Groupes d'approbation

Une liste de groupes d'approbation globaux. Au moins un groupe est requis pour activer la fonctionnalité MAV.



Si vous utilisez MAV avec la protection anti-ransomware autonome (ARP), définissez un nouveau groupe d'approbation ou un groupe d'approbation existant chargé d'approuver la pause ARP, de désactiver et d'effacer les demandes suspectes.

Approbateurs requis

Nombre d'approbateurs requis pour exécuter une opération protégée. La valeur par défaut et le nombre minimum sont 1.



Le nombre requis d'approbateurs doit être inférieur au nombre total d'approbateurs uniques dans les groupes d'approbation par défaut.

Expiration de l'approbation (heures, minutes, secondes)

Période pendant laquelle un administrateur MAV doit répondre à une demande d'approbation. La valeur par défaut est une heure (1h), la valeur minimale prise en charge est une seconde (1s) et la valeur maximale prise en charge est de 14 jours (14d).



Expiration de l'exécution (heures, minutes, secondes)

Période pendant laquelle l'administrateur requérant doit effectuer l'opération ∴. La valeur par défaut est une heure (1h), la valeur minimale prise en charge est une seconde (1s) et la valeur maximale prise en charge est de 14 jours (14d).

Vous pouvez également remplacer n'importe lequel de ces paramètres pour un particulier ["règles de fonctionnement."](#)



Procédure de System Manager

1. Identifiez les administrateurs pour qu'ils reçoivent une vérification multi-administrateur.

- a. Cliquez sur **Cluster > Paramètres**.
- b. Cliquez sur  en regard de **utilisateurs et rôles**.
- c. Cliquez  **Add** sous **utilisateurs**.
- d. Modifiez la liste si nécessaire.

Pour plus d'informations, voir ["Contrôlez l'accès administrateur."](#)

2. Activez la vérification multi-administration en créant au moins un groupe d'approbation et en ajoutant au moins une règle.

- a. Cliquez sur **Cluster > Paramètres**.
- b. Cliquez sur  en regard de **Multi-Admin Approval** dans la section **sécurité**.
- c. Cliquez  **Add** sur pour ajouter au moins un groupe d'approbation.
 - Nom – Entrez un nom de groupe.
 - Approbateurs : sélectionnez des approbateurs dans une liste d'utilisateurs.
 - Adresse e-mail – Entrez une ou plusieurs adresses e-mail.
 - Groupe par défaut : sélectionnez un groupe.
- d. Ajoutez au moins une règle.
 - Opération – sélectionnez une commande prise en charge dans la liste.
 - Requête – saisissez les options et les valeurs de commande souhaitées.
 - Paramètres facultatifs ; laissez vide pour appliquer des paramètres globaux ou attribuez une valeur différente pour des règles spécifiques afin de remplacer les paramètres globaux.
 - Nombre requis d'approbateurs
 - Groupes d'approbation
- e. Cliquez sur **Paramètres avancés** pour afficher ou modifier les valeurs par défaut.
 - Nombre d'approbateurs requis (par défaut : 1)
 - Expiration de la demande d'exécution (par défaut : 1 heure)
 - Expiration de la demande d'approbation (par défaut : 1 heure)
 - Serveur de messagerie*

- De l'adresse e-mail*

*Ces paramètres mettent à jour les paramètres de messagerie gérés sous "gestion des notifications". Vous êtes invité à les définir si elles n'ont pas encore été configurées.


f. Cliquez sur **Activer** pour terminer la configuration initiale du MAV.

Après la configuration initiale, l'état actuel du MAV est affiché dans la mosaïque **Multi-Admin Approval**.

- État (activé ou non)
- Opérations actives pour lesquelles des approbations sont requises
- Nombre de demandes ouvertes à l'état en attente

Vous pouvez afficher une configuration existante en cliquant sur ➔. L'approbation MAV est requise pour modifier une configuration existante.

Pour désactiver la vérification multi-administrateur :

1. Cliquez sur **Cluster > Paramètres**.
2. Cliquez sur  en regard de **Multi-Admin Approval** dans la section **sécurité**.
3. Cliquez sur le bouton bascule activé.

L'approbation MAV est requise pour effectuer cette opération.

Procédure CLI

Avant d'activer la fonctionnalité MAV au niveau de la CLI, au moins une "Groupe administrateur MAV" doit avoir été créé.

Si vous voulez...	Saisissez cette commande
Activer la fonctionnalité MAV	<pre>security multi-admin-verify modify -approval-groups group1[,group2...] [- required-approvers nn] -enabled true [-execution-expiry [nnh][nmm][nns]] [-approval-expiry [nnh][nmm][nns]]</pre> <p>Exemple : la commande suivante active MAV avec 1 groupe d'approbation, 2 approbateurs requis et périodes d'expiration par défaut.</p> <pre>cluster-1::> security multi-admin- verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true</pre> <p>Terminez la configuration initiale en ajoutant au moins une configuration "règle de fonctionnement."</p>

Si vous voulez...	Saisissez cette commande
Modifier une configuration MAV (nécessite l'approbation MAV)	<pre>security multi-admin-verify approval-group modify [-approval-groups group1 [,group2...]] [-required-approvers nn] [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]</pre>
Vérifier la fonctionnalité MAV	<pre>security multi-admin-verify show</pre> <p>Exemple:</p> <pre>cluster-1::> security multi-admin-verify show Is Required Execution Approval Approval Enabled Approvers Expiry Expiry Groups ----- true 2 1h 1h mav-grp1</pre>
Désactiver la fonctionnalité MAV (nécessite l'approbation MAV)	<pre>security multi-admin-verify modify -enabled false</pre>

Gérer les règles d'opération protégées

Vous créez des règles de vérification multi-administration (MAV) pour désigner des opérations nécessitant une approbation. Chaque fois qu'une opération est lancée, des opérations protégées sont interceptées et une demande d'approbation est générée.

Les règles peuvent être créées avant d'activer MAV par tout administrateur disposant des fonctionnalités RBAC appropriées, mais une fois MAV activé, toute modification de l'ensemble de règles nécessite l'approbation MAV.

Une seule règle MAV peut être créée par opération ; par exemple, vous ne pouvez pas en créer plusieurs `volume-snapshot-delete` règles. Toutes les contraintes de règle souhaitées doivent être contenues dans une règle.

Vous pouvez créer des règles à protéger "[ces commandes](#)". Vous pouvez protéger chaque commande en commençant par la version ONTAP dans laquelle la fonctionnalité de protection pour la commande a été mise à disposition pour la première fois.

Les règles pour les commandes par défaut du système MAV, le `security multi-admin-verify` "[commandes](#)", ne peut pas être modifié.

Outre les opérations définies par le système, les commandes suivantes sont protégées par défaut lorsque la

vérification multiadministrateur est activée, mais vous pouvez modifier les règles pour supprimer la protection de ces commandes.

- security login password
- security login unlock
- set

Contraintes de règle

Lorsque vous créez une règle, vous pouvez éventuellement spécifier le `-query` option permettant de limiter la demande à un sous-ensemble de la fonctionnalité de la commande. Le `-query` Option peut également être utilisée pour limiter les éléments de configuration tels que la SVM, le volume et les noms des snapshots.

Par exemple, dans le `volume snapshot delete` commande `-query` peut être défini sur `-snapshot !hourly*,!daily*,!weekly*`, Ce qui signifie que les instantanés de volume préfixés avec des attributs horaires, quotidiens ou hebdomadaires sont exclus des protections MAV.

```
smci-vsimg20::> security multi-admin-verify rule show
```

		Required	Approval
Vserver	Operation	Approvers	Groups
vs01	volume snapshot delete	-	-
	Query: -snapshot !hourly*,!daily*,!weekly*		



Tous les éléments de configuration exclus ne seraient pas protégés par MAV, et tout administrateur pourrait les supprimer ou les renommer.

Par défaut, les règles spécifient qu'un correspondant `security multi-admin-verify request create "protected_operation"` la commande est générée automatiquement lorsqu'une opération protégée est saisie. Vous pouvez modifier cette valeur par défaut pour exiger que la `request create` la commande doit être saisie séparément.

Par défaut, les règles héritent des paramètres généraux MAV suivants, bien que vous puissiez spécifier des exceptions spécifiques aux règles :

- Nombre requis d'approbateurs
- Groupes d'approbation
- Période d'expiration de l'approbation
- Période d'expiration de l'exécution

Procédure de System Manager

Pour ajouter une règle d'opération protégée pour la première fois, reportez-vous à la procédure de System Manager à ["activation de la vérification multi-administrateurs"](#)

Pour modifier le jeu de règles existant :

1. Sélectionnez **Cluster > Paramètres**.

2. Sélectionnez  en regard de **Multi-Admin Approval** dans la section **sécurité**.
3. Sélectionnez  **Add** cette option pour ajouter au moins une règle ; vous pouvez également modifier ou supprimer des règles existantes.
 - Opération – sélectionnez une commande prise en charge dans la liste.
 - Requête – saisissez les options et les valeurs de commande souhaitées.
 - Paramètres facultatifs – laissez vide pour appliquer des paramètres globaux ou attribuez une valeur différente pour des règles spécifiques afin de remplacer les paramètres globaux.
 - Nombre requis d'approbateurs
 - Groupes d'approbation

Procédure CLI



Tout `security multi-admin-verify rule` Les commandes exigent l'approbation de l'administrateur MAV avant leur exécution, sauf `security multi-admin-verify rule show`.

Si vous voulez...	Saisissez cette commande
Créer une règle	<code>security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]</code>
Modifier les informations d'identification des administrateurs actuels	<code>security login modify <parameters></code> Exemple : la règle suivante nécessite l'approbation pour supprimer le volume racine. <code>security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"</code>
Modifier une règle	<code>security multi-admin-verify rule modify -operation "protected_operation" [parameters]</code>
Supprimer une règle	<code>security multi-admin-verify rule delete -operation "protected_operation"</code>
Afficher les règles	<code>security multi-admin-verify rule show</code>

Pour plus d'informations sur la syntaxe de commande, reportez-vous à la section `security multi-admin-verify rule` pages de manuel.

Demander l'exécution d'opérations protégées

Lorsque vous lancez une opération ou une commande protégée sur un cluster activé pour la vérification multi-administrateur (MAV), ONTAP intercepte automatiquement

l'opération et demande de générer une requête qui doit être approuvée par un ou plusieurs administrateurs d'un groupe d'approbation MAV (administrateurs MAV). Vous pouvez également créer une requête MAV sans la boîte de dialogue.

Si elle est approuvée, vous devez alors répondre à la requête pour terminer l'opération dans le délai d'expiration de la requête. Si vous vous êtes opposé ou si les périodes de demande ou d'expiration sont dépassées, vous devez supprimer la demande et la renvoyer.

La fonctionnalité MAV permet de définir les paramètres RBAC existants. C'est-à-dire que votre rôle d'administrateur doit disposer de privilèges suffisants pour exécuter une opération protégée sans tenir compte des paramètres MAV. ["En savoir plus sur le RBAC"](#).

Si vous êtes administrateur MAV, vos demandes d'exécution d'opérations protégées doivent également être approuvées par un administrateur MAV.

Procédure de System Manager

Lorsqu'un utilisateur clique sur un élément de menu pour lancer une opération et que l'opération est protégée, une demande d'approbation est générée et l'utilisateur reçoit une notification semblable à ce qui suit :

```
Approval request to delete the volume was sent.  
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

La fenêtre **Multi-Admin Requests** est disponible lorsque MAV est activé, affichant les demandes en attente basées sur l'ID de connexion et le rôle MAV de l'utilisateur (approbateur ou non). Pour chaque demande en attente, les champs suivants sont affichés :

- Fonctionnement
- Index (nombre)
- État (en attente, approuvé, rejeté, exécuté ou expiré)

Si une demande est rejetée par un approbateur, aucune autre action n'est possible.

- Requête (tous les paramètres ou valeurs de l'opération demandée)
- Utilisateur demandeur
- La demande expire le
- (Nombre de) approbateurs en attente
- (Nombre de) approbateurs potentiels

Lorsque la demande est approuvée, l'utilisateur demandeur peut relancer l'opération dans la période d'expiration.

Si l'utilisateur tente de nouveau l'opération sans approbation, une notification s'affiche comme suit :

```
Request to perform delete operation is pending approval.  
Retry the operation after request is approved.
```

Procédure CLI

1. Entrez directement l'opération protégée ou à l'aide de la commande MAV request.

Exemples – pour supprimer un volume, entrez l'une des commandes suivantes :

° volume delete

```
cluster-1::*> volume delete -volume voll -vserver vs0
```

```
Warning: This operation requires multi-admin verification. To create  
a
```

```
    verification request use "security multi-admin-verify  
request  
    create".
```

```
    Would you like to create a request for this operation?  
    {y|n}: y
```

```
Error: command failed: The security multi-admin-verify request (index  
3) is  
    auto-generated and requires approval.
```

° security multi-admin-verify request create "volume delete"

```
Error: command failed: The security multi-admin-verify request (index  
3)  
    requires approval.
```

2. Vérifier l'état de la demande et répondre à l'avis MAV.

- a. Si la requête est approuvée, répondez au message de l'interface de ligne de commande pour terminer l'opération.

Exemple:

```
cluster-1::> security multi-admin-verify request show 3
```

```
    Request Index: 3
      Operation: volume delete
        Query: -vserver vs0 -volume voll1
        State: approved
Required Approvers: 1
Pending Approvers: 0
  Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
    Approvals: admin2
    User Vetoed: -
      Vserver: cluster-1
  User Requested: admin
    Time Created: 2/25/2022 13:32:03
    Time Approved: 2/25/2022 13:35:36
      Comment: -
  Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll1 -vserver vs0
```

Info: Volume "voll1" in Vserver "vs0" will be marked as deleted and placed in the volume recovery queue. The space used by the volume will be recovered only after the retention period of 12 hours has completed. To recover the space immediately, get the volume name using (privilege:advanced) "volume recovery-queue show voll_*" and then "volume recovery-queue purge -vserver vs0 -volume <volume_name>" command. To recover the volume use the (privilege:advanced) "volume recovery-queue recover -vserver vs0 -volume <volume_name>" command.

Warning: Are you sure you want to delete volume "voll1" in Vserver "vs0" ?
{y|n}: y

- b. Si la demande est voetotée ou si la période d'expiration est passée, supprimez la demande et relancez ou contactez l'administrateur MAV.

Exemple:

```
cluster-1::> security multi-admin-verify request show 3
```

```
Request Index: 3
  Operation: volume delete
    Query: -vserver vs0 -volume voll1
    State: vetoed
Required Approvers: 1
Pending Approvers: 1
Approval Expiry: 2/25/2022 14:38:47
Execution Expiry: -
  Approvals: -
    User Vetoed: admin2
    Vserver: cluster-1
User Requested: admin
  Time Created: 2/25/2022 13:38:47
  Time Approved: -
    Comment: -
Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll1 -vserver vs0
```

```
Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

Gérer les demandes d'opérations protégées

Lorsque les administrateurs d'un groupe d'approbation MAV (administrateurs MAV) sont avertis d'une demande d'exécution d'opération en attente, ils doivent répondre par un message d'approbation ou de veto dans un délai fixe (expiration de l'approbation). Si un nombre suffisant d'approbations n'est pas reçu, le demandeur doit supprimer la demande et en faire une autre.

Description de la tâche

Les demandes d'approbation sont identifiées par des numéros d'index, qui sont inclus dans les e-mails et sont affichées dans la file d'attente des demandes.

Les informations suivantes de la file d'attente de demandes peuvent être affichées :

Fonctionnement

Opération protégée pour laquelle la demande est créée.

Requête

Objet (ou objets) sur lequel l'utilisateur souhaite appliquer l'opération.

État

État actuel de la demande ; en attente, approuvé, rejeté, expiré, exécuté. Si une demande est rejetée par un approbateur, aucune autre action n'est possible.

Approbateurs requis

Nombre d'administrateurs MAV requis pour approuver la demande. Un utilisateur peut définir le paramètre approbateurs requis pour la règle d'opération. Si un utilisateur ne définit pas les approbateurs requis sur la règle, les approbateurs requis du paramètre global sont appliqués.

Approbateurs en attente

Nombre d'administrateurs MAV toujours requis pour approuver la demande pour que la demande soit marquée comme approuvée.

Expiration de l'approbation

Période pendant laquelle un administrateur MAV doit répondre à une demande d'approbation. Tout utilisateur autorisé peut définir la règle d'approbation-expiration d'une opération. Si l'approbation-expiration n'est pas définie pour la règle, l'approbation-expiration du paramètre global est appliquée.

Expiration de l'exécution

Période pendant laquelle l'administrateur requérant doit terminer l'opération. Tout utilisateur autorisé peut définir une règle d'exécution-expiration pour une opération. Si exécution-expiration n'est pas définie pour la règle, l'exécution-expiration du paramètre global est appliquée.

Utilisateurs approuvés

Les administrateurs MAV qui ont approuvé la demande.

L'utilisateur a refusé son droit d'veto

Les administrateurs MAV qui ont opposé leur veto à la demande.

VM de stockage (vServer)

SVM avec lequel la requête est associée. Seule le SVM d'administration est pris en charge dans cette version.

Utilisateur demandé

Nom d'utilisateur de l'utilisateur qui a créé la demande.

Heure de création

Heure de création de la demande.

Heure d'approbation

Heure à laquelle l'état de la demande passe à approuvé.

Commentaire

Tout commentaire associé à la demande.

Utilisateurs autorisés

Liste des utilisateurs autorisés à effectuer l'opération protégée pour laquelle la demande est approuvée. Si `users-permitted` est vide, alors tout utilisateur disposant des autorisations appropriées peut effectuer l'opération.

Toutes les demandes expirées ou exécutées sont supprimées lorsqu'une limite de 1000 demandes est atteinte ou lorsque la durée d'expiration est supérieure à 8 heures pour les demandes expirées. Les demandes de veto

sont supprimées dès qu'elles sont marquées comme expirées.

Procédure de System Manager

Les administrateurs MAV reçoivent des e-mails contenant les détails de la demande d'approbation, la période d'expiration de la demande et un lien pour approuver ou rejeter la demande. Ils peuvent accéder à une boîte de dialogue d'approbation en cliquant sur le lien dans l'e-mail ou accédez à **Events & Jobs> requêtes** dans System Manager.

La fenêtre **requêtes** est disponible lorsque la vérification multi-administrateur est activée, affichant les demandes en attente basées sur l'ID de connexion de l'utilisateur et le rôle MAV (approbateur ou non).

- Fonctionnement
- Index (nombre)
- État (en attente, approuvé, rejeté, exécuté ou expiré)

Si une demande est rejetée par un approbateur, aucune autre action n'est possible.

- Requête (tous les paramètres ou valeurs de l'opération demandée)
- Utilisateur demandeur
- La demande expire le
- (Nombre de) approbateurs en attente
- (Nombre de) approbateurs potentiels

Les administrateurs MAV disposent de contrôles supplémentaires dans cette fenêtre ; ils peuvent approuver, rejeter ou supprimer des opérations individuelles ou des groupes d'opérations sélectionnés. Toutefois, si l'administrateur MAV est l'utilisateur qui demande, il ne peut approuver, rejeter ou supprimer ses propres demandes.

Procédure CLI

1. Lorsqu'une demande est signalée par courrier électronique en attente, notez le numéro d'index de la demande et la période d'expiration de l'approbation. Le numéro d'index peut également être affiché à l'aide des options **show** ou **show-Pending** mentionnées ci-dessous.
2. Approuver ou opposer un veto à la demande.

Si vous voulez...	Saisissez cette commande
Approuver une demande	<code>security multi-admin-verify request approve nn</code>
Veto sur une demande	<code>security multi-admin-verify request veto nn</code>
Affiche toutes les demandes, les demandes en attente ou une seule demande	<code>`security multi-admin-verify request { show</code>

Si vous voulez...	Saisissez cette commande
<pre>show-pending } [nn] { -fields field1[,field2...]</pre>	<pre>[-instance] }</pre> <p>Vous pouvez afficher toutes les demandes dans la file d'attente ou uniquement les demandes en attente. Si vous saisissez le numéro d'index, seules les informations pour ce numéro sont affichées. Vous pouvez afficher des informations sur des champs spécifiques (en utilisant le <code>-fields</code> paramètre) ou à propos de tous les champs (en utilisant le <code>-instance</code> paramètre).</p>
Supprimer une demande	<pre>security multi-admin-verify request delete nn</pre>

Exemple :

La séquence suivante approuve une demande après que l'administrateur MAV ait reçu l'e-mail de demande avec l'index numéro 3, qui a déjà une approbation.

```

cluster1::> security multi-admin-verify request show-pending
                                Pending
Index Operation      Query State  Approvers Requestor
-----
3 volume delete -    pending 1      julia

```

```
cluster-1::> security multi-admin-verify request approve 3
```

```
cluster-1::> security multi-admin-verify request show 3
```

```

Request Index: 3
  Operation: volume delete
    Query: -
    State: approved
Required Approvers: 2
Pending Approvers: 0
Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
Approvals: mav-admin2
User Vetoed: -
  Vserver: cluster-1
User Requested: julia
Time Created: 2/25/2022 13:32:03
Time Approved: 2/25/2022 13:35:36
Comment: -
Users Permitted: -

```

Exemple :

La séquence suivante affiche une demande après que l'administrateur MAV ait reçu l'e-mail de demande avec l'index numéro 3, qui a déjà une approbation.

```

cluster1::> security multi-admin-verify request show-pending
                                Pending
Index Operation      Query State  Approvers Requestor
-----
3 volume delete -    pending 1      pavan

cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
  Operation: volume delete
    Query: -
    State: vetoed
Required Approvers: 2
Pending Approvers: 0
Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
  Approvals: mav-admin1
  User Vetoed: mav-admin2
    Vserver: cluster-1
User Requested: pavan
  Time Created: 2/25/2022 13:32:03
  Time Approved: 2/25/2022 13:35:36
    Comment: -
Users Permitted: -

```

Gérer l'autorisation dynamique

Présentation de l'autorisation dynamique

À partir de ONTAP 9.15.1, les administrateurs peuvent configurer et activer l'autorisation dynamique afin d'accroître la sécurité de l'accès à distance à ONTAP, tout en limitant les dommages potentiels causés par un acteur malveillant. Avec ONTAP 9.15.1, l'autorisation dynamique fournit une structure initiale pour attribuer une note de sécurité aux utilisateurs et, si leur activité semble suspecte, les défier avec des vérifications d'autorisation supplémentaires ou refuser complètement une opération. Les administrateurs peuvent créer des règles, attribuer des scores de confiance et restreindre des commandes pour déterminer si certaines activités sont autorisées ou refusées pour un utilisateur. Les administrateurs peuvent activer l'autorisation dynamique à l'échelle du cluster ou pour des machines virtuelles de stockage individuelles.

Fonctionnement de l'autorisation dynamique

L'autorisation dynamique utilise un système de notation de confiance pour attribuer aux utilisateurs un niveau de confiance différent en fonction des stratégies d'autorisation. En fonction du niveau de confiance de l'utilisateur, une activité qu'il effectue peut être autorisée ou refusée, ou l'utilisateur peut être invité à demander une authentification supplémentaire.

Reportez-vous ["Personnaliser l'autorisation dynamique"](#) à la pour en savoir plus sur la configuration de la pondération des scores des critères et d'autres attributs d'autorisation dynamique.

Périphériques de confiance

Lorsque l'autorisation dynamique est utilisée, la définition d'un périphérique approuvé est un périphérique utilisé par un utilisateur pour se connecter à ONTAP à l'aide de l'authentification par clé publique comme une des méthodes d'authentification. Le périphérique est approuvé car seul cet utilisateur possède la clé privée correspondante.

Exemple d'autorisation dynamique

Prenons l'exemple de trois utilisateurs différents qui tentent de supprimer un volume. Lorsqu'ils tentent d'effectuer l'opération, la cote de risque de chaque utilisateur est examinée :

- Le premier utilisateur se connecte à partir d'un périphérique de confiance avec très peu d'échecs d'authentification précédents, ce qui rend son niveau de risque faible ; l'opération est autorisée sans authentification supplémentaire.
- Le deuxième utilisateur se connecte à partir d'un périphérique de confiance avec un pourcentage modéré d'échecs d'authentification précédents, ce qui rend la note de risque modérée ; il est invité à demander une authentification supplémentaire avant que l'opération ne soit autorisée.
- Le troisième utilisateur se connecte à partir d'un périphérique non approuvé avec un pourcentage élevé d'échecs d'authentification précédents, ce qui rend l'indice de risque élevé ; l'opération n'est pas autorisée.

Et la suite

- ["Activer ou désactiver l'autorisation dynamique"](#)
- ["Personnaliser l'autorisation dynamique"](#)

Activer ou désactiver l'autorisation dynamique

À partir de ONTAP 9.15.1, les administrateurs peuvent configurer et activer l'autorisation dynamique dans `visibility` pour tester la configuration, ou dans `enforced Mode` pour activer la configuration des utilisateurs de l'interface de ligne de commande qui se connectent via SSH. Si vous n'avez plus besoin d'une autorisation dynamique, vous pouvez la désactiver. Lorsque vous désactivez l'autorisation dynamique, les paramètres de configuration restent disponibles et vous pouvez les utiliser ultérieurement si vous décidez de la réactiver.

Pour plus d'informations sur les paramètres de la `security dynamic-authorization modify` commande, reportez-vous au ["Pages de manuel ONTAP"](#).

Activer l'autorisation dynamique pour les tests

Vous pouvez activer l'autorisation dynamique en mode visibilité, ce qui vous permet de tester la fonction et de vous assurer que les utilisateurs ne seront pas accidentellement verrouillés. Dans ce mode, le score de

confiance est vérifié avec chaque activité restreinte, mais pas appliqué. Cependant, toute activité qui aurait été refusée ou qui aurait fait l'objet de défis d'authentification supplémentaires est consignée. Il est recommandé de tester les paramètres souhaités dans ce mode avant de les appliquer.



Vous pouvez suivre cette étape pour activer l'autorisation dynamique pour la première fois, même si vous n'avez pas encore configuré d'autres paramètres d'autorisation dynamique. Reportez-vous à la section "[Personnaliser l'autorisation dynamique](#)" pour savoir comment configurer d'autres paramètres d'autorisation dynamique afin de les personnaliser en fonction de votre environnement.

Étapes

1. Activez l'autorisation dynamique en mode visibilité en configurant les paramètres globaux et en définissant l'état de la fonction sur `visibility`. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Mettez à jour les valeurs entre parenthèses `<>` pour les adapter à votre environnement. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization modify \  
<strong>-state visibility</strong> \  
-lower-challenge-boundary <percent> \  
-upper-challenge-boundary <percent> \  
-suppression-interval <interval> \  
-vserver <storage_VM_name>
```

2. Vérifiez le résultat à l'aide de `show` commande pour afficher la configuration globale :

```
security dynamic-authorization show
```

Activer l'autorisation dynamique en mode imposé

Vous pouvez activer l'autorisation dynamique en mode imposé. En général, vous utilisez ce mode une fois les tests effectués en mode visibilité. Dans ce mode, le score de confiance est vérifié pour chaque activité restreinte et les restrictions d'activité sont appliquées si les conditions de restriction sont remplies. L'intervalle de suppression est également appliqué, ce qui évite des problèmes d'authentification supplémentaires dans l'intervalle spécifié.



Cette étape suppose que vous avez précédemment configuré et activé l'autorisation dynamique dans `visibility` ce qui est fortement recommandé.

Étapes

1. Activer l'autorisation dynamique dans `enforced` en changeant son état à `enforced`. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Mettez à jour les valeurs entre parenthèses `<>` pour les adapter à votre environnement. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization modify \  
<strong>-state enforced</strong> \  
-vserver <storage_VM_name>
```

2. Vérifiez le résultat à l'aide de `show` commande pour afficher la configuration globale :

```
security dynamic-authorization show
```

Désactiver l'autorisation dynamique

Vous pouvez désactiver l'autorisation dynamique si vous n'avez plus besoin de la sécurité d'authentification supplémentaire.

Étapes

1. Désactivez l'autorisation dynamique en changeant son état à `disabled`. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Mettez à jour les valeurs entre parenthèses `<>` pour les adapter à votre environnement. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage_VM_name>
```

2. Vérifiez le résultat à l'aide de `show` commande pour afficher la configuration globale :

```
security dynamic-authorization show
```

Et la suite

(Facultatif) en fonction de votre environnement, reportez-vous à la section "[Personnaliser l'autorisation dynamique](#)" pour configurer d'autres paramètres d'autorisation dynamique.

Personnaliser l'autorisation dynamique

En tant qu'administrateur, vous pouvez personnaliser différents aspects de votre configuration d'autorisation dynamique afin d'améliorer la sécurité des connexions SSH d'administrateur distant avec votre cluster ONTAP.

Vous pouvez personnaliser les paramètres d'autorisation dynamiques suivants en fonction de vos besoins en matière de sécurité :

- [Configurer les paramètres globaux d'autorisation dynamique](#)
- [Configurer les composants de score de confiance d'autorisation dynamique](#)
- [Configurez un fournisseur de score de confiance personnalisé](#)
- [Configurer les commandes restreintes](#)
- [Configurer des groupes d'autorisation dynamiques](#)

Configurer les paramètres globaux d'autorisation dynamique

Vous pouvez configurer des paramètres globaux pour l'autorisation dynamique, y compris la VM de stockage à sécuriser, l'intervalle de suppression pour les défis d'authentification et les paramètres de score de confiance.

Pour plus d'informations sur les paramètres et les valeurs par défaut de la `security dynamic-authorization modify` commande, reportez-vous au ["Pages de manuel ONTAP"](#).

Étapes

1. Configurer les paramètres globaux pour l'autorisation dynamique. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Mettez à jour les valeurs entre parenthèses `<>` pour les adapter à votre environnement :

```
security dynamic-authorization modify \  
-lower-challenge-boundary <percent> \  
-upper-challenge-boundary <percent> \  
-suppression-interval <interval> \  
-vserver <storage_VM_name>
```

2. Afficher la configuration résultante :

```
security dynamic-authorization show
```

Configurer les commandes restreintes

Lorsque vous activez l'autorisation dynamique, la fonction inclut un ensemble par défaut de commandes restreintes. Vous pouvez modifier cette liste en fonction de vos besoins. Reportez-vous à la ["Documentation de vérification multiadministrateur"](#) pour plus d'informations sur la liste par défaut des commandes restreintes.

Ajouter une commande restreinte

Vous pouvez ajouter une commande à la liste des commandes dont l'autorisation dynamique est limitée.

Pour plus d'informations sur les paramètres et les valeurs par défaut de la `security dynamic-authorization rule create` commande, reportez-vous au ["Pages de manuel ONTAP"](#).

Étapes

1. Ajoutez la commande. Mettez à jour les valeurs entre parenthèses `<>` pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization rule create \  
-query <query> \  
<strong>-operation <text></strong> \  
-index <integer> \  
-vserver <storage_VM_name>
```

2. Afficher la liste résultante des commandes restreintes :

```
security dynamic-authorization rule show
```

Supprime une commande restreinte

Vous pouvez supprimer une commande de la liste des commandes dont l'autorisation dynamique est limitée.

Pour plus d'informations sur les paramètres et les valeurs par défaut de la `security dynamic-authorization rule delete` commande, reportez-vous au ["Pages de manuel ONTAP"](#).

Étapes

1. Supprimez la commande. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization rule delete \  
<strong>-operation <text></strong> \  
-vserver <storage_VM_name>
```

2. Afficher la liste résultante des commandes restreintes :

```
security dynamic-authorization rule show
```

Configurer des groupes d'autorisation dynamiques

Par défaut, l'autorisation dynamique s'applique à tous les utilisateurs et groupes dès que vous l'activez. Toutefois, vous pouvez créer des groupes à l'aide de `security dynamic-authorization group create` de sorte que l'autorisation dynamique ne s'applique qu'à ces utilisateurs spécifiques.

Ajouter un groupe d'autorisation dynamique

Vous pouvez ajouter un groupe d'autorisation dynamique.

Pour plus d'informations sur les paramètres et les valeurs par défaut de la `security dynamic-authorization group create` commande, reportez-vous au ["Pages de manuel ONTAP"](#).

Étapes

1. Créez le groupe. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization group create \  
<strong>-group-name <group-name></strong> \  
-vserver <storage_VM_name> \  
-exclude-users <user1,user2,user3...>
```

2. Afficher les groupes d'autorisation dynamiques résultants :

```
security dynamic-authorization group show
```

Supprimer un groupe d'autorisation dynamique

Vous pouvez supprimer un groupe d'autorisation dynamique.

Pour plus d'informations sur les paramètres et les valeurs par défaut de la `security dynamic-authorization group delete` commande, reportez-vous au ["Pages de manuel ONTAP"](#).

Étapes

1. Supprimez le groupe. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization group delete \  
<strong>-group-name <group-name></strong> \  
-vserver <storage_VM_name>
```

2. Afficher les groupes d'autorisation dynamiques résultants :

```
security dynamic-authorization group show
```

Configurer les composants de score de confiance d'autorisation dynamique

Vous pouvez configurer la pondération maximale du score pour modifier la priorité des critères de notation ou pour supprimer certains critères de l'évaluation du risque.



Dans le cadre de la meilleure pratique, vous devez laisser les valeurs de pondération par défaut en place et les ajuster uniquement si nécessaire.

Pour plus d'informations sur les paramètres et les valeurs par défaut de la `security dynamic-authorization trust-score-component modify` commande, reportez-vous au ["Pages de manuel ONTAP"](#).

Vous pouvez modifier les composants suivants, ainsi que leur score par défaut et leur pondération en pourcentage :

Critères	Nom du composant	Pondération de score brut par défaut	Poids en pourcentage par défaut
Périphérique de confiance	trusted-device	20	50
Historique d'authentification de connexion utilisateur	authentication-history	20	50

Étapes

1. Modifier les composants du score de confiance. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. Afficher les paramètres des composants du score de confiance obtenu :

```
security dynamic-authorization trust-score-component show
```

Réinitialiser le score de confiance d'un utilisateur

Si l'accès d'un utilisateur est refusé en raison de stratégies système et qu'il est capable de prouver son identité, l'administrateur peut réinitialiser le score de confiance de l'utilisateur.

Pour plus d'informations sur les paramètres et les valeurs par défaut de la `security dynamic-authorization user-trust-score reset` commande, reportez-vous au ["Pages de manuel ONTAP"](#) .

Étapes

1. Ajoutez la commande. Reportez-vous à la section [Configurer les composants de score de confiance d'autorisation dynamique](#) pour obtenir une liste des composants de score de confiance que vous pouvez réinitialiser. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage_VM_name>
```

Afficher votre score de confiance

Un utilisateur peut afficher son propre score de confiance pour une session de connexion.

Étapes

1. Afficher votre score de confiance :

```
security login whoami
```

Vous devez voir les résultats similaires à ce qui suit :

```
User: admin
Role: admin
Trust Score: 50
```

Configurez un fournisseur de score de confiance personnalisé

Si vous recevez déjà des méthodes de notation d'un fournisseur de score de confiance externe, vous pouvez ajouter le fournisseur personnalisé à la configuration d'autorisation dynamique.

Avant de commencer

- Le fournisseur de score de confiance personnalisé doit renvoyer une réponse JSON. Les conditions de syntaxe suivantes doivent être remplies :
 - Le champ qui renvoie le score de confiance doit être un champ scalaire et non un élément d'un tableau.
 - Le champ qui renvoie le score de confiance peut être un champ imbriqué, tel que `trust_score.value`.
 - Il doit y avoir un champ dans la réponse JSON qui renvoie un score de confiance numérique. Si ce n'est pas disponible en natif, vous pouvez écrire un script wrapper pour renvoyer cette valeur.
- La valeur fournie peut être un score de confiance ou un score de risque. La différence est que le score de confiance est dans l'ordre croissant avec un score plus élevé indiquant un niveau de confiance plus élevé, alors que le score de risque est dans l'ordre décroissant. Par exemple, un score de confiance de 90 pour une plage de scores de 0 à 100 indique que le score est très digne de confiance et qu'il est susceptible d'aboutir à un « Autoriser » sans défi supplémentaire, bien qu'un score de risque de 90 pour une plage de scores de 0 à 100 indique un risque élevé et risque de donner lieu à un « refus » sans défi supplémentaire.
- Le fournisseur de score de confiance personnalisé doit être accessible via l'API REST de ONTAP.
- Le fournisseur de score de confiance personnalisé doit être configurable à l'aide de l'un des paramètres pris en charge. Les fournisseurs de score de confiance personnalisés qui nécessitent une configuration ne figurant pas dans la liste des paramètres pris en charge ne sont pas pris en charge.

Pour plus d'informations sur les paramètres et les valeurs par défaut de la `security dynamic-authorization trust-score-component create` commande, reportez-vous au ["Pages de manuel ONTAP"](#).

Étapes

1. Ajoutez un fournisseur de score de confiance personnalisé. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. Afficher les paramètres du fournisseur de score de confiance :

```
security dynamic-authorization trust-score-component show
```

Configurer les balises de fournisseur de score de confiance personnalisé

Vous pouvez communiquer avec des fournisseurs externes de score de confiance à l'aide de balises. Cela vous permet d'envoyer des informations dans l'URL au fournisseur de score de confiance sans exposer d'informations sensibles.

Pour plus d'informations sur les paramètres et les valeurs par défaut de la `security dynamic-authorization trust-score-component create` commande, reportez-vous au ["Pages de manuel ONTAP"](#).

Étapes

1. Activer les balises de fournisseur de score de confiance. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key_text>"</strong>
```

Par exemple :

```
security dynamic-authorization trust-score-component create -component
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score
-field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

Authentification et autorisation via OAuth 2.0

Présentation de la mise en œuvre de ONTAP OAuth 2.0

Depuis ONTAP 9.14, vous avez la possibilité de contrôler l'accès à vos clusters ONTAP à l'aide de l'infrastructure d'autorisation ouverte (OAuth 2.0). Vous pouvez configurer cette fonctionnalité à l'aide de n'importe quelle interface d'administration ONTAP, notamment l'interface de ligne de commandes ONTAP, System Manager et l'API REST. Cependant, les décisions d'autorisation et de contrôle d'accès OAuth 2.0 ne peuvent être appliquées que lorsqu'un client accède à ONTAP à l'aide de l'API REST.



La prise en charge d'OAuth 2.0 a été introduite pour la première fois avec ONTAP 9.14.0. Sa disponibilité dépend donc de la version ONTAP que vous utilisez. Voir la ["Notes de version de ONTAP"](#) pour en savoir plus.

Caractéristiques et avantages

Les principales caractéristiques et avantages de l'utilisation d'OAuth 2.0 avec ONTAP sont décrits ci-dessous.

Prise en charge de la norme OAuth 2.0

OAuth 2.0 est le cadre d'autorisation standard de l'industrie. Il permet de restreindre et de contrôler l'accès aux ressources protégées à l'aide de jetons d'accès signés. L'utilisation d'OAuth 2.0 présente plusieurs avantages :

- De nombreuses options pour la configuration de l'autorisation
- Ne jamais révéler les informations d'identification du client, y compris les mots de passe
- Les tokens peuvent être définis pour expirer en fonction de votre configuration
- La solution est idéale pour une utilisation avec les API REST

Testé avec plusieurs serveurs d'autorisation courants

L'implémentation ONTAP est conçue pour être compatible avec tout serveur d'autorisation compatible OAuth 2.0. Il a été testé avec les serveurs ou services populaires suivants, notamment :

- Auth0
- ADFS (Active Directory Federation Service)
- Porte-clés

Prise en charge de plusieurs serveurs d'autorisation simultanés

Vous pouvez définir jusqu'à huit serveurs d'autorisation pour un seul cluster ONTAP. Vous disposez ainsi de la flexibilité nécessaire pour répondre aux besoins de votre environnement de sécurité diversifié.

Intégration avec les rôles REST

Les décisions d'autorisation ONTAP sont finalement basées sur les rôles REST attribués aux utilisateurs ou aux groupes. Ces rôles sont soit portés dans le jeton d'accès en tant que étendues autonomes, soit basés sur des définitions ONTAP locales avec Active Directory ou des groupes LDAP.

Option permettant d'utiliser des jetons d'accès limités par l'expéditeur

Vous pouvez configurer ONTAP et les serveurs d'autorisation pour utiliser MTLS (Mutual transport Layer Security) qui renforce l'authentification des clients. Il garantit que les jetons d'accès OAuth 2.0 ne sont utilisés que par les clients auxquels ils ont été émis à l'origine. Cette fonction prend en charge et s'aligne sur plusieurs recommandations de sécurité courantes, y compris celles établies par FAPI et MITRE.

Implémentation et configuration

À un niveau élevé, il existe plusieurs aspects de la mise en œuvre et de la configuration d'OAuth 2.0 que vous devez prendre en compte lors de la mise en route.

OAuth 2.0 entités au sein de ONTAP

Le cadre d'autorisation OAuth 2.0 définit plusieurs entités qui peuvent être mappées à des éléments réels ou virtuels au sein de votre centre de données ou de votre réseau. Les entités OAuth 2.0 et leur adaptation à ONTAP sont présentées dans le tableau ci-dessous.

OAuth 2.0 entité	Description
Ressource	Les terminaux d'API REST qui fournissent l'accès aux ressources ONTAP via des commandes ONTAP internes.
Propriétaire de la ressource	Utilisateur du cluster ONTAP qui a créé ou possède la ressource protégée par défaut.
Serveur de ressources	Hôte des ressources protégées qui correspond au cluster ONTAP.
Client	Application demandant l'accès à un point de terminaison d'API REST pour le compte ou avec l'autorisation du propriétaire de la ressource.
Serveur d'autorisation	Généralement un serveur dédié responsable de l'émission des jetons d'accès et de l'application de la stratégie administrative.

Configuration ONTAP principale

Vous devez configurer le cluster ONTAP pour activer et utiliser OAuth 2.0. Cela inclut l'établissement d'une connexion au serveur d'autorisation et la définition de la configuration d'autorisation ONTAP requise. Vous pouvez effectuer cette configuration à l'aide de n'importe quelle interface d'administration, notamment :

- Interface de ligne de commande ONTAP
- System Manager
- L'API REST DE ONTAP

Environnement et services de soutien

Outre les définitions ONTAP, vous devez également configurer les serveurs d'autorisation. Si vous utilisez le mappage groupe-rôle, vous devez également configurer les groupes Active Directory ou l'équivalent LDAP.

Clients ONTAP pris en charge

À partir de ONTAP 9.14, un client d'API REST peut accéder à ONTAP à l'aide d'OAuth 2.0. Avant d'émettre un appel API REST, vous devez obtenir un jeton d'accès auprès du serveur d'autorisation. Le client transmet ensuite ce token au cluster ONTAP en tant que *bearer token* à l'aide de l'en-tête de requête d'autorisation

HTTP. Selon le niveau de sécurité requis, vous pouvez également créer et installer un certificat au niveau du client pour utiliser des jetons limités par l'expéditeur basés sur MTLS.

Terminologie sélectionnée

Lorsque vous commencez à explorer un déploiement OAuth 2.0 avec ONTAP, il est utile de vous familiariser avec une partie de la terminologie. Voir "[Ressources supplémentaires](#)" Pour obtenir des liens vers des informations supplémentaires sur OAuth 2.0.

Jeton d'accès

Jeton émis par un serveur d'autorisation et utilisé par une application client OAuth 2.0 pour faire des demandes d'accès aux ressources protégées.

Jeton Web JSON

Norme utilisée pour formater les jetons d'accès. JSON est utilisé pour représenter les réclamations OAuth 2.0 dans un format compact avec les réclamations disposées en trois sections principales.

Jeton d'accès contraint par l'expéditeur

Fonctionnalité facultative basée sur le protocole MTLS (Mutual transport Layer Security). En utilisant une demande de confirmation supplémentaire dans le jeton, cela garantit que le jeton d'accès n'est utilisé que par le client auquel il a été émis à l'origine.

Jeu de clés Web JSON

Un JWKS est un ensemble de clés publiques utilisées par ONTAP pour vérifier les jetons JWT présentés par les clients. Les jeux de clés sont généralement disponibles au niveau du serveur d'autorisation via un URI dédié.

Portée

Les étendues permettent de limiter ou de contrôler l'accès d'une application à des ressources protégées telles que l'API REST ONTAP. Ils sont représentés sous forme de chaînes dans le jeton d'accès.

Rôle REST ONTAP

Les rôles REST ont été introduits avec ONTAP 9.6 et constituent une partie centrale du framework ONTAP RBAC. Ces rôles sont différents des rôles traditionnels antérieurs qui sont encore pris en charge par ONTAP. L'implémentation OAuth 2.0 dans ONTAP ne prend en charge que les rôles REST.

En-tête d'autorisation HTTP

En-tête inclus dans la requête HTTP pour identifier le client et les autorisations associées dans le cadre d'un appel d'API REST. Plusieurs versions ou implémentations sont disponibles selon la manière dont l'authentification et l'autorisation sont effectuées. Lors de la présentation d'un jeton d'accès OAuth 2.0 à ONTAP, le jeton est identifié comme un *jeton porteur*.

Authentification de base HTTP

Une technique d'authentification HTTP précoce encore prise en charge par ONTAP. Les informations d'identification en texte clair (nom d'utilisateur et mot de passe) sont concaténées avec un deux-points et codées en base64. La chaîne est placée dans l'en-tête de la demande d'autorisation et envoyée au serveur.

FAPI

Un groupe de travail de la Fondation OpenID qui fournit des protocoles, des schémas de données et des recommandations de sécurité pour le secteur financier. L'API était à l'origine connue sous le nom d'API de qualité financière.

ONGLET

Une société privée à but non lucratif fournissant des conseils techniques et de sécurité à l'armée de l'air américaine et au gouvernement américain.

Ressources supplémentaires

Plusieurs ressources supplémentaires sont fournies ci-dessous. Vous devriez consulter ces sites pour obtenir plus d'informations sur OAuth 2.0 et les normes connexes.

Protocoles et normes

- ["RFC 6749 : cadre d'autorisation OAuth 2.0"](#)
- ["RFC 7519 : tokens Web JSON \(JWT\)"](#)
- ["RFC 7523 : profil JSON Web Token \(JWT\) pour les autorisations et l'authentification des clients OAuth 2.0"](#)
- ["RFC 7662 : introspection de tokens OAuth 2.0"](#)
- ["RFC 7800 : clé de preuve de possession pour JWT"](#)
- ["RFC 8705 : authentification du client mutuelle OAuth 2.0 et jetons d'accès liés au certificat"](#)

Organisations

- ["Fondation OpenID"](#)
- ["Groupe de travail de l'IAI"](#)
- ["ONGLET"](#)
- ["IANA - JWT"](#)

Produits et services

- ["Auth0"](#)
- ["Présentation de l'ADFS"](#)
- ["Porte-clés"](#)

Outils et utilitaires supplémentaires

- ["JWT par Auth0"](#)
- ["OpenSSL"](#)

Documentation et ressources de NetApp

- ["Automatisation ONTAP"](#) documentation

Concepts

Serveurs d'autorisation et jetons d'accès

Les serveurs d'autorisation effectuent plusieurs fonctions importantes en tant que composant central dans le cadre d'autorisation OAuth 2.0.

Serveurs d'autorisation OAuth 2.0

Les serveurs d'autorisation sont principalement responsables de la création et de la signature des jetons d'accès. Ces tokens contiennent des informations d'identité et d'autorisation permettant à une application

client d'accéder de manière sélective aux ressources protégées. Les serveurs sont généralement isolés les uns des autres et peuvent être mis en œuvre de différentes manières, notamment en tant que serveur dédié autonome ou dans le cadre d'un produit de gestion des identités et des accès plus large.



Une terminologie différente peut parfois être utilisée pour un serveur d'autorisation, en particulier lorsque la fonctionnalité OAuth 2.0 est intégrée dans un produit ou une solution de gestion des identités et des accès plus large. Par exemple, le terme **Identity Provider (IDP)** est fréquemment utilisé de manière interchangeable avec **Authorization Server**.

L'administration

Outre l'émission de jetons d'accès, les serveurs d'autorisation fournissent également des services administratifs connexes, généralement via une interface utilisateur Web. Par exemple, vous pouvez définir et administrer :

- Authentification des utilisateurs et des utilisateurs
- Étendues
- Ségrégation administrative par les locataires et les royaumes
- Application des règles
- Connexion à divers services externes
- Prise en charge d'autres protocoles d'identité (tels que SAML)

ONTAP est compatible avec les serveurs d'autorisation conformes à la norme OAuth 2.0.

Définition de ONTAP

Vous devez définir un ou plusieurs serveurs d'autorisation sur ONTAP. ONTAP communique en toute sécurité avec chaque serveur pour vérifier les tokens et effectuer d'autres tâches connexes pour la prise en charge des applications client.

Les principaux aspects de la configuration ONTAP sont présentés ci-dessous. Voir aussi ["Scénarios de déploiement OAuth 2.0"](#) pour en savoir plus.

Comment et où les jetons d'accès sont validés

Il existe deux options pour valider les jetons d'accès.

- Validation locale

ONTAP peut valider les jetons d'accès localement en fonction des informations fournies par le serveur d'autorisation qui a émis le token. Les informations extraites du serveur d'autorisation sont mises en cache par ONTAP et actualisées à intervalles réguliers.

- Introspection à distance

Vous pouvez également utiliser l'introspection à distance pour valider les tokens sur le serveur d'autorisation. L'introspection est un protocole permettant aux parties autorisées d'interroger un serveur d'autorisation sur un jeton d'accès. Il permet à ONTAP d'extraire certaines métadonnées d'un jeton d'accès et de valider le jeton. ONTAP met en cache une partie des données pour des raisons de performances.

Emplacement réseau

ONTAP peut se trouver derrière un pare-feu. Dans ce cas, vous devez identifier un proxy comme faisant partie

de la configuration.

Définition des serveurs d'autorisation

Vous pouvez définir un serveur d'autorisation pour ONTAP à l'aide de n'importe quelle interface d'administration, notamment l'interface de ligne de commandes, System Manager ou l'API REST. Par exemple, avec l'interface de ligne de commandes, vous utilisez la commande `security oauth2 client create`.

Nombre de serveurs d'autorisation

Vous pouvez définir jusqu'à huit serveurs d'autorisation sur un seul cluster ONTAP. Le même serveur d'autorisation peut être défini plusieurs fois sur le même cluster ONTAP tant que les demandes d'émetteur ou d'émetteur/d'audience sont uniques. Par exemple, avec Keycloak, ce sera toujours le cas lorsque vous utilisez des domaines différents.

Utilisation des jetons d'accès OAuth 2.0

Les jetons d'accès OAuth 2.0 émis par les serveurs d'autorisation sont vérifiés par ONTAP et utilisés pour prendre des décisions d'accès basées sur les rôles pour les requêtes client de l'API REST.

Acquisition d'un jeton d'accès

Vous devez acquérir un jeton d'accès à partir d'un serveur d'autorisation défini sur le cluster ONTAP où vous utilisez l'API REST. Pour acquérir un jeton, vous devez contacter directement le serveur d'autorisation.



ONTAP n'émet pas de tokens d'accès ni ne redirige pas les requêtes des clients vers les serveurs d'autorisation.

La façon dont vous demandez un jeton dépend de plusieurs facteurs, notamment :

- Serveur d'autorisation et ses options de configuration
- Type de subvention OAuth 2.0
- Client ou outil logiciel utilisé pour émettre la demande

Types de subventions

Un *Grant* est un processus bien défini, comprenant un ensemble de flux réseau, utilisé pour demander et recevoir un jeton d'accès OAuth 2.0. Plusieurs types d'octroi différents peuvent être utilisés en fonction du client, de l'environnement et des exigences de sécurité. Une liste des types de subventions les plus populaires est présentée dans le tableau ci-dessous.

Type de subvention	Description
Informations d'identification du client	Type de subvention populaire basé sur l'utilisation de références uniquement (par exemple, un ID et un secret partagé). Le client est supposé avoir une relation de confiance étroite avec le propriétaire de la ressource.
Mot de passe	Le type d'octroi d'autorisations de mot de passe du propriétaire de ressource peut être utilisé lorsque le propriétaire de la ressource a une relation de confiance établie avec le client. Elle peut également être utile lors de la migration de clients HTTP hérités vers OAuth 2.0.

Type de subvention	Description
Code d'autorisation	Il s'agit d'un type d'octroi idéal pour les clients confidentiels et basé sur un flux basé sur la redirection. Il peut être utilisé pour obtenir à la fois un jeton d'accès et un jeton d'actualisation.

Contenu JWT

Un jeton d'accès OAuth 2.0 est formaté en JWT. Le contenu est créé par le serveur d'autorisation en fonction de votre configuration. Cependant, les tokens sont opaques pour les applications client. Un client n'a aucune raison d'inspecter un jeton ou d'être au courant du contenu.

Chaque jeton d'accès JWT contient un ensemble de réclamations. Les réclamations décrivent les caractéristiques de l'émetteur et l'autorisation en fonction des définitions administratives du serveur d'autorisation. Certaines des réclamations enregistrées avec la norme sont décrites dans le tableau ci-dessous. Toutes les chaînes sont sensibles à la casse.

Réclamation	Mot-clé	Description
Émetteur	iss	Identifie le principal qui a émis le token. Le traitement de la demande est spécifique à l'application.
Objet	sous	L'objet ou l'utilisateur du jeton. Le nom est défini comme unique au niveau global ou local.
Public	aud	Destinataires pour lequel le token est destiné. Implémenté en tant que tableau de chaînes.
Expiration	date	Heure après laquelle le jeton expire et doit être rejeté.

Voir ["RFC 7519 : tokens Web JSON"](#) pour en savoir plus.

Options pour l'autorisation client ONTAP

Plusieurs options sont disponibles pour personnaliser votre autorisation client ONTAP. Les décisions d'autorisation sont finalement basées sur les rôles REST ONTAP contenus dans ou dérivés des jetons d'accès.



Vous pouvez uniquement utiliser ["Rôles REST ONTAP"](#) Lors de la configuration de l'autorisation pour OAuth 2.0. Les anciens rôles ONTAP traditionnels ne sont pas pris en charge.

Introduction

La mise en œuvre OAuth 2.0 au sein de ONTAP est conçue pour être flexible et robuste, offrant les options dont vous avez besoin pour sécuriser l'environnement ONTAP. À un niveau élevé, il existe trois principales catégories de configuration permettant de définir l'autorisation du client ONTAP. Ces options de configuration s'excluent mutuellement.

ONTAP applique l'option la plus appropriée en fonction de votre configuration. Voir ["Comment ONTAP détermine l'accès"](#) Pour en savoir plus sur la façon dont ONTAP traite vos définitions de configuration pour prendre des décisions d'accès.

Oscilloscopes autonomes OAuth 2.0

Ces étendues contiennent un ou plusieurs rôles REST personnalisés, chacun encapsulé dans une seule

chaîne. Ils sont indépendants des définitions de rôles ONTAP. Vous devez définir ces chaînes de portée sur votre serveur d'autorisation.

Utilisateurs et rôles REST spécifiques à ONTAP en local

En fonction de votre configuration, les définitions d'identité ONTAP locales peuvent être utilisées pour prendre des décisions d'accès. Les options sont les suivantes :

- Rôle REST nommé unique
- Correspondance du nom d'utilisateur avec un utilisateur ONTAP local

La syntaxe de portée d'un rôle nommé est **ontap-role-`<URL-encoded-ONTAP-role-name>`**. Par exemple, si le rôle est « admin », la chaîne de portée sera « ontap-role-admin ».

Groupes Active Directory ou LDAP

Si les définitions ONTAP locales sont examinées mais qu'aucune décision d'accès ne peut être prise, les groupes Active Directory (« domaine ») ou LDAP (« nsswitch ») sont utilisés. Les informations de groupe peuvent être spécifiées de deux manières :

- Chaîne de portée OAuth 2.0

Prend en charge les applications confidentielles en utilisant le flux d'informations d'identification du client lorsqu'aucun utilisateur n'est membre d'un groupe. Le périmètre doit être nommé **ontap-group-`<URL-encoded-ONTAP-group-name>`**. Par exemple, si le groupe est « développement », la chaîne de portée sera « ontap-groupe-développement ».

- Dans la réclamation « Groupe »

Ceci est destiné aux jetons d'accès émis par ADFS à l'aide du flux propriétaire de la ressource (mot de passe Grant).

Oscilloscopes OAuth 2.0 autonomes

Les étendues autonomes sont des chaînes portées dans le jeton d'accès. Chacune d'entre elles constitue une définition de rôle personnalisée complète et comprend tout ce dont ONTAP a besoin pour prendre une décision d'accès. Le périmètre est distinct et celui de tous les rôles REST définis au sein de ONTAP lui-même.

Format de la chaîne de portée

Au niveau de la base, la portée est représentée sous la forme d'une chaîne contiguë et composée de six valeurs séparées par deux points. Les paramètres utilisés dans la chaîne de portée sont décrits ci-dessous.

Littéral ONTAP

La portée doit commencer par la valeur littérale `ontap` en minuscules. Cette opération identifie la portée en tant que spécifique à ONTAP.

Cluster

Il définit le cluster ONTAP auquel la portée s'applique. Les valeurs peuvent inclure :

- UUID de cluster

Identifie un seul cluster.

- Astérisque (*)

Indique que la portée s'applique à tous les clusters.

Vous pouvez utiliser la commande CLI de ONTAP `cluster identity show` Pour afficher l'UUID de votre cluster. Si elle n'est pas spécifiée, la portée s'applique à tous les clusters.

Rôle

Nom du rôle REST contenu dans le périmètre autonome. Cette valeur n'est pas examinée par ONTAP ou associée à tout rôle REST existant défini sur ONTAP. Le nom est utilisé pour la journalisation.

Niveau d'accès

Cette valeur indique le niveau d'accès appliqué à l'application client lors de l'utilisation du noeud final de l'API dans le périmètre. Il existe six valeurs possibles, comme décrit dans le tableau ci-dessous.

Niveau d'accès	Description
Aucune	Refuse tout accès au noeud final spécifié.
lecture seule	Autorise uniquement l'accès en lecture à l'aide de GET.
read_create	Permet l'accès en lecture ainsi que la création de nouvelles instances de ressources à l'aide de POST.
lire_modifier	Permet l'accès en lecture ainsi que la mise à jour des ressources existantes à l'aide d'un CORRECTIF.
read_create_modify	Permet tous les accès sauf supprimer. Les opérations autorisées comprennent OBTENIR (lire), POST (créer) et PATCH (mettre à jour).
tous	Permet un accès complet.

SVM

Nom du SVM au sein du cluster auquel la portée s'applique. Utilisez la valeur * (astérisque) pour indiquer tous les SVM.



Cette fonctionnalité n'est pas entièrement prise en charge par ONTAP 9.14.1. Vous pouvez ignorer le paramètre du SVM et utiliser un astérisque comme emplacement réservé. Vérifiez le ["Notes de version de ONTAP"](#) Pour vérifier la prise en charge future des SVM.

URI DE L'API REST

Chemin complet ou partiel d'une ressource ou d'un ensemble de ressources associées. La chaîne doit commencer par `/api`. Si vous ne spécifiez pas de valeur, la portée s'applique à tous les terminaux d'API du cluster ONTAP.

Exemples de portée

Quelques exemples de portées autonomes sont présentés ci-dessous.

ontap*:joes-role:read_create_modify:*/api/cluster

Permet à l'utilisateur affecté à ce rôle d'accéder en lecture, création et modification à `/cluster` point final.

Outil d'administration CLI

Pour faciliter l'administration des étendues autonomes et réduire le risque d'erreur, ONTAP fournit la commande CLI `security oauth2 scope` pour générer des chaînes de portée basées sur vos paramètres d'entrée.

La commande `security oauth2 scope` propose deux cas d'utilisation basés sur vos commentaires :

- Paramètres de l'interface de ligne de commande pour la chaîne de périmètre

Vous pouvez utiliser cette version de la commande pour générer une chaîne de portée basée sur les paramètres d'entrée.

- Chaîne d'étendue aux paramètres CLI

Vous pouvez utiliser cette version de la commande pour générer les paramètres de la commande en fonction de la chaîne de périmètre d'entrée.

Exemple

L'exemple suivant génère une chaîne de périmètre avec le résultat inclus après l'exemple de commande ci-dessous. La définition s'applique à tous les clusters.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap*:joes-role:readonly:*/api/cluster
```

Comment ONTAP détermine l'accès

Pour bien concevoir et mettre en œuvre OAuth 2.0, vous devez comprendre comment ONTAP utilise votre configuration d'autorisation pour prendre des décisions d'accès pour les clients.

Étape 1 : oscilloscopes autonomes

Si le jeton d'accès contient des périmètres autonomes, ONTAP examine d'abord ces périmètres. S'il n'y a pas de portées autonomes, passez à l'étape 2.

Avec une ou plusieurs portées autonomes présentes, ONTAP applique chaque portée jusqu'à ce qu'une décision explicite **ALLOW** ou **DENY** puisse être prise. Si une décision explicite est prise, le traitement prend fin.

Si ONTAP ne peut pas prendre de décision explicite en matière d'accès, passez à l'étape 2.

Étape 2 : vérifiez l'indicateur de rôles locaux

ONTAP examine la valeur de l'indicateur `use-local-roles-if-present`. La valeur de cet indicateur est définie séparément pour chaque serveur d'autorisation défini sur ONTAP.

- Si la valeur est de `true` passez à l'étape 3.

- Si la valeur est de `false` le traitement se termine et l'accès est refusé.

Étape 3 : rôle REST ONTAP nommé

Si le jeton d'accès contient un rôle REST nommé, ONTAP utilise ce rôle pour prendre la décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

S'il n'y a pas de rôle REST nommé ou si le rôle est introuvable, passez à l'étape 4.

Étape 4 : utilisateurs ONTAP locaux

Extrayez le nom d'utilisateur du jeton d'accès et essayez de le faire correspondre à un utilisateur ONTAP local.

Si un utilisateur ONTAP local est associé, ONTAP utilise le rôle défini pour que l'utilisateur puisse prendre une décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

Si un utilisateur ONTAP local ne correspond pas ou s'il n'y a pas de nom d'utilisateur dans le jeton d'accès, passez à l'étape 5.

Étape 5 : mappage groupe-rôle

Extrayez le groupe du jeton d'accès et essayez de le faire correspondre à un groupe. Les groupes sont définis à l'aide d'Active Directory ou d'un serveur LDAP équivalent.

S'il existe une correspondance de groupe, ONTAP utilise le rôle défini pour le groupe pour prendre une décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

S'il n'y a pas de correspondance de groupe ou s'il n'y a pas de groupe dans le jeton d'accès, l'accès est refusé et le traitement se termine.

Scénarios de déploiement OAuth 2.0

Plusieurs options de configuration sont disponibles lors de la définition d'un serveur d'autorisation dans ONTAP. En fonction de ces options, vous pouvez créer un serveur d'autorisation adapté à votre environnement de déploiement.

Résumé des paramètres de configuration

Plusieurs paramètres de configuration sont disponibles lors de la définition d'un serveur d'autorisation dans ONTAP. Ces paramètres sont généralement pris en charge dans toutes les interfaces administratives.

Les noms des paramètres peuvent varier légèrement en fonction de l'interface d'administration de ONTAP. Par exemple, lors de la configuration de l'introspection à distance, le noeud final est identifié à l'aide du paramètre de commande CLI `-introspection-endpoint`. Mais avec System Manager, le champ équivalent est `URI` d'introspection de jeton de serveur d'autorisation. Pour prendre en charge toutes les interfaces administratives ONTAP, une description générale des paramètres est fournie. Le paramètre ou le champ exact doit être évident en fonction du contexte.

Paramètre	Description
Nom	Nom du serveur d'autorisation tel qu'il est connu de ONTAP.
Client supplémentaire	Application interne ONTAP à laquelle s'applique la définition. Ce doit être http .
URI de l'émetteur	Nom de domaine complet avec chemin identifiant le site ou l'organisation qui émet les jetons.

Paramètre	Description
URI du fournisseur JWKS	Nom de domaine complet avec chemin et nom de fichier où ONTAP obtient les jeux de clés Web JSON utilisés pour valider les jetons d'accès.
Intervalle de rafraîchissement JWKS	Intervalle de temps déterminant la fréquence à laquelle ONTAP actualise les informations de certificat à partir de l'URI JWKS du fournisseur. La valeur est spécifiée au format ISO-8601.
Point d'extrémité d'introspection	Nom de domaine complet avec chemin utilisé par ONTAP pour effectuer la validation de jeton à distance via l'introspection.
ID client	Nom du client tel que défini sur le serveur d'autorisation. Lorsque cette valeur est incluse, vous devez également fournir le secret client associé en fonction de l'interface.
Proxy sortant	Cela permet d'accéder au serveur d'autorisation lorsque ONTAP se trouve derrière un pare-feu. L'URI doit être au format curl.
Utilisez des rôles locaux, le cas échéant	Indicateur booléen déterminant si les définitions ONTAP locales sont utilisées, y compris un rôle REST nommé et des utilisateurs locaux.
Supprimer la réclamation utilisateur	Autre nom utilisé par ONTAP pour correspondre aux utilisateurs locaux. Utilisez le <code>sub</code> champ du jeton d'accès correspondant au nom d'utilisateur local.

Scénarios de déploiement

Vous trouverez ci-dessous plusieurs scénarios de déploiement courants. Ils sont organisés selon que la validation des tokens est effectuée localement par ONTAP ou à distance par le serveur d'autorisation. Chaque scénario inclut une liste des options de configuration requises. Voir "[Déployer OAuth 2.0 dans ONTAP](#)" pour des exemples de commandes de configuration.



Après avoir défini un serveur d'autorisation, vous pouvez afficher sa configuration via l'interface d'administration ONTAP. Par exemple, utilisez la commande `security oauth2 client show` Via l'interface de ligne de commandes ONTAP.

Validation locale

Les scénarios de déploiement suivants sont basés sur l'exécution locale de la validation des jetons par ONTAP.

Utilisez des oscilloscopes autonomes sans proxy

Il s'agit du déploiement le plus simple utilisant uniquement des oscilloscopes autonomes OAuth 2.0. Aucune définition d'identité ONTAP locale n'est utilisée. Vous devez inclure les paramètres suivants :

- Nom
- Application (http)
- URI du fournisseur JWKS
- URI de l'émetteur

Vous devez également ajouter les étendues au niveau du serveur d'autorisation.

Utiliser des portées autonomes avec un proxy

Ce scénario de déploiement utilise les étendues autonomes OAuth 2.0. Aucune définition d'identité ONTAP

locale n'est utilisée. Mais le serveur d'autorisation est derrière un pare-feu et vous devez donc configurer un proxy. Vous devez inclure les paramètres suivants :

- Nom
- Application (http)
- URI du fournisseur JWKS
- Proxy sortant
- URI de l'émetteur
- Public

Vous devez également ajouter les étendues au niveau du serveur d'autorisation.

Utilisez les rôles d'utilisateur local et le mappage de nom d'utilisateur par défaut avec un proxy

Ce scénario de déploiement utilise des rôles d'utilisateur local avec un mappage de noms par défaut. Le sinistre utilisateur distant utilise la valeur par défaut de `sub` ce champ du jeton d'accès est donc utilisé pour correspondre au nom d'utilisateur local. Le nom d'utilisateur doit comporter au maximum 40 caractères. Le serveur d'autorisation se trouve derrière un pare-feu, vous devez donc également configurer un proxy. Vous devez inclure les paramètres suivants :

- Nom
- Application (http)
- URI du fournisseur JWKS
- Utilisez des rôles locaux, le cas échéant (`true`)
- Proxy sortant
- Émetteur

Vous devez vous assurer que l'utilisateur local est défini sur ONTAP.

Utilisez des rôles d'utilisateur locaux et un mappage de nom d'utilisateur alternatif avec un proxy

Ce scénario de déploiement utilise des rôles d'utilisateur local avec un autre nom d'utilisateur qui est utilisé pour correspondre à un utilisateur ONTAP local. Le serveur d'autorisation est derrière un pare-feu, vous devez donc configurer un proxy. Vous devez inclure les paramètres suivants :

- Nom
- Application (http)
- URI du fournisseur JWKS
- Utilisez des rôles locaux, le cas échéant (`true`)
- Demande d'utilisateur à distance
- Proxy sortant
- URI de l'émetteur
- Public

Vous devez vous assurer que l'utilisateur local est défini sur ONTAP.

Introspection à distance

Les configurations de déploiement suivantes sont basées sur ONTAP qui effectue la validation des jetons à distance via l'introspection.

Utilisez des oscilloscopes autonomes sans proxy

Il s'agit d'un déploiement simple basé sur l'utilisation des oscilloscopes autonomes OAuth 2.0. Aucune définition d'identité ONTAP n'est utilisée. Vous devez inclure les paramètres suivants :

- Nom
- Application (http)
- Point d'extrémité d'introspection
- ID client
- URI de l'émetteur

Vous devez définir les étendues ainsi que le secret client et client sur le serveur d'autorisation.

Authentification du client à l'aide d'un protocole TLS mutuel

Selon vos besoins en matière de sécurité, vous pouvez éventuellement configurer le protocole MTLS (Mutual TLS) pour mettre en œuvre une authentification client forte. Lorsqu'il est utilisé avec ONTAP dans le cadre d'un déploiement OAuth 2.0, MTLS garantit que les jetons d'accès ne sont utilisés que par les clients auxquels ils ont été initialement émis.

Protocole commun avec OAuth 2.0

TLS (transport Layer Security) est utilisé pour établir un canal de communication sécurisé entre deux applications, généralement un navigateur client et un serveur Web. Le protocole mutuel TLS étend cette fonction en fournissant une identification forte du client par le biais d'un certificat client. Lorsqu'elle est utilisée dans un cluster ONTAP avec OAuth 2.0, la fonctionnalité MTLS de base est étendue en créant et en utilisant des jetons d'accès limités par l'expéditeur.

Un jeton d'accès limité par l'expéditeur ne peut être utilisé que par le client auquel il a été émis à l'origine. Pour prendre en charge cette fonction, une nouvelle demande de confirmation (`cnf`) est inséré dans le jeton. Le champ contient la propriété `x5t#S256` qui contient un résumé du certificat client utilisé lors de la demande du jeton d'accès. Cette valeur est vérifiée par ONTAP dans le cadre de la validation du jeton. Les jetons d'accès émis par les serveurs d'autorisation qui ne sont pas soumis à des contraintes d'expéditeur n'incluent pas la demande de confirmation supplémentaire.

Vous devez configurer ONTAP pour qu'il utilise MTLS séparément pour chaque serveur d'autorisation. Par exemple, la commande CLI `security oauth2 client` inclut le paramètre `use-mutual-tls` Contrôler le traitement MTLS en fonction de trois valeurs, comme indiqué dans le tableau ci-dessous.



Dans chaque configuration, le résultat et l'action de ONTAP dépendent de la valeur du paramètre de configuration, ainsi que du contenu du jeton d'accès et du certificat client. Les paramètres du tableau sont organisés du moins au plus restrictif.

Paramètre	Description
Aucune	L'authentification mutuelle TLS OAuth 2.0 est complètement désactivée pour le serveur d'autorisation. ONTAP n'effectuera pas l'authentification du certificat du client MTLS même si la demande de confirmation est présente dans le jeton ou si un certificat client est fourni avec la connexion TLS.
demande	L'authentification mutuelle TLS OAuth 2.0 est appliquée si un jeton d'accès limité par l'expéditeur est présenté par le client. C'est-à-dire que MTLS est appliqué uniquement si la demande de confirmation (avec la propriété <code>x5t#S256</code>) est présent dans le jeton d'accès. Il s'agit du paramètre par défaut.
obligatoire	L'authentification mutuelle TLS OAuth 2.0 est appliquée pour tous les jetons d'accès émis par le serveur d'autorisation. Par conséquent, tous les tokens d'accès doivent être soumis à des contraintes d'expéditeur. L'authentification et la demande de l'API REST échouent si la demande de confirmation n'est pas présente dans le jeton d'accès ou si un certificat client n'est pas valide.

Flux de mise en œuvre de haut niveau

Les étapes typiques de l'utilisation de MTLS avec OAuth 2.0 dans un environnement ONTAP sont présentées ci-dessous. Voir ["RFC 8705 : authentification du client mutuelle OAuth 2.0 et jetons d'accès liés au certificat"](#) pour en savoir plus.

Étape 1 : création et installation d'un certificat client

L'établissement de l'identité du client repose sur la preuve de la connaissance d'une clé privée du client. La clé publique correspondante est placée dans un certificat X.509 signé présenté par le client. À un niveau élevé, les étapes impliquées dans la création du certificat client comprennent :

1. Générez une paire de clés publique et privée
2. Créez une demande de signature de certificat
3. Envoyez le fichier CSR à une autorité de certification connue
4. CA vérifie la demande et émet le certificat signé

Vous pouvez normalement installer le certificat client dans votre système d'exploitation local ou l'utiliser directement avec un utilitaire commun tel que curl.

Étape 2 : configurer ONTAP pour utiliser MTLS

Vous devez configurer ONTAP pour utiliser MTLS. Cette configuration est effectuée séparément pour chaque serveur d'autorisation. Par exemple, avec l'interface de ligne de commandes, la commande `security oauth2 client` est utilisé avec le paramètre facultatif `use-mutual-tls`. Voir ["Déployer OAuth 2.0 dans ONTAP"](#) pour en savoir plus.

Étape 3 : le client demande un jeton d'accès

Le client doit demander un jeton d'accès au serveur d'autorisation configuré sur ONTAP. L'application client doit utiliser MTLS avec le certificat créé et installé à l'étape 1.

Étape 4 : le serveur d'autorisation génère le jeton d'accès

Le serveur d'autorisation vérifie la demande du client et génère un jeton d'accès. Dans ce cadre, il crée un résumé de message du certificat client qui est inclus dans le jeton en tant que demande de confirmation (champ `cnf`).

Étape 5 : l'application client présente le jeton d'accès à ONTAP

L'application client effectue un appel d'API REST vers le cluster ONTAP et inclut le jeton d'accès dans l'en-tête de la demande d'autorisation en tant que **jeton porteur**. Le client doit utiliser MTLS avec le même certificat que celui utilisé pour demander le jeton d'accès.

Étape 6 : ONTAP vérifie le client et le jeton.

ONTAP reçoit le jeton d'accès dans une requête HTTP ainsi que le certificat client utilisé dans le cadre du traitement MTLS. ONTAP valide d'abord la signature dans le jeton d'accès. En fonction de la configuration, ONTAP génère un résumé de message du certificat client et le compare à la demande de confirmation **cnf** du jeton. Si les deux valeurs correspondent, ONTAP a confirmé que le client faisant la demande d'API est le même client auquel le jeton d'accès a été émis à l'origine.

Configuration et déploiement

Préparez-vous à déployer OAuth 2.0 avec ONTAP

Avant de configurer OAuth 2.0 dans un environnement ONTAP, vous devez préparer le déploiement. Un résumé des principales tâches et décisions est inclus ci-dessous. L'agencement des sections est généralement aligné sur l'ordre que vous devez suivre. Toutefois, même si cette solution est applicable à la plupart des déploiements, vous devez l'adapter à votre environnement selon les besoins. Vous devez également envisager de créer un plan de déploiement formel.



En fonction de votre environnement, vous pouvez sélectionner la configuration des serveurs d'autorisation définis pour ONTAP. Cela inclut les valeurs de paramètre que vous devez spécifier pour chaque type de déploiement. Voir "[Scénarios de déploiement OAuth 2.0](#)" pour en savoir plus.

Ressources protégées et applications client

OAuth 2.0 est un cadre d'autorisation permettant de contrôler l'accès aux ressources protégées. Dans un premier temps, il est donc important de déterminer quelles sont les ressources disponibles et quels clients ont besoin d'y accéder.

Identifiez les applications client

Vous devez décider quels clients utiliseront OAuth 2.0 lors de l'émission d'appels API REST et à quels terminaux API ils ont besoin d'accéder.

Passez en revue les rôles REST ONTAP et les utilisateurs locaux existants

Vous devez examiner les définitions d'identité ONTAP existantes, y compris les rôles REST et les utilisateurs locaux. Selon la configuration d'OAuth 2.0, ces définitions peuvent être utilisées pour prendre des décisions d'accès.

Transition globale vers OAuth 2.0

Bien que vous puissiez implémenter l'autorisation OAuth 2.0 progressivement, vous pouvez également déplacer tous les clients API REST vers OAuth 2.0 immédiatement en définissant un indicateur global pour chaque serveur d'autorisation. Vous pouvez ainsi prendre des décisions d'accès en fonction de votre configuration ONTAP existante sans avoir à créer de étendues autonomes.

Serveurs d'autorisation

Les serveurs d'autorisation jouent un rôle important dans votre déploiement OAuth 2.0 en émettant des jetons d'accès et en appliquant une stratégie administrative.

Sélectionnez et installez le serveur d'autorisation

Vous devez sélectionner et installer un ou plusieurs serveurs d'autorisation. Il est important de se familiariser avec les options de configuration et les procédures de vos fournisseurs d'identité, y compris la définition des périmètres.

Déterminez si le certificat d'autorité de certification racine d'autorisation doit être installé

ONTAP utilise le certificat du serveur d'autorisation pour valider les jetons d'accès signés présentés par les clients. Pour ce faire, ONTAP a besoin du certificat de l'autorité de certification racine et de tous les certificats intermédiaires. Ils peuvent être pré-installés avec ONTAP. Si ce n'est pas le cas, vous devez les installer.

Évaluez l'emplacement et la configuration du réseau

Si le serveur d'autorisation est derrière un pare-feu, ONTAP doit être configuré pour utiliser un serveur proxy.

Authentification et autorisation du client

Il existe plusieurs aspects de l'authentification et de l'autorisation des clients que vous devez prendre en compte.

Étendues autonomes ou définitions d'identité ONTAP locales

À un niveau élevé, vous pouvez définir des étendues autonomes définies sur le serveur d'autorisation ou vous appuyer sur les définitions d'identité ONTAP locales existantes, y compris les rôles et les utilisateurs.

Options avec traitement ONTAP local

Si vous utilisez les définitions d'identité ONTAP, vous devez choisir celles qui doivent être appliquées, notamment :

- Rôle REST nommé
- Faire correspondre les utilisateurs locaux
- Groupes Active Directory ou LDAP

Validation locale ou introspection à distance

Vous devez décider si les jetons d'accès seront validés localement par ONTAP ou au niveau du serveur d'autorisation par introspection. Plusieurs valeurs connexes sont également à prendre en compte, telles que l'intervalle d'actualisation.

Jetons d'accès limités par l'expéditeur

Pour les environnements nécessitant un niveau de sécurité élevé, vous pouvez utiliser des jetons d'accès avec limite d'envoi basés sur MTLS. Cela nécessite un certificat pour chaque client.

Interface d'administration

Vous pouvez administrer OAuth 2.0 via n'importe quelle interface ONTAP, notamment :

- Interface de ligne de commandes
- System Manager
- API REST

Comment les clients demandent des jetons d'accès

Les applications client doivent demander des jetons d'accès directement à partir du serveur d'autorisation. Vous devez décider de la façon dont cela sera fait, y compris le type de subvention.

Configurer ONTAP

Vous devez effectuer plusieurs tâches de configuration ONTAP.

Définissez les rôles REST et les utilisateurs locaux

En fonction de votre configuration d'autorisation, le traitement local ONTAP Identify peut être utilisé. Dans ce cas, vous devez revoir et définir les rôles REST et les définitions d'utilisateur.

Configuration centrale

Trois étapes principales sont nécessaires pour effectuer la configuration principale de ONTAP, notamment :

- Vous pouvez également installer le certificat racine (ainsi que tous les certificats intermédiaires) de l'autorité de certification qui a signé le certificat du serveur d'autorisation.
- Définissez le serveur d'autorisation.
- Activez le traitement OAuth 2.0 pour le cluster.

Déployer OAuth 2.0 dans ONTAP

Le déploiement de la fonctionnalité principale OAuth 2.0 implique trois étapes principales.

Avant de commencer

Vous devez préparer le déploiement OAuth 2.0 avant de configurer ONTAP. Par exemple, vous devez évaluer le serveur d'autorisation, y compris la façon dont son certificat a été signé et s'il est derrière un pare-feu. Voir ["Préparez-vous à déployer OAuth 2.0 avec ONTAP"](#) pour en savoir plus.

Étape 1 : installez le certificat du serveur d'authentification

ONTAP inclut un grand nombre de certificats d'autorité de certification racine pré-installés. Ainsi, dans de nombreux cas, le certificat de votre serveur d'autorisation sera immédiatement reconnu par ONTAP sans configuration supplémentaire. Mais selon la façon dont le certificat du serveur d'autorisation a été signé, vous devrez peut-être installer un certificat d'autorité de certification racine et tous les certificats intermédiaires.

Suivez les instructions ci-dessous pour installer le certificat si nécessaire. Vous devez installer tous les certificats requis au niveau du cluster.

Choisissez la procédure appropriée en fonction de votre accès à ONTAP.

Exemple 17. Étapes

System Manager

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Faites défiler jusqu'à la section **sécurité**.
3. Cliquez sur → en regard de **certificats**.
4. Sous l'onglet **autorités de certification approuvées**, cliquez sur **Ajouter**.
5. Cliquez sur **Importer** et sélectionnez le fichier de certificat.
6. Renseignez les paramètres de configuration de votre environnement.
7. Cliquez sur **Ajouter**.

CLI

1. Commencez l'installation :

```
security certificate install -type server-ca
```

2. Recherchez le message de console suivant :

```
Please enter Certificate: Press <Enter> when done
```

3. Ouvrez le fichier de certificat à l'aide d'un éditeur de texte.
4. Copiez l'intégralité du certificat, y compris les lignes suivantes :

```
-----BEGIN CERTIFICATE-----  
  
-----END CERTIFICATE-----
```

5. Collez le certificat dans le terminal après l'invite de commande.
6. Appuyez sur **entrée** pour terminer l'installation.
7. Vérifiez que le certificat est installé à l'aide de l'une des méthodes suivantes :

```
security certificate show-user-installed  
  
security certificate show
```

Étape 2 : configurer le serveur d'autorisation

Vous devez définir au moins un serveur d'autorisation sur ONTAP. Vous devez choisir les valeurs de paramètre en fonction de votre configuration et de votre plan de déploiement. Révision "[Scénarios de déploiement OAuth2](#)" pour déterminer les paramètres exacts nécessaires à votre configuration.



Pour modifier une définition de serveur d'autorisation, vous pouvez supprimer la définition existante et en créer une nouvelle.

L'exemple ci-dessous est basé sur le premier scénario de déploiement simple à l'adresse "[Validation locale](#)". Les oscilloscopes autonomes sont utilisés sans proxy.

Choisissez la procédure appropriée en fonction de votre accès à ONTAP. La procédure CLI utilise des

variables symboliques que vous devez remplacer avant d'exécuter la commande.

Exemple 18. Étapes

System Manager

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Faites défiler jusqu'à la section **sécurité**.
3. Cliquez sur **+** en regard de **OAuth 2.0 autorisation**.
4. Sélectionnez **plus d'options**.
5. Indiquez les valeurs requises pour votre déploiement, notamment :
 - Nom
 - Application (http)
 - URI du fournisseur JWKS
 - URI de l'émetteur
6. Cliquez sur **Ajouter**.

CLI

1. Créez à nouveau la définition :

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri  
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

Par exemple :

```
security oauth2 client create \  
-config-name auth0 \  
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-  
realm/protocol/openid-connect/certs \  
-application http \  
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

Étape 3 : activez OAuth 2.0

La dernière étape consiste à activer OAuth 2.0. Il s'agit d'un paramètre global pour le cluster ONTAP.



N'activez pas le traitement OAuth 2.0 tant que vous n'avez pas confirmé que ONTAP, les serveurs d'autorisation et les services de support ont tous été correctement configurés.

Choisissez la procédure appropriée en fonction de votre accès à ONTAP.

Exemple 19. Étapes

System Manager

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Faites défiler jusqu'à la section **sécurité**.
3. Cliquez sur → en regard de **OAuth 2.0 autorisation**.
4. Activer **OAuth 2.0 autorisation**.

CLI

1. Activer OAuth 2.0 :

```
security oauth2 modify -enabled true
```

2. Confirmer que OAuth 2.0 est activé :

```
security oauth2 show  
Is OAuth 2.0 Enabled: true
```

Émettre un appel API REST à l'aide d'OAuth 2.0

L'implémentation OAuth 2.0 dans ONTAP prend en charge les applications clientes de l'API REST. Vous pouvez émettre un appel d'API REST simple en utilisant curl pour commencer à utiliser OAuth 2.0. L'exemple présenté ci-dessous récupère la version du cluster ONTAP.

Avant de commencer

Vous devez configurer et activer la fonction OAuth 2.0 pour votre cluster ONTAP. Cela inclut la définition d'un serveur d'autorisation.

Étape 1 : acquérir un jeton d'accès

Vous devez acquérir un jeton d'accès à utiliser avec l'appel de l'API REST. La requête de jeton est effectuée en dehors de ONTAP et la procédure exacte dépend du serveur d'autorisation et de sa configuration. Vous pouvez demander le token via un navigateur Web, une commande curl ou un langage de programmation.

À des fins d'illustration, un exemple de la façon dont un jeton d'accès peut être demandé à Keycloak à l'aide de curl est présenté ci-dessous.

Exemple de Keycloak

```
curl --request POST \  
--location  
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-  
connect/token' \  
--header 'Content-Type: application/x-www-form-urlencoded' \  
--data-urlencode 'client_id=dp-client-1' \  
--data-urlencode 'grant_type=client_credentials' \  
--data-urlencode 'client_secret=5iTUf9QKLGxAoYaliR33v1D5A2xq09V7'
```

Vous devez copier et enregistrer le jeton renvoyé.

Étape 2 : lancez l'appel de l'API REST

Après avoir un jeton d'accès valide, vous pouvez utiliser une commande curl avec le jeton d'accès pour émettre un appel d'API REST.

Paramètres et variables

Les deux variables de l'exemple curl sont décrites dans le tableau ci-dessous.

Variable	Description
\$FQDN_IP	Nom de domaine complet ou adresse IP du LIF de gestion ONTAP.
\$ACCESS_TOKEN	Jeton d'accès OAuth 2.0 émis par le serveur d'autorisation.

Vous devez d'abord définir ces variables dans l'environnement de shell Bash avant de lancer l'exemple de bouclage. Par exemple, dans l'interface de ligne de commande Linux, tapez la commande suivante pour définir et afficher la variable FQDN :

```
FQDN_IP=172.14.31.224  
echo $FQDN_IP  
172.14.31.224
```

Une fois les deux variables définies dans votre shell Bash local, vous pouvez copier la commande curl et la coller dans l'interface de ligne de commande. Appuyez sur **entrée** pour remplacer les variables et émettre la commande.

Exemple de boucle

```
curl --request GET \  
--location "https://$FQDN_IP/api/cluster?fields=version" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Bearer $ACCESS_TOKEN"
```

Configurez l'authentification SAML

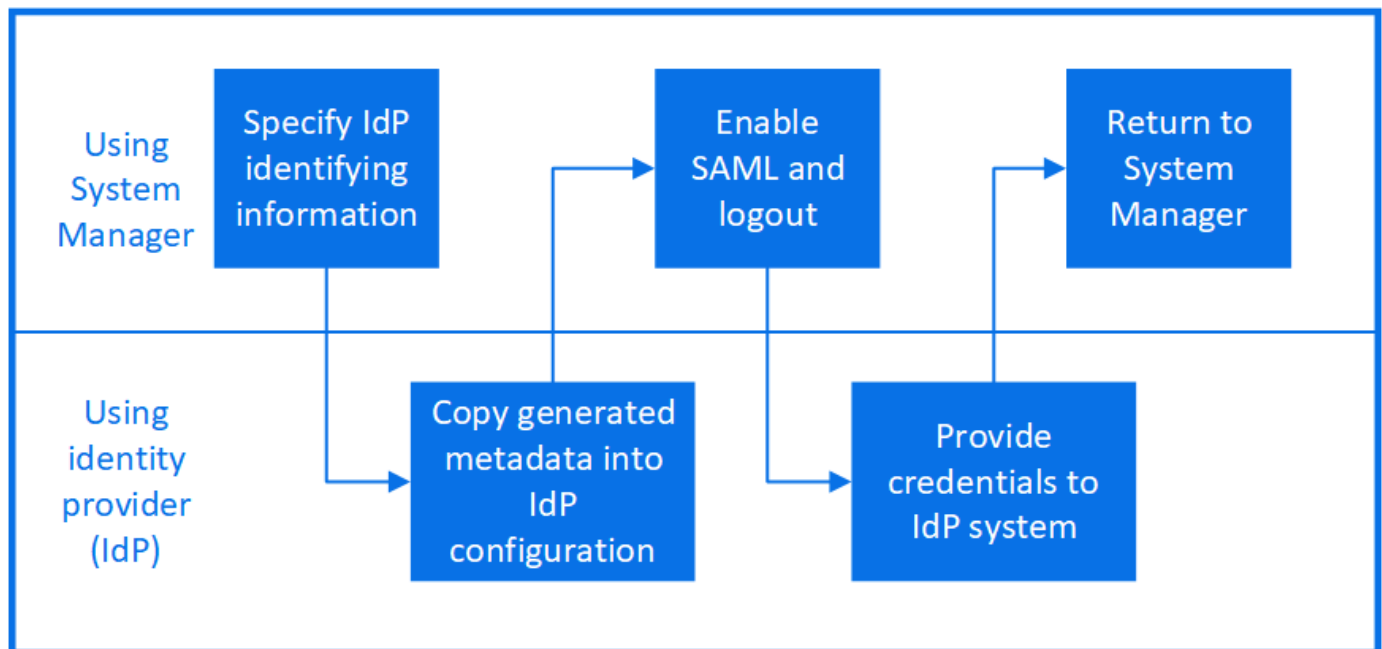
Depuis ONTAP 9.3, vous pouvez configurer l'authentification SAML pour les services Web. Lorsque l'authentification SAML est configurée et activée, les utilisateurs sont authentifiés par un fournisseur d'identité externe (IDP) au lieu des fournisseurs de services d'annuaire tels qu'Active Directory et LDAP.

Activez l'authentification SAML

Pour activer l'authentification SAML avec System Manager ou l'interface de ligne de commandes, effectuez les opérations suivantes. Si votre cluster exécute ONTAP 9.7 ou une version antérieure, les étapes à suivre dans System Manager sont différentes. Consultez l'aide en ligne de System Manager disponible sur votre système.



Après avoir activé l'authentification SAML, seuls les utilisateurs distants peuvent accéder à l'interface graphique de System Manager. Les utilisateurs locaux ne peuvent pas accéder à l'interface graphique de System Manager après l'authentification SAML.



Avant de commencer

- Le IDP que vous envisagez d'utiliser pour l'authentification à distance doit être configuré.



Consultez la documentation fournie par le PDI que vous avez configuré.

- Vous devez avoir l'URI du IDP.

Description de la tâche

- L'authentification SAML s'applique uniquement au `http` et `ontapi` en termes de latence.

Le `http` et `ontapi` Les applications sont utilisées par les services web suivants : infrastructure processeur de service, API ONTAP ou System Manager.

- L'authentification SAML est applicable uniquement pour l'accès au SVM d'administration.


Les PDI suivants ont été validés avec System Manager :

- Services de fédération Active Directory
- Cisco DUO (validé avec les versions ONTAP suivantes :)
 - 9.7P21 et versions ultérieures 9.7 (voir "[Documentation de System Manager Classic](#)")
 - 9.8P17 et versions ultérieures 9.8
 - 9.9.1P13 et versions ultérieures 9.9
 - 9.10.1P9 et versions ultérieures 9.10
 - 9.11.1P4 et versions ultérieures 9.11
 - versions 9.12.1 et ultérieures
- Hurlent

Effectuez les opérations suivantes en fonction de votre environnement :

Exemple 20. Étapes

System Manager

1. Cliquez sur **Cluster > Paramètres**.
2. En regard de **SAML Authentication**, cliquez sur .
3. Vérifiez que la case **Activer l'authentification SAML** est cochée.
4. Entrez l'URL de l'URI IDP (y compris "https://").
5. Modifiez l'adresse du système hôte, si nécessaire.
6. Assurez-vous que le bon certificat est utilisé :
 - Si votre système a été mappé avec un seul certificat de type « serveur », ce certificat est considéré comme le certificat par défaut et il n'est pas affiché.
 - Si votre système a été mappé avec plusieurs certificats comme type « serveur », l'un des certificats s'affiche. Pour sélectionner un autre certificat, cliquez sur **Modifier**.
7. Cliquez sur **Enregistrer**. Une fenêtre de confirmation affiche les informations sur les métadonnées, qui ont été automatiquement copiées dans le presse-papiers.
8. Accédez au système IDP que vous avez spécifié et copiez les métadonnées de votre presse-papiers pour mettre à jour les métadonnées système.
9. Revenez à la fenêtre de confirmation (dans System Manager) et cochez la case **J'ai configuré le IDP avec l'URI hôte ou les métadonnées**.
10. Cliquez sur **Déconnexion** pour activer l'authentification SAML. Le système IDP affiche un écran d'authentification.
11. Dans le système IDP, saisissez vos identifiants SAML. Une fois vos identifiants vérifiés, vous accédez à la page d'accueil de System Manager.

CLI

1. Créez une configuration SAML pour que ONTAP puisse accéder aux métadonnées IDP :

```
security saml-sp create -idp-uri idp_uri -sp-host ontap_host_name
```

`idp_uri` Est l'adresse FTP ou HTTP de l'hôte IDP à partir de laquelle les métadonnées IDP peuvent être téléchargées.

`ontap_host_name` Est le nom d'hôte ou l'adresse IP de l'hôte du fournisseur de services SAML, qui, dans le cas présent, correspond au système ONTAP. Par défaut, l'adresse IP de la LIF de cluster-management est utilisée.

Vous pouvez éventuellement fournir les informations de certificat de serveur ONTAP. Par défaut, les informations de certificat de serveur Web ONTAP sont utilisées.

```
cluster_12::> security saml-sp create -idp-uri  
https://example.url.net/idp/shibboleth
```

Warning: This restarts the web server. Any HTTP/S connections that are active

will be disrupted.

Do you want to continue? {y|n}: y

[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server domain to ensure that users are the same for different authentication methods. See the "security login show" command for the Data ONTAP user configuration.

L'URL permettant d'accéder aux métadonnées de l'hôte ONTAP s'affiche.

2. À partir de l'hôte IDP, configurez le IDP avec les métadonnées de l'hôte ONTAP.

Pour plus d'informations sur la configuration du IDP, reportez-vous à la documentation IDP.

3. Activer la configuration SAML :

```
security saml-sp modify -is-enabled true
```

Tout utilisateur existant qui accède à l' http ou ontapi L'application est automatiquement configurée pour l'authentification SAML.

4. Si vous souhaitez créer des utilisateurs pour le http ou ontapi Application après la configuration de SAML, spécifiez SAML comme méthode d'authentification pour les nouveaux utilisateurs.

- a. Créez une méthode de connexion pour les nouveaux utilisateurs avec l'authentification SAML :

```
security login create -user-or-group-name user_name -application [http |  
ontapi] -authentication-method saml -vserver svm_name
```

```
cluster_12::> security login create -user-or-group-name admin1  
-application http -authentication-method saml -vserver  
cluster_12
```

- b. Vérifiez que l'entrée utilisateur est créée :

```
security login show
```



```
cluster_12::> security login show
```

```
Vserver: cluster_12
```

```
Second
```

User/Group	Authentication		Acct
Authentication			
Name	Application	Method	Role Name
Method			Locked
-----	-----	-----	-----
admin	console	password	admin
none			
admin	http	password	admin
none			
admin	http	saml	admin
none			-
admin	ontapi	password	admin
none			
admin	ontapi	saml	admin
none			-
admin	service-processor		
		password	admin
none			
admin	ssh	password	admin
none			
admin1	http	password	backup
none			
**admin1	http	saml	backup
none**			-


Désactivez l'authentification SAML

Vous pouvez désactiver l'authentification SAML lorsque vous souhaitez arrêter l'authentification des utilisateurs Web à l'aide d'un fournisseur d'identité externe (IDP). Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés tels qu'Active Directory et LDAP sont utilisés pour l'authentification.

Effectuez les opérations suivantes en fonction de votre environnement :

Exemple 21. Étapes

System Manager

1. Cliquez sur **Cluster > Paramètres**.
2. Sous **authentification SAML**, cliquez sur le bouton bascule **activé**.
3. *Facultatif*. Vous pouvez également cliquer sur  en regard de **SAML Authentication**, puis décocher la case **Activer l'authentification SAML**.

CLI

1. Désactiver l'authentification SAML :

```
security saml-sp modify -is-enabled false
```

2. Si vous ne souhaitez plus utiliser l'authentification SAML ou si vous souhaitez modifier l'IDP, supprimez la configuration SAML :

```
security saml-sp delete
```

Résolution des problèmes liés à la configuration SAML

Si la configuration de l'authentification SAML échoue, vous pouvez réparer manuellement chaque nœud sur lequel la configuration SAML a échoué et effectuer une restauration suite à la défaillance. Au cours du processus de réparation, le serveur Web est redémarré et toutes les connexions HTTP ou HTTPS actives sont interrompues.

Description de la tâche

Lorsque vous configurez l'authentification SAML, ONTAP applique la configuration SAML par nœud. Lorsque vous activez l'authentification SAML, ONTAP tente automatiquement de réparer chaque nœud en cas de problèmes de configuration. Si la configuration SAML est problématique sur n'importe quel nœud, vous pouvez désactiver l'authentification SAML, puis réactiver l'authentification SAML. Lorsque la configuration SAML ne s'applique pas à un ou plusieurs nœuds, même après la réactivation de l'authentification SAML, cela peut se présenter. Vous pouvez identifier le nœud sur lequel la configuration SAML a échoué, puis réparer manuellement ce nœud.

Étapes

1. Connectez-vous au niveau de privilège avancé :

```
set -privilege advanced
```

2. Identifiez le nœud sur lequel la configuration SAML a échoué :

```
security saml-sp status show -instance
```

```
cluster_12::*> security saml-sp status show -instance

Node: node1
Update Status: config-success
Database Epoch: 9
Database Transaction Count: 997
Error Text:
SAML Service Provider Enabled: false
ID of SAML Config Job: 179

Node: node2
Update Status: config-failed
Database Epoch: 9
Database Transaction Count: 997
Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
ID of SAML Config Job: 180
2 entries were displayed.
```

3. Corrigez la configuration SAML sur le nœud défaillant :

security saml-sp repair -node *node_name*

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

Le serveur Web est redémarré et toutes les connexions HTTP ou HTTPS actives sont interrompues.

4. Vérifiez que le langage SAML est configuré sur tous les nœuds :

security saml-sp status show -instance

```
cluster_12::*> security saml-sp status show -instance

Node: node1
Update Status: config-success
Database Epoch: 9
Database Transaction Count: 997
Error Text:
SAML Service Provider Enabled: false
ID of SAML Config Job: 179

Node: node2
Update Status: **config-success**
Database Epoch: 9
Database Transaction Count: 997
Error Text:
SAML Service Provider Enabled: false
ID of SAML Config Job: 180
2 entries were displayed.
```

Informations associées

["Référence de commande ONTAP"](#)

Gérer les services Web

Présentation de la gestion des services Web

Vous pouvez activer ou désactiver un service Web pour le cluster ou une machine virtuelle de stockage (SVM), afficher les paramètres des services web et contrôler si les utilisateurs d'un rôle peuvent accéder à un service web.

Vous pouvez gérer les services web du cluster ou d'un SVM des manières suivantes :

- Activation ou désactivation d'un service Web spécifique
- Spécifier si l'accès à un service Web est limité à un seul HTTP crypté (SSL)
- Affichage de la disponibilité des services Web
- Autoriser ou interdire aux utilisateurs d'un rôle d'accéder à un service Web
- Affichage des rôles autorisés à accéder à un service Web

Pour qu'un utilisateur puisse accéder à un service Web, toutes les conditions suivantes doivent être remplies :

- L'utilisateur doit être authentifié.

Par exemple, un service Web peut demander un nom d'utilisateur et un mot de passe. La réponse de l'utilisateur doit correspondre à un compte valide.

- L'utilisateur doit être configuré avec la méthode d'accès correcte.

L'authentification ne réussit que pour les utilisateurs disposant de la méthode d'accès correcte pour le service Web donné. Pour le service Web de l'API ONTAP (`ontapi`), les utilisateurs doivent avoir le `ontapi` méthode d'accès. Pour tous les autres services Web, les utilisateurs doivent avoir le `http` méthode d'accès.



Vous utilisez le `security login` commandes permettant de gérer les méthodes d'accès et d'authentification des utilisateurs.

- Le service Web doit être configuré pour permettre le rôle de contrôle d'accès de l'utilisateur.



Vous utilisez le `vserver services web access` commandes permettant de contrôler l'accès d'un rôle à un service web.

Si un pare-feu est activé, la politique de pare-feu de la LIF à utiliser pour les services Web doit être configurée de manière à autoriser HTTP ou HTTPS.

Si vous utilisez HTTPS pour l'accès aux services Web, SSL pour le cluster ou le SVM qui offre le service Web doit également être activé et vous devez fournir un certificat numérique pour le cluster ou SVM.

Gérer l'accès aux services Web

Un service Web est une application que les utilisateurs peuvent accéder via HTTP ou HTTPS. L'administrateur du cluster peut configurer le moteur de protocole Web, configurer SSL, activer un service Web et permettre aux utilisateurs d'un rôle d'accéder à un service Web.

Depuis ONTAP 9.6, les services Web suivants sont pris en charge :

- Infrastructure du processeur de service (`spi`)

Ce service met à disposition les fichiers log, core dump et MIB des nœuds pour l'accès HTTP ou HTTPS via la LIF de cluster management ou une LIF de node-management. Le paramètre par défaut est `enabled`.

Lors d'une demande d'accès aux fichiers journaux ou aux fichiers « core dump » d'un nœud, la `spi` le service web crée automatiquement un point de montage d'un nœud vers le volume racine d'un autre nœud où les fichiers résident. Il n'est pas nécessaire de créer manuellement le point de montage. `

- Les API ONTAP (`ontapi`)

Ce service vous permet d'exécuter des API ONTAP pour exécuter des fonctions administratives avec un programme distant. Le paramètre par défaut est `enabled`.

Ce service peut être requis pour certains outils de gestion externes. Par exemple, si vous utilisez System Manager, vous devez laisser ce service activé.

- Détection Data ONTAP (`disco`)

Ce service permet aux applications de gestion externes de découvrir le cluster sur le réseau. Le paramètre

par défaut est `enabled`.

- Diagnostics du support (`supdiag`)

Ce service contrôle l'accès à un environnement privilégié sur le système afin d'aider à l'analyse et à la résolution des problèmes. Le paramètre par défaut est `disabled`. Vous ne devez activer ce service que si vous y êtes invité par le support technique.

- System Manager (`sysmgr`)

Ce service contrôle la disponibilité de System Manager, qui est inclus avec ONTAP. Le paramètre par défaut est `enabled`. Ce service est pris en charge uniquement sur le cluster.

- Mise à jour du contrôleur BMC (Baseboard Management Controller) du micrologiciel (`FW_BMC`)

Ce service vous permet de télécharger les fichiers du micrologiciel BMC. Le paramètre par défaut est `enabled`.

- Documentation ONTAP (`docs`)

Ce service fournit un accès à la documentation ONTAP. Le paramètre par défaut est `enabled`.

- API RESTful ONTAP (`docs_api`)

Ce service permet d'accéder à la documentation de l'API RESTful ONTAP. Le paramètre par défaut est `enabled`.

- Téléchargement de fichiers (`fud`)

Ce service permet le téléchargement et le téléchargement de fichiers. Le paramètre par défaut est `enabled`.

- Messagerie ONTAP (`ontapmsg`)

Ce service prend en charge une interface de publication et d'abonnement qui vous permet de vous abonner à des événements. Le paramètre par défaut est `enabled`.

- Portail ONTAP (`portal`)

Ce service implémente la passerelle dans un serveur virtuel. Le paramètre par défaut est `enabled`.

- Interface ONTAP RESTful (`rest`)

Ce service prend en charge une interface RESTful qui permet de gérer à distance tous les éléments de l'infrastructure du cluster. Le paramètre par défaut est `enabled`.

- Prise en charge des fournisseurs de services SAML (`saml`)

Ce service fournit des ressources pour prendre en charge le fournisseur de services SAML. Le paramètre par défaut est `enabled`.

- Fournisseur de services SAML (`saml-sp`)

Ce service offre des services tels que les métadonnées SP et le service client d'assertion au fournisseur de services. Le paramètre par défaut est `enabled`.

Depuis ONTAP 9.7, les services supplémentaires suivants sont pris en charge :

- Fichiers de sauvegarde de configuration (`backups`)

Ce service vous permet de télécharger les fichiers de sauvegarde de configuration. Le paramètre par défaut est `enabled`.

- Sécurité ONTAP (`security`)

Ce service prend en charge la gestion des jetons CSRF pour une authentification améliorée. Le paramètre par défaut est `enabled`.

Gérer le moteur de protocole Web

Vous pouvez configurer le moteur de protocole Web sur le cluster pour contrôler si l'accès Web est autorisé et quelles versions SSL peuvent être utilisées. Vous pouvez également afficher les paramètres de configuration du moteur de protocole Web.

Vous pouvez gérer le moteur de protocole Web au niveau du cluster de plusieurs manières :

- Vous pouvez indiquer si les clients distants peuvent utiliser HTTP ou HTTPS pour accéder au contenu du service Web à l'aide de l'`system services web modify` commande avec `-external` paramètre.
- Vous pouvez spécifier si SSLv3 doit être utilisé pour un accès Web sécurisé à l'aide de l'`security config modify` commande avec `-supported-protocol` paramètre.
Par défaut, SSLv3 est désactivé. La sécurité de la couche de transport 1.0 (TLSv1) est activée et elle peut être désactivée si nécessaire.
- Vous pouvez activer le mode de conformité Federal Information Processing Standard (FIPS) 140-2 pour les interfaces de service Web du plan de contrôle à l'échelle du cluster.



Par défaut, le mode de conformité FIPS 140-2 est désactivé.

- **Lorsque le mode de conformité FIPS 140-2 est désactivé**

Vous pouvez activer le mode de conformité FIPS 140-2 en configurant le `is-fips-enabled` paramètre à `true` pour le `security config modify` et en utilisant la commande `security config show` commande pour confirmer le statut en ligne.

- **Lorsque le mode de conformité FIPS 140-2 est activé**

- À partir de ONTAP 9.11.1, TLSv1, TLSv1.1 et SSLv3 sont désactivés et seuls TLSv1.2 et TLSv1.3 restent activés. Elle affecte d'autres systèmes et communications internes et externes à ONTAP 9. Si vous activez le mode de conformité FIPS 140-2 puis désactivez-le, TLSv1, TLSv1.1 et SSLv3 restent désactivés. TLSv1 ou TLSv1.1 restent activés en fonction de la configuration précédente.
- Pour les versions de ONTAP antérieures à 9.11.1, TLSv1 et SSLv3 sont tous deux désactivés et seuls les modèles TLSv1.1 et TLSv1.2 restent activés. ONTAP vous empêche d'activer à la fois TLSv1 et SSLv3 lorsque le mode de conformité FIPS 140-2 est activé. Si vous activez le mode de conformité FIPS 140-2 puis désactivez-le, TLSv1 et SSLv3 restent désactivés, mais TLSv1.2 ou les deux TLSv1.1 et TLSv1.2 sont activés en fonction de la configuration précédente.

- Vous pouvez afficher la configuration de la sécurité au niveau du cluster à l'aide de `system security config show` commande.

Si le pare-feu est activé, la politique de pare-feu pour l'interface logique (LIF) à utiliser pour les services Web doit être configurée de manière à autoriser l'accès HTTP ou HTTPS.

Si vous utilisez HTTPS pour l'accès aux services Web, SSL pour le cluster ou la machine virtuelle de stockage (SVM) qui offre le service Web doit également être activé, et vous devez fournir un certificat numérique pour le cluster ou la SVM.

Dans les configurations MetroCluster, les modifications de paramètre apportées au moteur de protocole Web sur un cluster ne sont pas répliquées sur le cluster partenaire.

Commandes de gestion du moteur de protocole Web

Vous utilisez le `system services web` commandes permettant de gérer le moteur de protocole web. Vous utilisez le `system services firewall policy create` et `network interface modify` commandes permettant d'autoriser les demandes d'accès web à passer par le pare-feu.

Les fonctions que vous recherchez...	Utilisez cette commande...
Configurer le moteur de protocole Web au niveau du cluster : <ul style="list-style-type: none"> • Activez ou désactivez le moteur de protocole Web pour le cluster • Activez ou désactivez SSLv3 pour le cluster • Activer ou désactiver la conformité FIPS 140-2 pour des services web sécurisés (HTTPS) 	<code>system services web modify</code>
Afficher la configuration du moteur de protocole Web au niveau du cluster, déterminer si les protocoles Web sont fonctionnels dans tout le cluster et indiquer si la conformité FIPS 140-2 est activée et en ligne	<code>system services web show</code>
Afficher la configuration du moteur de protocole Web au niveau du nœud et l'activité de gestion du service Web pour les nœuds du cluster	<code>system services web node show</code>
Créez une politique de pare-feu ou ajoutez un service de protocole HTTP ou HTTPS à une politique de pare-feu existante pour permettre aux demandes d'accès Web de passer par le pare-feu	<code>system services firewall policy create</code> Réglage du <code>-service</code> paramètre à <code>http</code> ou <code>https</code> permet aux demandes d'accès web de passer par le pare-feu.

Les fonctions que vous recherchez...	Utilisez cette commande...
Associer une politique de pare-feu à une LIF	<pre>network interface modify</pre> <p>Vous pouvez utiliser le <code>-firewall-policy</code> Paramètre pour modifier la politique de pare-feu d'une LIF.</p>

Configurer l'accès aux services Web

La configuration de l'accès aux services Web permet aux utilisateurs autorisés d'utiliser HTTP ou HTTPS pour accéder au contenu du service sur le cluster ou sur un SVM (Storage Virtual machine).

Étapes

1. Si un pare-feu est activé, assurez-vous que l'accès HTTP ou HTTPS est configuré dans la politique de pare-feu pour la LIF qui sera utilisée pour les services Web :



Vous pouvez vérifier si un pare-feu est activé à l'aide du `system services firewall show` commande.

- a. Pour vérifier que HTTP ou HTTPS est configuré dans la stratégie de pare-feu, utilisez le `system services firewall policy show` commande.

Vous définissez le `-service` paramètre du `system services firewall policy create` commande à `http` ou `https` pour activer la stratégie de prise en charge de l'accès web.

- b. Pour vérifier que la politique de pare-feu prenant en charge HTTP ou HTTPS est associée au LIF qui fournit des services Web, utilisez le `network interface show` commande avec `-firewall-policy` paramètre.

Vous utilisez le `network interface modify` commande avec `-firewall-policy` Paramètre pour mettre la politique de pare-feu en vigueur pour une LIF.

2. Pour configurer le moteur de protocole Web au niveau du cluster et rendre le contenu du service Web accessible, utilisez le `system services web modify` commande.
3. Si vous prévoyez d'utiliser des services Web sécurisés (HTTPS), activez SSL et fournissez les informations de certificat numérique pour le cluster ou la SVM à l'aide du `security ssl modify` commande.
4. Pour activer un service Web pour le cluster ou un SVM, utilisez le `vserver services web modify` commande.

Vous devez répéter cette étape pour chaque service que vous souhaitez activer pour le cluster ou la SVM.

5. Pour autoriser un rôle permettant d'accéder aux services web sur le cluster ou SVM, utilisez la `vserver services web access create` commande.

Le rôle auquel vous accordez l'accès doit déjà exister. Vous pouvez afficher les rôles existants à l'aide de la `security login role show` commande ou création de nouveaux rôles à l'aide de la commande `security login role create` commande.

6. Pour un rôle autorisé à accéder à un service Web, assurez-vous que ses utilisateurs sont également configurés avec la méthode d'accès correcte en vérifiant la sortie du `security login show` commande.

Pour accéder au service Web de l'API ONTAP (`ontapi`), un utilisateur doit être configuré avec le `ontapi` méthode d'accès. Pour accéder à tous les autres services Web, un utilisateur doit être configuré avec le `http` méthode d'accès.



Vous utilisez le `security login create` commande permettant d'ajouter une méthode d'accès pour un utilisateur.

Commandes pour la gestion des services Web

Vous utilisez le `vserver services web` Commandes permettant de gérer la disponibilité des services web pour le cluster ou une machine virtuelle de stockage (SVM). Vous utilisez le `vserver services web access` commandes permettant de contrôler l'accès d'un rôle à un service web.

Les fonctions que vous recherchez...	Utilisez cette commande...
Configurer un service web pour le cluster ou anSVM : <ul style="list-style-type: none">• Activer ou désactiver un service Web• Spécifiez si seul HTTPS peut être utilisé pour accéder à un service Web	<code>vserver services web modify</code>
Afficher la configuration et la disponibilité des services web pour le cluster ou anSVM	<code>vserver services web show</code>
Autoriser un rôle à accéder à un service web sur le cluster ou anSVM	<code>vserver services web access create</code>
Afficher les rôles autorisés pour accéder aux services web sur le cluster ou anSVM	<code>vserver services web access show</code>
Empêcher un rôle d'accéder à un service Web sur le cluster ou anSVM	<code>vserver services web access delete</code>

Informations associées

["Référence de commande ONTAP"](#)

Commandes permettant de gérer les points de montage sur les nœuds

Le `spi` le service web crée automatiquement un point de montage d'un nœud vers le volume racine d'un autre nœud lors d'une demande d'accès aux fichiers journaux ou fichiers « core » du nœud. Bien que vous n'ayez pas besoin de gérer manuellement les points de montage, vous pouvez le faire en utilisant le `system node root-mount` commandes.

Les fonctions que vous recherchez...	Utilisez cette commande...
Créer manuellement un point de montage d'un nœud vers le volume racine d'un autre nœud	<code>system node root-mount create</code> Un seul point de montage peut exister d'un nœud à un autre.
Affiche les points de montage existants sur les nœuds du cluster, y compris le moment où un point de montage a été créé et son état actuel	<code>system node root-mount show</code>
Supprimez un point de montage d'un nœud vers le volume racine d'un autre nœud et force les connexions vers le point de montage à fermer	<code>system node root-mount delete</code>

Informations associées

["Référence de commande ONTAP"](#)

Gérer SSL

Utilisez le `security ssl` Commandes permettant de gérer le protocole SSL pour le cluster ou une machine virtuelle de stockage (SVM). Le protocole SSL améliore la sécurité de l'accès au Web en utilisant un certificat numérique pour établir une connexion chiffrée entre un serveur Web et un navigateur.

Vous pouvez gérer SSL pour le cluster ou une machine virtuelle de stockage (SVM) de la manière suivante :

- Activation de SSL
- Génération et installation d'un certificat numérique et son association au cluster ou à la SVM
- Affichage de la configuration SSL pour voir si SSL a été activé et, le cas échéant, le nom du certificat SSL
- Configuration de politiques de pare-feu pour le cluster ou SVM, de sorte que les demandes d'accès Web puissent passer par
- Définition des versions SSL pouvant être utilisées
- Limiter l'accès aux requêtes HTTPS uniquement pour un service Web

Commandes pour la gestion de SSL



Vous utilisez le `security ssl` Commandes permettant de gérer le protocole SSL pour le cluster ou une machine virtuelle de stockage (SVM).



Les fonctions que vous recherchez...	Utilisez cette commande...
Activez le protocole SSL pour le cluster ou un SVM et associez un certificat numérique à celui-ci	<code>security ssl modify</code>
Afficher la configuration SSL et le nom du certificat pour le cluster ou un SVM	<code>security ssl show</code>


Résoudre les problèmes d'accès au service Web


Des erreurs de configuration provoquent des problèmes d'accès au service Web. Vous pouvez corriger les erreurs en vous assurant que la LIF, la politique de pare-feu, le moteur de protocole Web, les services Web, les certificats numériques, et l'autorisation d'accès utilisateur sont toutes correctement configurées.

Le tableau suivant vous aide à identifier et à résoudre les erreurs de configuration du service Web :

Ce problème d'accès...	Se produit en raison de cette erreur de configuration...	Pour résoudre l'erreur...
Votre navigateur Web renvoie un <code>unable to connect</code> ou <code>failure to establish a connection</code> erreur lorsque vous essayez d'accéder à un service web.	Votre LIF n'est peut-être pas configurée correctement.	Assurez-vous de pouvoir envoyer une requête ping à la LIF qui fournit le service Web.  Vous utilisez le <code>network ping</code> Commande ping d'une LIF. Pour plus d'informations sur la configuration du réseau, reportez-vous au <i>Network Management Guide</i> .
Votre pare-feu est peut-être configuré de manière incorrecte.	Assurez-vous qu'une politique de pare-feu est configurée pour prendre en charge HTTP ou HTTPS et que la politique est attribuée à la LIF qui fournit le service Web.  Vous utilisez le <code>system services firewall policy</code> commandes permettant de gérer les politiques de pare-feu. Vous utilisez le <code>network interface modify</code> commande avec <code>-firewall -policy</code> Paramètre pour associer une policy à une LIF.	Votre moteur de protocole Web peut être désactivé.

Ce problème d'accès...	Se produit en raison de cette erreur de configuration...	Pour résoudre l'erreur...
<p>Assurez-vous que le moteur de protocole Web est activé pour que les services Web soient accessibles.</p> <div data-bbox="167 464 220 516">  </div> <div data-bbox="279 373 535 609"> <p>Vous utilisez le <code>system services web</code> commandes permettant de gérer le moteur de protocole web pour le cluster.</p> </div>	<p>Votre navigateur Web renvoie un <code>not found</code> erreur lorsque vous essayez d'accéder à un service web.</p>	<p>Le service Web est peut-être désactivé.</p>
<p>Assurez-vous que chaque service Web auquel vous souhaitez autoriser l'accès est activé individuellement.</p> <div data-bbox="167 947 220 999">  </div> <div data-bbox="279 852 535 1087"> <p>Vous utilisez le <code>vserver services web modify</code> commande permettant d'activer un service web pour l'accès.</p> </div>	<p>Le navigateur Web ne parvient pas à se connecter à un service Web avec le nom de compte et le mot de passe d'un utilisateur.</p>	<p>L'utilisateur ne peut pas être authentifié, la méthode d'accès n'est pas correcte ou l'utilisateur n'est pas autorisé à accéder au service Web.</p>

Ce problème d'accès...	Se produit en raison de cette erreur de configuration...	Pour résoudre l'erreur...
<p>Assurez-vous que le compte utilisateur existe et est configuré avec la méthode d'accès et la méthode d'authentification appropriées. Assurez-vous également que le rôle de l'utilisateur est autorisé à accéder au service Web.</p> <div data-bbox="167 930 220 982">  </div> <p>Vous utilisez le <code>security login</code> commandes permettant de gérer les comptes utilisateurs, leurs méthodes d'accès et leurs méthodes d'authentification. Pour accéder au service Web de l'API ONTAP, vous devez utiliser le <code>ontapi</code> méthode d'accès. L'accès à tous les autres services Web nécessite le <code>http</code> méthode d'accès. Vous utilisez le <code>vserver</code> <code>services web</code> <code>access</code> commandes permettant de gérer l'accès d'un rôle à un service web.</p>	<p>Vous vous connectez à votre service Web via HTTPS et votre navigateur Web indique que votre connexion est interrompue.</p>	<p>Il se peut que vous n'ayez pas activé SSL sur le cluster ou la machine virtuelle de stockage (SVM) qui fournit le service Web.</p>

Ce problème d'accès...	Se produit en raison de cette erreur de configuration...	Pour résoudre l'erreur...
<p>S'assurer que le cluster ou le SVM a activé SSL et que le certificat numérique est valide.</p> <div>  <p>Vous utilisez le <code>security ssl</code> Commandes permettant de gérer la configuration SSL des serveurs HTTP et du <code>security certificate show</code> commande permettant d'afficher les informations relatives au certificat numérique.</p> </div>	<p>Vous vous connectez à votre service Web via HTTPS et votre navigateur Web indique que la connexion n'est pas fiable.</p>	<p>Vous utilisez peut-être un certificat numérique auto-signé.</p>

Vérifiez l'identité des serveurs distants à l'aide de certificats

Vérifiez l'identité des serveurs distants à l'aide de la présentation des certificats

ONTAP prend en charge les fonctions de certificat de sécurité pour vérifier l'identité des serveurs distants.

Le logiciel ONTAP permet des connexions sécurisées à l'aide des fonctionnalités et protocoles de certificat numérique suivants :

- Le protocole OCSP (Online Certificate Status Protocol) valide le statut des demandes de certificat numérique des services ONTAP à l'aide de connexions SSL et TLS (transport Layer Security). Cette fonction est désactivée par défaut.
- Un ensemble par défaut de certificats racine de confiance est inclus avec le logiciel ONTAP.
- Les certificats KMIP (Key Management Interoperability Protocol) permettent d'effectuer une authentification mutuelle d'un cluster et d'un serveur KMIP.

Vérifiez que les certificats numériques sont valides à l'aide du protocole OCSP

Depuis ONTAP 9.2, le protocole OCSP (Online Certificate Status Protocol) permet aux applications ONTAP qui utilisent les communications TLS (transport Layer Security) de recevoir le statut du certificat numérique lorsque le protocole OCSP est activé. Vous pouvez à tout moment activer ou désactiver les vérifications d'état des certificats OCSP pour des applications spécifiques. Par défaut, la vérification du statut du certificat OCSP est désactivée.

Ce dont vous avez besoin

Vous avez besoin d'un accès de niveau de privilège avancé pour effectuer cette tâche.

Description de la tâche

OCSP prend en charge les applications suivantes :

- AutoSupport
- Système de gestion des événements (EMS)
- LDAP sur TLS
- Protocole KMIP (Key Management Interoperability Protocol)
- Consignation d'audits
- FabricPool
- SSH (à partir de ONTAP 9.13.1)

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`.
2. Pour activer ou désactiver les vérifications du statut des certificats OCSP pour des applications ONTAP spécifiques, utilisez la commande appropriée.

Si vous souhaitez que l'état du certificat OCSP soit vérifié pour certaines applications...	Utilisez la commande...
Activé	<code>security config ocsp enable -app app name</code>
Désactivé	<code>security config ocsp disable -app app name</code>

La commande suivante active la prise en charge OCSP pour AutoSupport et EMS.

```
cluster::*> security config ocsp enable -app asup,ems
```

Lorsque OCSP est activé, l'application reçoit l'une des réponses suivantes :

- Bon - le certificat est valide et la communication continue.
 - Révoqué - le certificat est considéré comme non digne de confiance par son autorité de certification émettrice et la communication ne peut pas se poursuivre.
 - Inconnu - le serveur n'a pas d'informations d'état sur le certificat et la communication ne peut pas se poursuivre.
 - Il manque des informations de serveur OCSP dans le certificat. Le serveur agit comme si OCSP est désactivé et continue avec la communication TLS, mais aucune vérification d'état n'a lieu.
 - Aucune réponse du serveur OCSP - l'application ne peut pas continuer.
3. Pour activer ou désactiver les vérifications d'état des certificats OCSP pour toutes les applications utilisant les communications TLS, utilisez la commande appropriée.

Si vous souhaitez que l'état du certificat OCSP soit vérifié pour toutes les applications...	Utilisez la commande...
Activé	<pre>security config ocsd enable -app all</pre>
Désactivé	<pre>security config ocsd disable -app all</pre>

Lorsque cette option est activée, toutes les applications reçoivent une réponse signée indiquant le statut du certificat spécifié : bon, révoqué ou inconnu. Dans le cas d'un certificat révoqué, l'application ne pourra pas continuer. Si l'application ne parvient pas à recevoir de réponse du serveur OCSP ou si le serveur est inaccessible, l'application ne pourra pas continuer.

4. Utilisez le `security config ocsd show` Commande pour afficher toutes les applications qui prennent en charge OCSP et leur état de support.

```
cluster::*> security config ocsd show
Application                                OCSP Enabled?
-----
autosupport                                false
audit_log                                  false
fabricpool                                 false
ems                                         false
kmip                                        false
ldap_ad                                    true
ldap_nis_namemap                           true
ssh                                         true

8 entries were displayed.
```

Afficher les certificats par défaut pour les applications basées sur TLS

Depuis ONTAP 9.2, ONTAP fournit un ensemble par défaut de certificats racine de confiance pour les applications ONTAP utilisant TLS (transport Layer Security).

Ce dont vous avez besoin

Les certificats par défaut ne sont installés que sur le SVM d'admin pendant sa création ou lors d'une mise à niveau vers ONTAP 9.2.

Description de la tâche

Les applications actuelles qui agissent en tant que client et qui nécessitent une validation de certificat sont AutoSupport, EMS, LDAP, Audit Logging, FabricPool, Et KMIP.

Lorsque les certificats expirent, un message EMS est appelé pour demander à l'utilisateur de supprimer les

certificats. Les certificats par défaut ne peuvent être supprimés qu'au niveau de privilège avancé.



La suppression des certificats par défaut peut entraîner l'absence de fonctionnement de certaines applications ONTAP (par exemple, AutoSupport et Audit Logging).

Étape

1. Vous pouvez afficher les certificats par défaut qui sont installés sur le SVM d'admin en utilisant la commande `Security Certificate show` :

`security certificate show -vserver -type server-ca`

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver      Serial Number  Common Name                                     Type
-----
fas2552-2n-abc-3
              01              AAACertificateServices
server-ca
Certificate Authority: AAA Certificate Services
Expiration Date: Sun Dec 31 18:59:59 2028
```

Authentifier mutuellement le cluster et un serveur KMIP

Authentification mutuelle du cluster et présentation d'un serveur KMIP

L'authentification mutuelle du cluster et d'un gestionnaire de clés externe, tel qu'un serveur KMIP (Key Management Interoperability Protocol), permettent au gestionnaire de clés de communiquer avec le cluster via KMIP sur SSL. Dans ce cas, une application ou certaines fonctionnalités (par exemple, la fonctionnalité Storage Encryption) nécessitent des clés sécurisées pour assurer un accès sécurisé aux données.

Générer une demande de signature de certificat pour le cluster

Vous pouvez utiliser le certificat de sécurité `generate-csr` Commande pour générer une requête de signature de certificat (CSR). Après le traitement de votre demande, l'autorité de certification vous envoie le certificat numérique signé.

Ce dont vous avez besoin

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou un administrateur SVM.

Étapes

1. Générer une RSC :

`security certificate generate-csr -common-name FQDN_or_common_name -size 512|1024|1536|2048 -country country -state state -locality locality`

```
-organization organization -unit unit -email-addr email_of_contact -hash  
-function SHA1|SHA256|MD5
```

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

La commande suivante crée une RSC avec une clé privée de 2,048 bits générée par la fonction de hachage SHA256, utilisée par le groupe Software dans LE département IT d'une société dont le nom commun personnalisé est server1.companyname.com, située à Sunnyvale (Californie), aux États-Unis. L'adresse e-mail de l'administrateur du contact SVM est web@example.com. Le système affiche la RSC et la clé privée dans la sortie.

```
cluster1::>security certificate generate-csr -common-name  
server1.companyname.com -size 2048 -country US -state California -  
locality Sunnyvale -organization IT -unit Software -email-addr  
web@example.com -hash-function SHA256  
Certificate Signing Request :  
-----BEGIN CERTIFICATE REQUEST-----  
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMakGA1UEBhMCVVMx  
CTAHBgNVBAgTADAEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAStADEPMA0G  
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApt1nzS  
xOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJbmXuj6U3alwoUsb13wfEvQnHVFNCi  
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBChUAA0EA6EagLfso5+4g+ejiRKKTUPQO  
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==  
-----END CERTIFICATE REQUEST-----  
Private Key :  
24 | Administrator Authentication and RBAC  
-----BEGIN RSA PRIVATE KEY-----  
MIIBOwIBAAJBAPXFanNoJApt1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJb  
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu  
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM  
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu  
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NctEYxd0Q5  
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA  
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==  
-----END RSA PRIVATE KEY-----  
Note: Please keep a copy of your certificate request and private key  
for future reference.
```

2. Copiez la demande de certificat à partir de la sortie CSR, puis envoyez-la sous forme électronique (par exemple, un courriel) à une autorité de certification tierce approuvée pour signature.

Après le traitement de votre demande, l'AC vous envoie le certificat numérique signé. Vous devez conserver une copie de la clé privée et du certificat numérique signé par l'autorité de certification.

Installez un certificat de serveur signé par l'autorité de certification pour le cluster

Pour permettre à un serveur SSL d'authentifier le cluster ou la machine virtuelle de stockage (SVM) en tant que client SSL, vous installez un certificat numérique avec le type client sur le cluster ou le SVM. Ensuite, vous fournissez le certificat client-CA à l'administrateur du serveur SSL pour l'installation sur le serveur.

Ce dont vous avez besoin

Vous devez déjà avoir installé le certificat root du serveur SSL sur le cluster ou SVM avec le `server-ca` type de certificat.

Étapes

1. Pour utiliser un certificat numérique auto-signé pour l'authentification client, utilisez le `security certificate create` commande avec `type client` paramètre.
2. Pour utiliser un certificat numérique signé par une autorité de certification pour l'authentification client, procédez comme suit :
 - a. Générez une demande de signature de certificat numérique (RSC) à l'aide du certificat de sécurité `generate-csr` commande.

ONTAP affiche la sortie CSR, qui comprend une demande de certificat et une clé privée, et vous rappelle de copier la sortie dans un fichier pour référence ultérieure.
 - b. Envoyez la demande de certificat de la sortie CSR sous forme électronique (par exemple, un courriel) à une autorité de certification approuvée pour signature.

Vous devez conserver une copie de la clé privée et du certificat signé par l'AC pour référence ultérieure.

Après le traitement de votre demande, l'AC vous envoie le certificat numérique signé.

- a. Installez le certificat signé par l'autorité de certification à l'aide du `security certificate install` commande avec `-type client` paramètre.
- b. Entrez le certificat et la clé privée lorsque vous y êtes invité, puis appuyez sur **entrée**.
- c. Entrez tout certificat racine ou intermédiaire supplémentaire lorsque vous y êtes invité, puis appuyez sur **entrée**.

Vous installez un certificat intermédiaire sur le cluster ou le SVM si une chaîne de certificats qui commence à l'autorité de certification racine de confiance et se termine par le certificat SSL qui vous est délivré, manque les certificats intermédiaires. Un certificat intermédiaire est un certificat subordonné délivré par la racine de confiance spécifiquement pour délivrer des certificats de serveur d'entité finale. Le résultat est une chaîne de certificats qui commence au niveau de l'autorité de certification racine de confiance, passe par le certificat intermédiaire et se termine par le certificat SSL qui vous a été délivré.

3. Fournir le `client-ca` Certificat du cluster ou SVM à l'administrateur du serveur SSL pour installation sur le serveur.

Commande du certificat de sécurité `show` avec `-instance` et `-type client-ca` paramètres affiche le `client-ca` informations sur le certificat.

Installez un certificat client signé par une autorité de certification pour le serveur KMIP

Le sous-type de certificat du protocole KMIP (Key Management Interoperability Protocol) (paramètre `-subtype kmip-cert`), ainsi que les types `client` et `serveur-ca`, spécifie que le certificat est utilisé pour authentifier mutuellement le cluster et un gestionnaire de clés externe, comme un serveur KMIP.

Description de la tâche

Installez un certificat KMIP pour authentifier un serveur KMIP en tant que serveur SSL sur le cluster.

Étapes

1. Utilisez le `security certificate install` commande avec `-type server-ca` et `-subtype kmip-cert` Paramètres pour installer un certificat KMIP pour le serveur KMIP.
2. Lorsque vous y êtes invité, entrez le certificat, puis appuyez sur entrée.

ONTAP vous rappelle de conserver une copie du certificat à des fins de référence ultérieure.

```
cluster1::> security certificate install -type server-ca -subtype kmip-  
cert  
-vserver cluster1
```

```
Please enter Certificate: Press <Enter> when done
```

```
-----BEGIN CERTIFICATE-----
```

```
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG  
2JhucwNhkcV8sEVAbkSdjbCxlRhLQ2pRdKkkirWmnWXbj9T/UWZyB2oK0z5XqcJ  
2HUw19JlYDln1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
```

```
...
```

```
-----END CERTIFICATE-----
```

```
You should keep a copy of the CA-signed digital certificate for future  
reference.
```

```
cluster1::>
```

Sécurité et chiffrement des données

À propos de la protection contre les ransomware de NetApp

Attaques par ransomware et portefeuille de solutions de protection de NetApp

Les ransomwares restent l'une des menaces les plus importantes qui ont entraîné des interruptions d'activité pour les entreprises en 2024. D'après le "[Sophos : État des ransomware 2024](#)", les attaques par ransomware ont affecté 72 % de leur public interrogé. Les attaques par ransomware ont évolué pour être plus sophistiquées et ciblées : les acteurs de menaces utilisent des techniques avancées, telles que l'intelligence artificielle, pour optimiser leur impact et leurs bénéfices.

Les entreprises doivent regarder l'ensemble de leur posture de sécurité du périmètre, du réseau, de l'identité, des applications et de l'emplacement des données au niveau du stockage, et sécuriser ces couches. L'adoption d'une approche axée sur les données en matière de cybersécurité au niveau de la couche de stockage est cruciale dans le paysage actuel des menaces. Bien qu'aucune solution ne puisse déjouer toutes les attaques, l'utilisation d'un portefeuille de solutions, notamment des partenariats et des tiers, offre une défense multicouche.

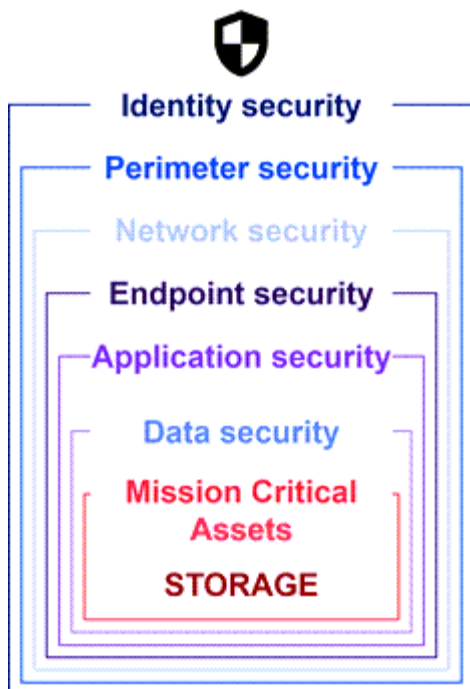
Le [Gamme de produits NetApp](#) fournit divers outils efficaces pour la visibilité, la détection et la résolution des problèmes, ce qui vous aide à détecter rapidement les ransomware, à prévenir la propagation et à restaurer rapidement, si nécessaire, pour éviter les interruptions coûteuses. Les solutions de défense à plusieurs couches classiques restent répandues, tout comme les solutions tierces et partenaires pour la visibilité et la détection. Une solution efficace reste une partie essentielle de la réponse à toute menace. L'approche unique du secteur qui repose sur la technologie NetApp Snapshot immuable et la solution SnapLock Logical Air Gap est un atout concurrentiel dans le secteur et constitue la bonne pratique du secteur pour la résolution des problèmes par ransomware.



Depuis juillet 2024, le contenu du rapport technique *TR-4572: NetApp ransomware protection*, qui a été publié au format PDF, a été intégré au reste de la documentation produit de ONTAP.

Les données sont la cible principale

Les cybercriminels ciblent de plus en plus directement les données, en reconnaissant leur valeur. Bien que la sécurité du périmètre, du réseau et des applications soit importante, il est possible de les contourner. La couche de stockage, qui se concentre sur la protection des données à la source, constitue une dernière ligne de défense critique. Les attaques par ransomware ont pour objectif d'accéder aux données de production et de les chiffrer ou de les rendre inaccessibles. Pour y parvenir, les attaquants doivent déjà avoir percé les défenses existantes déployées par les entreprises aujourd'hui, du périmètre à la sécurité des applications.



Malheureusement, de nombreuses entreprises ne tirent pas parti des fonctionnalités de sécurité au niveau de la couche de données. C'est là qu'intervient la gamme de solutions NetApp pour la protection contre les ransomwares, pour vous protéger dans votre dernier domaine de défense.

Le vrai coût des ransomwares

Le paiement d'une rançon en elle-même n'a pas le plus grand effet financier sur une entreprise. Bien que le paiement ne soit pas insignifiant, il reste insignifiant comparé au coût des temps d'indisponibilité liés à un incident d'ransomware.

Le paiement d'une rançon n'est qu'un élément du coût de la récupération lorsqu'il s'agit de faire face à des attaques par ransomware. En excluant toute rançon payée, les entreprises ont déclaré en 2024 un coût moyen de restauration suite à une attaque par ransomware de 2,7 millions de dollars, soit une augmentation de près de 1 million de dollars par rapport aux 1,2 million de dollars rapportés en 2023 ["2024 Sophos State of ransomware"](#). Les coûts peuvent être 10 fois plus élevés pour les entreprises qui dépendent fortement de la disponibilité INFORMATIQUE, telles que l'e-commerce, les actions boursières et les soins de santé.

Les coûts de la cyberassurance continuent également d'augmenter, étant donné la très réelle probabilité d'une attaque par ransomware sur les entreprises assurées.

Protection contre les ransomware au niveau de la couche de données

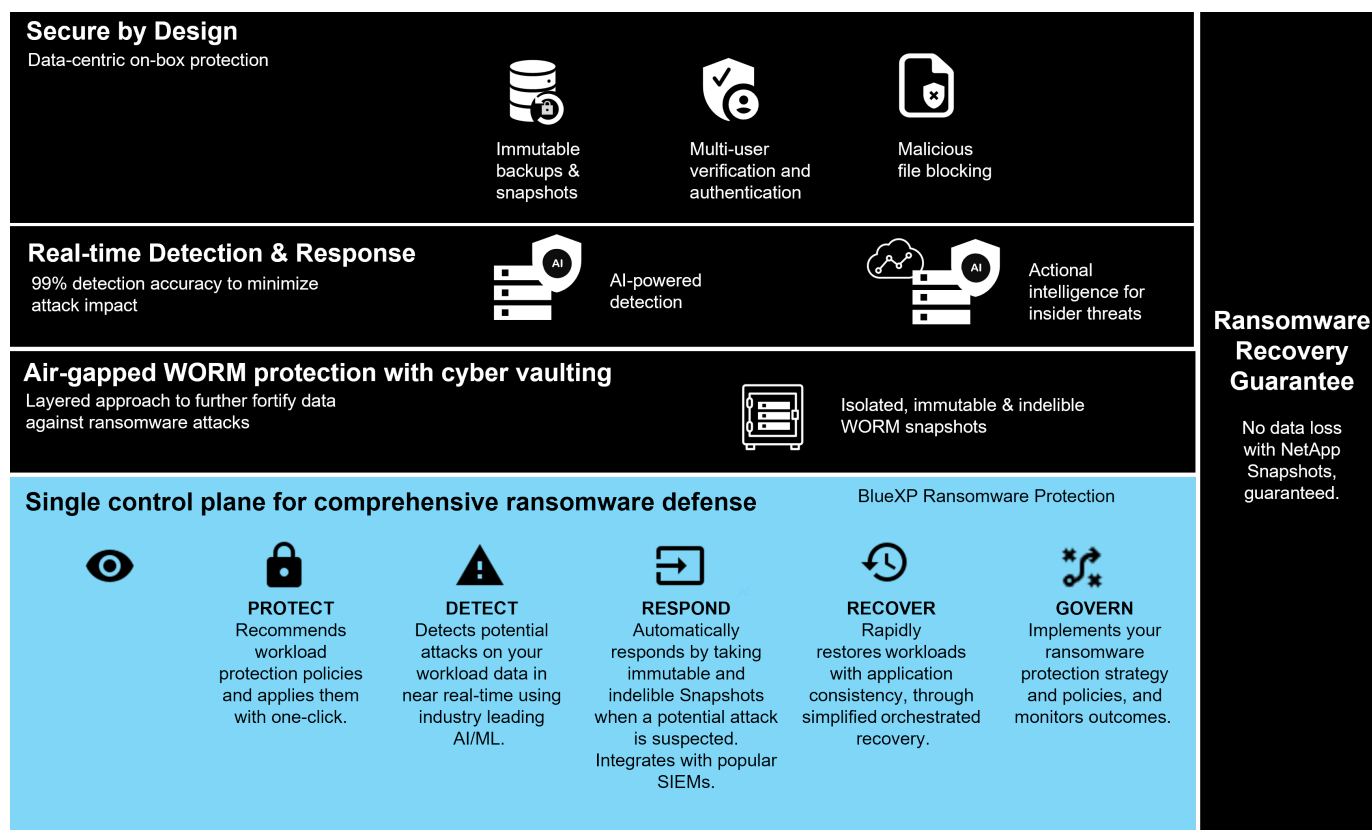
NetApp comprend que la sécurité de votre entreprise est vaste et approfondie dans tout le périmètre, jusqu'à l'emplacement des données au niveau de la couche de stockage. Votre pile de sécurité est complexe et doit assurer la sécurité à tous les niveaux de votre pile technologique.

La protection en temps réel au niveau de la couche de données est encore plus importante et a des exigences uniques. Pour être efficace, les solutions de cette couche doivent offrir les attributs critiques suivants :

- **Sécurité par conception** pour minimiser les risques d'attaque réussie
- **Détection et réponse en temps réel** pour minimiser l'impact d'une attaque réussie
- **Protection WORM à air Gap** pour isoler les sauvegardes de données critiques

- **Un seul plan de contrôle** pour une défense complète contre les ransomware

NetApp peut vous offrir tout cela et bien plus encore.



Le portefeuille de solutions NetApp pour la protection contre les ransomwares

NetApp "[protection intégrée contre les ransomware](#)" propose une défense à facettes et robuste en temps réel pour vos données stratégiques. Au cœur de ces outils, des algorithmes avancés de détection optimisés par l'IA surveillent en continu les modèles de données, ce qui permet d'identifier rapidement les menaces de ransomware avec une précision de 99 %. En réagissant rapidement aux attaques, notre stockage peut créer rapidement des snapshots de données et sécuriser les copies, assurant ainsi une restauration rapide.

Pour renforcer encore davantage les données, la "[cyber-archivage](#)" capacité de NetApp isole les données avec un air Gap logique. En protégeant les données stratégiques, nous assurons une continuité rapide de l'activité.

NetApp "[Protection BlueXP contre les ransomware](#)" réduit la charge opérationnelle à l'aide d'un plan de contrôle unique pour coordonner et exécuter intelligemment une défense anti-ransomware de bout en bout axée sur la charge de travail. Vous pouvez ainsi identifier et protéger les données de workloads stratégiques à risque d'un simple clic, détecter et répondre de manière précise et automatique pour limiter l'impact d'une attaque potentielle. Vous pouvez également restaurer vos workloads en quelques minutes au lieu de plusieurs jours, en protégeant vos données de workloads stratégiques et en minimisant les interruptions coûteuses.

En tant que solution ONTAP intégrée native pour protéger les accès non autorisés à vos données, "[Vérification multiadministrateur](#)" bénéficiez de fonctionnalités robustes qui assurent l'exécution des opérations telles que la suppression de volumes, la création d'utilisateurs administratifs ou la suppression de copies Snapshot uniquement après approbation d'un second administrateur désigné. Cela empêche les administrateurs compromis, malveillants ou peu expérimentés d'effectuer des modifications ou de supprimer des données indésirables. Vous pouvez configurer autant d'approbateurs administrateurs désignés que vous le souhaitez avant de supprimer une copie snapshot.



NetApp ONTAP répond à la condition requise pour "[Authentification multifacteur \(MFA\)](#)" l'authentification Web dans System Manager et l'authentification via l'interface de ligne de commandes SSH.

Avec la protection contre les ransomwares de NetApp, travaillez sereinement dans un environnement aux menaces qui ne cesse d'évoluer. Son approche globale ne se contente pas de vous défendre contre les variantes actuelles des ransomwares. Elle s'adapte également aux menaces émergentes, assurant ainsi la sécurité à long terme de votre infrastructure de données.

Découvrez les autres options de protection

- "[La protection contre les ransomware de Active IQ](#)"
- "[Sécurité des workloads de stockage Cloud Insights \(CISWS\)](#)"
- "[FPolicy](#)"
- "[SnapLock et copies Snapshot inviolables](#)"

Garantie de restauration contre les ransomwares

NetApp garantit la restauration des données Snapshot en cas d'attaque par ransomware. Notre garantie : si nous ne pouvons pas vous aider à restaurer vos données de snapshot, nous nous engageons à trouver la solution. La garantie est disponible pour tout achat de systèmes AFF A-Series, AFF C-Series, ASA et FAS.

En savoir plus >>

- "[Description du service de garantie de récupération](#)"
- "[Blog sur la garantie de restauration contre les ransomwares](#)".

Informations associées

- Page des ressources du site de support NetApp <http://mysupport.netapp.com/ontap/resources>
- Sécurité des produits NetApp <https://security.netapp.com/resources/>

SnapLock et copies Snapshot inviolables pour la protection contre les ransomwares

SnapLock, l'une des armes essentielles de l'arsenal de NetApp Snap, s'est avéré très efficace pour protéger les données contre les menaces de ransomware. En empêchant la suppression non autorisée des données, SnapLock fournit une couche de sécurité supplémentaire qui garantit l'intégrité et l'accessibilité des données critiques, même en cas d'attaques malveillantes.

Conformité SnapLock

SnapLock Compliance (SLC) assure une protection indélébile de vos données. SLC interdit la suppression de données même lorsqu'un administrateur tente de réinitialiser la baie. Contrairement à d'autres produits concurrents, SnapLock Compliance n'est pas vulnérable aux piratages d'ingénierie sociale par l'intermédiaire des équipes de support de ces produits. Les données protégées par des volumes SnapLock Compliance peuvent être récupérables jusqu'à leur date d'expiration.

Pour activer SnapLock, une "[ONTAP One](#)" licence est requise.

En savoir plus >>

- ["Documentation SnapLock"](#)

Copies Snapshot inviolables

Les copies Snapshot inviolables constituent un moyen pratique et rapide de protéger vos données contre les actes malveillants. Contrairement à SnapLock Compliance, TPS est généralement utilisé sur les systèmes principaux où l'utilisateur peut protéger les données pendant un temps déterminé et les laisser localement pour des restaurations rapides ou où les données n'ont pas besoin d'être répliquées hors du système principal. TPS utilise les technologies SnapLock pour empêcher la suppression de la copie Snapshot primaire, même par un administrateur ONTAP, pendant la même période d'expiration de la conservation SnapLock. La suppression de copie Snapshot est impossible même si le volume n'est pas activé sur SnapLock, bien que les snapshots ne possèdent pas la même nature indélébile que les volumes SnapLock Compliance.

Pour que les copies Snapshot soient inviolables, une ["ONTAP One"](#) licence est requise.

En savoir plus >>

- ["Verrouillez une copie Snapshot pour vous protéger contre les attaques par ransomware"](#).

Blocage des fichiers FPolicy

FPolicy empêche le stockage des fichiers indésirables sur votre appliance de stockage haute performance. FPolicy vous permet également de bloquer les extensions de fichiers ransomware connues. Un utilisateur dispose toujours des autorisations d'accès complètes au dossier de départ, mais FPolicy ne permet pas à un utilisateur de stocker les fichiers marqués par votre administrateur comme bloqués. Le cas échéant, il n'est pas important que ces fichiers soient des fichiers MP3 ou des extensions de fichiers ransomware connues.

Bloquez les fichiers malveillants avec le mode natif FPolicy

Le mode natif NetApp FPolicy (une évolution du nom, la stratégie de fichiers) est un framework de blocage d'extension de fichiers qui vous permet de bloquer les extensions de fichiers indésirables dans votre environnement. Fait partie de ONTAP depuis plus de dix ans, il est incroyablement utile pour vous protéger contre les ransomware. Ce moteur « zéro confiance » est très utile, car vous bénéficiez de mesures de sécurité supplémentaires qui vont au-delà des autorisations de liste de contrôle d'accès (ACL).

Dans le Gestionnaire système ONTAP et BlueXP, une liste de plus de 3000 extensions de fichier est disponible pour référence.



Certaines extensions peuvent être légitimes dans votre environnement et leur blocage peut entraîner des problèmes inattendus. Créez votre propre liste adaptée à votre environnement avant de configurer FPolicy natif.

Le mode natif FPolicy est inclus dans toutes les licences ONTAP.

En savoir plus >>

- ["Blog : lutter contre les ransomware : troisième partie : ONTAP FPolicy, un autre outil puissant et natif \(appelé gratuitement\)"](#)

Activez l'analyse du comportement des utilisateurs et des entités (UEBA) avec le mode externe FPolicy

Le mode externe FPolicy est un framework de notification et de contrôle de l'activité des fichiers qui offre une visibilité sur l'activité des fichiers et des utilisateurs. Ces notifications peuvent être utilisées par une solution externe pour effectuer des analyses basées sur l'IA afin de détecter les comportements malveillants.

Le mode externe FPolicy peut également être configuré pour attendre l'approbation du serveur FPolicy avant de permettre l'exécution d'activités spécifiques. Vous pouvez configurer plusieurs règles de ce type sur un cluster, ce qui vous apporte une grande flexibilité.



Les serveurs FPolicy doivent répondre aux requêtes FPolicy s'ils sont configurés pour être approuvés. Sinon, les performances du système de stockage risquent d'être affectées.

Le mode externe FPolicy est inclus dans ["Toutes les licences ONTAP"](#).

En savoir plus >>

- ["Blog : lutter contre les ransomware : quatrième partie — UBA et ONTAP avec le mode externe FPolicy."](#)

Sécurité des workloads de stockage Cloud Insights (CISWS)

La fonction Storage Workload Security (SWS) est une fonctionnalité de NetApp Cloud Insights qui améliore considérablement la sécurité, la capacité de restauration et la responsabilisation d'un environnement ONTAP. SWS adopte une approche axée sur l'utilisateur, en suivant l'activité de tous les fichiers de chaque utilisateur authentifié dans l'environnement. Il utilise des analyses avancées pour établir des modèles d'accès normaux et saisonniers pour chaque utilisateur. Ces modèles sont utilisés pour identifier rapidement les comportements suspects sans avoir besoin de signatures de ransomware.

Lorsque SWS détecte un ransomware, une suppression de données ou une attaque d'exfiltration, il peut prendre des mesures automatiques, telles que :

- Prenez un instantané du volume affecté.
- Bloquez le compte utilisateur et l'adresse IP suspectés d'activité malveillante.
- Envoyez une alerte aux administrateurs.

Comme il peut prendre des mesures automatisées pour arrêter rapidement une menace interne et suivre chaque activité de fichier, SWS simplifie et accélère la restauration suite à un événement de ransomware. Grâce aux outils avancés d'audit et d'analyse intégrés, les utilisateurs peuvent immédiatement voir quels volumes et fichiers ont été affectés par une attaque, quel compte d'utilisateur l'attaque a été et quelle action malveillante a été exécutée. Les snapshots automatiques atténuent les dommages et accélèrent la restauration des fichiers.

Total Attack Results

5	0	1,488
Affected Volumes	Deleted Files	Encrypted Files

1,488 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of Ransomware Attack.

The extension ".wanna" was added to each file.

Les alertes issues de la protection anti-ransomware autonome (ARP) de ONTAP sont également visibles dans SWS, fournissant une interface unique aux clients qui utilisent à la fois ARP et SWS pour se protéger contre les attaques par ransomware.

En savoir plus >>

- ["NetApp Cloud Insights"](#)

Détection et réponse basées sur l'IA intégrées à NetApp ONTAP

Comme les menaces de ransomware sont de plus en plus sophistiquées, vos mécanismes de défense aussi devraient-ils le faire. La protection anti-ransomware autonome (ARP) de NetApp est optimisée par l'IA avec la détection d'anomalies intelligente intégrée à ONTAP. Activez-la pour ajouter une couche de défense supplémentaire à votre cyberrésilience.

ARP et ARP/ai sont configurables via l'interface de gestion intégrée ONTAP, System Manager et activées par volume.

Protection autonome contre les ransomwares (ARP)

La protection anti-ransomware autonome (ARP), une autre solution ONTAP intégrée native depuis 9.10.1, examine l'activité des fichiers de workloads de volume de stockage NAS et l'entropie des données pour détecter automatiquement les ransomwares. ARP fournit aux administrateurs une détection en temps réel, des informations et un point de restauration des données pour une détection intégrée sans précédent des ransomwares.

Pour ONTAP 9.15.1 et les versions antérieures qui prennent en charge ARP, ARP démarre en mode d'apprentissage pour apprendre l'activité typique des données de charge de travail. Cela peut prendre sept jours pour la plupart des environnements. Une fois le mode d'apprentissage terminé, le protocole ARP passe automatiquement en mode actif et commence à rechercher les activités anormales des workloads qui pourraient être des ransomware.

En cas d'activité anormale, une copie Snapshot automatique est immédiatement effectuée, ce qui fournit un point de restauration aussi proche que possible du moment de l'attaque avec un minimum de données infectées. Simultanément, une alerte automatique (configurable) est générée et permet aux administrateurs de voir l'activité anormale des fichiers afin qu'ils puissent déterminer si l'activité est malveillante et prendre les mesures appropriées.

Si l'activité correspond à une charge de travail attendue, les administrateurs peuvent facilement la marquer comme un faux positif. ARP apprend ce changement comme une activité normale de la charge de travail et ne

le signale plus comme une attaque potentielle à l'avenir.

Pour activer ARP, une ["ONTAP One"](#) licence est requise.

En savoir plus >>

- ["Protection autonome contre les ransomwares"](#)

Protection anti-ransomware autonome/IA (ARP/ai)

Présenté en tant que préversion technologique d'ONTAP 9.15.1, ARP/ai va encore plus loin avec la détection en temps réel intégrée des systèmes de stockage NAS. La nouvelle technologie de détection optimisée par l'IA est entraînée sur plus d'un million de fichiers et diverses attaques par ransomware connues. En plus des signaux utilisés dans ARP, ARP/ai détecte également le chiffrement des en-têtes. La puissance ai et les signaux supplémentaires permettent à ARP/ai d'offrir une précision de détection supérieure à 99 %. Ce résultat a été validé par se Labs, un laboratoire de test indépendant qui a donné à ARP/ai son meilleur classement AAA.

L'entraînement des modèles étant effectué en continu dans le cloud, l'ARP/l'IA ne requiert pas de mode d'apprentissage. Elle est active dès sa mise sous tension. La formation continue implique également que l'ARP/l'IA est toujours validée contre les nouveaux types d'attaques par ransomware dès qu'ils surviennent. ARP/ai est également fourni avec des fonctionnalités de mise à jour automatique qui fournissent de nouveaux paramètres à tous les clients pour maintenir la détection des ransomware à jour. Toutes les autres fonctionnalités de détection, d'aperçu et de point de restauration des données d'ARP sont conservées pour ARP/ai.

Pour activer ARP/ai, une ["ONTAP One"](#) licence est requise.

En savoir plus >>

- ["Blog : la solution NetApp de détection des ransomwares en temps réel basée sur l'IA classe AAA"](#)

Protection WORM protégée par air avec archivage électronique

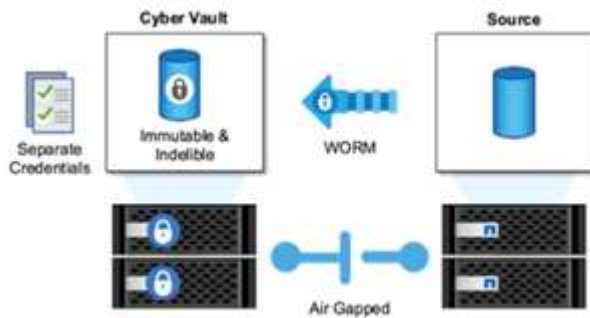
L'approche de NetApp en matière de cyber-coffre est une architecture de référence dédiée pour un cyber-coffre à air Gap logique. Cette approche tire parti des technologies de renforcement de la sécurité et de conformité, telles que SnapLock, pour permettre des snapshots immuables et indélébiles.

Cyber-archivage avec SnapLock Compliance et un air Gap logique

La tendance est de plus en plus marquée aux pirates informatiques qui détruisent les copies de sauvegarde et, dans certains cas, même les chiffrent. C'est pourquoi beaucoup dans le secteur de la cybersécurité recommandent d'utiliser des sauvegardes « air Gap » dans le cadre d'une stratégie globale de cyberrésilience.

Le problème, c'est que les lacunes traditionnelles (bandes et supports hors ligne) peuvent considérablement augmenter le temps de restauration, augmentant ainsi les temps d'indisponibilité et les coûts globaux associés. Même une approche plus moderne de la solution de l'air Gap peut s'avérer problématique. Par exemple, si le coffre-fort de sauvegarde est temporairement ouvert pour recevoir de nouvelles copies de sauvegarde, puis déconnecte et ferme sa connexion réseau aux données primaires pour être à nouveau « à air Gap », un attaquant pourrait tirer parti de l'ouverture temporaire. Au cours de la connexion, un attaquant pourrait frapper pour compromettre ou détruire les données. Ce type de configuration ajoute également généralement une complexité indésirable. L'air Gap logique est un excellent substitut à un air Gap traditionnel ou moderne car il possède les mêmes principes de protection de sécurité tout en conservant la sauvegarde en ligne. Avec NetApp, simplifiez la gestion des bandes et des disques grâce aux air Gap logiques, que vous

pouvez obtenir avec des copies Snapshot immuables et NetApp SnapLock Compliance.



NetApp a publié la fonctionnalité SnapLock il y a plus de 10 ans pour répondre aux exigences de conformité des données, telles que la loi HIPAA (Health Insurance Portability and Accountability Act), la loi Sarbanes-Oxley et d'autres règles relatives aux données réglementaires. Vous pouvez également archiver ces copies snapshot primaires dans des volumes SnapLock de façon à ce qu'elles puissent être validées sur WORM, ce qui empêche leur suppression. Il existe deux versions de licence SnapLock : SnapLock Compliance et SnapLock Enterprise. Pour une protection contre les ransomwares, NetApp recommande SnapLock Compliance, car vous pouvez définir une période de conservation spécifique pendant laquelle les copies Snapshot sont verrouillées et ne peuvent pas être supprimées, même par les administrateurs ONTAP ou le support NetApp.

En savoir plus >>

- ["Blog : protection multicouche contre les ransomware avec la solution Cyber Vault de NetApp"](#)

Copies Snapshot inviolables

En utilisant SnapLock Compliance comme air Gap logique, vous bénéficiez d'une protection ultime pour empêcher les pirates de supprimer vos copies de sauvegarde, mais vous devez déplacer les copies Snapshot à l'aide de SnapVault vers un volume SnapLock secondaire. Par conséquent, de nombreux clients déploient cette configuration sur un système de stockage secondaire sur le réseau. Cela peut entraîner des temps de restauration plus longs qu'avec la restauration d'une copie Snapshot d'un volume primaire sur un système de stockage primaire.

À partir de la version ONTAP 9.12.1, les copies Snapshot inviolables assurent une protection proche du niveau SnapLock Compliance de vos copies Snapshot sur le stockage primaire et dans les volumes primaires. Il n'est pas nécessaire d'archiver la copie Snapshot à l'aide de SnapVault sur un volume secondaire SnapLocaché. Les copies Snapshot inviolables utilisent la technologie SnapLock pour empêcher la suppression de la copie Snapshot primaire, même si un administrateur ONTAP complet utilise la même période d'expiration de conservation SnapLock. Cela permet d'accélérer les délais de restauration et de sauvegarder un volume FlexClone à l'aide d'une copie Snapshot protégée et inviolable, ce que vous ne pouvez pas faire avec une copie Snapshot classique dans un stockage SnapLock Compliance.

La principale différence entre les copies SnapLock Compliance et les copies Snapshot inviolables est que SnapLock Compliance n'autorise pas l'initialisation et la suppression de la baie ONTAP si des volumes SnapLock Compliance existent avec des copies Snapshot archivées qui n'ont pas encore atteint leur date d'expiration. Pour que les copies Snapshot soient inviolables, vous devez disposer d'une licence SnapLock Compliance.

En savoir plus >>

- ["Verrouillez une copie Snapshot pour vous protéger contre les attaques par ransomware"](#)

La protection contre les ransomware de Active IQ

NetApp Active IQ est un conseiller digital qui simplifie le support proactif et l'optimisation du stockage NetApp grâce à des informations exploitables et une gestion des données optimale. Alimenté par les données de télémétrie de notre base installée diversifiée, il emploie des techniques avancées d'intelligence artificielle et de MACHINE LEARNING pour découvrir les opportunités de réduction des risques et d'amélioration des performances et de l'efficacité de votre environnement de stockage.

Non seulement peut "[NetApp Active IQ](#)" vous y aider "[éliminez les failles de sécurité](#)", mais il fournit également des informations et des recommandations spécifiques pour vous protéger contre les ransomwares. Une carte d'intégrité dédiée présente les actions nécessaires et les risques résolus. Vous êtes ainsi sûr que vos systèmes respectent ces recommandations en matière de bonnes pratiques.



Les risques et les actions suivis sur la page ransomware Defense Wellness incluent notamment les éléments suivants :

- Le nombre de copies Snapshot des volumes est faible, ce qui réduit la protection potentielle contre les ransomware.
- FPolicy n'est pas activé pour toutes les machines virtuelles de stockage (SVM) configurées pour les protocoles NAS.

Pour voir la protection contre les ransomware de Active IQ en action, consultez "[NetApp Active IQ](#)".

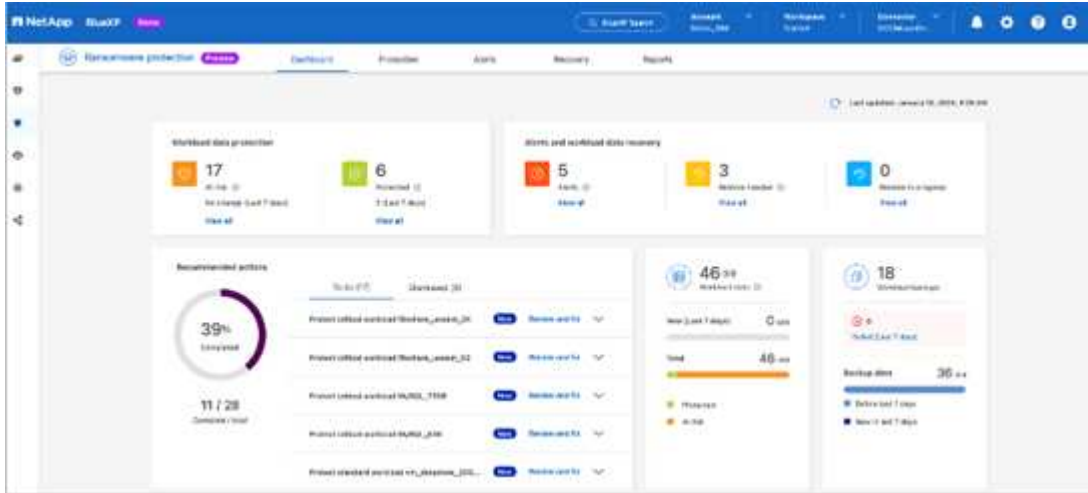
Résilience complète avec la protection BlueXP contre les ransomware

Il est important que la détection des ransomwares se produise le plus tôt possible afin d'éviter la propagation des ransomwares et d'éviter des interruptions coûteuses. Toutefois, une stratégie efficace de détection des ransomwares doit inclure plusieurs couches de protection. La protection contre les ransomware de NetApp repose sur une approche complète qui inclut des capacités en temps réel intégrées s'étendant aux services de données via BlueXP et une solution isolée en couches pour la cybercopie.

Protection BlueXP contre les ransomware

BlueXP est un plan de contrôle unique pour orchestrer intelligemment une défense anti-ransomware complète et axée sur les workloads. La protection contre les ransomwares BlueXP réunit les puissantes fonctionnalités de cyberrésilience d'ONTAP, telles que ARP, FPolicy, les copies Snapshot inviolables et les services de données BlueXP, tels que la sauvegarde et la restauration BlueXP. Elle propose également des

recommandations et des conseils avec des workflows automatisés pour fournir une défense de bout en bout via une seule interface utilisateur. Il fonctionne au niveau des workloads pour s'assurer que les applications sur lesquelles s'exécute votre entreprise sont protégées et peuvent être restaurées aussi rapidement que possible en cas d'attaque.



Avantages pour le client :

- La préparation assistée par ransomware réduit la surcharge opérationnelle et améliore l'efficacité
- La détection d'anomalies optimisée par l'IA et le ML améliore la précision et accélère la réponse pour maîtriser les risques
- La restauration guidée cohérente au niveau des applications vous permet de restaurer les workloads plus facilement et en quelques minutes

"Protection BlueXP contre les ransomware" Facilite la réalisation de ces fonctions NIST :

- Automatiquement **découvrir** et hiérarchiser les données dans le stockage NetApp **en mettant l'accent sur les principales charges de travail basées sur les applications.**
- **Protection en un clic** de la sauvegarde des données de la charge de travail la plus importante, immuable, configuration sécurisée, blocage des fichiers malveillants et domaine de sécurité différent.
- **Détectez avec précision** les ransomware au plus vite * en utilisant **la détection d'anomalies basée sur l'IA nouvelle génération.**
- Réponse automatisée et flux de travail et intégration avec les meilleures solutions * SIEM et XDR.*
- Restaurer rapidement les données à l'aide d'une récupération * orchestrée simplifiée* pour accélérer la continuité des applications.
- Mettez en œuvre votre **stratégie** et **politiques** de protection contre les ransomware et **surveillez les résultats.**

Protection autonome contre les ransomwares

Présentation de la protection autonome contre les ransomwares

Depuis ONTAP 9.10.1, la fonctionnalité ARP (autonome ransomware protection) utilise l'analyse des workloads dans les environnements NAS (NFS et SMB) pour détecter et avertir de manière proactive les activités anormales qui pourraient indiquer une attaque par ransomware.

Lorsqu'une attaque est suspectée, ARP crée également de nouvelles copies Snapshot, en plus de la protection existante à partir de copies Snapshot planifiées.

Licences et activation

ARP requiert une licence. ARP est disponible avec le ["Licence ONTAP ONE"](#). Si vous ne disposez pas de la licence ONTAP One, d'autres licences sont disponibles pour utiliser ARP, qui varient selon votre version de ONTAP.

Versions d'ONTAP	Licence
ONTAP 9.11.1 et versions ultérieures	Protection contre les ransomwares
ONTAP 9.10.1	MT_EK_MGMT (gestion des clés mutualisée)

- Si vous effectuez une mise à niveau vers ONTAP 9.11.1 ou version ultérieure et que ARP est déjà configuré sur votre système, vous n'avez pas besoin d'acheter la nouvelle licence anti-ransomware. Pour les nouvelles configurations ARP, la nouvelle licence est requise.
- Si vous effectuez une restauration depuis ONTAP 9.11.1 ou une version ultérieure vers ONTAP 9.10.1 et que vous avez activé ARP avec la licence anti-ransomware, un message d'avertissement s'affiche et vous devrez peut-être reconfigurer ARP. ["Découvrez le rétablissement ARP"](#).

Vous pouvez configurer le protocole ARP par volume à l'aide de System Manager ou de l'interface de ligne de commandes de ONTAP.

Stratégie ONTAP de protection contre les ransomwares

Une stratégie efficace de détection des ransomwares doit inclure plus d'une couche de protection unique

On pourrait comparer les caractéristiques de sécurité d'un véhicule. Vous ne vous fiez pas à une seule fonction, telle qu'une ceinture de sécurité, pour vous protéger complètement en cas d'accident. Les sacs gonflables, les freins antiblocage et l'avertissement de collision avant sont tous des dispositifs de sécurité supplémentaires qui permettront d'obtenir un meilleur résultat. La protection contre les ransomwares doit être vue de la même manière.

Tandis que ONTAP inclut des fonctionnalités comme FPolicy, les copies Snapshot, SnapLock et Active IQ Digital Advisor pour vous protéger contre les attaques par ransomware, les informations suivantes se concentrent sur la fonctionnalité intégrée ARP avec des fonctionnalités de machine learning.

Pour en savoir plus sur les autres fonctionnalités de ONTAP contre les ransomware, consultez ["Ransomware et le portefeuille de solutions de protection de NetApp"](#).

Ce que le protocole ARP détecte

Le protocole ARP est conçu pour vous protéger contre les attaques par déni de service où l'attaquant conserve ses données jusqu'au paiement d'une rançon. ARP propose une détection en temps réel des ransomware basée sur :

- Identification des données entrantes comme cryptées ou en texte clair.
- Les analyses, qui détectent
 - **Entropy**: Une évaluation du caractère aléatoire des données dans un fichier

- **Types d'extension de fichier** : extension non conforme au type d'extension normal
- **File IOPS** : une augmentation de l'activité de volume anormale avec le chiffrement des données (à partir de ONTAP 9.11.1)

ARP peut détecter la propagation de la plupart des attaques par ransomware après le chiffrement d'un petit nombre de fichiers uniquement, l'action automatique pour protéger les données et vous avertir qu'une attaque suspectée a lieu.



Aucun système de détection ou de prévention par ransomware ne peut garantir la sécurité en cas d'attaque par ransomware. Bien qu'il soit possible qu'une attaque ne soit pas détectée, ARP agit comme une couche supplémentaire importante de défense si un logiciel antivirus ne parvient pas à détecter une intrusion.

Modes d'apprentissage et actifs

ARP a deux modes :

- **Apprentissage** (ou mode de fonctionnement à sec)
- **Actif** (ou mode « activé »)

Lorsque vous activez ARP, il s'exécute en *mode d'apprentissage*. En mode apprentissage, le système ONTAP développe un profil d'alerte basé sur les zones analytiques : entropie, types d'extension de fichier et IOPS de fichier. Après avoir exécuté ARP en mode d'apprentissage pendant suffisamment de temps pour évaluer les caractéristiques de la charge de travail, vous pouvez passer en mode actif et commencer à protéger vos données. Une fois que le protocole ARP est passé en mode actif, ONTAP crée des copies Snapshot ARP pour protéger les données en cas de détection d'une menace.

Il est recommandé de laisser ARP en mode d'apprentissage pendant 30 jours. À partir de ONTAP 9.13.1, ARP détermine automatiquement la période d'apprentissage optimale et automatise le commutateur, qui peut se produire avant 30 jours.

En mode actif, si une extension de fichier est marquée comme anormale, vous devez évaluer l'alerte. Vous pouvez agir sur l'alerte pour protéger vos données ou marquer l'alerte comme un faux positif. Le fait de marquer une alerte comme un faux positif met à jour le profil d'alerte. Par exemple, si l'alerte est déclenchée par une nouvelle extension de fichier et que vous marquez l'alerte comme un faux positif, vous ne recevrez pas d'alerte la prochaine fois que l'extension de fichier sera observée. La commande `security anti-ransomware volume workload-behavior show` affiche les extensions de fichier qui ont été détectées dans le volume. (Si vous exécutez cette commande très tôt en mode d'apprentissage et qu'elle affiche une représentation précise des types de fichiers, vous ne devez pas utiliser ces données comme base pour passer en mode actif, car ONTAP collecte toujours d'autres metrics.)

À partir de ONTAP 9.11.1, vous pouvez personnaliser les paramètres de détection pour ARP. Pour plus d'informations, voir [Gérer les paramètres de détection d'attaque ARP](#).

Évaluation des menaces et copies Snapshot ARP

En mode actif, ARP évalue la probabilité de menace en fonction des données entrantes mesurées par rapport aux analyses apprises. Une mesure est attribuée lorsque ARP détecte une menace :

- **Faible** : la première détection d'une anomalie dans le volume (par exemple, une nouvelle extension de fichier est observée dans le volume).
- **Modéré** : Plusieurs fichiers avec la même extension de fichier jamais vu-avant sont observés.

- Dans ONTAP 9.10.1, le seuil de remontée à modéré est de 100 fichiers ou plus. À partir de ONTAP 9.11.1, la quantité du fichier peut être modifiée ; sa valeur par défaut est 20.

En cas de menace faible, ONTAP détecte une anomalie et crée une copie Snapshot du volume pour créer le meilleur point de restauration. ONTAP ajoute au nom de la copie snapshot ARP le préfixe `Anti-ransomware-backup` pour le rendre facilement identifiable, par exemple `Anti_ransomware_backup.2022-12-20_1248`.

La menace passe au niveau modéré après l'exécution d'un rapport d'analytique par ONTAP qui détermine si l'anomalie correspond à un profil de ransomware. Les menaces qui restent au niveau bas sont consignées et visibles dans la section **événements** de System Manager. Lorsque la probabilité d'attaque est modérée, ONTAP génère une notification EMS vous invitant à évaluer la menace. ONTAP n'envoie pas d'alertes en cas de menaces faibles, mais à partir de ONTAP 9.14.1, vous pouvez le faire [modifier les paramètres des alertes](#). Pour plus d'informations, voir [Réagir à une activité anormale](#).

Vous pouvez afficher des informations sur une menace, quel que soit le niveau, dans la section **événements** de System Manager ou avec le `security anti-ransomware volume show` commande.

Les copies Snapshot ARP sont conservées pendant au moins deux jours. À partir de ONTAP 9.11.1, vous pouvez modifier les paramètres de rétention. Pour plus d'informations, voir [Modifiez les options des copies Snapshot](#).

Comment récupérer des données dans ONTAP après une attaque par ransomware

Lorsqu'une attaque est suspectée, le système prend une copie Snapshot du volume à ce moment-là et verrouille cette copie. Si l'attaque est confirmée ultérieurement, le volume peut être restauré à l'aide de la copie ARP Snapshot.

La suppression des copies Snapshot verrouillées ne peut pas être effectuée par des moyens normaux. Cependant, si vous décidez plus tard de marquer l'attaque comme un faux positif, la copie verrouillée sera supprimée.

En connaissant les fichiers affectés et l'heure de l'attaque, il est possible de restaurer de manière sélective les fichiers affectés à partir de plusieurs copies Snapshot, plutôt que de simplement restaurer le volume entier vers l'une des copies Snapshot.

ARP s'appuie donc sur la technologie de protection des données et de reprise après incident ONTAP éprouvée pour répondre aux attaques par ransomware. Pour plus d'informations sur la récupération de données, reportez-vous aux rubriques suivantes.

- ["Restauration à partir de copies Snapshot \(System Manager\)"](#)
- ["Restauration de fichiers à partir de copies Snapshot \(interface de ligne de commandes\)"](#)
- ["Restauration intelligente par ransomware"](#)

Cas d'utilisation et considérations relatives à la protection autonome contre les ransomwares

La protection anti-ransomware autonome (ARP) est disponible pour les charges de travail NAS à partir de ONTAP 9.10.1. Avant de déployer ARP, vous devez connaître les utilisations recommandées et les configurations prises en charge, ainsi que les implications en termes de performances.

Configurations prises en charge et non prises en charge

Lorsque vous décidez d'utiliser ARP, il est important de vous assurer que la charge de travail de votre volume est adaptée à ARP et qu'elle répond aux configurations système requises.

Charges de travail adaptées

ARP est adapté pour :

- Les bases de données sur le stockage NFS
- Répertoires locaux Windows ou Linux

Comme les utilisateurs pouvaient créer des fichiers avec des extensions qui n'ont pas été détectées pendant la période d'apprentissage, les risques de faux positifs sont plus élevés dans cette charge de travail.

- Images et vidéos

Par exemple, les dossiers médicaux et les données EDA

Charges de travail non adaptées

ARP n'est pas adapté pour :

- Les workloads comportant une fréquence élevée de création ou de suppression de fichiers (des centaines de milliers de fichiers en quelques secondes, par exemple des workloads de test/développement).
- La détection des menaces par ARP dépend de sa capacité à reconnaître une augmentation inhabituelle de l'activité de création, de renommage ou de suppression de fichiers. Si l'application elle-même est la source de l'activité des fichiers, elle ne peut pas être efficacement distinguée de l'activité des ransomware.
- Charges de travail où l'application ou l'hôte chiffre les données.
ARP dépend de la distinction des données entrantes comme chiffrées ou non chiffrées. Si l'application elle-même est en train de chiffrer les données, l'efficacité de la fonction est réduite. Toutefois, la fonction peut toujours fonctionner en fonction de l'activité du fichier (supprimer, écraser ou créer, ou créer ou renommer avec une nouvelle extension de fichier) et du type de fichier.

Configurations compatibles

ARP est disponible pour les volumes NFS et SMB dans les systèmes ONTAP sur site à partir de ONTAP 9.10.1.

La prise en charge d'autres configurations et types de volumes est disponible dans les versions ONTAP suivantes :

	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Volumes protégés avec réplication asynchrone SnapMirror	✓	✓	✓	✓		

	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
SVM protégé avec réplication asynchrone SnapMirror (reprise d'activité SVM)	✓	✓	✓	✓		
Mobilité des données des SVM (vserver migrate)	✓	✓	✓	✓		
Volumes FlexGroup	✓	✓	✓			
Vérification multi-administrateurs	✓	✓	✓			

Interopérabilité SnapMirror et ARP

Depuis ONTAP 9.12.1, ARP est pris en charge sur les volumes de destination asynchrones SnapMirror. ARP est **non** pris en charge avec SnapMirror Synchronous.

Si un volume source SnapMirror est compatible ARP, le volume de destination SnapMirror acquiert automatiquement l'état de configuration ARP (apprentissage, activation, etc.), les données d'entraînement ARP et le snapshot créé par ARP du volume source. Aucune activation explicite n'est requise.

Alors que le volume de destination se compose de copies Snapshot RO (lecture seule), aucun traitement ARP n'est effectué sur ses données. Toutefois, lorsque le volume de destination SnapMirror est converti en lecture-écriture (RW), ARP est automatiquement activé sur le volume de destination converti en RW. Le volume de destination ne nécessite pas de procédure d'apprentissage supplémentaire en plus de ce qui est déjà enregistré sur le volume source.

Dans ONTAP 9.10.1 et 9.11.1, SnapMirror ne transfère pas l'état de configuration ARP, les données d'entraînement et les copies Snapshot des volumes source vers les volumes de destination. Ainsi, lorsque le volume de destination SnapMirror est converti en RW, ARP sur le volume de destination doit être explicitement activé en mode apprentissage une fois la conversion terminée.

ARP et machines virtuelles

ARP est pris en charge avec les machines virtuelles (VM). La détection ARP se comporte différemment pour les modifications à l'intérieur et à l'extérieur de la machine virtuelle. ARP n'est pas recommandé pour les workloads avec des fichiers fortement entropie dans la machine virtuelle.

Modifications en dehors de la VM

ARP peut détecter les modifications d'extension de fichier sur un volume NFS en dehors de la machine virtuelle si une nouvelle extension entre dans le volume chiffré ou si une extension de fichier change. Les modifications d'extension de fichier détectables sont les suivantes :

- .vmx
- .vmxf
- .vmdk
- -flat.vmdk
- nvram
- .vmem
- .vmsd
- .vmsn
- .vswp
- .vmss
- .log
- -\#.log

Modifications au sein de la machine virtuelle

Si l'attaque par ransomware cible la machine virtuelle et les fichiers à l'intérieur de la machine virtuelle sont modifiés sans effectuer de modifications à l'extérieur de la machine virtuelle, ARP détecte la menace si l'entropie par défaut de la machine virtuelle est faible (par exemple, fichiers .txt, .docx ou .mp4). Bien que ARP crée un instantané de protection dans ce scénario, il ne génère pas d'alerte de menace car les extensions de fichiers en dehors de la machine virtuelle n'ont pas été falsifiées.

Si, par défaut, les fichiers sont à haute entropie (par exemple, les fichiers .gzip ou protégés par mot de passe), les capacités de détection d'ARP sont limitées. ARP peut toujours prendre des snapshots proactifs dans ce cas ; cependant, aucune alerte ne sera déclenchée si les extensions de fichier n'ont pas été falsifiées en externe.

Configurations non prises en charge

ARP n'est pas pris en charge dans les configurations système suivantes :

- Les environnements ONTAP S3
- Environnements SAN

ARP ne prend pas en charge les configurations de volume suivantes :

- Volumes FlexGroup (dans ONTAP 9.10.1 à 9.12.1. À partir de ONTAP 9.13.1, les volumes FlexGroup sont pris en charge)
- Volumes FlexCache (ARP est pris en charge sur les volumes FlexVol d'origine, mais pas sur les volumes de cache)
- Les volumes hors ligne
- Volumes SAN uniquement
- Volumes SnapLock
- SnapMirror synchrone
- SnapMirror asynchrone (non pris en charge uniquement dans ONTAP 9.10.1 et 9.11.1. La réplication asynchrone SnapMirror est prise en charge à partir de ONTAP 9.12.1. Pour plus d'informations, voir [\[snapmirror\].](#))

- Volumes restreints
- Volumes root des VM de stockage
- Volumes des machines virtuelles de stockage arrêtées

Considérations relatives aux performances ARP et à la fréquence

Le protocole ARP peut avoir un impact minimal sur les performances du système, mesuré en débit et en pic d'IOPS. L'impact de la fonctionnalité ARP dépend des charges de travail de volume spécifiques. Pour les charges de travail courantes, les limites de configuration suivantes sont recommandées :

Caractéristiques de la charge de travail	Limite de volume recommandée par nœud	Dégradation des performances lorsque la limite de volume par nœud est dépassée :[*]
Ces données intensives en lecture ou compressées peuvent être compressées.	150	4 % des IOPS maximales
Des opérations d'écriture intensives et des données ne peuvent pas être compressées.	60	10 % des IOPS maximales

Pass:[*] les performances du système ne sont pas dégradées au-delà de ces pourcentages, quel que soit le nombre de volumes ajoutés au-delà des limites recommandées.

L'analyse ARP étant exécutée selon une séquence prioritaire, à mesure que le nombre de volumes protégés augmente, l'analyse s'exécute moins souvent sur chaque volume.

Vérification multiadministrateur avec volumes protégés par ARP

À partir de ONTAP 9.13.1, vous pouvez activer la vérification multiadministrateur (MAV) pour une sécurité supplémentaire avec ARP. MAV s'assure qu'au moins deux administrateurs authentifiés sont requis pour désactiver ARP, mettre en pause ARP ou marquer une attaque suspecte comme faux positif sur un volume protégé. Découvrez comment ["Activez MAV pour les volumes protégés par ARP"](#).

Vous devez définir des administrateurs pour un groupe MAV et créer des règles MAV pour le `security anti-ransomware volume disable`, `security anti-ransomware volume pause`, et `security anti-ransomware volume attack clear-suspect` Commandes ARP à protéger. Chaque administrateur du groupe MAV doit approuver chaque nouvelle demande de règle et ["Ajoutez à nouveau la règle MAV"](#) Dans les paramètres MAV.

Depuis ONTAP 9.14.1, ARP propose des alertes pour la création d'un instantané ARP et pour l'observation d'une nouvelle extension de fichier. Les alertes pour ces événements sont désactivées par défaut. Les alertes peuvent être définies au niveau du volume ou des SVM. Vous pouvez créer des règles MAV au niveau du SVM à l'aide de `security anti-ransomware vserver event-log modify` ou au niveau du volume avec `security anti-ransomware volume event-log modify`.

Étapes suivantes

- ["Activation de la protection autonome contre les ransomwares"](#)
- ["Activez MAV pour les volumes protégés par ARP"](#)

Activation de la protection autonome contre les ransomwares

Depuis ONTAP 9.10.1, la protection autonome contre les ransomwares (ARP) peut être activée sur les volumes nouveaux ou existants. Vous commencez par activer ARP en mode d'apprentissage, dans lequel le système analyse la charge de travail pour caractériser le comportement normal. Vous pouvez activer ARP sur un volume existant ou créer un nouveau volume et activer ARP depuis le début.

Description de la tâche

Vous devez toujours activer le protocole ARP au départ en mode d'apprentissage (ou d'exécution à sec). Le démarrage en mode actif peut entraîner des rapports faux positifs excessifs.

Il est recommandé de laisser ARP fonctionner en mode d'apprentissage pendant au moins 30 jours. À partir de ONTAP 9.13.1, ARP détermine automatiquement la période d'apprentissage optimale et automatise le commutateur, qui peut se produire avant 30 jours. Pour plus d'informations, voir "[Modes d'apprentissage et actifs](#)".



Dans les volumes existants, les modes d'apprentissage et actif s'appliquent uniquement aux données nouvellement écrites, et non aux données existantes du volume. Les données existantes ne sont pas analysées et analysées, car les caractéristiques du trafic de données normal antérieur sont présumées basées sur les nouvelles données une fois que le volume est activé pour ARP.

Avant de commencer

- Une VM de stockage (SVM) doit être activée pour NFS ou SMB (ou les deux).
- Le [licence correcte](#) Doit être installé pour votre version ONTAP.
- Vous devez avoir une charge de travail NAS avec des clients configurés.
- Le volume sur lequel vous souhaitez définir ARP doit être protégé et doit avoir un actif "[chemin de jonction](#)".
- Le volume doit être rempli à moins de 100 %.
- Il est recommandé de configurer le système EMS pour envoyer des notifications par e-mail, qui incluront des notifications d'activité ARP. Pour plus d'informations, voir "[Configurez les événements EMS pour envoyer des notifications par e-mail](#)".
- À partir de la version ONTAP 9.13.1, il est recommandé d'activer la vérification multiadministrateur afin que deux administrateurs d'utilisateurs authentifiés ou plus soient requis pour la configuration ARP (Autonomous ransomware protection). Pour plus d'informations, voir "[Activez la vérification multiadministrateur](#)".

Activez ARP

Vous pouvez activer le protocole ARP à l'aide de System Manager ou de l'interface de ligne de commande ONTAP.

System Manager

Étapes

1. Sélectionnez **stockage > volumes**, puis sélectionnez le volume à protéger.
2. Dans l'onglet **sécurité** de la vue d'ensemble **volumes**, sélectionnez **État** pour passer de Désactivé à activé en mode apprentissage dans la zone **anti-ransomware**.
3. Lorsque la période d'apprentissage est terminée, passez ARP en mode actif.



À partir de ONTAP 9.13.1, ARP détermine automatiquement la période d'apprentissage optimale et automatise le commutateur. C'est possible "[Désactivez ce paramètre sur la machine virtuelle de stockage associée](#)" si vous souhaitez contrôler manuellement le mode d'apprentissage en mode actif.

- a. Sélectionnez **stockage > volumes**, puis sélectionnez le volume prêt pour le mode actif.
 - b. Dans l'onglet **sécurité** de la vue d'ensemble **volumes**, sélectionnez **basculer** en mode actif dans la zone anti-ransomware.
4. Vous pouvez vérifier l'état ARP du volume dans la zone **anti-ransomware**.

Pour afficher l'état ARP de tous les volumes : dans le volet **volumes**, sélectionnez **Afficher/Masquer**, puis assurez-vous que l'état **anti-ransomware** est vérifié.

CLI

Le processus d'activation de ARP avec l'interface de ligne de commande diffère si vous l'activez sur un volume existant par rapport à un nouveau volume.

Activez ARP sur un volume existant

1. Modifiez un volume existant pour activer la protection par ransomware en mode d'apprentissage :

```
security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
```

Si vous utilisez ONTAP 9.13.1 ou une version ultérieure, l'apprentissage adaptatif est activé de sorte que le changement d'état actif soit effectué automatiquement. Si vous ne souhaitez pas que ce comportement soit automatiquement activé, modifier le paramètre au niveau du SVM sur tous les volumes associés :

```
vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to-enabled false
```

2. Lorsque la période d'apprentissage est terminée, modifiez le volume protégé pour passer en mode actif si ce n'est pas déjà fait automatiquement :

```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

Vous pouvez également passer en mode actif à l'aide de la commande modifier le volume :

```
volume modify -volume vol_name -vserver svm_name -anti-ransomware-state active
```

3. Vérifiez l'état ARP du volume.

```
security anti-ransomware volume show
```

Activez ARP sur un nouveau volume

1. Créez un volume avec la protection anti-ransomware activée avant le provisionnement des données.

```
volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size nn -anti-ransomware-state dry-run -junction-path /path_name
```

Si vous utilisez ONTAP 9.13.1 ou une version ultérieure, l'apprentissage adaptatif est activé de sorte que le changement d'état actif soit effectué automatiquement. Si vous ne souhaitez pas que ce comportement soit automatiquement activé, modifier le paramètre au niveau du SVM sur tous les volumes associés :

```
vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to-enabled false
```

2. Lorsque la période d'apprentissage est terminée, modifiez le volume protégé pour passer en mode actif si ce n'est pas déjà fait automatiquement :

```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

Vous pouvez également passer en mode actif à l'aide de la commande modifier le volume :

```
volume modify -volume vol_name -vserver svm_name -anti-ransomware-state active
```

3. Vérifiez l'état ARP du volume.

```
security anti-ransomware volume show
```

Activez la protection autonome par défaut contre les ransomwares dans les nouveaux volumes

Depuis ONTAP 9.10.1, vous pouvez configurer des machines virtuelles de stockage (SVM) de manière à ce que les nouveaux volumes soient activés par défaut pour le mode d'apprentissage ARP (autonome ransomware protection).

Description de la tâche

Par défaut, de nouveaux volumes sont créés avec ARP en mode désactivé. Vous pouvez modifier ce paramètre dans System Manager et via l'interface de ligne de commandes. Les volumes activés par défaut sont définis sur ARP en mode d'apprentissage (ou d'exécution à sec).

ARP ne sera activé que sur les volumes créés dans le SVM après avoir modifié le paramètre. ARP ne sera pas activé sur les volumes existants. Découvrez comment ["Activez ARP dans un volume existant"](#).

À partir de ONTAP 9.13.1, l'apprentissage adaptatif a été ajouté à l'analyse ARP et le passage du mode d'apprentissage au mode actif s'effectue automatiquement. Pour plus d'informations, voir ["Modes d'apprentissage et actifs"](#).

Avant de commencer

- Le [licence correcte](#) Doit être installé pour votre version ONTAP.
- Le volume doit être rempli à moins de 100 %.

- Les chemins de jonction doivent être actifs.
- À partir de la version ONTAP 9.13.1, il est recommandé d'activer la vérification multiadministrateur afin que deux administrateurs d'utilisateurs authentifiés minimum soient requis pour les opérations anti-ransomware. ["En savoir plus >>"](#).

Basculez ARP du mode d'apprentissage au mode actif

À partir de la ONTAP 9.13.1, l'apprentissage adaptatif a été ajouté à l'analyse ARP. Le passage du mode d'apprentissage au mode actif s'effectue automatiquement. La décision autonome prise par ARP de passer automatiquement du mode d'apprentissage au mode actif est basée sur les paramètres de configuration des options suivantes :

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent  
-anti-ransomware-auto-switch-duration-without-new-file-extension  
-anti-ransomware-auto-switch-minimum-learning-period  
-anti-ransomware-auto-switch-minimum-file-count  
-anti-ransomware-auto-switch-minimum-file-extension
```


Après 30 jours d'apprentissage, un volume passe automatiquement en mode actif même si une ou plusieurs de ces conditions ne sont pas satisfaites. Autrement dit, si le commutateur automatique est activé, le volume passe en mode actif au bout de 30 jours maximum. La valeur maximale de 30 jours est fixe et non modifiable.

Pour plus d'informations sur les options de configuration ARP, y compris les valeurs par défaut, reportez-vous au ["Référence de commande ONTAP"](#).

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour activer le protocole ARP par défaut.

System Manager

1. Sélectionnez **Storage > Storage VM**, puis sélectionnez la VM de stockage contenant les volumes que vous souhaitez protéger avec ARP.
2. Accédez à l'onglet **Paramètres**. Sous **sécurité**, localisez la mosaïque **anti-ransomware**, puis sélectionnez .
3. Cochez la case pour activer ARP pour les volumes NAS. Cochez la case supplémentaire pour activer ARP sur tous les volumes NAS éligibles de la machine virtuelle de stockage.



Si vous avez effectué une mise à niveau vers ONTAP 9.13.1, le **passage automatique du mode apprentissage au mode actif après un apprentissage suffisant** est activé automatiquement. Cela permet à ARP de déterminer l'intervalle de la période d'apprentissage optimale et d'automatiser le passage en mode actif. Désactivez le paramètre si vous souhaitez passer manuellement en mode actif.

CLI

1. Modifier un SVM existant pour activer ARP par défaut dans les nouveaux volumes :

```
vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
```

Au niveau de l'interface de ligne de commandes, vous pouvez également créer un nouveau SVM avec ARP activé par défaut pour les nouveaux volumes.

```
vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]
```

Si vous avez mis à niveau vers ONTAP 9.13.1 ou une version ultérieure, l'apprentissage adaptatif est activé de sorte que le changement d'état actif s'effectue automatiquement. Si vous ne souhaitez pas que ce comportement soit automatiquement activé, utilisez la commande suivante :

```
vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to-enabled false
```

Mettez en pause la protection autonome contre les ransomwares pour exclure les événements des charges de travail de l'analyse

Si vous attendez des événements inhabituels des charges de travail, vous pouvez suspendre et reprendre temporairement l'analyse ARP (autonome ransomware protection) à tout moment.

À partir de ONTAP 9.13.1, vous pouvez activer la vérification multiadministrateur (MAV) de sorte que deux administrateurs d'utilisateurs authentifiés ou plus soient requis pour interrompre le protocole ARP. "[En savoir plus >>](#)".

Description de la tâche

Lors d'une pause ARP, aucun événement n'est enregistré et aucune action n'est en cours pour les nouvelles écritures. Toutefois, le processus d'analytique continue pour les journaux précédents en arrière-plan.



N'utilisez pas la fonction de désactivation ARP pour interrompre l'analyse. Ceci désactive ARP sur le volume et toutes les informations existantes concernant le comportement de la charge de travail apprise sont perdues. Cela nécessiterait un redémarrage de la période d'apprentissage.

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour interrompre le protocole ARP.

System Manager

1. Sélectionnez **stockage > volumes**, puis sélectionnez le volume sur lequel vous souhaitez mettre en pause ARP.
2. Dans l'onglet **sécurité** de la vue d'ensemble des volumes, sélectionnez **Pause anti-ransomware** dans la zone **anti-ransomware**.



À partir de ONTAP 9.13.1, si vous utilisez MAV pour protéger vos paramètres ARP, l'opération de pause vous invite à obtenir l'approbation d'un ou de plusieurs administrateurs supplémentaires. "L'approbation doit être reçue de tous les administrateurs" Associé au groupe d'approbation MAV ou l'opération échouera.

CLI

1. Suspendre ARP sur un volume :

```
security anti-ransomware volume pause -vserver svm_name -volume vol_name
```

2. Pour reprendre le traitement, utilisez resume commande :

```
security anti-ransomware volume resume -vserver svm_name -volume vol_name
```

3. **Si vous utilisez MAV (disponible avec ARP à partir de ONTAP 9.13.1) pour protéger vos paramètres ARP**, l'opération de pause vous invite à obtenir l'approbation d'un ou de plusieurs administrateurs supplémentaires. L'approbation doit être reçue de tous les administrateurs associés au groupe d'approbation MAV, faute de quoi l'opération échouera.

Si vous utilisez MAV et qu'une opération de pause attendue nécessite des approbations supplémentaires, chaque approbateur de groupe MAV effectue les opérations suivantes :

- a. Afficher la demande :

```
security multi-admin-verify request show
```

- b. Approuver la demande :

```
security multi-admin-verify request approve -index[number returned from show request]
```

La réponse du dernier approbateur de groupe indique que le volume a été modifié et que l'état du protocole ARP est mis en pause.

Si vous utilisez MAV et que vous êtes un approbateur de groupe MAV, vous pouvez rejeter une demande d'opération de pause :

```
security multi-admin-verify request veto -index[number returned from show request]
```

Gérez les paramètres de détection des attaques par protection anti-ransomware autonome

À partir de la version ONTAP 9.11.1, vous pouvez modifier les paramètres de détection des ransomwares sur un volume spécifique optimisé par la protection anti-ransomware autonome et signaler une augmentation connue sous le nom d'activité de fichier normale. Le réglage des paramètres de détection permet d'améliorer la précision des rapports en fonction de votre charge de travail de volume spécifique.

Fonctionnement de la détection des attaques

Lorsque la protection anti-ransomware autonome (ARP) est en mode d'apprentissage, elle développe des valeurs de base pour les comportements de volume. Il s'agit d'entropie, d'extensions de fichiers et, à partir de ONTAP 9.11.1, d'IOPS. Ces données de base sont utilisées pour évaluer les menaces de ransomware. Pour plus d'informations sur ces critères, reportez-vous à la section [Ce que le protocole ARP détecte](#).

Dans ONTAP 9.10.1, ARP émet un avertissement s'il détecte les deux conditions suivantes :

- plus de 20 fichiers avec des extensions de fichier qui n'ont pas été observées précédemment dans le volume
- données d'entropie élevées

À partir de ONTAP 9.11.1, ARP émet un avertissement de menace si *seule* une condition est remplie. Par exemple, si plus de 20 fichiers avec des extensions de fichier qui n'ont pas été observées précédemment dans le volume sont observés dans une période de 24 heures, ARP catégorise ceci comme une menace *indépendamment* de l'entropie observée. (Les valeurs de fichier 24 heures et 20 sont des valeurs par défaut, qui peuvent être modifiées.)

À partir de ONTAP 9.14.1, vous pouvez configurer des alertes lorsque ARP observe une nouvelle extension de fichier et lorsque ARP crée un instantané. Pour plus d'informations, voir [\[modify-alerts\]](#)

Certains volumes et charges de travail requièrent des paramètres de détection différents. Par exemple, votre volume ARP peut héberger de nombreux types d'extensions de fichiers. Dans ce cas, vous pouvez modifier le nombre de seuils pour les extensions de fichiers jamais vues à un nombre supérieur à la valeur par défaut de 20 ou désactiver les avertissements basés sur des extensions de fichiers jamais vues. À partir de ONTAP 9.11.1, vous pouvez modifier les paramètres de détection des attaques afin qu'ils s'adaptent mieux à vos workloads spécifiques.

Modifier les paramètres de détection d'attaque

Selon les comportements attendus de votre volume ARP, vous pouvez modifier les paramètres de détection d'attaque.

Étapes

1. Afficher les paramètres de détection d'attaque existants :

```
security anti-ransomware volume attack-detection-parameters show -vserver  
svm_name -volume volume_name
```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume vol1
```

```

Vserver Name : vs1
Volume Name : vol1
Is Detection Based on High Entropy Data Rate? : true
Is Detection Based on Never Seen before File Extension? : true
Is Detection Based on File Create Rate? : true
Is Detection Based on File Rename Rate? : true
Is Detection Based on File Delete Rate? : true
Is Detection Relaxing Popular File Extensions? : true
High Entropy Data Surge Notify Percentage : 100
File Create Rate Surge Notify Percentage : 100
File Rename Rate Surge Notify Percentage : 100
File Delete Rate Surge Notify Percentage : 100
Never Seen before File Extensions Count Notify Threshold : 20
Never Seen before File Extensions Duration in Hour : 24
```

2. Tous les champs affichés peuvent être modifiés avec des valeurs booléennes ou entières. Pour modifier un champ, utilisez `security anti-ransomware volume attack-detection-parameters modify` commande.

Pour obtenir la liste complète des paramètres, reportez-vous à la section "[Référence de commande ONTAP](#)".

Signaler les surtensions connues

ARP continue de modifier les valeurs de base pour les paramètres de détection, même en mode actif. Si vous connaissez des surtensions dans votre activité de volume—des surtensions ou une surtension qui est caractéristique d'une nouvelle normale—you devriez la signaler comme sûre. La déclaration manuelle de ces surtensions comme étant sûres contribue à améliorer la précision des évaluations des menaces d'ARP.

Signaler une surtension ponctuelle

1. Si une surtension ponctuelle se produit dans des circonstances connues et que vous souhaitez que ARP signale une surtension similaire dans des circonstances futures, éliminez la poussée du comportement de la charge de travail :

```
security anti-ransomware volume workload-behavior clear-surge -vserver
svm_name -volume volume_name
```

Modifier la surtension de la ligne de base

1. Si une surtension signalée doit être considérée comme un comportement normal de l'application, signalez-la en tant que telle pour modifier la valeur de surtension de la ligne de base.

```
security anti-ransomware volume workload-behavior update-baseline-from-surge
-vserver svm_name -volume volume_name
```


Configurez les alertes ARP

Depuis ONTAP 9.14.1, ARP vous permet de spécifier des alertes pour deux événements ARP :

- Observation de la nouvelle extension de fichier sur un volume
- Création d'un instantané ARP

Les alertes liées à ces deux événements peuvent être définies sur des volumes individuels ou pour l'ensemble du SVM. Si vous activez des alertes pour le SVM, les paramètres d'alerte ne sont hérités que par les volumes créés après l'activation de l'alerte. Par défaut, les alertes ne sont activées sur aucun volume.


Les alertes d'événements peuvent être contrôlées par une vérification multiadministrateur. Pour plus d'informations, voir [Vérification multiadministrateur avec volumes protégés par ARP](#).

System Manager

Définir des alertes pour un volume

1. Accédez à **volumes**. Sélectionnez le volume individuel pour lequel vous souhaitez modifier les paramètres.
2. Sélectionnez l'onglet **sécurité**, puis **Paramètres de sécurité des événements**.
3. Pour recevoir des alertes pour **Nouvelle extension de fichier détectée** et **instantané de ransomware créé**, sélectionnez le menu déroulant sous l'en-tête **gravité**. Modifiez le paramètre de **ne pas générer l'événement** à **Avis**.
4. Sélectionnez **Enregistrer**.

Définir des alertes pour un SVM

1. Naviguer jusqu'à **Storage VM** puis sélectionner le SVM pour lequel vous voulez activer les paramètres.
2. Sous la rubrique **sécurité**, repérez la carte **anti-ransomware**. Sélectionnez  , puis **Modifier la gravité des événements ransomware**.
3. Pour recevoir des alertes pour **Nouvelle extension de fichier détectée** et **instantané de ransomware créé**, sélectionnez le menu déroulant sous l'en-tête **gravité**. Modifiez le paramètre de **ne pas générer l'événement** à **Avis**.
4. Sélectionnez **Enregistrer**.

CLI

Définir des alertes pour un volume

- Pour définir des alertes pour une nouvelle extension de fichier :

```
security anti-ransomware volume event-log modify -vserver svm_name -is  
-enabled-on-new-file-extension-seen true
```

- Pour définir des alertes pour la création d'un instantané ARP :

```
security anti-ransomware volume event-log modify -vserver svm_name -is  
-enabled-on-snapshot-copy-creation true
```

- Confirmez vos paramètres à l'aide du `anti-ransomware volume event-log show` commande.

Définir des alertes pour un SVM

- Pour définir des alertes pour une nouvelle extension de fichier :

```
security anti-ransomware vserver event-log modify -vserver svm_name -is  
-enabled-on-new-file-extension-seen true
```

- Pour définir des alertes pour la création d'un instantané ARP :

```
security anti-ransomware vserver event-log modify -vserver svm_name -is  
-enabled-on-snapshot-copy-creation true
```

- Confirmez vos paramètres à l'aide du `security anti-ransomware vserver event-log show` commande.

Plus d'informations

- ["Apprenez à comprendre les attaques de protection anti-ransomware autonomes et le snapshot de protection anti-ransomware autonome"](#).

Réagir à une activité anormale

Lorsque la protection autonome contre les attaques par ransomware (ARP) détecte une activité anormale dans un volume protégé, elle émet un avertissement. Vous devez évaluer la notification pour déterminer si l'activité est acceptable (faux positif) ou si une attaque semble malveillante.

Description de la tâche

ARP affiche une liste des fichiers suspects lorsqu'il détecte une combinaison de données entropie élevée, une activité de volume anormale avec chiffrement des données et des extensions de fichier inhabituelles.

Lorsque l'avertissement est émis, répondez en désignant l'activité de fichier de l'une des deux manières suivantes :

- **Faux positif**

Le type de fichier identifié est attendu dans votre charge de travail et peut être ignoré.

- **Attaque potentielle par ransomware**

Le type de fichier identifié est inattendu dans votre charge de travail et doit être traité comme une attaque potentielle.

Dans les deux cas, la surveillance normale reprend après la mise à jour et la suppression des avis. ARP enregistre votre évaluation dans le profil d'évaluation des menaces, en utilisant votre choix pour surveiller les activités de fichiers suivantes.

Dans le cas d'une attaque suspectée, vous devez déterminer s'il s'agit d'une attaque, y répondre si c'est le cas et restaurer les données protégées avant d'effacer les notifications. ["En savoir plus sur la manière de procéder à une reprise après une attaque par ransomware"](#).



Si vous restaurez un volume entier, il n'y a pas d'avis à effacer.

Avant de commencer

ARP doit être exécuté en mode actif.

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour répondre à une tâche anormale.

System Manager


1. Lorsque vous recevez une notification d'activité anormale, suivez le lien. Vous pouvez également accéder à l'onglet **sécurité** de la présentation **volumes**.

Les avertissements s'affichent dans le volet **vue d'ensemble** du menu **Events**.

2. Lorsqu'un message "activité de volume anormale détectée" s'affiche, consultez les fichiers suspects.

Dans l'onglet **sécurité**, sélectionnez **Afficher les types de fichiers suspects**.

3. Dans la boîte de dialogue **types de fichiers suspects**, examinez chaque type de fichier et marquez-le comme "Faux positif" ou "attaque par ransomware potentielle".

Si vous avez sélectionné cette valeur...	Prendre cette action...
Faux positif	<p>Sélectionnez mettre à jour et Effacer les types de fichiers suspects pour enregistrer votre décision et reprendre la surveillance ARP normale.</p> <div><p>À partir de ONTAP 9.13.1, si vous utilisez MAV pour protéger vos paramètres ARP, l'opération Effacer-suspect vous invite à obtenir l'approbation d'un ou de plusieurs administrateurs supplémentaires. "L'approbation doit être reçue de tous les administrateurs" Associé au groupe d'approbation MAV ou l'opération échouera.</p></div>
Attaques par ransomware potentielles	<p>Répondez aux attaques et restaurez les données protégées. Sélectionnez ensuite Update et Clear suspect File types pour enregistrer votre décision et reprendre la surveillance ARP normale.</p> <p>Il n'existe aucun type de fichier suspect à effacer si vous avez restauré un volume entier.</p>

CLI

1. Lorsque vous recevez une notification d'attaque par ransomware suspectée, vérifiez l'heure et la gravité de l'attaque :

```
security anti-ransomware volume show -vserver svm_name -volume vol_name
```

Sortie d'échantillon :

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

Vous pouvez également vérifier les messages EMS :

```
event log show -message-name callhome.arw.activity.seen
```

2. Générez un rapport d'attaque et notez l'emplacement de sortie :

```
security anti-ransomware volume attack generate-report -volume vol_name  
-dest-path file_location/
```

Sortie d'échantillon :

```
Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path  
"vs0:vol1/"
```

3. Afficher le rapport sur un système client d'administration. Par exemple :

```
[root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08  
  
19  "9/14/2021 01:03:23"    test_dir_1/test_file_1.jpg.lckd  
20  "9/14/2021 01:03:46"    test_dir_2/test_file_2.jpg.lckd  
21  "9/14/2021 01:03:46"    test_dir_3/test_file_3.png.lckd`
```

4. Suivez l'une des actions suivantes en fonction de votre évaluation des extensions de fichier :

◦ Faux positif

Entrez la commande suivante pour enregistrer votre décision, en ajoutant la nouvelle extension à la liste de ceux autorisés et en redonnant une surveillance anti-ransomware normale :

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume  
vol_name [extension identifiers] -false-positive true
```

Utilisez l'un des paramètres suivants pour identifier les extensions :

`[-seq-no integer]` Numéro de séquence du fichier dans la liste des suspects.

`[-extension text, ...]` Extensions de fichier

`[-start-time date_time -end-time date_time]` Heures de début et de fin pour la plage de fichiers à effacer, sous la forme "MM/JJ/AAAA HH:MM:SS".

◦ Attaque par ransomware potentielle

Répondez à l'attaque et ["Récupérez les données à partir de l'instantané de sauvegarde créé par ARP"](#). Une fois les données récupérées, entrez la commande suivante pour enregistrer votre décision et reprendre la surveillance ARP normale :

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume  
vol_name [extension identifiers] -false-positive false
```

Utilisez l'un des paramètres suivants pour identifier les extensions :

`[-seq-no integer]` Numéro de séquence du fichier dans la liste des suspects

`[-extension text, ...]` Extension de fichier

`[-start-time date_time -end-time date_time]` Heures de début et de fin pour la plage de fichiers à effacer, sous la forme "MM/JJ/AAAA HH:MM:SS".

Il n'existe aucun type de fichier suspect à effacer si vous avez restauré un volume entier. L'instantané de sauvegarde créé par ARP sera supprimé et le rapport d'attaque sera effacé.

5. Si vous utilisez MAV et un attendu `clear-suspect` L'opération nécessite des approbations supplémentaires, chaque approbateur de groupe MAV doit :

- a. Afficher la demande :

```
security multi-admin-verify request show
```

- b. Approuver la demande de reprise de la surveillance anti-ransomware classique :

```
security multi-admin-verify request approve -index[number returned from show request]
```

La réponse du dernier approbateur de groupe indique que le volume a été modifié et qu'un faux positif est enregistré.

6. Si vous utilisez MAV et que vous êtes un approbateur de groupe MAV, vous pouvez également rejeter une demande claire-suspecte :

```
security multi-admin-verify request veto -index[number returned from show request]
```

Plus d'informations

- ["Base de connaissances : comprendre les attaques de protection anti-ransomware autonomes et le snapshot de protection anti-ransomware autonome"](#).

Restaurez les données après une attaque par ransomware

La protection anti-ransomware autonome (ARP) crée des copies Snapshot nommées `Anti_ransomware_backup` lorsqu'il détecte une menace potentielle de ransomware. Vous pouvez utiliser l'une de ces copies snapshot ARP ou une autre copie Snapshot de votre volume pour restaurer les données.

Description de la tâche

Si le volume possède des relations SnapMirror, répliquez manuellement toutes les copies miroir du volume immédiatement après la restauration à partir d'une copie Snapshot. Cette opération risque d'entraîner des copies miroir inutilisables qui doivent d'être supprimées et recrées.

Pour effectuer une restauration à partir d'une copie Snapshot autre que le `Anti_ransomware_backup` Instantané après l'identification d'une attaque système, vous devez d'abord libérer l'instantané ARP.

Si aucune attaque système n'a été signalée, vous devez d'abord restaurer à partir du `Anti_ransomware_backup` La copie Snapshot effectue ensuite une restauration ultérieure du volume à partir de la copie Snapshot de votre choix.

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour restaurer vos données.

System Manager

Restauration après une attaque système


1. Pour effectuer une restauration à partir de l'instantané ARP, passez à l'étape 2. Pour effectuer une restauration à partir d'une copie Snapshot antérieure, vous devez d'abord libérer le verrouillage de l'instantané ARP.
 - a. Sélectionnez **stockage > volumes**.
 - b. Sélectionnez **sécurité** puis **Afficher les types de fichiers suspects**
 - c. Marquez les fichiers comme « Faux positif » .
 - d. Sélectionnez **mettre à jour** et **Effacer les types de fichiers suspects**
2. Afficher les copies Snapshot dans des volumes :

Sélectionnez **stockage > volumes**, puis sélectionnez le volume et **copies Snapshot**.

3. Sélectionnez  en regard de la copie Snapshot à restaurer, puis **Restaurer**.

Restaurez si aucune attaque système n'a été identifiée

1. Afficher les copies Snapshot dans des volumes :

Sélectionnez **stockage > volumes**, puis sélectionnez le volume et **copies Snapshot**.
2. Sélectionnez  -les Choisissez l' `Anti_ransomware_backup` instantané.
3. Sélectionnez **Restaurer**.
4. Revenez au menu **copies Snapshot**, puis choisissez la copie Snapshot que vous souhaitez utiliser. Sélectionnez **Restaurer**.

CLI

Restauration après une attaque système

1. Pour effectuer une restauration à partir de la copie ARP Snapshot, passez à l'étape 2. Pour restaurer des données à partir de copies Snapshot antérieures, vous devez libérer le verrouillage de l'instantané ARP.



Si vous utilisez la, vous devez libérer la fonctionnalité anti-ransomware SnapLock avant de restaurer vos données à partir de copies Snapshot antérieures `volume snap restore` comme décrit ci-dessous. Si vous restaurez des données à l'aide de Flex Clone, de Single File Snap Restore ou d'autres méthodes, cela n'est pas nécessaire.

Marquer l'attaque comme « faux positif » et « suspect clair » :

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true
```

Utilisez l'un des paramètres suivants pour identifier les extensions :

`[-seq-no integer]` Numéro de séquence du fichier dans la liste des suspects.

`[-extension text, ...]` Extensions de fichier

`[-start-time date_time -end-time date_time]` Heures de début et de fin pour la plage de fichiers à effacer, sous la forme "MM/JJ/AAAA HH:MM:SS".

2. Lister les copies Snapshot dans un volume :

```
volume snapshot show -vserver <SVM> -volume <volume>
```

L'exemple suivant montre les copies Snapshot dans vol1:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
-----	-----	-----	-----	-----	-----	-----
vs1	vol1	hourly.2013-01-25_0005	valid	224KB	0%	0%
		daily.2013-01-25_0010	valid	92KB	0%	0%
		hourly.2013-01-25_0105	valid	228KB	0%	0%
		hourly.2013-01-25_0205	valid	236KB	0%	0%
		hourly.2013-01-25_0305	valid	244KB	0%	0%
		hourly.2013-01-25_0405	valid	244KB	0%	0%
		hourly.2013-01-25_0505	valid	244KB	0%	0%

7 entries were displayed.

3. Restaurer le contenu d'un volume à partir d'une copie Snapshot :

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot  
<snapshot>
```

L'exemple suivant restaure le contenu de vol1:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1  
-snapshot daily.2013-01-25_0010
```

Restaurer si aucune attaque système n'a été identifiée

1. Lister les copies Snapshot dans un volume :

```
volume snapshot show -vserver <SVM> -volume <volume>
```

L'exemple suivant montre les copies Snapshot dans vol1:


```
clus1::> volume snapshot show -vserver vs1 -volume voll
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vs1	voll	hourly.2013-01-25_0005	valid	224KB	0%	0%
		daily.2013-01-25_0010	valid	92KB	0%	0%
		hourly.2013-01-25_0105	valid	228KB	0%	0%
		hourly.2013-01-25_0205	valid	236KB	0%	0%
		hourly.2013-01-25_0305	valid	244KB	0%	0%
		hourly.2013-01-25_0405	valid	244KB	0%	0%
		hourly.2013-01-25_0505	valid	244KB	0%	0%

7 entries were displayed.

2. Restaurer le contenu d'un volume à partir d'une copie Snapshot :

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot  
<snapshot>
```

L'exemple suivant restaure le contenu de voll:

```
cluster1::> volume snapshot restore -vserver vs0 -volume voll  
-snapshot daily.2013-01-25_0010
```

3. Répétez les étapes 1 et 2 pour restaurer le volume à l'aide de la copie Snapshot souhaitée.

Plus d'informations

- ["Base de connaissances : prévention des ransomwares et restauration dans ONTAP"](#)

Modifiez les options des copies Snapshot automatiques

Depuis la version ONTAP 9.11.1, vous pouvez utiliser l'interface de ligne de commandes pour contrôler les paramètres de conservation des copies Snapshot ARP (Autonomous ransomware protection) qui sont générées automatiquement en réponse à des attaques de ransomware suspectées.

Avant de commencer

Vous pouvez uniquement modifier les options ARP snapshots sur une SVM de nœud.

Étapes

1. Pour afficher tous les paramètres de copie snapshot ARP actuels, entrez :

```
vserver options -vserver svm_name arw*
```



Le `vserver options` commande est une commande masquée. Pour afficher la page `man`, entrez `man vserver options` Sur l'interface de ligne de commandes de ONTAP.


2. Pour afficher les paramètres de copie snapshot ARP actuels sélectionnés, entrez :

```
vserver options -vserver svm_name -option-name arw_setting_name
```

3. Pour modifier les paramètres de copie snapshot ARP, entrez :

```
vserver options -vserver svm_name -option-name arw_setting_name -option-value arw_setting_value
```

Les paramètres suivants peuvent être modifiés :

Réglage ARW	Description
<code>arw.snap.max.count</code>	<p>Spécifie le nombre maximal de copies snapshot ARP pouvant exister dans un volume à tout moment. Les anciennes copies sont supprimées pour garantir que le nombre total de copies snapshot ARP se situe dans cette limite spécifiée.</p> <p>Le <code>-option-value</code> le paramètre accepte des entiers compris entre 3 et 8, inclus. La valeur par défaut est 6.</p>
<code>arw.snap.create.interval.hours</code>	<p>Spécifie l'intervalle <i>en heures</i> entre les copies snapshot ARP. Une nouvelle copie ARP Snapshot est créée lorsqu'une attaque basée sur l'entropie des données est suspectée et que la dernière copie ARP Snapshot créée est antérieure à l'intervalle spécifié.</p> <p>Le <code>-option-value</code> le paramètre accepte des entiers compris entre 1 et 48, inclus. La valeur par défaut est 4.</p>
<code>arw.snap.normal.retain.interval.hours</code>	<p>Spécifie la durée <i>en heures</i> pendant laquelle une copie snapshot ARP est conservée. Lorsqu'une copie snapshot ARP atteint le seuil de rétention, toute autre copie snapshot ARP créée avant d'être supprimée. Il ne peut exister plus d'une copie snapshot ARP antérieure au seuil de rétention.</p> <p>Le <code>-option-value</code> le paramètre accepte des entiers compris entre 4 et 96, inclus. La valeur par défaut est 48.</p>
<code>arw.snap.max.retain.interval.days</code>	<p>Spécifie la durée maximale <i>en jours</i> pendant laquelle une copie snapshot ARP peut être conservée. Toute copie snapshot ARP antérieure à cette durée est supprimée lorsqu'aucune attaque n'est signalée sur le volume.</p> <div><p>L'intervalle de rétention maximal pour les copies snapshot ARP est ignoré si une menace modérée est détectée. La copie snapshot ARP créée en réponse à la menace est conservée jusqu'à ce que vous ayez répondu à la menace. Le marquage d'une menace comme faux positif entraîne la suppression des copies Snapshot ARP sur le volume.</p><p>Le <code>-option-value</code> le paramètre accepte des entiers compris entre 1 et 365, inclus. La valeur par défaut est 5.</p></div>

Réglage ARW	Description
<code>arw.snap.create.interval.hours.post.max.count</code>	<p>Spécifie l'intervalle <i>en heures</i> entre les copies snapshot ARP lorsque le volume contient déjà le nombre maximal de copies snapshot ARP. Lorsque le nombre maximum est atteint, une copie snapshot ARP est supprimée pour faire place à une nouvelle copie. La nouvelle vitesse de création de copie Snapshot ARP peut être réduite pour conserver l'ancienne copie à l'aide de cette option. Si le volume contient déjà le nombre maximal de copies snapshot ARP, l'intervalle spécifié dans cette option est utilisé pour la création de la copie Snapshot ARP suivante, au lieu de <code>arw.snap.create.interval.hours</code>.</p> <p>Le <code>-option-value</code> le paramètre accepte des entiers compris entre 4 et 48, inclus. La valeur par défaut est 8.</p>
<code>arw.surge.snap.interval.days</code>	<p>Spécifie l'intervalle <i>en jours</i> entre les copies snapshot ARP créées en réponse aux pics d'E/S. ONTAP crée une copie snapshot ARP en cas de surcharge du trafic d'E/S et lorsque la dernière copie Snapshot ARP créée est antérieure à l'intervalle spécifié. Cette option spécifie également la période de rétention <i>in Day</i> pour les copies snapshot de surtension ARP.</p> <p>Le <code>-option-value</code> le paramètre accepte des entiers compris entre 1 et 365, inclus. La valeur par défaut est 5.</p>
<code>arw.snap.new.extns.interval.hours</code>	<p>Cette option spécifie l'intervalle <i>en heures</i> entre les copies snapshot ARP créées lorsqu'une nouvelle extension de fichier est détectée. Une nouvelle copie snapshot ARP est créée lorsque</p> <p>Une nouvelle extension de fichier est observée ; l'instantané précédent créé lors de l'observation d'une nouvelle extension de fichier est plus ancien que cet intervalle spécifié. Sur une charge de travail qui crée fréquemment de nouvelles extensions de fichiers, cet intervalle permet de contrôler la fréquence des copies Snapshot ARP. Cette option existe indépendamment de <code>arw.snap.create.interval.hours</code>, Qui spécifie l'intervalle pour les copies Snapshot ARP basées sur l'entropie des données.</p> <p>Le <code>-option-value</code> le paramètre accepte des entiers compris entre 24 et 8760. La valeur par défaut est 48.</p>

Protection antivirus avec Vscan

Présentation de la configuration antivirus

Vscan est une solution d'analyse antivirus développée par NetApp qui permet aux clients de protéger leurs données contre toute compromission par des virus ou d'autres codes malveillants.

Vscan effectue des analyses antivirus lorsque les clients accèdent aux fichiers via SMB. Vous pouvez configurer Vscan pour scanner à la demande ou selon une planification. Vous pouvez interagir avec Vscan en utilisant l'interface de ligne de commande (CLI) ONTAP ou les interfaces de programmation d'applications (API) ONTAP.

Informations associées

["Solutions partenaires Vscan"](#)

À propos de la protection antivirus NetApp

À propos de l'analyse antivirus NetApp

Vscan est une solution d'analyse antivirus développée par NetApp qui permet aux clients de protéger leurs données contre toute compromission par des virus ou d'autres codes malveillants. Il associe un logiciel antivirus fourni par le partenaire aux fonctionnalités de ONTAP pour offrir aux clients la flexibilité dont ils ont besoin pour gérer l'analyse des fichiers.

Fonctionnement de l'analyse antivirus

Les systèmes de stockage délèguent des opérations d'analyse à des serveurs externes hébergeant le logiciel antivirus de fournisseurs tiers.

En fonction du mode d'analyse actif, ONTAP envoie des demandes d'analyse lorsque les clients accèdent aux fichiers via SMB (on-Access) ou accèdent à des fichiers dans des emplacements spécifiques, selon une planification ou immédiatement (on-Demand).

- Vous pouvez utiliser *On-Access scan* pour rechercher des virus lorsque les clients ouvrent, lisent, renomment ou ferment des fichiers sur SMB. Les opérations sur les fichiers sont suspendues jusqu'à ce que le serveur externe indique l'état d'analyse du fichier. Si le fichier a déjà été numérisé, ONTAP autorise l'opération de fichier. Dans le cas contraire, il demande un scan à partir du serveur.

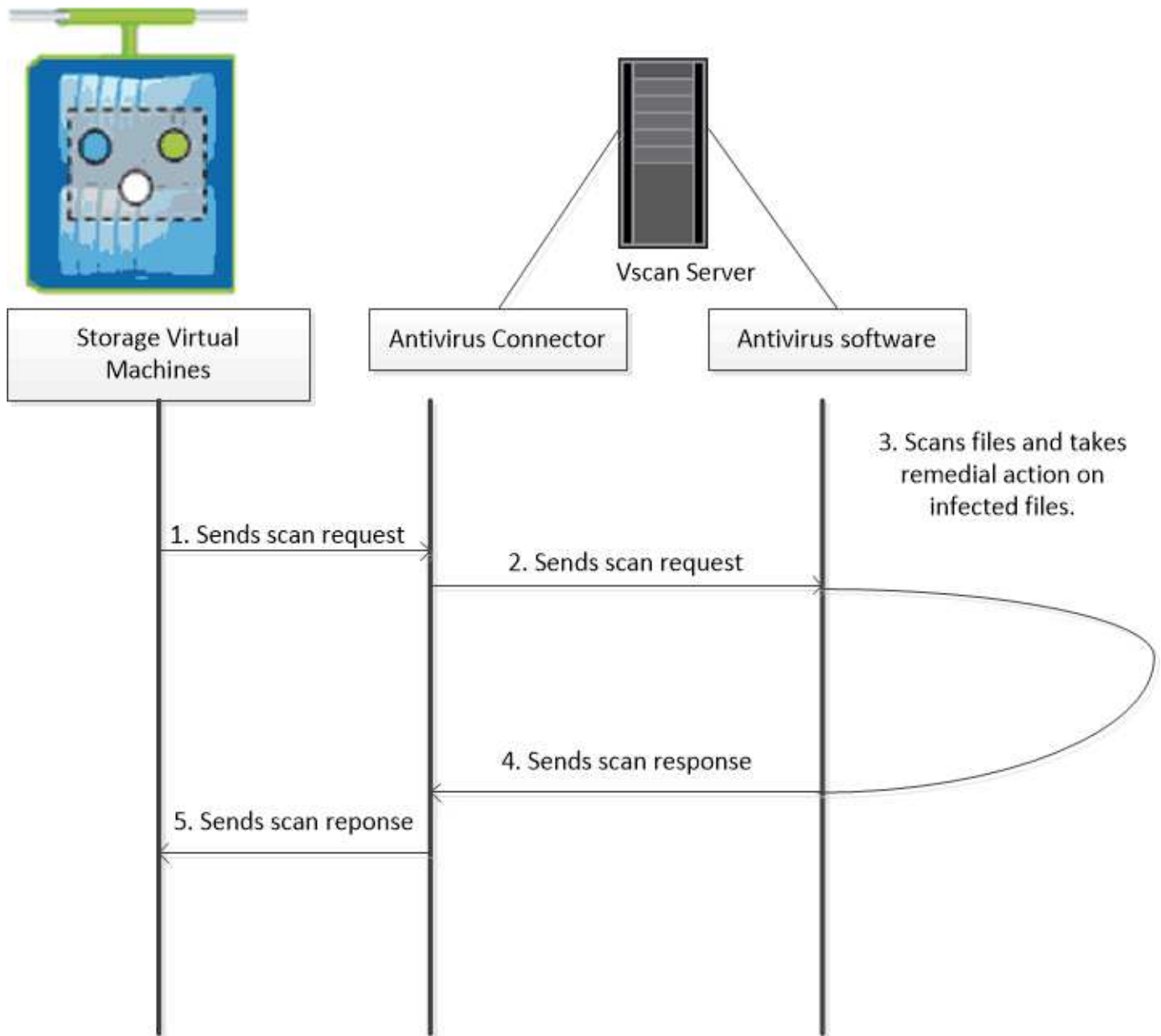
L'analyse lors de l'accès n'est pas prise en charge par NFS.

- Vous pouvez utiliser *On-Demand scan* pour vérifier immédiatement ou selon un planning les fichiers à la recherche de virus. Nous recommandons que les analyses à la demande ne s'exécutent qu'en dehors des heures de pointe pour éviter de surcharger l'infrastructure AV existante, qui est normalement dimensionnée pour l'analyse à l'accès. Le serveur externe met à jour l'état d'analyse des fichiers vérifiés afin de réduire la latence d'accès aux fichiers par rapport à SMB. S'il y a eu des modifications de fichier ou des mises à jour de version de logiciel, il demande une nouvelle analyse de fichier à partir du serveur externe.

Vous pouvez utiliser l'analyse à la demande pour n'importe quel chemin du namespace du SVM, même pour les volumes exportés uniquement via NFS.

Il est généralement possible d'activer les modes d'analyse à la fois on-Access et on-Demand sur une SVM. Dans les deux modes, le logiciel antivirus effectue des actions correctives sur les fichiers infectés en fonction des paramètres de votre logiciel.

Le connecteur antivirus ONTAP, fourni par NetApp et installé sur le serveur externe, gère la communication entre le système de stockage et le logiciel antivirus.

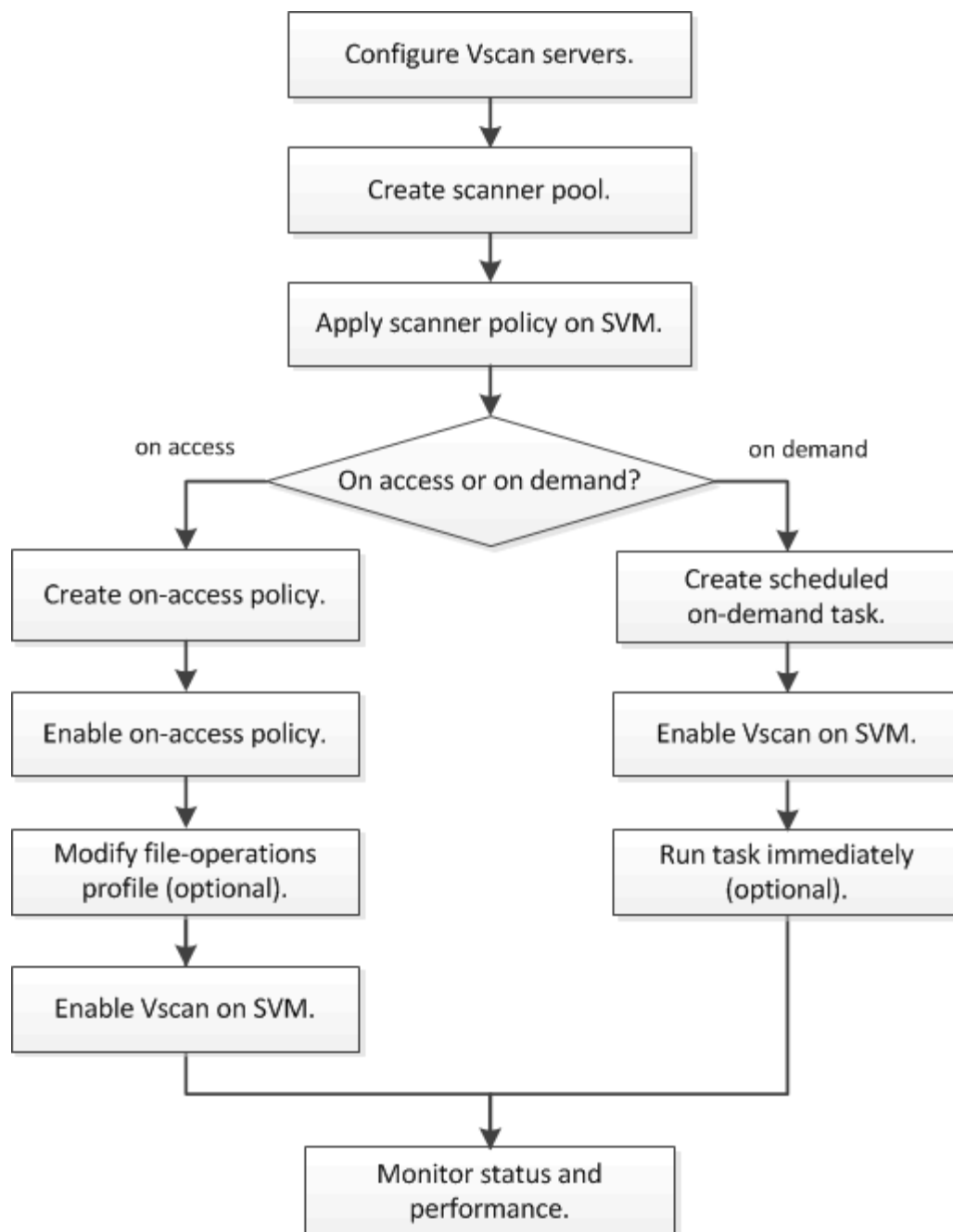


Workflow d'analyse de virus

Vous devez créer un pool de scanner et appliquer une politique de scanner avant de pouvoir activer la numérisation. Il est généralement possible d'activer les modes d'analyse à la fois on-Access et on-Demand sur une SVM.



Vous devez avoir terminé la configuration CIFS.



Étapes suivantes

- [Créer un pool de scanner sur un seul cluster](#)
- [Appliquer une politique scanner sur un seul cluster](#)
- [Création d'une règle on-Access](#)

Architecture antivirus

L'architecture antivirus NetApp se compose du logiciel du serveur Vscan et des paramètres associés.

Logiciel du serveur Vscan

Vous devez installer ce logiciel sur le serveur Vscan.

- **ONTAP antivirus Connector**

Il s'agit d'un logiciel fourni par NetApp qui gère les communications de demande et de réponse de scan entre les SVM et le logiciel antivirus. Il peut être exécuté sur une machine virtuelle, mais pour optimiser les performances, il convient d'utiliser une machine physique. Vous pouvez télécharger ce logiciel sur le site du support NetApp (vous devez disposer d'un identifiant).

- **Logiciel antivirus**

Il s'agit d'un logiciel fourni par un partenaire qui analyse les fichiers à la recherche de virus ou d'autres codes malveillants. Lors de la configuration du logiciel, vous spécifiez les actions correctives à effectuer sur les fichiers infectés.

Paramètres du logiciel Vscan

Vous devez configurer ces paramètres logiciels sur le serveur Vscan.

- **Scanner pool**

Ce paramètre définit les serveurs Vscan et les utilisateurs privilégiés qui peuvent se connecter aux SVM. Il définit également une période de temporisation de la demande de scan, après laquelle la requête de scan est envoyée à un autre serveur Vscan si un serveur est disponible.



Vous devez définir la période de temporisation dans le logiciel antivirus sur le serveur Vscan à cinq secondes de moins que le délai d'expiration de la demande de scan-pool. Cela permet d'éviter les situations dans lesquelles l'accès aux fichiers est retardé ou refusé car le délai d'expiration du logiciel est supérieur au délai d'expiration de la demande d'analyse.

- **Utilisateur privilégié**

Ce paramétrage est un compte utilisateur de domaine qu'un serveur Vscan utilise pour se connecter à la SVM. Le compte doit figurer dans la liste des utilisateurs privilégiés du scanner pool.

- **Politique du scanner**

Ce paramètre détermine si un scanner pool est actif. Les règles de scanner sont définies par le système ; vous ne pouvez donc pas créer de règles de scanner personnalisées. Seules les trois règles suivantes sont disponibles :

- `Primary` indique que le pool de scanner est actif.
- `Secondary` Précise que le pool de scanner est actif uniquement si aucun des serveurs Vscan du pool de scanner principal n'est connecté.
- `Idle` indique que le pool de scanner est inactif.

- **Politique sur accès**

Ce paramètre définit la portée d'une analyse à l'accès. Vous pouvez spécifier la taille maximale du fichier à numériser, les extensions de fichier et les chemins à inclure dans la numérisation, ainsi que les extensions de fichier et les chemins à exclure de la numérisation.

Par défaut, seuls les volumes en lecture-écriture sont analysés. Vous pouvez spécifier des filtres qui permettent la numérisation de volumes en lecture seule ou qui limitent la numérisation aux fichiers ouverts avec l'accès d'exécution :

- `scan-ro-volume` permet d'analyser les volumes en lecture seule.
- `scan-execute-access` limite la numérisation aux fichiers ouverts avec l'accès d'exécution.



« Exécuter l'accès » est différent de « Exécuter l'autorisation ». Un client donné aura « accès à l'exécution » sur un fichier exécutable uniquement si le fichier a été ouvert avec « intention d'exécution ».

Vous pouvez définir le `scan-mandatory` Option désactivée pour spécifier que l'accès aux fichiers est autorisé lorsqu'aucun serveur Vscan n'est disponible pour l'analyse antivirus. En mode On-Access, vous pouvez choisir parmi les deux options mutuellement exclusives suivantes :

- **Obligatoire** : avec cette option, Vscan tente de livrer la demande de scan au serveur jusqu'à expiration du délai. Si la demande d'analyse n'est pas acceptée par le serveur, la demande d'accès client est refusée.
- **Non obligatoire** : avec cette option, Vscan permet toujours l'accès client, qu'un serveur Vscan soit disponible ou non pour l'analyse antivirus.

• Tâche à la demande

Ce paramètre définit l'étendue d'une acquisition à la demande. Vous pouvez spécifier la taille maximale du fichier à numériser, les extensions de fichier et les chemins à inclure dans la numérisation, ainsi que les extensions de fichier et les chemins à exclure de la numérisation. Les fichiers des sous-répertoires sont analysés par défaut.

Vous utilisez une planification cron pour spécifier quand la tâche s'exécute. Vous pouvez utiliser le `vserver vscan on-demand-task run` commande permettant d'exécuter la tâche immédiatement.

• Profil d'opérations fichier Vscan (analyse sur accès uniquement)

Le `vscan-fileop-profile` paramètre pour le `vserver cifs share create` Définit les opérations de fichier SMB qui déclenchent l'analyse antivirus. Par défaut, le paramètre est défini sur `standard`, Qui est la meilleure pratique de NetApp. Vous pouvez ajuster ce paramètre si nécessaire lors de la création ou de la modification d'un partage SMB :

- `no-scan` spécifie que les analyses antivirus ne sont jamais déclenchées pour le partage.
- `standard` indique que les analyses antivirus sont déclenchées par les opérations ouvrir, fermer et renommer.
- `strict` spécifie que les analyses antivirus sont déclenchées par les opérations d'ouverture, de lecture, de fermeture et de renommage.

Le `strict` le profil offre une sécurité améliorée dans les situations où plusieurs clients accèdent simultanément à un fichier. Si un client ferme un fichier après avoir écrit un virus, et que le même fichier reste ouvert sur un deuxième client, `strict` assure qu'une opération de lecture sur le second client déclenche une analyse avant la fermeture du fichier.

Veillez à restreindre le `strict`` le profil des partages contenant des fichiers que vous prévoyez sera accessible simultanément. Étant donné que ce profil génère davantage de demandes d'analyse, il peut avoir un impact sur les performances.

- `writes-only` spécifie que les analyses de virus ne sont déclenchées que lorsque les fichiers modifiés sont fermés.

Depuis `writes-only` génère moins de demandes d'analyse, ce qui améliore généralement les performances.

Si vous utilisez ce profil, le scanner doit être configuré pour supprimer ou mettre en quarantaine les fichiers infectés irréparables, afin qu'ils ne soient pas accessibles. Si, par exemple, un client ferme un fichier après l'écriture d'un virus, et que le fichier n'est pas réparé, supprimé ou mis en quarantaine, tout client qui accède au fichier `without écrire` à elle sera infecté.



Si une application client effectue une opération de renommage, le fichier est fermé avec le nouveau nom et n'est pas analysé. Si de telles opérations posent un problème de sécurité dans votre environnement, vous devez utiliser le `standard` ou `strict` profil.

Solutions partenaires Vscan

NetApp collabore avec Trellix, Symantec, Trend micro et Sentinel One afin de proposer des solutions anti-malware et anti-virus de pointe basées sur la technologie ONTAP Vscan. Ces solutions vous aident à rechercher des programmes malveillants dans les fichiers et à corriger les fichiers affectés.

Comme le montre le tableau ci-dessous, les informations d'interopérabilité pour Trellix, Symantec et Trend micro sont conservées dans la matrice d'interopérabilité NetApp. Les détails sur l'interopérabilité de Trellix et Symantec sont également disponibles sur les sites Web des partenaires. Les informations d'interopérabilité pour Sentinel One et les autres nouveaux partenaires seront conservées par le partenaire sur son site Web.

En tant que partenaire	Documentation de la solution	Détails sur l'interopérabilité
Trellix (anciennement McAfee)	"Documentation produit Trellix"	<ul style="list-style-type: none">• "Matrice d'interopérabilité NetApp"• "Plates-formes prises en charge pour la protection du stockage Endpoint Security (trellix.com)"
Symantec	"Symantec protection Engine 9.0.0"	<ul style="list-style-type: none">• "Matrice d'interopérabilité NetApp"• "Matrice de prise en charge des périphériques partenaires certifiés avec Symantec protection Engine (SPE) pour le stockage en réseau (NAS) 9.x.x."• "Matrice de prise en charge des périphériques partenaires certifiés avec Symantec protection Engine (SPE) pour le stockage en réseau (NAS) 8.x (broadcom.com)"

En tant que partenaire	Documentation de la solution	Détails sur l'interopérabilité
Trend micro	"Guide de démarrage de Trend micro ServerProtect for Storage 6.0"	"Matrice d'interopérabilité NetApp"
Sentinel One	<ul style="list-style-type: none"> • "Sécurité des données du cloud de singularité de SentinelOne" • "Assistance SentinelOne" <p>Ce lien requiert une connexion utilisateur. Vous pouvez demander l'accès à Sentinel One.</p>	Instinct profond

Installation et configuration du serveur Vscan

Installation et configuration du serveur Vscan

Configurez un ou plusieurs serveurs Vscan pour vous assurer que les fichiers de votre système sont analysés pour détecter d'éventuels virus. Suivez les instructions fournies par votre fournisseur pour installer et configurer le logiciel antivirus sur le serveur.

Suivez les instructions du fichier README fourni par NetApp pour installer et configurer ONTAP antivirus Connector. Vous pouvez également suivre les instructions du ["Installez la page ONTAP antivirus Connector"](#).



Pour les configurations de reprise après incident et MetroCluster, vous devez installer et configurer des serveurs Vscan distincts pour les clusters ONTAP principal/local et secondaire/partenaire.

Configuration logicielle requise pour l'antivirus

- Pour plus d'informations sur la configuration requise pour le logiciel antivirus, reportez-vous à la documentation du fournisseur.
- Pour plus d'informations sur les fournisseurs, les logiciels et les versions pris en charge par Vscan, rendez-vous ["Solutions partenaires Vscan"](#) sur la page.

Conditions requises pour ONTAP antivirus Connector

- Vous pouvez télécharger ONTAP antivirus Connector à partir de la page **Téléchargement de logiciels** du site de support NetApp. ["Téléchargements NetApp : logiciels"](#)
- Pour plus d'informations sur les versions de Windows prises en charge par le connecteur antivirus ONTAP et sur les conditions d'interopérabilité, voir ["Solutions partenaires Vscan"](#).



Vous pouvez installer différentes versions de serveurs Windows pour différents serveurs Vscan dans un cluster.

- .NET 3.0 ou version ultérieure doit être installé sur le serveur Windows.
- SMB 2.0 doit être activé sur le serveur Windows.

Installez ONTAP antivirus Connector

Installer le ONTAP antivirus Connector sur le serveur Vscan pour permettre la communication entre le système exécutant ONTAP et le serveur Vscan. Une fois ONTAP antivirus Connector installé, le logiciel antivirus peut communiquer avec un ou plusieurs SVM.

Description de la tâche

- Reportez-vous "[Solutions partenaires Vscan](#)" à la page pour obtenir des informations sur les protocoles pris en charge, les versions de logiciels des fournisseurs antivirus, les versions de ONTAP, les exigences d'interopérabilité et les serveurs Windows.
- .NET 4.5.1 ou version ultérieure doit être installé.
- ONTAP antivirus Connector peut s'exécuter sur une machine virtuelle. Toutefois, pour de meilleures performances, NetApp recommande l'utilisation d'une machine virtuelle dédiée à l'analyse antivirus.
- SMB 2.0 doit être activé sur le serveur Windows sur lequel vous installez et exécutez ONTAP antivirus Connector.

Avant de commencer

- Téléchargez le fichier d'installation de ONTAP antivirus Connector à partir du site de support et enregistrez-le dans un répertoire de votre disque dur.
- Vérifiez que vous répondez aux exigences requises pour installer ONTAP antivirus Connector.
- Vérifiez que vous disposez des privilèges d'administrateur pour installer l'antivirus Connector.

Étapes

1. Démarrez l'assistant d'installation de l'antivirus Connector en exécutant le fichier d'installation approprié.
2. Sélectionnez *Suivant*. La boîte de dialogue dossier de destination s'ouvre.
3. Sélectionnez *Next* pour installer l'antivirus Connector dans le dossier qui est répertorié ou sélectionnez *change* pour l'installer dans un autre dossier.
4. La boîte de dialogue informations d'identification du service Windows du connecteur AV ONTAP s'ouvre.
5. Entrez vos informations d'identification de service Windows ou sélectionnez **Ajouter** pour sélectionner un utilisateur. Pour un système ONTAP, cet utilisateur doit être un utilisateur de domaine valide et doit exister dans la configuration scanner pool de la SVM.
6. Sélectionnez **Suivant**. La boîte de dialogue prêt à installer le programme s'ouvre.
7. Sélectionnez **installer** pour commencer l'installation ou sélectionnez **Précédent** si vous souhaitez modifier les paramètres.
Une boîte de dialogue d'état s'ouvre et indique la progression de l'installation, suivie de la boîte de dialogue Assistant InstallShield terminé.
8. Cochez la case configurer les LIFs ONTAP si vous souhaitez poursuivre la configuration des LIFs de données ou de gestion ONTAP.
Vous devez configurer au moins une LIF de données ou de gestion ONTAP avant d'utiliser ce serveur Vscan.
9. Cochez la case Afficher le journal **Windows installer** si vous souhaitez afficher les journaux d'installation.
10. Sélectionnez **Terminer** pour terminer l'installation et fermer l'assistant InstallShield.
L'icône **Configurer ONTAP LIFs** est enregistrée sur le bureau pour configurer les LIFs ONTAP.
11. Ajouter un SVM au antivirus Connector.
Vous pouvez ajouter un SVM à l'antivirus Connector en ajoutant une LIF de gestion ONTAP, interrogée sur

la liste des LIFs de données, ou en configurant directement la LIF de données.
Si la LIF de gestion ONTAP est configurée, vous devez également fournir les informations d'interrogation et les informations d'identification du compte admin ONTAP.

- Vérifier que la LIF de management ou l'adresse IP du SVM est Enabled for management-https. Cela n'est pas nécessaire lorsque vous configurez uniquement les LIFs de données.
- Vérifiez que vous avez créé un compte d'utilisateur pour l'application HTTP et que vous avez attribué un rôle ayant (au moins en lecture seule) accès au système /api/network/ip/interfaces API REST.
Pour plus d'informations sur la création d'un utilisateur, reportez-vous à la section "[création d'un rôle de connexion de sécurité](#)" et "[création d'une connexion de sécurité](#)" Pages de manuel ONTAP.



Vous pouvez également utiliser l'utilisateur du domaine en tant que compte en ajoutant un SVM de tunnel d'authentification pour une SVM d'administration. Pour plus d'informations, reportez-vous à la section "[connexion de sécurité domaine-tunnel créer](#)" ONTAP ou utilisez /api/security/accounts et /api/security/roles API REST pour configurer le compte et le rôle admin

Étapes

1. Cliquez avec le bouton droit de la souris sur l'icône **configurer ONTAP LIFs**, qui a été enregistrée sur votre bureau lorsque vous avez terminé l'installation du connecteur antivirus, puis sélectionnez **Exécuter en tant qu'administrateur**.
2. Dans la boîte de dialogue Configure ONTAP LIFs, sélectionnez le type de configuration préféré, puis effectuez les actions suivantes :

Pour créer ce type de LIF...	Procédez comme suit...
LIF de données	<div>a. Définissez « rôle » sur « données ».</div> <div>b. Définissez « protocole de données » sur « cifs ».</div> <div>c. Définissez la « politique de pare-feu » sur « données ».</div> <div>d. Définissez « stratégie de service » sur « fichiers-données-par-défaut ».</div>
LIF de management	<div>a. Définir « rôle* » sur « données »</div> <div>b. Définissez « protocole de données » sur « aucun ».</div> <div>c. Définissez la « politique de pare-feu » sur « gestion ».</div> <div>d. Définissez « stratégie de service » sur « gestion par défaut ».</div>

En savoir plus sur "[Création d'une LIF](#)".

Après avoir créé une LIF, entrer la LIF de données ou de gestion ou l'adresse IP du SVM que vous souhaitez ajouter. Vous pouvez également entrer dans la LIF de cluster management. Si vous spécifiez la LIF de cluster management, tous les SVM au sein de ce cluster qui servent SMB peuvent utiliser le serveur Vscan.



Lorsque l'authentification Kerberos est requise pour les serveurs Vscan, chaque LIF de données du SVM doit avoir un nom DNS unique, et vous devez enregistrer ce nom en tant que nom principal du serveur (SPN) avec Windows Active Directory. Lorsqu'un nom DNS unique n'est pas disponible pour chaque LIF de données ou enregistré en tant que SPN, le serveur Vscan utilise le mécanisme NT LAN Manager pour l'authentification. Si vous ajoutez ou modifiez les noms DNS et les SPN après la connexion du serveur Vscan, vous devez redémarrer le service antivirus Connector sur le serveur Vscan pour appliquer les modifications.

3. Pour configurer une LIF de gestion, entrez la durée d'interrogation en secondes. La durée de l'interrogation est la fréquence à laquelle l'antivirus Connector recherche des modifications des SVM ou de la configuration LIF du cluster. L'intervalle d'interrogation par défaut est de 60 secondes.
4. Entrez le nom et le mot de passe du compte admin ONTAP pour configurer une LIF de gestion.
5. Cliquez sur **Test** pour vérifier la connectivité et l'authentification. L'authentification est uniquement vérifiée pour une configuration LIF de management.
6. Cliquez sur **mettre à jour** pour ajouter la LIF à la liste des LIFs à interroger ou à se connecter.
7. Cliquez sur **Enregistrer** pour enregistrer la connexion au registre.
8. Cliquez sur **Exporter** si vous souhaitez exporter la liste des connexions vers un fichier d'importation de registre ou d'exportation de registre. Ceci est utile si plusieurs serveurs Vscan utilisent le même ensemble de LIFs de gestion ou de données.

Voir la "[Configurez la page ONTAP antivirus Connector](#)" pour les options de configuration.

Configurer ONTAP antivirus Connector

Configurer ONTAP antivirus Connector pour spécifier un ou plusieurs SVM (Storage Virtual machines) auxquels vous souhaitez vous connecter en entrant dans la LIF de gestion ONTAP, en interrogeant qu'information et les informations d'identification du compte d'administrateur ONTAP, ou simplement dans la LIF de données. Vous pouvez également modifier les détails d'une connexion SVM ou supprimer une connexion SVM. Par défaut, ONTAP antivirus Connector utilise les API REST pour récupérer la liste des LIFs de données si le LIF de management ONTAP est configuré.

Modifier le détail d'une connexion SVM

Vous pouvez mettre à jour les détails d'une connexion SVM (Storage Virtual machine), qui a été ajoutée à l'antivirus Connector, en modifiant la LIF de gestion ONTAP et les informations d'interrogation. Une fois ajoutées, les LIF de données ne peuvent pas être mises à jour. Pour mettre à jour les LIF de données, vous devez d'abord les supprimer, puis les ajouter de nouveau avec la nouvelle LIF ou adresse IP.

Avant de commencer

Vérifiez que vous avez créé un compte d'utilisateur pour l'application HTTP et que vous avez attribué un rôle ayant (au moins en lecture seule) accès au système `/api/network/ip/interfaces` API REST. Pour plus d'informations sur la création d'un utilisateur, reportez-vous à la section "[création d'un rôle de connexion de sécurité](#)" et le "[création d'une connexion de sécurité](#)" commandes.

Vous pouvez également utiliser l'utilisateur du domaine en tant que compte en ajoutant un SVM de tunnel d'authentification pour une SVM d'administration.

Pour plus d'informations, reportez-vous à la section "[connexion de sécurité domaine-tunnel créer](#)" Page de manuel ONTAP.

Étapes

1. Cliquez avec le bouton droit de la souris sur l'icône **configurer ONTAP LIFs**, qui a été enregistrée sur votre bureau lorsque vous avez terminé l'installation du connecteur antivirus, puis sélectionnez **Exécuter en tant qu'administrateur**. La boîte de dialogue Configure ONTAP LIFs s'ouvre.
2. Sélectionner l'adresse IP du SVM, puis cliquer sur **Update**.
3. Mettez à jour les informations, si nécessaire.
4. Cliquez sur **Enregistrer** pour mettre à jour les détails de la connexion dans le registre.
5. Cliquez sur **Exporter** si vous souhaitez exporter la liste des connexions vers une importation de registre ou un fichier d'exportation de registre.
Ceci est utile si plusieurs serveurs Vscan utilisent le même ensemble de LIFs de gestion ou de données.

Retirer une connexion SVM du connecteur antivirus

Si vous n'avez plus besoin d'une connexion SVM, vous pouvez la supprimer.

Étapes

1. Cliquez avec le bouton droit de la souris sur l'icône **configurer ONTAP LIFs**, qui a été enregistrée sur votre bureau lorsque vous avez terminé l'installation du connecteur antivirus, puis sélectionnez **Exécuter en tant qu'administrateur**. La boîte de dialogue Configure ONTAP LIFs s'ouvre.
2. Sélectionner une ou plusieurs adresses IP de SVM, puis cliquer sur **Supprimer**.
3. Cliquez sur **Enregistrer** pour mettre à jour les détails de la connexion dans le registre.
4. Cliquez sur **Exporter** si vous souhaitez exporter la liste des connexions vers un fichier d'importation de registre ou d'exportation de registre.
Ceci est utile si plusieurs serveurs Vscan utilisent le même ensemble de LIFs de gestion ou de données.

Résoudre les problèmes

Avant de commencer

Lorsque vous créez des valeurs de registre dans cette procédure, utilisez le volet droit.

Vous pouvez activer ou désactiver les journaux antivirus Connector à des fins de diagnostic. Par défaut, ces journaux sont désactivés. Pour améliorer les performances, vous devez conserver les journaux du connecteur antivirus désactivés et les activer uniquement pour les événements critiques.

Étapes

1. Sélectionnez **Démarrer**, tapez "regedit" dans la zone de recherche, puis sélectionnez `regedit.exe` Dans la liste programmes.
2. Dans **Éditeur du Registre**, localisez la sous-clé suivante pour ONTAP antivirus Connector :
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Créez des valeurs de registre en fournissant le type, le nom et les valeurs indiqués dans le tableau suivant :

Type	Nom	Valeurs
Chaîne	Chemin de traçabilité	c:\avshim.log

Cette valeur de registre peut être n'importe quel autre chemin valide.

4. Créez une autre valeur de registre en fournissant le type, le nom, les valeurs et les informations de journalisation indiquées dans le tableau suivant :

Type	Nom	Journalisation critique	Journalisation intermédiaire	Journalisation détaillée
DWORD	TRACELEVEL	1	2 ou 3	4

Cela active les journaux antivirus Connector qui sont enregistrés à la valeur de chemin fournie dans TracePath à l'étape 3.

5. Désactivez les journaux du connecteur antivirus en supprimant les valeurs de registre que vous avez créées aux étapes 3 et 4.
6. Créez une autre valeur de registre de type "MULTI_SZ" avec le nom "LogRotation" (sans guillemets). Dans « LogRotation », Indiquez « logFileSize:1 » comme entrée pour la taille de rotation (où 1 représente 1 Mo) et dans la ligne suivante, indiquez « logFileCount:5 » comme entrée pour la limite de rotation (5 est la limite).



Ces valeurs sont facultatives. Si elles ne sont pas fournies, les valeurs par défaut des fichiers 20 Mo et 10 sont utilisées respectivement pour la taille de rotation et la limite de rotation. Les valeurs entières fournies ne fournissent pas de valeurs décimales ou de fraction. Si vous indiquez des valeurs supérieures aux valeurs par défaut, les valeurs par défaut sont utilisées à la place.

7. Pour désactiver la rotation du journal configurée par l'utilisateur, supprimez les valeurs de registre que vous avez créées à l'étape 6.

Bannière personnalisable

Une bannière personnalisée vous permet de placer une déclaration juridiquement contraignante et une clause de non-responsabilité d'accès au système dans la fenêtre *Configure ONTAP LIF API*.

Étape

1. Modifiez la bannière par défaut en mettant à jour le contenu de l' `banner.txt` dans le répertoire d'installation, puis en enregistrant les modifications.
Vous devez rouvrir la fenêtre configurer l'API LIF ONTAP pour voir les modifications reflétées dans la bannière.

Activer le mode Eo (Extended Ordinance)

Vous pouvez activer et désactiver le mode Extended Ordinance (EO) pour un fonctionnement sécurisé.

Étapes

1. Sélectionnez **Démarrer**, tapez "regedit" dans la zone de recherche, puis sélectionnez `regedit.exe` Dans la liste programmes.
2. Dans **Éditeur du Registre**, localisez la sous-clé suivante pour ONTAP antivirus Connector :
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Dans le volet de droite, créez une nouvelle valeur de registre de type "DWORD" avec le nom "EO_mode" (sans guillemets) et la valeur "1" (sans guillemets) pour activer le mode EO ou la valeur "0" (sans

guillemets) pour désactiver le mode EO.



Par défaut, si l' `EO_Mode` L'entrée de registre est absente, le mode EO est désactivé. Lorsque vous activez le mode EO, vous devez configurer à la fois le serveur syslog externe et l'authentification mutuelle des certificats.

Configurez le serveur syslog externe

Avant de commencer

Notez que lorsque vous créez des valeurs de registre dans cette procédure, utilisez le volet de droite.

Étapes

1. Sélectionnez **Démarrer**, tapez "regedit" dans la zone de recherche, puis sélectionnez `regedit.exe` Dans la liste programmes.
2. Dans **Éditeur du Registre**, créez la sous-clé suivante pour ONTAP antivirus Connector pour la configuration syslog :
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. Créez une valeur de registre en fournissant le type, le nom et la valeur, comme indiqué dans le tableau suivant :

Type	Nom	Valeur
DWORD	syslog_enabled	1 ou 0

Veuillez noter qu'une valeur « 1 » active le syslog et qu'une valeur « 0 » le désactive.

4. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom
REG_SZ	Hôte_syslog

Indiquez l'adresse IP ou le nom de domaine de l'hôte syslog pour le champ valeur.

5. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom
REG_SZ	Syslog_port

Indiquez le numéro de port sur lequel le serveur syslog s'exécute dans le champ valeur.

6. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom
REG_SZ	Protocole_syslog

Saisissez le protocole utilisé sur le serveur syslog, soit « tcp », soit « udp », dans le champ valeur.

7. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom	JOURNAL_CRI T	LOG_NOTICE	INFO_JOURNA L	LOG_DEBUG
DWORD	Syslog_level	2	5	6	7

8. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom	Valeur
DWORD	syslog_tls	1 ou 0

Notez qu'une valeur « 1 » active syslog avec TLS (transport Layer Security) et une valeur « 0 » désactive syslog avec TLS.

Assurez-vous qu'un serveur syslog externe configuré fonctionne correctement

- Si la clé est absente ou a une valeur nulle :
 - Le protocole par défaut est « tcp ».
 - Le port par défaut est "514" pour "tcp/udp" et par défaut "6514" pour TLS.
 - Par défaut, le niveau syslog est 5 (LOG_NOTICE).
- Vous pouvez confirmer que syslog est activé en vérifiant que le système `syslog_enabled` la valeur est « 1 ». Lorsque le `syslog_enabled` La valeur est "1", vous devriez pouvoir vous connecter au serveur distant configuré, que le mode EO soit activé ou non.
- Si le mode EO est réglé sur « 1 » et que vous modifiez le `syslog_enabled` valeur comprise entre « 1 » et « 0 », ce qui suit s'applique :
 - Vous ne pouvez pas démarrer le service si syslog n'est pas activé en mode EO.
 - Si le système fonctionne dans un état stable, un avertissement s'affiche indiquant que syslog ne peut pas être désactivé en mode EO et que syslog est fermement défini sur « 1 », que vous pouvez voir dans le registre. Si cela se produit, vous devez d'abord désactiver le mode EO, puis désactiver syslog.
- Si le serveur syslog ne peut pas fonctionner correctement lorsque le mode EO et syslog sont activés, le service s'arrête. Ceci peut se produire pour l'une des raisons suivantes :
 - Un hôte `syslog_non` valide ou non configuré.
 - Un protocole non valide, hormis UDP ou TCP, est configuré.
 - Un numéro de port n'est pas valide.
- Dans le cas d'une configuration TCP ou TLS sur TCP, si le serveur n'écoute pas le port IP, la connexion échoue et le service s'arrête.

Configurer l'authentification de certificat mutuel X.509

L'authentification mutuelle basée sur certificat X.509 est possible pour la communication SSL (Secure Sockets Layer) entre l'antivirus Connector et ONTAP dans le chemin de gestion. Si le mode EO est activé et que le certificat n'est pas trouvé, le connecteur AV se termine. Effectuez la procédure suivante sur l'antivirus Connector :

Étapes

1. Le connecteur antivirus recherche le certificat client du connecteur antivirus et le certificat de l'autorité de certification du serveur NetApp dans le chemin d'accès au répertoire à partir duquel le connecteur antivirus exécute le répertoire d'installation. Copiez les certificats dans ce chemin de répertoire fixe.
2. Intégrez le certificat client et sa clé privée au format PKCS12 et nommez-le « AV_client.P12 ».
3. Assurez-vous que le certificat de l'autorité de certification (ainsi que toute autorité de signature intermédiaire jusqu'à l'autorité de certification racine) utilisé pour signer le certificat du serveur NetApp est au format PEM (Privacy Enhanced Mail) et nommé ONTAP_CA.pem. Placez-le dans le répertoire d'installation de l'antivirus Connector. Sur le système NetApp ONTAP, installez le certificat de l'autorité de certification (ainsi que toute autorité de signature intermédiaire jusqu'à l'autorité de certification racine) utilisé pour signer le certificat client pour le connecteur antivirus à « ONTAP » en tant que certificat de type « client-ca ».

Configurer les scanner pool

Présentation de la configuration des scanner pool

Un scanner pool définit les serveurs Vscan et les utilisateurs privilégiés qui peuvent se connecter aux SVM. Une politique scanner détermine si un pool de scanner est actif.



Si vous utilisez une export policy sur un serveur SMB, vous devez ajouter chaque serveur Vscan à la export policy.

Créer un pool de scanner sur un seul cluster

Un scanner pool définit les serveurs Vscan et les utilisateurs privilégiés qui peuvent se connecter aux SVM. On peut créer un pool de scanner pour un SVM individuel ou pour tous les SVM d'un cluster.

Ce dont vous avez besoin

- Les SVM et les serveurs Vscan doivent se trouver dans le même domaine ou dans des domaines de confiance.
- Pour les scanner-pool définis pour un SVM individuel, vous devez avoir configuré ONTAP antivirus Connector avec la LIF de management du SVM ou la LIF de donnée du SVM.
- Pour les scanner-pool définis pour tous les SVM d'un cluster, vous devez avoir configuré ONTAP antivirus Connector avec la LIF cluster management.
- La liste des utilisateurs privilégiés doit inclure le compte d'utilisateur de domaine que le serveur Vscan utilise pour se connecter à la SVM.
- Une fois le scanner pool configuré, vérifiez l'état de la connexion aux serveurs.

Étapes

1. Créer un pool de scanner :

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users privileged_users
```

- Spécifier un SVM de données pour un pool défini pour un SVM individuel et spécifier un SVM d'administration du cluster pour un pool défini pour tous les SVM d'un cluster.

- Spécifiez une adresse IP ou un FQDN pour chaque nom d'hôte de serveur Vscan.
- Spécifiez le domaine et le nom d'utilisateur pour chaque utilisateur privilégié.
Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante crée un pool de scanner nommé SP sur le vs1 SVM :

```
cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
cifs\u1,cifs\u2
```

2. Vérifiez que le scanner pool a été créé :

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool
```

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante affiche les détails de SP scanner pool :

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                Vserver: vs1
                                Scanner Pool: SP
                                Applied Policy: idle
                                Current Status: off
                                Cluster on Which Policy Is Applied: -
                                Scanner Pool Config Owner: vserver
                                List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
                                List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
                                27.fsct.nb
                                List of Privileged Users: cifs\u1, cifs\u2
```

Vous pouvez également utiliser le `vserver vscan scanner-pool show` Commande pour afficher tous les scanner pool d'un SVM. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Créer des pools de scanner dans les configurations MetroCluster

Il faut créer des pools de scanner primaires et secondaires sur chaque cluster dans une configuration MetroCluster, ce qui correspond aux SVM principal et secondaire sur le cluster.

Ce dont vous avez besoin

- Les SVM et les serveurs Vscan doivent se trouver dans le même domaine ou dans des domaines de confiance.

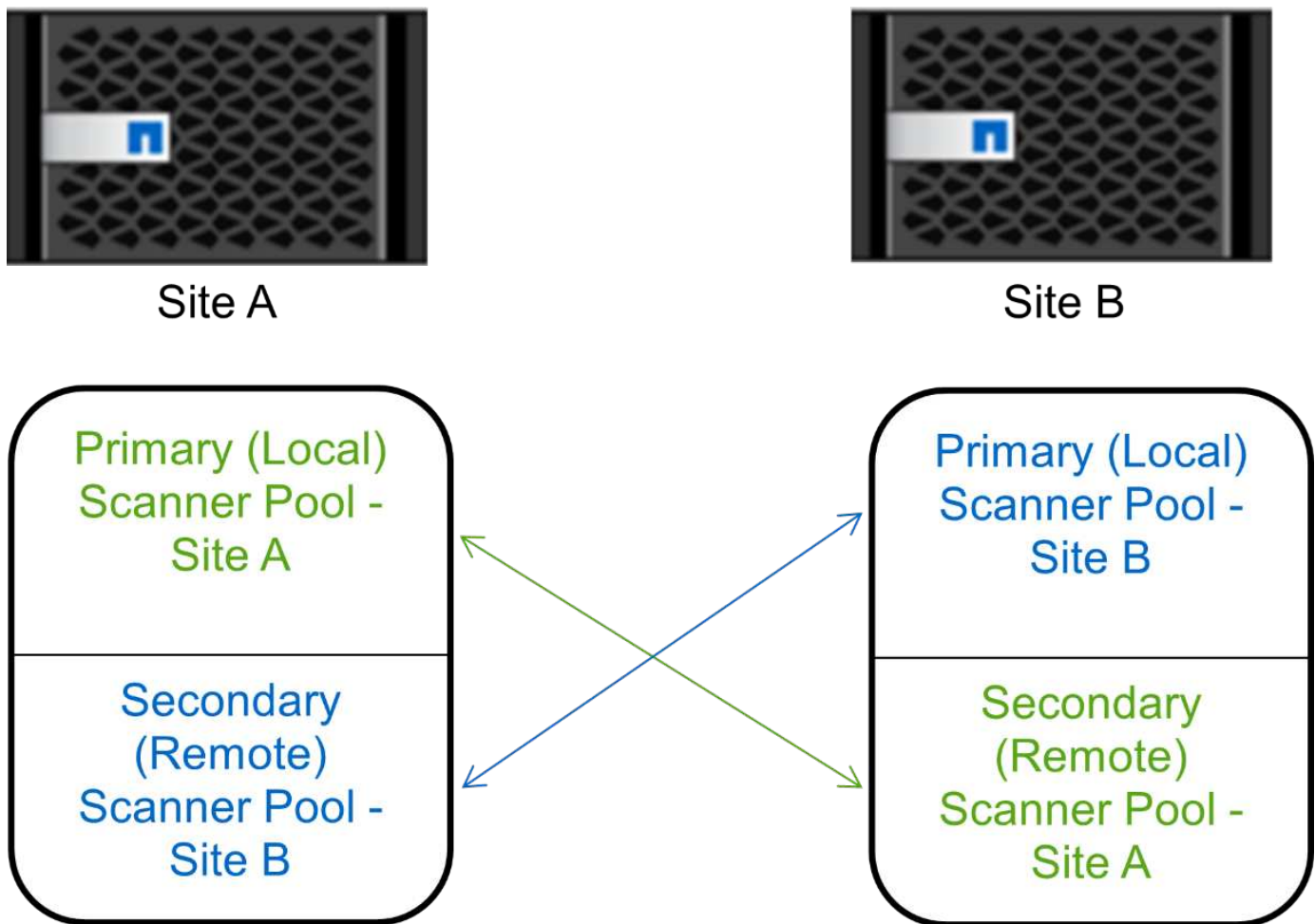
- Pour les scanner-pool définis pour un SVM individuel, vous devez avoir configuré ONTAP antivirus Connector avec la LIF de management du SVM ou la LIF de donnée du SVM.
- Pour les scanner-pool définis pour tous les SVM d'un cluster, vous devez avoir configuré ONTAP antivirus Connector avec la LIF cluster management.
- La liste des utilisateurs privilégiés doit inclure le compte d'utilisateur de domaine que le serveur Vscan utilise pour se connecter à la SVM.
- Une fois le scanner pool configuré, vérifiez l'état de la connexion aux serveurs.

Description de la tâche

Les configurations MetroCluster protègent les données grâce à la mise en œuvre de deux clusters en miroir séparés physiquement. Chaque cluster réplique de manière synchrone les données et la configuration SVM de l'autre. Un SVM principal sur le cluster local diffuse des données lorsque le cluster est en ligne. Un SVM secondaire situé sur le cluster local transmet des données lorsque le cluster distant est hors ligne.

Cela signifie que vous devez créer des scanner pools principal et secondaire sur chaque cluster d'une configuration MetroCluster. Le pool secondaire devient actif lorsque le cluster commence à transmettre des données depuis le SVM secondaire. Pour la reprise sur incident, la configuration est similaire à celle de MetroCluster.

Cette figure présente une configuration MetroCluster/DR classique.



Étapes

1. Créer un pool de scanner :

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner  
-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users  
privileged_users
```

- Spécifier un SVM de données pour un pool défini pour un SVM individuel et spécifier un SVM d'administration du cluster pour un pool défini pour tous les SVM d'un cluster.
- Spécifiez une adresse IP ou un FQDN pour chaque nom d'hôte de serveur Vscan.
- Spécifiez le domaine et le nom d'utilisateur pour chaque utilisateur privilégié.



On doit créer tous les scanner pool depuis le cluster contenant le SVM principal.

Pour obtenir la liste complète des options, consultez la page man de la commande.

Les commandes suivantes créent des scanner pool principal et secondaire sur chaque cluster en configuration MetroCluster :

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -  
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs  
\u1,cifs\u2
```

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -  
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs  
\u1,cifs\u2
```

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -  
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs  
\u1,cifs\u2
```

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -  
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs  
\u1,cifs\u2
```

2. Vérifiez que les scanner pool ont été créés :

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner  
-pool scanner_pool
```

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante affiche les détails du scanner pool `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

Vserver: cifssvm1
Scanner Pool: pool1_for_site1
Applied Policy: idle
Current Status: off
Cluster on Which Policy Is Applied: -
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
List of Privileged Users: cifs\u1,cifs\u2
```

Vous pouvez également utiliser le `vserver vscan scanner-pool show` Commande pour afficher tous les scanner pool d'un SVM. Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

Appliquer une politique scanner sur un seul cluster

Une politique scanner détermine si un pool de scanner est actif. On doit activer un scanner pool avant que les serveurs Vscan qu'il définit puissent se connecter à une SVM.

Description de la tâche

- Vous ne pouvez appliquer qu'une seule politique scanner à un pool de scanner.
- Si vous avez créé un pool de scanner pour tous les SVM d'un cluster, vous devez appliquer une scanner policy sur chaque SVM individuellement.

Étapes

1. Appliquer une politique scanner :

```
vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
scanner_pool -scanner-policy primary|secondary|idle -cluster
cluster_to_apply_policy_on
```

Une politique scanner peut avoir l'une des valeurs suivantes :

- `Primary` indique que le pool de scanner est actif.
- `Secondary` Spécifie que le pool de scanner est actif uniquement si aucun des serveurs Vscan du pool de scanner principal n'est connecté.
- `Idle` indique que le pool de scanner est inactif.

L'exemple suivant montre que le pool de scanner est nommé `SP` sur le `vs1` Le SVM est actif :

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
-scanner-pool SP -scanner-policy primary
```

2. Vérifiez que le pool de scanner est actif :

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner  
-pool scanner_pool
```

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante affiche les détails de SP scanner pool :

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool  
SP  
  
Vserver: vs1  
Scanner Pool: SP  
Applied Policy: primary  
Current Status: on  
Cluster on Which Policy Is Applied: cluster1  
Scanner Pool Config Owner: vserver  
List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27  
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-  
27.fsct.nb  
List of Privileged Users: cifs\u1, cifs\u2
```

Vous pouvez utiliser le `vserver vscan scanner-pool show-active` Commande pour afficher les scanner pool actifs sur un SVM. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man de la commande.

Appliquez les politiques de scanner dans les configurations MetroCluster

Une politique scanner détermine si un pool de scanner est actif. Vous devez appliquer une scanner policy aux scanner pool principal et secondaire sur chaque cluster dans une configuration MetroCluster.

Description de la tâche

- Vous ne pouvez appliquer qu'une seule politique scanner à un pool de scanner.
- Si vous avez créé un pool de scanner pour tous les SVM d'un cluster, vous devez appliquer une scanner policy sur chaque SVM individuellement.
- Pour les configurations MetroCluster et de reprise après incident, vous devez appliquer une stratégie scanner à chaque pool de scanner du cluster local et distant.
- Dans la règle que vous créez pour le cluster local, vous devez spécifier le cluster local dans le `cluster` paramètre. Dans la stratégie que vous créez pour le cluster distant, vous devez spécifier le cluster distant dans `cluster` paramètre. Le cluster distant peut alors prendre le contrôle des opérations d'analyse antivirus en cas d'incident.

Étapes

1. Appliquer une politique scanner :

```
vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool  
scanner_pool -scanner-policy primary|secondary|idle -cluster  
cluster_to_apply_policy_on
```

Une politique scanner peut avoir l'une des valeurs suivantes :

- ° Primary indique que le pool de scanner est actif.
- ° Secondary Spécifie que le pool de scanner est actif uniquement si aucun des serveurs Vscan du pool de scanner principal n'est connecté.
- ° Idle indique que le pool de scanner est inactif.



Vous devez appliquer toutes les scanner policy à partir du cluster qui contient la SVM principale.

Les commandes suivantes appliquent des scanner policy aux scanner pool principal et secondaire sur chaque cluster de la configuration MetroCluster :

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1  
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1  
  
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1  
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster  
cluster1  
  
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1  
-scanner-pool pool2_for_site2 -scanner-policy primary -cluster cluster2  
  
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1  
-scanner-pool pool1_for_site2 -scanner-policy secondary -cluster  
cluster2
```

2. Vérifiez que le pool de scanner est actif :

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner  
-pool scanner_pool
```

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante affiche les détails du scanner pool pool1:


```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1
```

```

Vserver: cifssvm1
Scanner Pool: pool1_for_site1
Applied Policy: primary
Current Status: on
Cluster on Which Policy Is Applied: cluster1
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
List of Privileged Users: cifs\u1,cifs\u2
```

Vous pouvez utiliser le `vserver vscan scanner-pool show-active` Commande pour afficher les scanner pool actifs sur un SVM. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Commandes pour la gestion des scanner pool

Vous pouvez modifier et supprimer des pools de scanner et gérer des utilisateurs privilégiés et des serveurs Vscan pour un pool de scanner. Vous pouvez également afficher des informations récapitulatives sur le pool de scanner.

Les fonctions que vous recherchez...	Saisissez la commande suivante...
Modifier un pool de scanner	<code>vserver vscan scanner-pool modify</code>
Supprimer un pool de scanner	<code>vserver vscan scanner-pool delete</code>
Ajouter des utilisateurs privilégiés à un pool de scanner	<code>vserver vscan scanner-pool privileged-users add</code>
Supprimer des utilisateurs privilégiés d'un pool de scanner	<code>vserver vscan scanner-pool privileged-users remove</code>
Ajout de serveurs Vscan à un pool de scanner	<code>vserver vscan scanner-pool servers add</code>
Supprimer les serveurs Vscan d'un pool de scanner	<code>vserver vscan scanner-pool servers remove</code>
Afficher le résumé et les détails d'un pool de scanner	<code>vserver vscan scanner-pool show</code>
Afficher les utilisateurs privilégiés d'un pool de scanner	<code>vserver vscan scanner-pool privileged-users show</code>

Afficher les serveurs Vscan pour tous les pools de scanner	<code>vserver vscan scanner-pool servers show</code>
--	--

Pour plus d'informations sur ces commandes, consultez les pages de manuels.

Configurer la numérisation à l'accès

Création d'une règle on-Access

Une règle On-Access définit l'étendue d'une analyse on-Access. On peut créer une on-Access policy pour un SVM individuel ou pour tous les SVM d'un cluster. Si vous avez créé une on-Access policy pour tous les SVM d'un cluster, vous devez activer la politique sur chaque SVM individuellement.

Description de la tâche

- Vous pouvez spécifier la taille maximale du fichier à numériser, les extensions de fichier et les chemins à inclure dans la numérisation, ainsi que les extensions de fichier et les chemins à exclure de la numérisation.
- Vous pouvez définir le `scan-mandatory` Option désactivée pour spécifier que l'accès aux fichiers est autorisé lorsqu'aucun serveur Vscan n'est disponible pour l'analyse antivirus.
- Par défaut, ONTAP crée une on-Access policy nommée « `default_CIFS` » et l'active pour tous les SVM d'un cluster.
- Tout fichier admissible à l'exclusion de numérisation en fonction du `paths-to-exclude`, `file-ext-to-exclude`, ou `max-file-size` les paramètres ne sont pas pris en compte pour l'acquisition, même si l' `scan-mandatory` l'option est activée. (Cochez cette case "[dépannage](#)" pour les problèmes de connectivité liés au `scan-mandatory` option.)
- Par défaut, seuls les volumes en lecture-écriture sont analysés. Vous pouvez spécifier des filtres qui permettent la numérisation de volumes en lecture seule ou qui limitent la numérisation aux fichiers ouverts avec l'accès d'exécution.
- L'analyse antivirus n'est pas effectuée sur un partage SMB pour lequel le paramètre disponible en continu est défini sur Oui.
- Voir la "[Architecture antivirus](#)" Pour plus d'informations sur le profil *Vscan file-Operations*.
- Vous pouvez créer un maximum de dix (10) règles d'accès par SVM. Toutefois, vous ne pouvez activer qu'une seule stratégie d'accès à la fois.
 - Vous pouvez exclure un maximum de cent (100) chemins et extensions de fichiers de l'analyse antivirus dans une stratégie d'accès.
- Quelques recommandations d'exclusion de fichiers :
 - Pensez à exclure les fichiers volumineux (la taille de fichier peut être spécifiée) de l'analyse antivirus car ils peuvent entraîner un temps de réponse lent ou des délais de requête d'analyse pour les utilisateurs CIFS. La taille de fichier par défaut pour l'exclusion est de 2 Go.
 - Pensez à exclure les extensions de fichier telles que `.vhd` et `.tmp` car les fichiers avec ces extensions peuvent ne pas être appropriés pour la numérisation.
 - Pensez à exclure les chemins de fichiers tels que le répertoire de quarantaine ou les chemins dans lesquels seuls les disques durs virtuels ou les bases de données sont stockés.
 - Vérifiez que toutes les exclusions sont spécifiées dans la même stratégie, car une seule stratégie peut

être activée à la fois. NetApp recommande vivement de disposer du même ensemble d'exclusions que celui spécifié dans le moteur antivirus.

- Une stratégie d'accès est requise pour un [analyse à la demande](#). Pour éviter la numérisation à l'accès, vous devez définir `-scan-files-with-no-ext` pour faux et `-file-ext-to-exclude` à `*` pour exclure tous les postes.

Étapes

1. Création d'une règle on-Access :

```
vserver vscan on-access-policy create -vserver data_SVM|cluster_admin_SVM
-policy-name policy_name -protocol CIFS -max-file-size
max_size_of_files_to_scan -filters [scan-ro-volume,][scan-execute-access]
-file-ext-to-include extensions_of_files_to_include -file-ext-to-exclude
extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to
-exclude paths_of_files_to_exclude -scan-mandatory on|off
```

- Spécifier un SVM de données pour une politique définie pour un SVM individuel, un SVM d'administration du cluster pour une politique définie pour tous les SVM d'un cluster.
- Le `-file-ext-to-exclude` le réglage remplace le `-file-ext-to-include` réglage.
- Réglez `-scan-files-with-no-ext` à vrai pour numériser des fichiers sans extensions. La commande suivante crée une on-Access policy nommée Policy1 sur le vs1 SVM :

```
cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
-name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
-file-ext-to-include "mp*", "tx*" -file-ext-to-exclude "mp3", "txt" -scan
-files-with-no-ext false -paths-to-exclude "\\vol\\a b\\", "\\vol\\a, b\\"
```

2. Vérifiez que la stratégie on-Access a été créée : `vserver vscan on-access-policy show` `-instance data_SVM|cluster_admin_SVM -policy-name name`

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante affiche les détails de Policy1 règle :

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1
```

```
                Vserver: vs1
                Policy: Policy1
                Policy Status: off
                Policy Config Owner: vserver
                File-Access Protocol: CIFS
                Filters: scan-ro-volume
                Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
                File Paths Not to Scan: \vol\ a b\, \vol\ a,b\
                File Extensions Not to Scan: mp3, txt
                File Extensions to Scan: mp*, tx*
                Scan Files with No Extension: false
```

Activez une stratégie on-Access

Une règle On-Access définit l'étendue d'une analyse on-Access. Vous devez activer une on-Access policy sur un SVM avant que ses fichiers ne puissent être analysés.

Si vous avez créé une on-Access policy pour tous les SVM d'un cluster, vous devez activer la politique sur chaque SVM individuellement. Vous ne pouvez activer qu'une seule stratégie à la fois sur un SVM.

Étapes

1. Activer une stratégie on-Access :

```
vserver vscan on-access-policy enable -vserver data_SVM -policy-name
policy_name
```

La commande suivante active une on-Access policy nommée Policy1 sur le vs1 SVM :

```
cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
-name Policy1
```

2. Vérifiez que la stratégie on-Access est activée :

```
vserver vscan on-access-policy show -instance data_SVM -policy-name
policy_name
```

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante affiche les détails de Policy1 règle d'accès :

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1
```

```
                Vserver: vs1
                Policy: Policy1
                Policy Status: on
                Policy Config Owner: vserver
                File-Access Protocol: CIFS
                Filters: scan-ro-volume
                Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
                File Paths Not to Scan: \vol\ a b\, \vol\ a,b\
                File Extensions Not to Scan: mp3, txt
                File Extensions to Scan: mp*, tx*
                Scan Files with No Extension: false
```

Modifier le profil des opérations-fichiers Vscan pour un partage SMB

Le profil `_Vscan opérations-fichiers_` pour un partage SMB définit les opérations sur le partage qui peuvent déclencher le scan. Par défaut, le paramètre est défini sur `standard`. Vous pouvez régler le paramètre si nécessaire lors de la création ou de la modification d'un partage SMB.

Voir la ["Architecture antivirus"](#) Pour plus d'informations sur le profil *Vscan file-Operations*.



L'analyse antivirus n'est pas effectuée sur un partage SMB disposant du `continuously-available` paramètre défini sur `Yes`.

Étape

1. Modifier la valeur du profil Vscan file-Operations pour un partage SMB :

```
vserver cifs share modify -vserver data_SVM -share-name share -path share_path
-vscan-fileop-profile no-scan|standard|strict|writes-only
```

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante remplace le profil des opérations de fichier Vscan pour un partage SMB par `strict`:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name
SALES_SHARE -path /sales -vscan-fileop-profile strict
```

Commandes permettant de gérer les règles d'accès

Vous pouvez modifier, désactiver ou supprimer une stratégie On-Access. Vous pouvez

afficher un résumé et les détails de la règle.

Les fonctions que vous recherchez...	Saisissez la commande suivante...
Création d'une règle on-Access	<code>vserver vscan on-access-policy create</code>
Modifier une stratégie d'accès	<code>vserver vscan on-access-policy modify</code>
Activez une stratégie on-Access	<code>vserver vscan on-access-policy enable</code>
Désactivez une stratégie on-Access	<code>vserver vscan on-access-policy disable</code>
Supprimez une on-Access policy	<code>vserver vscan on-access-policy delete</code>
Afficher un récapitulatif et des détails d'une stratégie d'accès	<code>vserver vscan on-access-policy show</code>
Ajouter à la liste des chemins à exclure	<code>vserver vscan on-access-policy paths-to-exclude add</code>
Supprimer de la liste des chemins à exclure	<code>vserver vscan on-access-policy paths-to-exclude remove</code>
Afficher la liste des chemins à exclure	<code>vserver vscan on-access-policy paths-to-exclude show</code>
Ajouter à la liste des extensions de fichier à exclure	<code>vserver vscan on-access-policy file-ext-to-exclude add</code>
Supprimer de la liste des extensions de fichier à exclure	<code>vserver vscan on-access-policy file-ext-to-exclude remove</code>
Afficher la liste des extensions de fichier à exclure	<code>vserver vscan on-access-policy file-ext-to-exclude show</code>
Ajouter à la liste des extensions de fichier à inclure	<code>vserver vscan on-access-policy file-ext-to-include add</code>
Supprimer de la liste des extensions de fichier à inclure	<code>vserver vscan on-access-policy file-ext-to-include remove</code>
Afficher la liste des extensions de fichier à inclure	<code>vserver vscan on-access-policy file-ext-to-include show</code>

Pour plus d'informations sur ces commandes, consultez les pages de manuels.

Configurer l'acquisition à la demande

Configuration de la numérisation à la demande

Vous pouvez utiliser l'analyse à la demande pour rechercher immédiatement ou planifier la présence de virus dans les fichiers.

Vous pouvez exécuter des analyses uniquement pendant les heures creuses, par exemple. Vous pouvez également rechercher des fichiers très volumineux exclus de cette analyse lors d'une analyse à l'accès. Vous pouvez utiliser une planification cron pour spécifier quand la tâche s'exécute.

À propos de cette rubrique

- Vous pouvez affecter un planning lorsque vous créez une tâche.
- Une seule tâche peut être planifiée à la fois sur un SVM.
- La numérisation à la demande ne prend pas en charge la lecture de liens symboliques ou de fichiers de flux.



La numérisation à la demande ne prend pas en charge la lecture de liens symboliques ou de fichiers de flux.



Pour créer une tâche à la demande, au moins une stratégie d'accès doit être activée. Il peut s'agir de la stratégie par défaut ou d'une stratégie d'accès créée par l'utilisateur.

Créer une tâche à la demande

Une tâche à la demande définit la portée de l'analyse antivirus à la demande. Vous pouvez spécifier la taille maximale des fichiers à scanner, les extensions et les chemins des fichiers à inclure dans le scan, ainsi que les extensions et chemins des fichiers à exclure du scan. Les fichiers des sous-répertoires sont analysés par défaut.

Description de la tâche

- Dix (10) tâches à la demande au maximum peuvent être effectuées pour chaque SVM, mais une seule peut être active.
- Une tâche à la demande crée un rapport, qui contient des informations sur les statistiques relatives aux analyses. Ce rapport est accessible à l'aide d'une commande ou en téléchargeant le fichier de rapport créé par la tâche à l'emplacement défini.

Avant de commencer

- Vous devez avoir [création d'une stratégie d'accès](#). La stratégie peut être créée par défaut ou par l'utilisateur. Sans la stratégie On-Access, vous ne pouvez pas activer la numérisation.

Étapes

1. Créer une tâche à la demande :

```
vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
-scan-paths paths_of_files_to_scan -report-directory report_directory_path
-report-expiry-time expiration_time_for_report -schedule cron_schedule -max
-file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to
-exclude file_extensions -file-ext-to-include file_extensions -scan-files-with
```

`-no-ext true|false -directory-recursion true|false`

- Le `-file-ext-to-exclude` le réglage remplace le `-file-ext-to-include` réglage.
- Réglez `-scan-files-with-no-ext` à vrai pour numériser des fichiers sans extensions.

Pour obtenir la liste complète des options, reportez-vous au ["référence de commande"](#).

La commande suivante crée une tâche à la demande nommée Task1 Sur la `vs1'Svm:

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/", "/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?", "mp*" -file-ext-to-exclude "mp3", "mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

+



Vous pouvez utiliser le `job show` commande permettant d'afficher l'état du travail. Vous pouvez utiliser le `job pause` et `job resume` commandes permettant d'interrompre et de redémarrer le travail, ou le `job stop` commande pour mettre fin au travail.

2. Vérifiez que la tâche à la demande a été créée :

```
vserver vscan on-demand-task show -instance data_SVM -task-name task_name
```

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante affiche les détails de Task1 tâche :


```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name Task1
```

```
                Vserver: vs1
                Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
                Report Directory Path: /report
                Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
                File Paths Not to Scan: /vol1/cold-files/
                File Extensions Not to Scan: mp3, mp4
                File Extensions to Scan: vmdk?, mp*
Scan Files with No Extension: false
                Request Service Timeout: 5m
                Cross Junction: true
                Directory Recursion: true
                Scan Priority: low
                Report Log Level: info
                Expiration Time for Report: -
```

Une fois que vous avez terminé

Vous devez activer l'analyse sur la SVM avant que la tâche ne soit planifiée.

Planifiez une tâche à la demande

Vous pouvez créer une tâche sans affecter de planification et utiliser le `vserver vscan on-demand-task schedule` pour attribuer un planning ou pour ajouter un planning lors de la création de la tâche.

Description de la tâche

Planification affectée avec `vserver vscan on-demand-task schedule` la commande remplace un planning déjà affecté par le `vserver vscan on-demand-task create` commande.

Étapes

1. Planifier une tâche à la demande :

```
vserver vscan on-demand-task schedule -vserver data_SVM -task-name task_name -schedule cron_schedule
```

La commande suivante planifie une tâche à accès nommée Task2 sur le vs2 SVM :

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task -name Task2 -schedule daily
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142" command to view the status.
```

Pour afficher l'état du travail, utilisez le `job show` commande. Le `job pause` et `job resume` les commandes, respectivement, permettent de suspendre et de redémarrer le travail ; le `job stop` la commande met fin au travail.

2. Vérifiez que la tâche à la demande a été planifiée :

```
vserver vscan on-demand-task show -instance data_SVM -task-name task_name
```

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante affiche les détails de Task 2 tâche :

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name Task2

Vserver: vs2
Task Name: Task2
List of Scan Paths: /vol1/, /vol2/cifs/
Report Directory Path: /report
Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
File Paths Not to Scan: /vol1/cold-files/
File Extensions Not to Scan: mp3, mp4
File Extensions to Scan: vmdk, mp*
Scan Files with No Extension: false
Request Service Timeout: 5m
Cross Junction: true
Directory Recursion: true
Scan Priority: low
Report Log Level: info
```

Une fois que vous avez terminé

Vous devez activer l'analyse sur la SVM avant que la tâche ne soit planifiée.

Exécutez immédiatement une tâche à la demande

Vous pouvez exécuter une tâche à la demande immédiatement, que vous ayez affecté ou non un planning.

Avant de commencer

On doit avoir activé l'analyse sur le SVM.

Étape

1. Exécuter une tâche à la demande immédiatement :

```
vserver vscan on-demand-task run -vserver data_SVM -task-name task_name
```

La commande suivante exécute une tâche à accès nommée Task1 sur le vs1 SVM :

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name Task1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161" command to view the status.
```



Vous pouvez utiliser le `job show` commande permettant d'afficher l'état du travail. Vous pouvez utiliser le `job pause` et `job resume` commandes permettant d'interrompre et de redémarrer le travail, ou le `job stop` commande pour mettre fin au travail.

Commandes permettant de gérer des tâches à la demande

Vous pouvez modifier, supprimer ou annuler la planification d'une tâche à la demande. Vous pouvez afficher un résumé et des détails de la tâche et gérer les rapports de la tâche.

Les fonctions que vous recherchez...	Saisissez la commande suivante...
Créer une tâche à la demande	<code>vserver vscan on-demand-task create</code>
Modifier une tâche à la demande	<code>vserver vscan on-demand-task modify</code>
Supprimer une tâche à la demande	<code>vserver vscan on-demand-task delete</code>
Exécutez une tâche à la demande	<code>vserver vscan on-demand-task run</code>
Planifiez une tâche à la demande	<code>vserver vscan on-demand-task schedule</code>
Annulez la planification d'une tâche à la demande	<code>vserver vscan on-demand-task unschedule</code>
Consultez le récapitulatif des tâches à la demande et les détails correspondant	<code>vserver vscan on-demand-task show</code>
Consultez les rapports à la demande	<code>vserver vscan on-demand-task report show</code>
Supprimer des rapports à la demande	<code>vserver vscan on-demand-task report delete</code>

Pour plus d'informations sur ces commandes, consultez les pages de manuels.

Bonnes pratiques de configuration de la fonctionnalité antivirus externe dans ONTAP

Envisagez les recommandations suivantes pour la configuration de la fonctionnalité

externe dans ONTAP.

- Limiter les utilisateurs privilégiés aux opérations d'analyse antivirus. Les utilisateurs normaux doivent être déconseillés d'utiliser des informations d'identification d'utilisateur privilégiées. Cette restriction peut être obtenue en désactivant les droits de connexion pour les utilisateurs privilégiés sur Active Directory.
- Les utilisateurs privilégiés ne sont pas tenus de faire partie d'un groupe d'utilisateurs disposant d'un grand nombre de droits dans le domaine, tels que le groupe d'administrateurs ou le groupe d'opérateurs de sauvegarde. Les utilisateurs privilégiés doivent être validés uniquement par le système de stockage de sorte qu'ils soient autorisés à créer des connexions au serveur Vscan et à accéder aux fichiers pour l'analyse antivirus.
- Utiliser les ordinateurs exécutant des serveurs Vscan uniquement à des fins d'analyse antivirus. Pour décourager l'utilisation générale, désactivez les services de terminal Windows et les autres dispositions d'accès à distance sur ces ordinateurs et accordez le droit d'installer de nouveaux logiciels sur ces ordinateurs uniquement aux administrateurs.
- Dédiez les serveurs Vscan à l'analyse antivirus et ne les utilisez pas pour d'autres opérations, telles que les sauvegardes. Vous pouvez décider d'exécuter le serveur Vscan en tant que machine virtuelle (VM). Si vous exécutez le serveur Vscan en tant que VM, assurez-vous que les ressources allouées à la VM ne sont pas partagées et suffisantes pour effectuer une analyse antivirus.
- Fournir le CPU, la mémoire et la capacité disque appropriés au serveur Vscan pour éviter toute sur-allocation des ressources. La plupart des serveurs Vscan sont conçus pour utiliser plusieurs serveurs CPU core et pour répartir la charge entre les CPU.
- NetApp recommande d'utiliser un réseau dédié avec un VLAN privé pour la connexion de la SVM au serveur Vscan de sorte que le trafic de scan n'est pas affecté par d'autres trafic réseau client. Créer une carte d'interface réseau (NIC) distincte dédiée au VLAN antivirus sur le serveur Vscan et à la LIF de données sur la SVM. Cette étape simplifie l'administration et le dépannage en cas de problèmes réseau. Le trafic antivirus doit être isolé à l'aide d'un réseau privé. Le serveur antivirus doit être configuré pour communiquer avec le contrôleur de domaine (DC) et ONTAP de l'une des manières suivantes :
 - Le DC doit communiquer avec les serveurs antivirus via le réseau privé utilisé pour isoler le trafic.
 - Le serveur DC et antivirus doivent communiquer via un autre réseau (pas le réseau privé mentionné précédemment), qui n'est pas le même que le réseau client CIFS.
 - Pour activer l'authentification Kerberos pour la communication antivirus, créez une entrée DNS pour les LIFs privées et un nom principal de service sur le DC correspondant à l'entrée DNS créée pour la LIF privée. Utiliser ce nom lors de l'ajout d'une LIF au antivirus Connector. Le DNS doit pouvoir renvoyer un nom unique pour chaque LIF privée connectée au connecteur antivirus.



Si la LIF du trafic Vscan est configurée sur un port différent de la LIF pour le trafic client, la LIF Vscan peut basculer vers un autre nœud en cas de défaillance de port. La modification rend le serveur Vscan inaccessible depuis le nouveau nœud et les notifications de scan pour les opérations de fichier sur le nœud échouent. Vérifier que le serveur Vscan est accessible via au moins une LIF sur un nœud de sorte qu'il puisse traiter les demandes de scan pour les opérations de fichier effectuées sur ce nœud.

- Connecter le système de stockage NetApp et le serveur Vscan en utilisant au moins un réseau 1GbE.
- Pour un environnement avec plusieurs serveurs Vscan, connectez tous les serveurs qui ont des connexions réseau hautes performances similaires. La connexion des serveurs Vscan améliore les performances en permettant le partage de charge.
- Pour les sites distants et les succursales, NetApp recommande d'utiliser un serveur Vscan local plutôt qu'un serveur Vscan distant, car le premier est le candidat idéal à une latence élevée. Si le coût est un facteur, utilisez un ordinateur portable ou un PC pour une protection antivirus modérée. Vous pouvez

planifier des analyses complètes périodiques du système de fichiers en partageant les volumes ou les trées et en les analysant à partir de n'importe quel système du site distant.

- Utiliser plusieurs serveurs Vscan pour scanner les données sur la SVM à des fins d'équilibrage de charge et de redondance La quantité de charge de travail CIFS et le trafic antivirus résultant varient selon les SVM. Surveillez la latence CIFS et l'analyse antivirus sur le contrôleur de stockage. Surveiller la tendance des résultats au fil du temps. Si la latence CIFS et la latence de l'analyse antivirus augmentent en raison des files d'attente des processeurs ou des applications sur les serveurs Vscan, les clients CIFS peuvent rencontrer de longs délais d'attente. Ajouter des serveurs Vscan supplémentaires pour distribuer la charge.
- Installez la dernière version de ONTAP antivirus Connector.
- Maintenez les moteurs antivirus et les définitions à jour. Consultez vos partenaires pour obtenir des recommandations sur la fréquence de mise à jour.
- Dans un environnement multi-tenancy, un pool de scanner (pool de serveurs Vscan) peut être partagé avec plusieurs SVM à condition que les serveurs Vscan et les SVM fassent partie du même domaine ou du même domaine de confiance.
- La stratégie de logiciel antivirus pour les fichiers infectés doit être définie sur « delete » ou « quarantine », qui est la valeur par défaut définie par la plupart des fournisseurs d'antivirus. Si le « vscan-fileop-profile » est défini sur « write_only » et si un fichier infecté est trouvé, le fichier reste dans le partage et peut être ouvert car l'ouverture d'un fichier ne déclenche pas de scan. Le scan antivirus est déclenché uniquement après la fermeture du fichier.
- Le scan-engine timeout la valeur doit être inférieure à scanner-pool request-timeout valeur. Si la valeur est supérieure, l'accès aux fichiers peut être retardé et peut éventuellement prendre du temps. Pour éviter cela, configurez le scan-engine timeout à 5 secondes de moins que le scanner-pool request-timeout valeur. Reportez-vous à la documentation du fournisseur du moteur de numérisation pour obtenir des instructions sur la façon de modifier le scan-engine timeout paramètres. Le scanner-pool timeout peut être modifié à l'aide de la commande suivante en mode avancé et en fournissant la valeur appropriée pour request-timeout paramètre :
`vserver vscan scanner-pool modify.`
- Pour un environnement dimensionné pour les charges de travail d'analyse à l'accès et nécessitant l'analyse à la demande, NetApp recommande de planifier la tâche d'analyse à la demande en dehors des heures de pointe afin d'éviter toute charge supplémentaire sur l'infrastructure antivirus existante.

Pour en savoir plus sur les meilleures pratiques propres aux partenaires "[Solutions partenaires Vscan](#)", rendez-vous sur .

Activer l'analyse antivirus sur un SVM

Vous devez activer l'analyse antivirus sur un SVM avant de pouvoir exécuter une analyse à la demande ou à l'accès.

Étapes

1. Activer l'analyse antivirus sur un SVM :

```
vserver vscan enable -vserver data_SVM
```



Vous pouvez utiliser le `vserver vscan disable` pour désactiver l'analyse antivirus, si nécessaire.

La commande suivante active l'analyse antivirus sur le `vs1` SVM :

```
cluster1::> vserver vscan enable -vserver vs1
```

2. Vérifier que l'analyse antivirus est activée sur le SVM :

```
vserver vscan show -vserver data_SVM
```

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante affiche le statut Vscan du vs1 SVM :

```
cluster1::> vserver vscan show -vserver vs1
```

```
Vserver: vs1  
Vscan Status: on
```

Réinitialisez l'état des fichiers numérisés

Il peut arriver que vous souhaitiez réinitialiser l'état d'analyse des fichiers numérisés correctement sur un SVM en utilisant le `vserver vscan reset` commande pour ignorer les informations mises en cache pour les fichiers. Vous pouvez utiliser cette commande pour redémarrer le traitement de l'analyse antivirus en cas de mauvaise configuration d'une analyse, par exemple.

Description de la tâche

Après avoir exécuté le `vserver vscan reset` commande, tous les fichiers admissibles seront numérisés la prochaine fois qu'ils seront consultés.



Cette commande peut avoir un impact négatif sur les performances, en fonction du nombre et de la taille des fichiers à réanalyser.

Avant de commencer

Des privilèges avancés sont requis pour cette tâche.

Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Réinitialiser l'état des fichiers numérisés :

```
vserver vscan reset -vserver data_SVM
```

La commande suivante réinitialise l'état des fichiers numérisés sur le vs1 SVM :

```
cluster1::> vserver vscan reset -vserver vs1
```

Afficher les informations du journal des événements Vscan

Vous pouvez utiliser le `vserver vscan show-events` Commande pour afficher les informations du journal des événements concernant les fichiers infectés, les mises à jour vers les serveurs Vscan, et le même type. Vous pouvez afficher les informations d'événements pour le cluster ou pour des nœuds, SVM ou serveurs Vscan spécifiques.

Avant de commencer

Des privilèges avancés sont requis pour afficher le journal des événements Vscan.

Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Afficher les informations du journal des événements Vscan :

```
vserver vscan show-events
```

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante affiche les informations du journal des événements du cluster `cluster1`:

```
cluster1::*> vserver vscan show-events
```

Vserver	Node	Server	Event Type	Event Time
-----	-----	-----	-----	
vs1	Cluster-01	192.168.1.1	file-infected	9/5/2014
11:37:38				
vs1	Cluster-01	192.168.1.1	scanner-updated	9/5/2014
11:37:08				
vs1	Cluster-01	192.168.1.1	scanner-connected	9/5/2014
11:34:55				
3 entries were displayed.				

Surveillez et résolvez les problèmes de connectivité

Problèmes de connectivité potentiels impliquant l'option Scan-obligatoire

Vous pouvez utiliser le `vserver vscan connection-status show` Commandes pour afficher des informations sur les connexions du serveur Vscan qui vous seront peut-être utiles dans le dépannage des problèmes de connectivité.

Par défaut, le `scan-mandatory` L'option d'analyse On-Access refuse l'accès aux fichiers lorsqu'une connexion au serveur Vscan n'est pas disponible pour l'analyse. Bien que cette option offre des fonctions de sécurité importantes, elle peut entraîner des problèmes dans quelques situations.

- Avant d'activer l'accès client, il faut s'assurer qu'au moins un serveur Vscan est connecté à un SVM sur chaque nœud qui dispose d'une LIF. Si vous devez connecter les serveurs aux SVM après avoir autorisé l'accès client, vous devez désactiver le `scan-mandatory` Option sur le SVM pour s'assurer que l'accès aux fichiers n'est pas refusé car une connexion au serveur Vscan n'est pas disponible. Vous pouvez réactiver l'option après la connexion du serveur.
- Si une LIF cible héberge toutes les connexions de serveur Vscan pour un SVM, la connexion entre le serveur et la SVM sera perdue si la LIF est migrée. Pour vous assurer que l'accès aux fichiers n'est pas refusé car une connexion au serveur Vscan n'est pas disponible, vous devez désactiver le système `scan-mandatory` Option avant de migrer la LIF. Vous pouvez réactiver l'option après la migration de la LIF.

Chaque SVM doit disposer d'au moins deux serveurs Vscan qui lui sont affectés. Il s'agit d'une meilleure pratique de connexion des serveurs Vscan au système de stockage sur un réseau différent de celui utilisé pour l'accès client.

Commandes pour afficher l'état de connexion du serveur Vscan

Vous pouvez utiliser le `vserver vscan connection-status show` Commandes pour afficher les informations récapitulatives et détaillées sur l'état de la connexion au serveur Vscan.

Les fonctions que vous recherchez...	Saisissez la commande suivante...
Afficher un récapitulatif des connexions du serveur Vscan	<code>vserver vscan connection-status show</code>
Afficher les détails des connexions du serveur Vscan	<code>vserver vscan connection-status show-all</code>
Afficher les détails des serveurs Vscan connectés	<code>vserver vscan connection-status show-connected</code>
Afficher les détails des serveurs Vscan disponibles qui ne sont pas connectés	<code>vserver vscan connection-status show-not-connected</code>

Pour plus d'informations sur ces commandes, reportez-vous à la section ["Pages de manuel ONTAP"](#).

Résolution des problèmes liés à l'analyse antivirus

Pour les problèmes courants d'analyse antivirus, il existe des causes possibles et des moyens de les résoudre. L'analyse antivirus est également appelée Vscan.

Problème	Comment le résoudre
----------	---------------------

Les serveurs Vscan ne peuvent pas se connecter à Système de stockage clustered ONTAP.	Vérifier si la configuration scanner pool spécifie l'adresse IP du serveur Vscan. Vérifiez également si les utilisateurs privilégiés autorisés dans la liste scanner pool sont actifs. Pour vérifier le scanner pool, exécutez le <code>vserver vscan scanner-pool show</code> dans l'invite de commande du système de stockage. Si les serveurs Vscan ne peuvent toujours pas se connecter, il peut y avoir un problème au niveau du réseau.
Les clients observent une latence élevée.	Il est probablement temps d'ajouter d'autres serveurs Vscan au pool de scanner.
Trop d'acquisitions sont déclenchées.	Modifier la valeur du <code>vscan-fileop-profile</code> paramètre permettant de limiter le nombre d'opérations de fichiers surveillées pour l'analyse antivirus.
Certains fichiers ne sont pas numérisés.	Vérifiez la stratégie d'accès. Il est possible que le chemin de ces fichiers ait été ajouté à la liste d'exclusion de chemin ou que leur taille dépasse la valeur configurée pour les exclusions. Pour vérifier la stratégie On-Access, exécutez <code>vserver vscan on-access-policy show</code> dans l'invite de commande du système de stockage.
Accès au fichier refusé.	Vérifiez si le paramètre <i>scan-obligatoire</i> est spécifié dans la configuration de la stratégie. Ce paramètre refuse l'accès aux données si aucun serveur Vscan n'est connecté. Modifiez le paramètre si nécessaire.

Surveiller l'état et les activités de performance

Vous pouvez surveiller les aspects critiques du module Vscan, tels que le statut de connexion du serveur Vscan,

La santé des serveurs Vscan et le nombre de fichiers analysés. Ces informations sont utiles

Vous diagnostiquez les problèmes liés au serveur Vscan.

Afficher les informations de connexion au serveur Vscan

Vous pouvez afficher le statut de connexion des serveurs Vscan pour gérer les connexions qui sont déjà utilisées

et les connexions disponibles. Diverses commandes affichent des informations

À propos du statut de connexion des serveurs Vscan.

Commande...	Informations affichées...
<code>vserver vscan connection-status show</code>	Résumé de l'état de la connexion

<code>vserver vscan connection-status show-all</code>	Informations détaillées sur l'état de la connexion
<code>vserver vscan connection-status show-not-connected</code>	État des connexions disponibles mais non connectées
<code>vserver vscan connection-status show-connected</code>	Informations sur le serveur Vscan connecté

Pour plus d'informations sur ces commandes, reportez-vous au ["Référence de commande ONTAP"](#).

Afficher les statistiques du serveur Vscan

Vous pouvez afficher les statistiques spécifiques au serveur Vscan pour surveiller les performances et diagnostiquer les problèmes liés à analyse antivirus Vous devez collecter un échantillon de données avant de pouvoir utiliser le `statistics show` commande à

Afficher les statistiques du serveur Vscan.

Pour compléter un échantillon de données, procédez comme suit :

Étape

1. Exécutez le `statistics start` commande et le optional `statistics` commande d'arrêt.

Afficher les statistiques des requêtes et des latences du serveur Vscan

Vous pouvez utiliser ONTAP `offbox_vscan` Compteurs par SVM pour surveiller le taux de Vscan Requêtes de serveur envoyées et reçues par seconde et latences de serveur dans tous les Vscan serveurs. Pour afficher ces statistiques, procédez comme suit :

Étape

1. Exécutez les statistiques `show object offbox_vscan -instance SVM` commande avec compteurs suivants :

Compteur...	Informations affichées...
<code>scan_request_dispatched_rate</code>	Nombre de requêtes antivirus envoyées par ONTAP aux serveurs Vscan par seconde
<code>scan_noti_received_rate</code>	Nombre de requêtes antivirus reçues par ONTAP des serveurs Vscan par seconde
<code>dispatch_latency</code>	Latence dans ONTAP pour identifier un serveur Vscan disponible et envoyer la demande à ce serveur Vscan
<code>scan_latency</code>	Latence aller-retour de ONTAP au serveur Vscan, y compris le temps que le scan doit s'exécuter

Exemple de statistiques générées à partir d'un compteur ONTAP externe vscan

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-----
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-----
```

Afficher les statistiques des requêtes et des latences individuelles du serveur Vscan

Vous pouvez utiliser ONTAP offbox_vscan_server Compteurs sur un serveur Vscan par SVM, par serveur Vscan externe,
Et par nœud pour surveiller le taux des requêtes du serveur Vscan expédiées et la latence du serveur sur Chaque serveur Vscan individuellement. Pour collecter ces informations, procédez comme suit :

Étape

- 1. Exécutez le `statistics show -object offbox_vscan -instance SVM:servername:nodename` avec les compteurs suivants :

Compteur...	Informations affichées...
scan_request_dispatched_rate	Nombre de demandes d'analyse antivirus envoyées par ONTAP
scan_latency	Latence aller-retour de ONTAP au serveur Vscan, y compris le temps que le scan doit s'exécuter Vers les serveurs Vscan par seconde

Exemple de statistiques générées à partir d'un compteur ONTAP offbox_vscan_Server

```

Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value

```

```

-----
scan_request_dispatched_rate 291
scan_latency 3433830us
-----

```

Afficher les statistiques d'utilisation du serveur Vscan

Vous pouvez également utiliser ONTAP `offbox_vscan_server` Compteurs pour la collecte de l'utilisation Vscan côté serveur

statistiques. Ces statistiques sont suivies par SVM, par serveur Vscan externe et par nœud. Ils Inclure l'utilisation des CPU sur le serveur Vscan, la profondeur de file d'attente pour les opérations de scan sur le serveur Vscan

(actuel et maximal), mémoire utilisée et réseau utilisé.

Ces statistiques sont transmises par l'antivirus Connector aux compteurs statistiques de ONTAP. Ils sont basées sur des données interrogées toutes les 20 secondes et doivent être collectées plusieurs fois pour plus de précision ;

sinon, les valeurs affichées dans les statistiques reflètent uniquement la dernière interrogation. L'utilisation du processeur et les files d'attente sont

il est particulièrement important de surveiller et d'analyser. Une valeur élevée pour une file d'attente moyenne peut indiquer que l'

Le serveur Vscan présente un goulet d'étranglement.

Pour collecter les statistiques d'utilisation du serveur Vscan sur un SVM, un serveur Vscan par—serveur externe, et par—nœud

basis, effectuez l'étape suivante :

Étape

1. Collectez les statistiques d'utilisation du serveur Vscan

Exécutez le `statistics show -object offbox_vscan_server -instance`

`SVM:servername:nodename` avec les commandes suivantes `offbox_vscan_server` compteurs :

Compteur...	Informations affichées...
<code>scanner_stats_pct_cpu_used</code>	Utilisation du CPU sur le serveur Vscan
<code>scanner_stats_pct_input_queue_avg</code>	File d'attente moyenne des requêtes de scan sur le serveur Vscan
<code>scanner_stats_pct_input_queue_hiwatermark</code>	File d'attente de pointe des requêtes de scan sur le serveur Vscan

scanner_stats_pct_mem_used	Mémoire utilisée sur le serveur Vscan
scanner_stats_pct_network_used	Réseau utilisé sur le serveur Vscan

Exemple de statistiques d'utilisation pour le serveur Vscan

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-----
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
-----
```

Instructions de renforcement de la sécurité ONTAP

Présentation du renforcement de la sécurité ONTAP

ONTAP propose un ensemble de commandes qui vous permettent d'utiliser en toute sécurité le système d'exploitation du stockage ONTAP, le logiciel de gestion des données n° 1 du secteur. Utilisez les conseils et les paramètres de configuration de ONTAP pour aider votre entreprise à atteindre les objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité des systèmes d'information.

L'évolution du paysage actuel des menaces présente à une entreprise des défis uniques pour protéger ses ressources les plus précieuses : les données et les informations. Les menaces et vulnérabilités dynamiques et avancées auxquelles nous sommes confrontés sont de plus en plus sophistiquées. Associés à une augmentation de l'efficacité des techniques d'obfuscation et de reconnaissance de la part des intrus potentiels, les gestionnaires de systèmes doivent aborder de façon proactive la sécurité des données et de l'information.



Depuis juillet 2024, le contenu des rapports techniques publiés au format PDF a été intégré à la documentation produit de ONTAP. La documentation relative à la sécurité de ONTAP inclut désormais du contenu de *TR-4569: Guide de renforcement de la sécurité pour ONTAP*.

Validation des images ONTAP

ONTAP fournit des mécanismes permettant de s'assurer que l'image ONTAP est valide

lors de la mise à niveau et au démarrage.

Validation des images de mise à niveau

La signature de code permet de vérifier que les images ONTAP installées via des mises à jour d'images sans interruption ou des mises à jour d'images automatisées sans interruption, des interfaces de ligne de commande ou des API ONTAP sont produites de manière authentique par NetApp et n'ont pas été falsifiées. La validation des images de mise à niveau a été introduite dans ONTAP 9.3.

Cette fonction est une amélioration de la sécurité sans intervention de la mise à niveau ou de la restauration ONTAP. L'utilisateur ne doit rien faire différemment, sauf pour vérifier éventuellement la signature de premier niveau `image.tgz`.

Validation de l'image de démarrage

À partir de ONTAP 9.4, le démarrage sécurisé UEFI (Unified extensible Firmware interface) est activé pour les systèmes NetApp AFF A800, AFF A220, FAS2750 et FAS2720, ainsi que pour les systèmes nouvelle génération qui utilisent le BIOS UEFI.

Lors de la mise sous tension, le chargeur d'amorçage valide la base de données de la liste blanche des clés d'amorçage sécurisées avec la signature associée à chaque module chargé. Une fois que chaque module est validé et chargé, le processus de démarrage continue avec l'initialisation ONTAP. Si la validation de la signature échoue pour un module, le système redémarre.



Ces éléments s'appliquent aux images ONTAP et au BIOS de la plate-forme.

Comptes d'administrateur du stockage local

Rôles, applications et authentification

ONTAP offre aux entreprises soucieuses de leur sécurité la possibilité de fournir un accès granulaire à différents administrateurs via différentes applications et méthodes de connexion. Les clients peuvent ainsi créer un modèle zéro confiance centré sur les données.

Il s'agit des rôles disponibles pour les administrateurs admin et Storage Virtual machine. Les méthodes d'application de connexion et les méthodes d'authentification de connexion sont spécifiées.

Rôles

Grâce au contrôle d'accès basé sur des rôles (RBAC), les utilisateurs n'ont accès qu'aux systèmes et aux options requis pour leurs rôles et fonctions. La solution RBAC d'ONTAP limite l'accès administratif des utilisateurs au niveau correspondant à leur rôle, ce qui permet aux administrateurs de gérer les utilisateurs par rôle attribué. ONTAP fournit plusieurs rôles prédéfinis. Les opérateurs et les administrateurs peuvent créer, modifier ou supprimer des rôles de contrôle d'accès personnalisés et peuvent spécifier des restrictions de compte pour des rôles spécifiques.

Rôles prédéfinis pour les administrateurs du cluster

Ce rôle...	Dispose de ce niveau d'accès...	Aux commandes ou répertoires de commandes suivants
------------	---------------------------------	--

admin	Tout	Tous les répertoires de commandes (DEFAULT)
admin-no-fsa (Disponible à partir de ONTAP 9.12.1)	Lecture/écriture	<ul style="list-style-type: none"> • Tous les répertoires de commandes (DEFAULT) • security login rest-role • security login role
Lecture seule	<ul style="list-style-type: none"> • security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics 	Aucune
volume file show-disk-usage	autosupport	Tout
<ul style="list-style-type: none"> • set • system node autosupport 	Aucune	Tous les autres répertoires de commandes (DEFAULT)
backup	Tout	vserver services ndmp
Lecture seule	volume	Aucune

Tous les autres répertoires de commandes (DEFAULT)	readonly	Tout
<ul style="list-style-type: none"> • security login password <p>Pour la gestion du mot de passe local et des informations clés du compte utilisateur</p> <ul style="list-style-type: none"> • set 	Aucune	security
Lecture seule	Tous les autres répertoires de commandes (DEFAULT)	none



Le autosupport le rôle est affecté au prédéfini autosupport Compte, utilisé par AutoSupport OnDemand. ONTAP vous empêche de modifier ou de supprimer le autosupport compte. ONTAP vous empêche également d'attribuer le autosupport rôle vers d'autres comptes utilisateur.

Rôles prédéfinis pour les administrateurs des machines virtuelles de stockage (SVM)

Nom du rôle	Capacités
vsadmin	<ul style="list-style-type: none"> • Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gérez les volumes, à l'exception des déplacements de volumes • Gérez les quotas, les qtrees, les copies Snapshot et les fichiers • Gérer les LUN • Effectuer des opérations SnapLock, sauf la suppression privilégiée • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Surveiller les tâches • Surveiller les connexions réseau et l'interface réseau • Surveiller l'état de santé du SVM

vsadmin-volume	<ul style="list-style-type: none"> • Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gérez les volumes, notamment les déplacements de volumes • Gérez les quotas, les qtrees, les copies Snapshot et les fichiers • Gérer les LUN • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Interface réseau du moniteur • Surveiller l'état de santé du SVM
vsadmin-protocol	<ul style="list-style-type: none"> • Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Gérer les LUN • Interface réseau du moniteur • Surveiller l'état de santé du SVM
vsadmin-backup	<ul style="list-style-type: none"> • Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gestion des opérations NDMP • Effectuez une lecture/écriture de volume restauré • Gestion des relations SnapMirror et des copies Snapshot • Afficher les volumes et les informations réseau

vsadmin-snaplock	<ul style="list-style-type: none"> • Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gérez les volumes, à l'exception des déplacements de volumes • Gérez les quotas, les qtrees, les copies Snapshot et les fichiers • Effectuer des opérations SnapLock, y compris la suppression privilégiée • Configuration des protocoles : NFS et SMB • Configuration des services : DNS, LDAP et NIS • Surveiller les tâches • Surveiller les connexions réseau et l'interface réseau
vsadmin-readonly	<ul style="list-style-type: none"> • Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Surveiller l'état de santé du SVM • Interface réseau du moniteur • Vision des volumes et des LUN • Vision des services et protocoles

Méthodes d'application

La méthode d'application spécifie le type d'accès de la méthode de connexion. Les valeurs possibles incluent `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, et `telnet`.

La définition de ce paramètre sur `service-processor` l'utilisateur l'accès au processeur de service. Lorsque ce paramètre est défini sur `service-processor`, le `-authentication-method` paramètre doit être défini sur `password` car le processeur de service prend uniquement en charge `password` l'authentification. Les comptes utilisateurs SVM ne peuvent pas accéder au processeur de service. Par conséquent, les opérateurs et les administrateurs ne peuvent pas utiliser le `-vserver` paramètre lorsque ce paramètre est défini sur `service-processor`.

Pour restreindre davantage l'accès à l' `service-processor` , utilisez la commande `system service-processor ssh add-allowed-addresses`. La commande `system service-processor api-service` peut être utilisée pour mettre à jour les configurations et les certificats.

Pour des raisons de sécurité, Telnet et le shell distant (RSH) sont désactivés par défaut car NetApp recommande le shell sécurisé (SSH) pour un accès distant sécurisé. S'il existe une exigence ou un besoin unique de Telnet ou RSH, ils doivent être activés.

La `security protocol modify` commande modifie la configuration existante de RSH et Telnet au niveau du cluster. Activez RSH et Telnet dans le cluster en définissant le champ activé sur `true`.

Méthodes d'authentification

Le paramètre de méthode d'authentification spécifie la méthode d'authentification utilisée pour les connexions.

METHODE d'authentification	Description
cert	Authentification par certificat SSL
community	Chaînes de communauté SNMP
domain	Authentification Active Directory
nsswitch	Authentification LDAP ou NIS
password	Mot de passe
publickey	Authentification par clé publique
usm	Modèle de sécurité utilisateur SNMP



L'utilisation de NIS n'est pas recommandée en raison des faiblesses de sécurité du protocole.

À partir de la version ONTAP 9.3, une authentification à deux facteurs est disponible en chaîne pour les comptes SSH locaux admin à l'aide des `publickey` deux méthodes d'authentification et `password`. En plus du `-authentication-method` champ de la `security login` commande, un nouveau champ nommé `-second-authentication-method` a été ajouté. `publickey` ou `password` peut être spécifié en tant que `-authentication-method` ou `-second-authentication-method`. Cependant, lors de l'authentification SSH, l'ordre est toujours `publickey` avec une authentification partielle, suivie de l'invite de mot de passe pour une authentification complète.

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

À partir de ONTAP 9.4, `nsswitch` peut être utilisé comme deuxième méthode d'authentification avec `publickey`.

A partir de ONTAP 9.12.1, FIDO2 peut également être utilisé pour l'authentification SSH à l'aide d'un dispositif d'authentification matérielle YubiKey ou d'autres appareils compatibles FIDO2.

À partir de ONTAP 9.13.1 :

- `domain` les comptes peuvent être utilisés comme deuxième méthode d'authentification avec `publickey`.
- Mot de passe à usage unique basé sur l'heure (`totp`) est un code d'accès temporaire généré par un algorithme qui utilise l'heure actuelle comme l'un de ses facteurs d'authentification pour la deuxième méthode d'authentification.
- La révocation des clés publiques est prise en charge avec les clés publiques SSH ainsi que les certificats qui seront vérifiés pour leur expiration/révocation au cours de SSH.

Pour plus d'informations sur l'authentification multifacteur (MFA) pour ONTAP System Manager, Active IQ Unified Manager et SSH, consultez la section ["Tr-4647 : authentification multifacteur dans ONTAP 9"](#).

Comptes d'administration par défaut

Le compte admin doit être restreint car le rôle d'administrateur est autorisé à accéder à

l'aide de toutes les applications. Le compte diag permet l'accès à l'interpréteur de commandes du système et ne doit être réservé qu'au support technique pour effectuer les tâches de dépannage.

Il existe deux comptes d'administration par défaut : admin et diag.

Les comptes orphelins sont un vecteur de sécurité majeur qui entraîne souvent des vulnérabilités, y compris l'escalade des privilèges. Il s'agit de comptes inutiles et inutilisés qui restent dans le référentiel de comptes d'utilisateurs. Il s'agit principalement de comptes par défaut qui n'ont jamais été utilisés ou pour lesquels les mots de passe n'ont jamais été mis à jour ou modifiés. Pour résoudre ce problème, ONTAP prend en charge la suppression et le changement de nom des comptes.



ONTAP ne peut ni supprimer ni renommer les comptes intégrés. Cependant, NetApp recommande de verrouiller tous les comptes intégrés inutiles à l'aide de la commande lock.

Bien que les comptes orphelins constituent un problème de sécurité important, NetApp recommande fortement de tester l'effet de la suppression des comptes du référentiel de comptes local.

Répertoire les comptes locaux

Pour lister les comptes locaux, exécutez la security login show commande.

```
cluster1::*> security login show -vserver cluster1

Vserver: cluster1

User/Group Name  Application  Authentication Method  Role Name  Acct Locked  Is-Nsswitch Group
-----
admin            console      password  admin      no       no
admin            http         password  admin      no       no
admin            ontapi       password  admin      no       no
admin            service-processor password  admin      no       no
admin            ssh          password  admin      no       no
autosupport      console      password  autosupport no       no
6 entries were displayed.
```

Supprimez le compte admin par défaut

Le admin compte a le rôle d'administrateur et est autorisé à accéder à l'aide de toutes les applications.

Étapes

- 1. Créez un autre compte de niveau administrateur.

Pour supprimer complètement le compte par défaut admin , vous devez d'abord créer un autre compte de niveau administrateur qui utilise l' console application de connexion.



Ces modifications peuvent avoir des effets indésirables. Testez toujours d'abord les nouveaux paramètres susceptibles d'affecter l'état de sécurité de la solution sur un cluster hors production.

Exemple :

```
cluster1::*> security login create -user-or-group-name NewAdmin
-application console -authentication-method password -vserver cluster1
```

```
cluster1::*> security login show -vserver cluster1
```

Vserver: cluster1

		Authentication		Acct	Is-
Nsswitch					
User/Group Name	Application	Method	Role Name	Locked	Group
-----	-----	-----	-----	-----	
NewAdmin	console	password	admin	no	no
admin	console	password	admin	no	no
admin	http	password	admin	no	no
admin	ontapi	password	admin	no	no
admin	service-processor	password	admin	no	no
admin	ssh	password	admin	no	no
autosupport	console	password	autosupport	no	no
7 entries were displayed.					

- Une fois que vous avez créé le nouveau compte admin, testez l'accès à ce compte avec la NewAdmin connexion du compte. Avec la NewAdmin connexion, configurez le compte pour qu'il ait les mêmes applications de connexion que le compte admin par défaut ou précédent (par exemple, http, , ontapi service-processor`ou `ssh). Cette étape permet de s'assurer que le contrôle d'accès est maintenu.

Exemple :

```
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application ssh -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application http -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application ontapi -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application service-processor -authentication-method password
```

- Une fois toutes les fonctions testées, vous pouvez désactiver le compte admin pour toutes les applications avant de le supprimer de ONTAP. Cette étape sert de test final pour confirmer qu'il n'y a pas de fonctions

persistantes qui s'appuient sur le compte admin précédent.

```
cluster1::*> security login lock -vserver cluster1 -user-or-group-name
admin -application *
```

4. Pour supprimer le compte admin par défaut et toutes les entrées qui lui sont destinées, exécutez la commande suivante :

```
cluster1::*> security login delete -vserver cluster1 -user-or-group-name
admin -application *
cluster1::*> security login show -vserver cluster1
```

```
Vserver: cluster1

                                Authentication                Acct   Is-
Nsswitch
User/Group Name  Application Method    Role Name                Locked Group
-----
-----
NewAdmin         console    password  admin                    no      no
NewAdmin         http       password  admin                    no      no
NewAdmin         ontapi     password  admin                    no      no
NewAdmin         service-processor password admin                    no      no
NewAdmin         ssh        password  admin                    no      no
autosupport      console    password  autosupport              no      no
7 entries were displayed.
```

Définissez le mot de passe du compte de diagnostic (diag)

Un compte de diagnostic nommé `diag` est fourni avec votre système de stockage. Vous pouvez utiliser le `diag` compte pour effectuer des tâches de dépannage dans `systemshell`. Le `diag` compte est le seul compte qui peut être utilisé pour accéder au `systemshell` via la `diag` commande `Privileged systemshell`.



Le `systemshell` et le compte associé `diag` sont destinés à des fins de diagnostic de bas niveau. Leur accès requiert le niveau de privilège diagnostic et est réservé uniquement pour être utilisé avec l'aide du support technique pour effectuer des tâches de dépannage. Ni le compte ni le `n' diag systemshell` est destiné à des fins administratives générales.

Avant de commencer

Avant d'accéder au `systemshell`, vous devez définir le `diag` mot de passe du compte à l'aide de la `security login password` commande. Vous devez utiliser des principes de mot de passe forts et modifier le `diag` mot de passe à intervalles réguliers.

Étapes

1. Définissez le `diag` mot de passe de l'utilisateur du compte :

```
cluster1::> set -privilege diag
```

```
Warning: These diagnostic commands are for use by NetApp personnel only.  
Do you want to continue? \{y|n\}: y
```

```
cluster1::*> systemshell -node node-01  
      (system node systemshell)  
diag@node-01's password:
```

```
Warning: The system shell provides access to low-level  
diagnostic tools that can cause irreparable damage to  
the system if not used properly. Use this environment  
only when directed to do so by support personnel.
```

```
node-01%
```

Vérification multi-administrateurs

À partir de ONTAP 9.11.1, vous pouvez utiliser la vérification multiadministrateur pour permettre l'exécution de certaines opérations, telles que la suppression de volumes ou de copies Snapshot, uniquement après approbation par les administrateurs désignés. Cela empêche les administrateurs compromis, malveillants ou peu expérimentés d'effectuer des modifications ou de supprimer des données indésirables.

La configuration de MAV comprend les éléments suivants :

- "Création d'un ou plusieurs groupes d'approbation administrateur."
- "Activation de la fonctionnalité de vérification multi-administrateurs."
- "Ajout ou modification de règles."

Après la configuration initiale, seuls les administrateurs d'un groupe d'approbation MAV (administrateurs MAV) peuvent modifier ces éléments.

Lorsque MAV est activé, la réalisation de chaque opération protégée nécessite trois étapes :

1. Lorsqu'un utilisateur lance l'opération, un "la demande a été générée."
2. Avant de pouvoir l'exécuter, le nombre requis de "Les administrateurs MAV doivent approuver."
3. Après approbation, l'utilisateur termine l'opération.

La MAV n'est pas destinée à être utilisée avec des volumes ou des flux de travail qui impliquent une automatisation poussée car chaque tâche automatisée nécessite une approbation avant que l'opération ne puisse être terminée. Si vous souhaitez utiliser l'automatisation et la vérification multiniveau ensemble, NetApp vous recommande d'utiliser des requêtes pour des opérations de vérification multiniveau spécifiques. Par exemple, vous pouvez appliquer `volume delete` des règles MAV uniquement aux volumes pour lesquels l'automatisation n'est pas impliquée, et vous pouvez désigner ces volumes avec un schéma de nommage particulier.

Pour plus d'informations sur MAV, reportez-vous à la ["Documentation de vérification multiadministrateur ONTAP"](#).

Verrouillage des copies Snapshot

Le verrouillage des copies Snapshot est une fonctionnalité SnapLock qui permet de rendre les copies Snapshot indélébiles, manuellement ou automatiquement, avec une période de conservation définie dans la règle Snapshot du volume. L'objectif du verrouillage des copies Snapshot est d'empêcher les administrateurs peu scrupuleux ou non approuvés de supprimer les snapshots sur le système ONTAP principal ou secondaire.

Le verrouillage des copies Snapshot a été introduit dans ONTAP 9.12.1. Le verrouillage des copies Snapshot est également appelé verrouillage inviolable des copies Snapshot. Bien qu'il nécessite une licence SnapLock et l'initialisation de l'horloge de conformité, le verrouillage des copies Snapshot n'est pas lié à SnapLock Compliance ou SnapLock Enterprise. Il n'existe aucun administrateur de confiance dans le stockage, comme pour SnapLock Enterprise, et il ne protège pas l'infrastructure de stockage physique sous-jacente, comme pour SnapLock Compliance. Il s'agit d'une amélioration par rapport aux copies Snapshot SnapVaulting sur un système secondaire. La restauration rapide des copies Snapshot verrouillées sur les systèmes primaires peut être effectuée pour restaurer les volumes corrompus par des ransomwares.

Pour plus de détails sur le verrouillage des copies Snapshot, reportez-vous au ["Documentation de l'ONTAP"](#).

Configurez l'accès à l'API basée sur un certificat

Au lieu de l'authentification par ID utilisateur et mot de passe pour l'accès à ONTAP par l'API REST ou l'API du SDK de gestion NetApp, l'authentification basée sur certificat doit être utilisée.



Comme alternative à l'authentification basée sur certificat pour l'API REST, utilisez ["Authentification par jeton OAuth 2.0"](#).)

Vous pouvez générer et installer un certificat auto-signé sur ONTAP comme décrit dans ces étapes.

Étapes

1. À l'aide d'OpenSSL, générez un certificat en exécutant la commande suivante :

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'test.key'
```

Cette commande génère un certificat public nommé `test.pem` et une clé privée nommée `key.out`. Le nom commun, CN, correspond à l'ID utilisateur ONTAP.

2. Installez le contenu du certificat public au format courrier amélioré confidentiel (pem) dans ONTAP en exécutant la commande suivante et en collant le contenu du certificat lorsque vous y êtes invité :


```
security certificate install -type client-ca -vserver cluster1
```

Please enter Certificate: Press <Enter> when done

3. Activez ONTAP pour autoriser l'accès client via SSL et définissez l'ID utilisateur pour l'accès API.

```
security ssl modify -vserver cluster1 -client-enabled true  
security login create -user-or-group-name cert_user -application ontapi  
-authmethod cert -role admin -vserver cluster1
```

Dans l'exemple suivant, l'ID utilisateur `cert_user` est désormais activé pour utiliser l'accès à l'API authentifié par certificat. Un script Python du SDK de gestion simple utilisant `cert_user` pour afficher la version ONTAP apparaît comme suit :

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

La sortie du script affiche la version ONTAP.

```
./version.py
```

```
V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. Pour effectuer une authentification basée sur un certificat avec l'API REST ONTAP, procédez comme suit :
 - a. Dans ONTAP, définissez l'ID utilisateur pour l'accès http :

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

- b. Sur votre client Linux, exécutez la commande suivante qui produit la version ONTAP en tant que sortie :

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key ./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
  "version": {
    "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
    "generation": 9,
    "major": 7,
    "minor": 0
  },
  "_links": {
    "self": {
      "href": "/api/cluster"
    }
  }
}
```

Plus d'informations

- ["Authentification basée sur certificat avec le SDK de gestion NetApp pour ONTAP"](#).

Authentification basée sur jeton OAuth 2.0 ONTAP pour l'API REST

En alternative à l'authentification basée sur certificat, vous pouvez utiliser l'authentification basée sur jeton OAuth 2.0 pour l'API REST.

Depuis ONTAP 9.14.1, vous avez la possibilité de contrôler l'accès à vos clusters ONTAP à l'aide de l'infrastructure d'autorisation ouverte (OAuth 2.0). Vous pouvez configurer cette fonctionnalité à l'aide de n'importe quelle interface d'administration ONTAP, notamment l'interface de ligne de commandes ONTAP, System Manager et l'API REST. Cependant, les décisions d'autorisation et de contrôle d'accès OAuth 2.0 ne peuvent être appliquées que lorsqu'un client accède à ONTAP à l'aide de l'API REST.

Les jetons OAuth 2.0 remplacent les mots de passe pour l'authentification des comptes utilisateur.

Pour plus d'informations sur l'utilisation d'OAuth 2.0, consultez le ["Documentation ONTAP sur l'authentification et l'autorisation via OAuth 2.0"](#).

Paramètres de connexion et de mot de passe

Une stratégie de sécurité efficace est conforme aux politiques, aux directives et à toute gouvernance ou norme établies de l'entreprise. La durée de vie du nom d'utilisateur, les exigences de longueur du mot de passe, les exigences en termes de caractères et le stockage de ces comptes sont des exemples de ces exigences. La solution ONTAP offre des fonctionnalités pour traiter ces constructions de sécurité.

Nouvelles fonctionnalités de compte local

Pour prendre en charge les stratégies, directives ou normes de compte utilisateur d'une entreprise, notamment la gouvernance, les fonctionnalités suivantes sont prises en charge dans ONTAP :

- Configuration des stratégies de mot de passe pour appliquer un nombre minimum de chiffres, de minuscules ou de majuscules
- Délai nécessaire après un échec de la tentative de connexion
- Définition de la limite d'inactivité du compte
- Expiration d'un compte utilisateur
- Affichage d'un message d'avertissement d'expiration de mot de passe
- Notification d'une connexion non valide



Les paramètres configurables sont gérés à l'aide de la commande `Security login role config modify`.

Prise en charge de SHA-512

Pour améliorer la sécurité des mots de passe, ONTAP 9 prend en charge la fonction de hachage SHA-2 et utilise par défaut la fonction SHA-512 pour hacher les nouveaux mots de passe ou les mots de passe modifiés. Les opérateurs et les administrateurs peuvent également expirer ou verrouiller les comptes selon les besoins.

Les comptes utilisateur ONTAP 9 préexistants avec des mots de passe inchangés continuent d'utiliser la fonction de hachage MD5 après la mise à niveau vers ONTAP 9.0 ou version ultérieure. Cependant, NetApp recommande vivement de migrer ces comptes utilisateur vers la solution SHA-512 plus sécurisée en demandant aux utilisateurs de modifier leur mot de passe.

La fonctionnalité de hachage de mot de passe vous permet d'effectuer les tâches suivantes :

- Afficher les comptes utilisateur correspondant à la fonction de hachage spécifiée :

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver  user-or-group-name  application  authentication-method  hash-
function
-----
-----
cluster1 NewAdmin          console     password       sha512
cluster1 NewAdmin          ontapi      password       sha512
cluster1 NewAdmin          ssh         password       sha512
```

- Comptes expirés utilisant une fonction de hachage spécifiée (MD5, par exemple), qui oblige les utilisateurs à modifier leur mot de passe lors de la connexion suivante :

```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```

- Verrouiller les comptes avec des mots de passe utilisant la fonction de hachage spécifiée.

```
cluster1::*> security login lock -vserver * -username * -hash-function md5
```

La fonction de hachage password est inconnue pour l'utilisateur interne `autosupport` du SVM d'administration de votre cluster. Ce problème est cosmétique. La fonction de hachage est inconnue car cet utilisateur interne ne dispose pas d'un mot de passe configuré par défaut.

- Pour afficher la fonction de hachage du mot de passe de l' `autosupport` utilisateur, exécutez les commandes suivantes :

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

Vserver: cluster1
User Name or Group Name: autosupport
Application: console
Authentication Method: password
Remote Switch IP Address: -
Role Name: autosupport
Account Locked: no
Comment Text: -
Whether Ns-switch Group: no
Password Hash Function: unknown
Second Authentication Method2: none
```

- Pour définir la fonction de hachage du mot de passe (par défaut : sha512), exécutez la commande suivante :

```
::> security login password -username autosupport
```

La définition du mot de passe n'a pas d'importance.

```
security login show -user-or-group-name autosupport -instance
```

```
Vserver: cluster1
User Name or Group Name: autosupport
Application: console
Authentication Method: password
Remote Switch IP Address: -
Role Name: autosupport
Account Locked: no
Comment Text: -
Whether Ns-switch Group: no
Password Hash Function: sha512
Second Authentication Method2: none
```

Paramètres de mot de passe

La solution ONTAP prend en charge les paramètres de mot de passe qui répondent aux exigences et directives de l'entreprise et qui les prennent en charge.

Attribut	Description	Valeur par défaut	Gamme
username-minlength	Longueur minimale du nom d'utilisateur requise	3	3-16
username-alphanum	Nom d'utilisateur alphanumérique	désactivé	Activé/Désactivé
passwd-minlength	Longueur minimale du mot de passe requise	8	3-64
passwd-alphanum	Mot de passe alphanumérique	activé	Activé/Désactivé
passwd-min-special-chars	Nombre minimum de caractères spéciaux requis dans le mot de passe	0	0-64
passwd-expiry-time	Heure d'expiration du mot de passe (en jours)	Illimité, ce qui signifie que les mots de passe n'expirent jamais	0-illimité 0 == expire maintenant
require-initial-passwd-update	Exiger la mise à jour initiale du mot de passe lors de la première connexion	Désactivé	Activé/Désactivé Modifications autorisées via la console ou SSH
max-failed-login-attempts	Nombre maximal de tentatives infructueuses	0, ne pas verrouiller le compte	-

Attribut	Description	Valeur par défaut	Gamme
lockout-duration	Durée maximale de verrouillage (en jours)	La valeur par défaut est 0, ce qui signifie que le compte est verrouillé pendant une journée	-
disallowed-reuse	Interdire les N derniers mots de passe	6	Le minimum est de 6
change-delay	Délai entre les modifications du mot de passe (en jours)	0	-
delay-after-failed-login	Délai après chaque tentative de connexion échouée (en secondes)	4	-
passwd-min-lowercase-chars	Nombre minimum de caractères alphabétiques minuscules requis dans le mot de passe	0, qui ne nécessite pas de caractères minuscules	0-64
passwd-min-uppercase-chars	Nombre minimum de caractères alphabétiques majuscules requis	0, qui ne nécessite pas de majuscules	0-64
passwd-min-digits	Nombre minimum de chiffres requis dans le mot de passe	0, qui ne nécessite pas de chiffres	0-64
passwd-expiry-warn-time	Afficher le message d'avertissement avant l'expiration du mot de passe (en jours)	Illimité, ce qui signifie ne jamais avertir de l'expiration du mot de passe	0, ce qui signifie avertir l'utilisateur de l'expiration du mot de passe à chaque connexion réussie
account-expiry-time	Le compte expire dans N jours	Illimité, ce qui signifie que les comptes n'expirent jamais	Le délai d'expiration du compte doit être supérieur à la limite d'inactivité du compte
account-inactive-limit	Durée maximale d'inactivité avant l'expiration du compte (en jours)	Illimité, ce qui signifie que les comptes inactifs n'expirent jamais	La limite d'inactivité du compte doit être inférieure à l'heure d'expiration du compte

Exemple

```
cluster1::*> security login role config show -vserver cluster1 -role admin

Vserver: cluster1
Role Name: admin
Minimum Username Length Required: 3
Username Alpha-Numeric: disabled
Minimum Password Length Required: 8
Password Alpha-Numeric: enabled
Minimum Number of Special Characters Required in the Password: 0
Password Expires In (Days): unlimited
Require Initial Password Update on First Login: disabled
Maximum Number of Failed Attempts: 0
Maximum Lockout Period (Days): 0
Disallow Last 'N' Passwords: 6
Delay Between Password Changes (Days): 0
Delay after Each Failed Login Attempt (Secs): 4
Minimum Number of Lowercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Uppercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Digits Required in the Password: 0
Display Warning Message Days Prior to Password Expiry (Days): unlimited
Account Expires in (Days): unlimited
Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```



À partir de 9.14.1, les mots de passe sont de plus en plus complexes et les règles de verrouillage. Ceci s'applique uniquement aux nouvelles installations de ONTAP.

Méthodes d'administration du système

Ce sont des paramètres importants pour renforcer l'administration du système ONTAP.

Accès en ligne de commande

L'établissement d'un accès sécurisé aux systèmes est un élément essentiel du maintien de la sécurité de la solution. Les options d'accès en ligne de commande les plus courantes sont SSH, Telnet et RSH. Parmi ces technologies, SSH est la meilleure pratique standard du secteur et la plus sécurisée pour l'accès à distance en ligne de commande. NetApp recommande vivement d'utiliser SSH pour l'accès en ligne de commande à la solution ONTAP.

Configurations SSH

La `security ssh show` commande affiche les configurations des algorithmes d'échange de clés SSH, du chiffrement et des algorithmes MAC pour le cluster et les SVM. La méthode d'échange de clés utilise ces algorithmes et ces chiffrements pour spécifier comment les clés de session à usage unique sont générées pour le cryptage et l'authentification et comment l'authentification du serveur a lieu.


```
cluster1::> security ssh show
```

Vserver	Ciphers	Key Exchange Algorithms	MAC Algorithms
-----	-----	-----	-----
nsadhanaccluster-2			
	aes256-ctr,	diffie-helman-group-	hmac-sha2-256
	aes192-ctr,	exchange-sha256,	hmac-sha2-512
	aes128-ctr	ecdh-sha2-nistp384	
vs0	aes128-gcm	curve25519-sha256	hmac-sha1
vs1	aes256-ctr,	diffie-hellman-group-	hmac-sha1-96
	aes192-ctr,	exchange-sha256	hmac-sha2-256
	aes128-ctr,	ecdh-sha2-nistp384	hmac-sha2-256-
	3des-cbc,	ecdh-sha2-nistp512	etm
	aes128-gcm		hmac-sha2-512
3 entries were displayed.			

Bannières de connexion

Les bannières de connexion permettent aux entreprises de présenter aux opérateurs, administrateurs, voire même aux utilisateurs malveillants, les conditions d'utilisation. Elles indiquent qui est autorisé à accéder au système. Cette approche est utile pour établir les attentes en matière d'accès et d'utilisation du système. La `security login banner modify` commande modifie la bannière de connexion. La bannière de connexion s'affiche juste avant l'étape d'authentification lors du processus de connexion SSH et du périphérique de la console. Le texte de la bannière doit être entre guillemets (" "), comme dans l'exemple suivant.

```
cluster1::> security login banner modify -vserver cluster1 -message  
"Authorized users ONLY!"
```

Paramètres de bannière de connexion

Paramètre	Description
vserver	Utiliser ce paramètre pour spécifier le SVM avec la bannière modifiée. Utiliser le nom du SVM admin du cluster pour modifier le message au niveau du cluster. La message au niveau du cluster est utilisée par défaut pour les SVM de données qui ne disposent pas de message défini.

Paramètre	Description
message	<p>Ce paramètre facultatif peut être utilisé pour spécifier un message de bannière de connexion. Si le cluster a un ensemble de messages de bannière de connexion, la bannière de connexion au cluster est également utilisée par tous les SVM de données. La définition de la bannière de connexion d'un SVM de données remplace l'affichage de la bannière de connexion du cluster. Pour réinitialiser une bannière de connexion SVM de données afin d'utiliser la bannière de connexion au cluster, utilisez ce paramètre avec la valeur « - ».</p> <p>Si vous utilisez ce paramètre, la bannière de connexion ne peut pas contenir de nouvelles lignes (également appelées extrémités de lignes [EOL] ou sauts de ligne). Pour saisir un message de bannière de connexion avec des lignes de rappel, ne spécifiez aucun paramètre. Vous êtes invité à saisir le message de manière interactive. Les messages entrés de manière interactive peuvent contenir des nouvelles lignes.</p> <p>Les caractères non ASCII doivent utiliser Unicode UTF-8.</p>
uri	`(ftp
http://(hostname	IPv4` <p>Utilisez ce paramètre pour spécifier l'URI à partir de laquelle la bannière de connexion est téléchargée.</p> <p>La longueur du message ne doit pas dépasser 2048 octets. Les caractères non ASCII doivent être fournis au format Unicode UTF-8.</p>

Message du jour

La `security login motd modify` commande met à jour le message du jour (MOTD).

Il existe deux catégories de MOTD : le MOTD au niveau du cluster et le MOTD au niveau du SVM de données. Un utilisateur se connectant au cluster d'un SVM de données peut voir deux messages : le MOTD au niveau du cluster suivi du MOTD au niveau du SVM pour ce SVM.

L'administrateur du cluster peut activer ou désactiver le MOTD au niveau du cluster sur chaque SVM individuellement si nécessaire. Si l'administrateur du cluster désactive le MOTD au niveau du cluster pour un SVM, un utilisateur se connectant au SVM ne voit pas le message au niveau du cluster. Seul un administrateur de cluster peut activer ou désactiver le message au niveau du cluster.

Paramètre MOTD	Description
Un vServer	Utiliser ce paramètre pour spécifier le SVM pour lequel le MOTD est modifié. Utiliser le nom du SVM admin du cluster pour modifier le message au niveau du cluster.

Paramètre MOTD	Description
messagerie	<p>Ce paramètre facultatif peut être utilisé pour spécifier un message. Si vous utilisez ce paramètre, le MOTD ne peut pas contenir de nouvelles lignes. Si vous ne spécifiez aucun paramètre autre que le <code>-vserver</code> paramètre, vous êtes invité à saisir le message de manière interactive. Les messages entrés de manière interactive peuvent contenir des nouvelles lignes. Les caractères non ASCII doivent être fournis au format Unicode UTF-8. Le message peut contenir du contenu généré de façon dynamique à l'aide des séquences d'échappement suivantes :</p> <ul style="list-style-type: none"> • <code>\</code> - Un seul caractère de jeu • <code>\b</code> - Pas de sortie (pris en charge pour la compatibilité avec Linux uniquement) • <code>\C</code> - Nom du cluster • <code>\d</code> - La date actuelle telle qu'elle est définie sur le nœud de connexion • <code>\t</code> - Heure actuelle définie sur le nœud de connexion • <code>\I</code> - Adresse IP de LIF entrante (imprime la console pour une <code>console</code> connexion) • <code>\l</code> - Nom du périphérique de connexion (imprime la console pour une <code>console</code> connexion) • <code>\L</code> - Dernière connexion de l'utilisateur sur n'importe quel nœud du cluster • <code>\m</code> - Architecture de la machine • <code>\n</code> - Nom du nœud ou du SVM de données • <code>\N</code> - Nom de l'utilisateur se connectant • <code>\o</code> - Identique à <code>\O</code>. Fourni pour la compatibilité Linux. • <code>\O</code> - Nom de domaine DNS du nœud. Notez que la sortie dépend de la configuration du réseau et peut être vide. • <code>\r</code> - Numéro de version du logiciel • <code>\s</code> - Nom du système d'exploitation • <code>\u</code> - Nombre de sessions clustershell actives sur le nœud local. Pour l'administrateur du cluster : tous les utilisateurs du cluster shell. Pour le SVM de données admin : sessions actives uniquement pour ce SVM de données. • <code>\U</code> - Identique à <code>\u</code>, mais a ou a <code>user users</code> ajouté • <code>\v</code> - Chaîne de version de cluster effective • <code>\W</code> - Sessions actives sur le cluster pour l'utilisateur se connectant (<code>who</code>)

Pour plus d'informations sur la configuration du message du jour dans ONTAP, reportez-vous au ["Documentation ONTAP sur message du jour"](#).

Expiration de la session CLI

Le délai d'expiration par défaut de la session CLI est de 30 minutes. Le délai d'expiration est important pour éviter les sessions obsolètes et le piggydorsal de session.

Utilisez `system timeout show` la commande pour afficher le délai d'expiration actuel de la session de l'interface de ligne de commande. Pour définir la valeur du délai d'expiration, utilisez la `system timeout modify -timeout <minutes>` commande.

Accès Internet avec NetApp ONTAP System Manager

Si un administrateur ONTAP préfère utiliser une interface graphique au lieu de l'interface de ligne de commandes pour accéder au cluster et le gérer, utilisez NetApp ONTAP System Manager. Il est inclus avec ONTAP en tant que service Web, activé par défaut et accessible à l'aide d'un navigateur. Pointez le navigateur sur le nom d'hôte si vous utilisez DNS ou l'adresse IPv4 ou IPv6 via `https://cluster-management-LIF`.

Si le cluster utilise un certificat numérique auto-signé, il est possible que le navigateur affiche un avertissement indiquant que le certificat n'est pas approuvé. Vous pouvez soit reconnaître le risque de continuer l'accès, soit installer un certificat numérique signé par l'autorité de certification (CA) sur le cluster pour l'authentification du serveur.

Depuis ONTAP 9.3, l'authentification SAML (Security assertion Markup Language) est une option disponible dans ONTAP System Manager.

Authentification SAML pour ONTAP System Manager

SAML 2.0 est une norme du secteur largement adoptée qui permet à tout fournisseur d'identités tiers conforme à la norme SAML d'effectuer un MFA à l'aide de mécanismes propres à l'IDP choisi par l'entreprise et en tant que source d'authentification unique (SSO).

Trois rôles sont définis dans la spécification SAML : le principal, l'IDP et le fournisseur de services. Dans l'implémentation de ONTAP, un principal est l'administrateur du cluster qui accède à ONTAP via ONTAP System Manager ou NetApp Active IQ Unified Manager. Le PDI est un logiciel tiers IDP. Depuis ONTAP 9.3, Microsoft Active Directory Federated Services (ADFS) et l'IDP open source Shibboleth sont des PDI pris en charge. À partir de ONTAP 9.12.1, Cisco DUO est un IDP pris en charge. Le fournisseur de services est la fonctionnalité SAML intégrée à ONTAP qui est utilisée par ONTAP System Manager ou l'application Web Active IQ Unified Manager.

Contrairement au processus de configuration à deux facteurs SSH, une fois l'authentification SAML activée, l'accès à ONTAP System Manager ou au processeur de service ONTAP requiert l'authentification de tous les administrateurs existants via ce protocole. Aucune modification n'est requise pour les comptes utilisateur du cluster. Lorsque l'authentification SAML est activée, une nouvelle méthode d'authentification de `saml` est ajoutée aux utilisateurs existants disposant des rôles d'administrateur pour `http` et `ontapi` les applications.

Une fois l'authentification SAML activée, les nouveaux comptes supplémentaires nécessitant l'accès SAML IDP doivent être définis dans ONTAP avec le rôle d'administrateur et la méthode d'authentification `saml` pour et les `http` `ontapi` applications. Si l'authentification SAML est désactivée à un moment ou à un autre, ces nouveaux comptes requièrent que la `password` méthode d'authentification soit définie avec le rôle d'administrateur pour `http` et `ontapi` les applications et qu'elle ajoute l' `console` application pour l'authentification ONTAP locale à ONTAP System Manager.

Une fois l'IDP SAML activé, il effectue l'authentification pour l'accès au Gestionnaire système ONTAP à l'aide des méthodes disponibles pour ce dernier, telles que le protocole LDAP (Lightweight Directory Access Protocol), Active Directory (AD), Kerberos, le mot de passe, etc. Les méthodes disponibles sont uniques au PDI. Il est important que les comptes configurés dans ONTAP aient des ID utilisateur qui correspondent aux méthodes d'authentification IDP.

Les PDI validés par NetApp sont Microsoft ADFS, Cisco DUO et Shibboleth IDP open source.

À partir de ONTAP 9.14.1, Cisco DUO peut être utilisé comme second facteur d'authentification pour SSH.

Pour plus d'informations sur MFA pour ONTAP System Manager, Active IQ Unified Manager et SSH, voir ["Tr-4647 : authentification multifacteur dans ONTAP 9"](#).

Informations ONTAP System Manager

À partir de ONTAP 9.11.1, ONTAP System Manager fournit des informations exploitables pour aider les administrateurs du cluster à rationaliser leurs tâches quotidiennes. Les informations de sécurité sont basées sur les recommandations de ce rapport technique.

Analyse de la sécurité	Détermination
Telnet est activé	NetApp recommande un accès sécurisé à distance (SSH).
Le shell distant (RSH) est activé	NetApp recommande SSH pour un accès distant sécurisé.
AutoSupport utilise un protocole non sécurisé	AutoSupport n'est pas configuré pour être envoyé via lien:HTTPS.
La bannière de connexion n'est pas configurée au niveau du cluster	Avertissement si la bannière de connexion n'est pas configurée pour le cluster.
SSH utilise des chiffrements non sécurisés	Avertissement si SSH utilise des chiffrements non sécurisés.
Trop peu de serveurs NTP sont configurés	Avertissement si le nombre de serveurs NTP configurés est inférieur à trois.
Utilisateur admin par défaut non verrouillé	Lorsque vous n'utilisez aucun compte d'administration par défaut (admin ou diag) pour vous connecter à System Manager et que ces comptes ne sont pas verrouillés, il est recommandé de les verrouiller.
Défense contre les ransomwares : les volumes n'ont pas de règles Snapshot	Aucune règle Snapshot adéquate n'est associée à un ou plusieurs volumes.
Défense contre les ransomware : désactivez la suppression automatique de Snapshot	La suppression automatique des snapshots est définie pour un ou plusieurs volumes.
Les attaques par ransomware ne font pas l'objet d'une surveillance des volumes	La protection anti-ransomware autonome est prise en charge sur plusieurs volumes, mais pas encore configurée.
Les SVM ne sont pas configurés pour la protection autonome contre les ransomware	La protection anti-ransomware autonome est prise en charge sur plusieurs SVM, mais pas encore configurée.
FPolicy natif n'est pas configuré	FPolicy n'est pas défini pour les SVM NAS.
Activez le mode actif de protection anti-ransomware autonome	Plusieurs volumes ont terminé leur mode d'apprentissage et vous pouvez activer le mode actif
La conformité à la norme FIPS 140-2 globale est désactivée	La conformité à la norme FIPS 140-2 globale n'est pas activée.
Le cluster n'est pas configuré pour les notifications	Les e-mails, les webhooks ou les traphosts SNMP ne sont pas configurés pour recevoir des notifications.

Pour plus d'informations sur ONTAP System Manager Insights, consultez le ["Informations exploitables avec ONTAP System Manager"](#).

La protection anti-ransomware autonome de ONTAP

Pour compléter l'analytique du comportement des utilisateurs pour Storage Workload

Security, la protection anti-ransomware autonome de ONTAP analyse les workloads de volume et l'entropie pour détecter les ransomware, puis prend une Snapshot et notifie l'administrateur lorsqu'une attaque est suspectée.

Outre la détection et la prévention des ransomwares grâce à l'analytique comportementale des utilisateurs (UBA) FPolicy externes avec NetApp Cloud Insights/Cloud Secure et l'écosystème de partenaires NetApp FPolicy, ONTAP 9.10.1 propose une protection anti-ransomware autonome. La protection anti-ransomware autonome de ONTAP utilise une fonctionnalité intégrée de machine learning (ML) qui analyse l'activité des workloads de volume et l'entropie des données pour détecter automatiquement les ransomware. Il surveille les activités différentes de l'UBA afin de détecter les attaques qui ne l'ont pas été.

Pour plus d'informations sur cette fonctionnalité, voir ["Solutions NetApp pour ransomware"](#) ou ["Documentation sur la protection anti-ransomware autonome de ONTAP"](#).

Audit du système d'administration du stockage

Assurez l'intégrité de l'audit des événements en transférant les événements ONTAP vers un serveur syslog distant. Ce serveur peut être un système de gestion des événements liés aux informations de sécurité tel que Splunk.

Envoyer syslog

Les informations d'audit et de journalisation sont extrêmement précieuses pour le support et la disponibilité. En outre, les informations figurant dans les journaux (syslog) ainsi que dans les rapports et résultats d'audit sont généralement sensibles. Pour préserver les contrôles et le niveau de sécurité, les entreprises doivent impérativement gérer les données de journalisation et d'audit de manière sécurisée.

Le déstage des données des syslog est nécessaire pour limiter l'impact d'une faille à un seul système ou une seule solution. Par conséquent, NetApp recommande de décharger des informations syslog en toute sécurité vers un emplacement de stockage ou de conservation sécurisé.

Créez une destination de transfert de journaux

Utilisez `cluster log-forwarding create` la commande pour créer des destinations de transfert de journaux pour la journalisation à distance.

Paramètres

Utiliser les paramètres suivants pour configurer la `cluster log-forwarding create` commande :

- **Hôte de destination.** Ce nom est le nom d'hôte ou l'adresse IPv4 ou IPv6 du serveur vers lequel transférer les journaux.

```
-destination <Remote InetAddress>
```

- **Port de destination.** Il s'agit du port sur lequel le serveur de destination écoute.

```
[-port <integer>]
```

- **Protocole de transfert de journaux.** Ce protocole est utilisé pour envoyer des messages à la destination.

```
[-protocol \{udp-unencrypted|tcp-unencrypted|tcp-encrypted}]
```

Le protocole de transfert de journaux peut utiliser l'une des valeurs suivantes :

- `udp-unencrypted`. Protocole de datagramme utilisateur sans sécurité.
- `tcp-unencrypted`. TCP sans sécurité.
- `tcp-encrypted`. TCP avec TLS (transport Layer Security).
- **Vérifiez l'identité du serveur de destination.** Lorsque ce paramètre est défini sur `true`, l'identité de la destination de transfert de journaux est vérifiée en validant son certificat. La valeur peut être définie sur `true` uniquement lorsque la `tcp-encrypted` valeur est sélectionnée dans le champ de protocole.

```
[-verify-server \{true|false}]
```

- **Fonction Syslog.** Cette valeur est la fonction syslog à utiliser pour les journaux transmis.

```
[-facility <Syslog Facility>]
```

- **Ignorez le test de connectivité.** Normalement, la `cluster log-forwarding create` commande vérifie que la destination est accessible en envoyant une requête ping ICMP (Internet Control message Protocol) et échoue si elle n'est pas accessible. La définition de cette valeur `true` permet de contourner la vérification ping afin que vous puissiez configurer la destination lorsqu'elle est inaccessible.

```
[-force [true]]
```



NetApp recommande d'utiliser la `cluster log-forwarding create` commande pour forcer la connexion à un `-tcp-encrypted` type.

Notification d'événement

La sécurisation des informations et des données quittant un système est essentielle au maintien et à la gestion du niveau de sécurité du système. Les événements générés par la solution ONTAP sont une mine d'informations sur le problème rencontré par la solution, les informations traitées, etc. La vitalité de ces données souligne la nécessité de les gérer et de les migrer de manière sécurisée.

La `event notification create` commande envoie une nouvelle notification d'un ensemble d'événements défini par un filtre d'événements à une ou plusieurs destinations de notification. Les exemples suivants illustrent la configuration de la notification d'événements et la `event notification show` commande, qui affiche les destinations et les filtres de notification d'événements configurés.

```
cluster1::> event notification create -filter-name filter1 -destinations
email_dest,syslog_dest,snmp-traphost

cluster1::> event notification show
ID      Filter Name      Destinations
-----
1 filter1 email_dest, syslog_dest, snmp-traphost
```

Chiffrement du stockage

Pour protéger les données sensibles en cas de vol, de retour ou de reconversion d'un disque, utilisez le chiffrement de stockage NetApp matériel ou le chiffrement logiciel de volume NetApp/chiffrement d'agrégat NetApp. Ces deux mécanismes sont validés conformément à la norme FIPS-140-2 et lors de l'utilisation de mécanismes matériels avec des mécanismes logiciels, la solution est admissible au programme CSfC (commercial Solutions for Classified Program). Il offre une protection renforcée des données secrètes et les plus secrètes au repos, à la fois au niveau du matériel et des logiciels.

Le chiffrement des données au repos est important pour protéger les données sensibles en cas de vol, de retour ou de reconversion d'un disque.

ONTAP 9 propose trois solutions de chiffrement des données au repos conformes à la norme FIPS 140-2 :

- NetApp Storage Encryption (NSE) est une solution matérielle qui utilise des disques à chiffrement automatique.
- NetApp Volume Encryption (NVE) est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque où il est activé avec une clé unique pour chaque volume.
- NetApp Aggregate Encryption (NAE) est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque grâce à des clés uniques pour chaque agrégat.

NSE, NVE et NAE peuvent utiliser soit la gestion des clés externe, soit le gestionnaire de clés intégré (OKM). L'utilisation de NSE, NVE et NAE n'affecte pas les fonctionnalités d'efficacité du stockage ONTAP. Toutefois, les volumes NVE sont exclus de la déduplication dans les agrégats. Les volumes NAE participent à la déduplication dans les agrégats et en tirent profit.

Le gestionnaire de clés intégré OKM fournit une solution de chiffrement autonome pour les données au repos avec NSE, NVE ou NAE.

NVE, NAE et OKM utilisent le module de chiffrement ONTAP. CryptoMod figure dans la liste des modules validés CCVP FIPS 140-2. Voir ["FIPS 140-2 Cert. No 4144"](#).

Pour commencer la configuration de OKM, utilisez la `security key-manager onboard enable` commande. Pour configurer les gestionnaires de clés KMIP (Key Management Interoperability Protocol) externes, utilisez la `security key-manager external enable` commande. À partir de ONTAP 9.6, la colocation est prise en charge pour les gestionnaires de clés externes. Utiliser le `-vserver <vserver name>` paramètre pour activer la gestion externe des clés pour un SVM spécifique. Avant la version 9.6, la `security key-manager setup` commande servait à configurer OKM et des gestionnaires de clés externes. Pour la gestion intégrée des clés, cette configuration guide l'opérateur ou l'administrateur tout au

long de la configuration de la phrase de passe et des paramètres supplémentaires pour la configuration de OKM.

Une partie de la configuration est fournie dans l'exemple suivant :

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default
or omit a question, do not enter a value.

Would you like to configure onboard key management? {yes, no} [yes]:
Enter the cluster-wide passphrase for onboard key management. To continue
the configuration, enter the passphrase, otherwise
type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, save the encrypted configuration
data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager backup show"
command.
```

À partir de ONTAP 9.4, vous pouvez utiliser l' `-enable-cc-mode` option vrai avec `security key-manager setup` pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage. Pour ONTAP 9.6 et versions ultérieures, la syntaxe de la commande est `security key-manager onboard enable -cc -mode-enabled yes`.

À partir de ONTAP 9.4, vous pouvez utiliser la `secure-purge` fonctionnalité avec privilèges avancés pour « nettoyer » les données sur des volumes NVE sans interruption. Le nettoyage des données sur un volume chiffré garantit qu'elles ne peuvent pas être restaurées à partir du support physique. La commande suivante purge de manière sécurisée les fichiers supprimés sur vol1 sur SVM vs1 :

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

À partir de ONTAP 9.7, NAE et NVE sont activés par défaut si la licence VE est en place, OKM ou des gestionnaires de clés externes sont configurés et NSE n'est pas utilisé. Les volumes NAE sont créés par défaut sur les agrégats NAE et les volumes NVE sont créés par défaut sur des agrégats non NAE. Vous pouvez le remplacer en saisissant la commande suivante :

```
cluster1::*> options -option-name  
encryption.data_at_rest_encryption.disable_by_default true
```

À partir de la version ONTAP 9.6, vous pouvez utiliser une étendue SVM pour configurer la gestion externe des clés pour un SVM de données dans le cluster. Cette configuration est idéale pour les environnements mutualisés dans lesquels chaque locataire utilise un SVM différent (ou un ensemble de SVM) pour le service des données. Seul l'administrateur du SVM pour un locataire donné peut accéder aux clés pour ce locataire. Pour plus d'informations, reportez-vous à la section ["Activez la gestion externe des clés dans ONTAP 9.6 et versions ultérieures"](#) de la documentation ONTAP.

À partir de la version ONTAP 9.11.1, vous pouvez configurer la connectivité aux serveurs de gestion externe des clés en cluster en désignant des serveurs clés principaux et secondaires sur une SVM. Pour plus d'informations, reportez-vous à la section ["configurez les serveurs de clés externes en cluster"](#) de la documentation ONTAP.

À partir de ONTAP 9.13.1, vous pouvez configurer des serveurs de gestionnaire de clés externes dans le gestionnaire de système. Pour plus d'informations, reportez-vous à la section ["Gestion de gestionnaires de clés externes"](#) de la documentation ONTAP.

Chiffrement de réplication des données

Pour compléter le chiffrement des données au repos, vous pouvez chiffrer le trafic de réplication des données ONTAP entre les clusters à l'aide de TLS 1.2 avec une clé prépartagée pour SnapMirror, SnapVault ou FlexCache.

Lors de la réplication de données pour la reprise sur incident, la mise en cache ou la sauvegarde, vous devez protéger ces données lors du transport sur le réseau entre un cluster ONTAP et un autre. Cela permet d'éviter les attaques de l'homme du milieu malveillantes contre les données sensibles lorsqu'elles sont en transit.

À partir de ONTAP 9.6, le chiffrement de peering de cluster prend en charge le chiffrement TLS 1.2 AES-256 GCM pour les fonctionnalités de réplication des données ONTAP telles que SnapMirror, SnapVault et FlexCache. Le chiffrement est configuré au moyen d'une clé pré-partagée (PSK) entre deux pairs de cluster.

Les clients qui utilisent des technologies comme NSE, NVE et NAE pour protéger les données au repos peuvent également utiliser le chiffrement des données de bout en bout en passant à ONTAP 9.6 ou version ultérieure pour utiliser le chiffrement de cluster.

Le cluster peering chiffre toutes les données entre les pairs de cluster. Par exemple, lorsque vous utilisez SnapMirror, toutes les informations de peering ainsi que toutes les relations SnapMirror entre l'homologue du cluster source et l'homologue du cluster destination sont chiffrées. Vous ne pouvez pas envoyer de données en texte clair entre les pairs de cluster lorsque le chiffrement de peering de cluster est activé.

Depuis ONTAP 9.6, le chiffrement est activé par défaut pour les nouvelles relations entre clusters. Pour activer le chiffrement sur les relations entre clusters créées avant ONTAP 9.6, vous devez mettre à niveau le cluster source et le cluster de destination vers la version 9.6. En outre, vous devez utiliser `cluster peer modify` la commande pour modifier les pairs de cluster source et cible afin d'utiliser le chiffrement de peering de cluster.

Vous pouvez convertir une relation de pairs existante pour utiliser le chiffrement de peering de clusters dans ONTAP 9.6, comme illustré dans l'exemple suivant :

On the Destination Cluster Peer

```
cluster2::> cluster peer modify cluster1 -auth-status-admin use-  
authentication -encryption-protocol-proposed tls-psk
```

When prompted enter a passphrase.

On the Source Cluster Peer

```
cluster1::> cluster peer modify cluster2 -auth-status-admin use-  
authentication -encryption-protocol-proposed tls-psk
```

When prompted enter the same passphrase you created in the previous step.

Chiffrement IPsec des données en transit

Les clients qui utilisent des technologies de chiffrement des données au repos, telles que NetApp Storage Encryption (NSE) ou NetApp Volume Encryption (NVE) et Cluster Peering Encryption (CPE) pour le trafic de réplication des données peuvent désormais utiliser le chiffrement de bout en bout entre le client et le stockage dans l'ensemble de leur structure de données multicloud hybride en passant à ONTAP 9.8 ou version ultérieure et en utilisant IPsec : IPsec offre une alternative au chiffrement NFS ou SMB/CIFS et est la seule option de chiffrement à la volée pour le trafic iSCSI.

Dans certains cas, il peut être nécessaire de protéger toutes les données client transportées sur le réseau (ou en transit) vers le SVM ONTAP. Vous empêchez ainsi les attaques par réexécution et les attaques de l'homme du milieu malveillantes contre les données sensibles lorsqu'elles sont en transit.

À partir de la version ONTAP 9.8, IPsec offre la prise en charge du chiffrement de bout en bout pour l'ensemble du trafic IP entre un client et un SVM ONTAP. Le cryptage de données IPsec pour tout le trafic IP inclut les protocoles NFS, iSCSI et SMB/CIFS. IPsec fournit la seule option de cryptage en vol pour le trafic iSCSI.

Le chiffrement NFS sur le réseau est l'un des principaux cas d'utilisation d'IPsec. Avant ONTAP 9.8, le chiffrement NFS over-the-wire exigeait l'installation et la configuration de Kerberos pour utiliser krb5p afin de chiffrer les données NFS à la volée. Ce n'est pas toujours simple ou facile à accomplir dans chaque environnement client.

Les clients qui utilisent des technologies de chiffrement des données au repos, telles que NetApp Storage Encryption (NSE) ou NetApp Volume Encryption (NVE) et Cluster Peering Encryption (CPE) pour le trafic de réplication des données peuvent désormais utiliser le chiffrement de bout en bout entre le client et le stockage dans l'ensemble de leur structure de données multicloud hybride en passant à ONTAP 9.8 ou version ultérieure et en utilisant IPsec :

IPsec est une norme IETF. ONTAP utilise IPsec en mode transport. Il utilise également le protocole Internet Key Exchange (IKE) version 2, qui utilise une clé communiquée à l'avance (PSK) pour négocier les éléments clés entre le client et ONTAP avec IPv4 ou IPv6. Par défaut, IPsec utilise le chiffrement Suite-B AES-GCM 256 bits. Les normes Suite-B AES-GMAC256 et AES-CBC256 avec cryptage 256 bits sont également prises en charge.

Bien que la fonctionnalité IPsec doive être activée sur le cluster, elle s'applique aux adresses IP de SVM individuelles via l'utilisation d'une entrée de base de données de stratégie de sécurité (SPD). L'entrée de règle (SPD) contient l'adresse IP du client (sous-réseau IP distant), l'adresse IP du SVM (sous-réseau IP local), la suite de chiffrement à utiliser et le secret prépartagé (PSK) requis pour l'authentification via IKEv2 et l'établissement de la connexion IPsec. En plus de l'entrée de stratégie IPsec, le client doit être configuré avec les mêmes informations (IP locale et distante, PSK et suite de chiffrement) avant que le trafic puisse circuler sur la connexion IPsec. À partir de ONTAP 9.10.1, la prise en charge de l'authentification par certificat IPsec est ajoutée. Ceci supprime les limites de stratégie IPsec et active la prise en charge du système d'exploitation Windows pour IPsec.

S'il y a un pare-feu entre le client et l'adresse IP du SVM, il doit permettre aux protocoles ESP et UDP (port 500 et 4500), tant entrants (entrée) que sortants (sortie), de réussir la négociation IKEv2 et ainsi d'autoriser le trafic IPsec.

Pour NetApp SnapMirror et le chiffrement du trafic de peering de cluster, le chiffrement de peering de cluster (CPE) est toujours recommandé sur IPsec pour assurer la sécurité en transit sur le réseau. CPE fonctionne mieux pour ces charges de travail que IPsec. Vous n'avez pas besoin d'une licence pour IPsec et il n'y a pas de restrictions d'importation ou d'exportation.

Vous pouvez activer IPsec sur le cluster et créer une entrée SPD pour un seul client et une adresse IP de SVM unique, comme dans l'exemple suivant :

On the Destination Cluster Peer

```
cluster1::> security ipsec config modify -is-enabled true
```

```
cluster1::> security ipsec policy create -vserver vs1 -name test34 -local  
-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
```

When prompted enter and confirm the pre shared secret (PSK).

Mode FIPS et gestion TLS et SSL

La norme FIPS 140-2 spécifie les exigences de sécurité pour les modules cryptographiques dans les systèmes de sécurité qui protègent les informations sensibles dans les systèmes informatiques et de télécommunication. La norme FIPS 140-2 s'applique *spécifiquement* au module cryptographique plutôt qu'au produit, à l'architecture, aux données ou à l'écosystème. Le module cryptographique est le composant spécifique (matériel, logiciel, micrologiciel ou une combinaison des trois) qui implémente les fonctions de sécurité approuvées par le NIST.

L'activation de la conformité FIPS 140-2 a des effets sur d'autres systèmes et communications internes et externes à ONTAP 9. NetApp recommande vivement de tester ces paramètres sur un système hors production disposant d'un accès à la console.

À partir de la prise en charge de ONTAP 9.11.1 et TLS 1.3, vous pouvez valider FIPS 140-3.



La configuration FIPS s'applique à ONTAP et au contrôleur BMC de la plate-forme.

La configuration NetApp ONTAP FIPS-mode

NetApp ONTAP dispose d'une configuration FIPS-mode qui instancie un niveau de sécurité supplémentaire dans le plan de contrôle :

- À partir de ONTAP 9.11.1, lorsque le mode de conformité FIPS 140-2 est activé, TLSv1, TLSv1.1 et SSLv3 sont désactivés et seuls TLSv1.2 et TLSv1.3 restent activés. Elle affecte d'autres systèmes et communications internes et externes à ONTAP 9. Si vous activez le mode de conformité FIPS 140-2 puis désactivez-le, TLSv1, TLSv1.1 et SSLv3 restent désactivés. TLSv1 ou TLSv1.2 restent activés en fonction de la configuration précédente.
- Pour les versions de ONTAP antérieures à 9.11.1 lorsque le mode de conformité FIPS 140-2 est activé, TLSv1 et SSLv3 sont désactivés et seuls TLSv1.1 et TLSv1.2 restent activés. ONTAP vous empêche d'activer à la fois TLSv1 et SSLv3 lorsque le mode de conformité FIPS 140-2 est activé. Si vous activez le mode de conformité FIPS 140-2 puis désactivez-le, TLSv1 et SSLv3 restent désactivés, mais TLSv1.2 ou les deux TLSv1.1 et TLSv1.2 sont activés en fonction de la configuration précédente.
- ["Module de chiffrement NetApp \(NCSM\)"](#), Qui est certifié conforme à la norme FIPS 140-2 de niveau 1, assure la conformité logicielle.



Le NIST a soumis une norme FIPS-140-3 et NCSM sera conforme aux normes FIPS-140-2 et FIPS-140-3. Toutes les validations conformes à la norme FIPS 140-2 seront transférées à l'état historique le 21 septembre 2026, soit cinq ans après le dernier jour de soumission de nouveaux certificats.

Activez le mode de conformité FIPS-140-2 et FIPS-140-3

À partir de ONTAP 9, vous pouvez activer le mode de conformité FIPS-140-2 et FIPS-140-3 pour les interfaces du plan de contrôle au niveau du cluster.

- ["Activez FIPS"](#)
- ["Afficher le statut FIPS"](#)

Protocoles et activation FIPS

La `security config modify` commande permet de modifier la configuration de sécurité existante au niveau du cluster. Si vous activez le mode conforme FIPS, le cluster ne sélectionne automatiquement que les protocoles TLS.

- Utilisez le `-supported-protocols` paramètre pour inclure ou exclure des protocoles TLS indépendamment du mode FIPS. Par défaut, le mode FIPS est désactivé et ONTAP prend en charge les protocoles TLSv1.2, TLSv1.1 et TLSv1.
- Pour une compatibilité descendante, ONTAP prend en charge l'ajout de SSLv3 à la liste des protocoles pris en charge lorsque le mode FIPS est désactivé.

Activation et chiffrement FIPS

- Utilisez le `-supported-cipher-suites` paramètre pour configurer uniquement AES (Advanced Encryption Standard) ou AES et 3DES.
- Vous pouvez désactiver les chiffrements faibles tels que RC4 en spécifiant `!RC4`. Par défaut, le paramètre de chiffrement pris en charge est `ALL: !LOW: !aNULL: !EXP: !eNULL`. Ce paramètre signifie que toutes les suites de chiffrement prises en charge pour les protocoles sont activées, sauf celles utilisant des algorithmes de cryptage 64 bits ou 56 bits sans authentification, sans chiffrement, sans exportation et avec des suites de chiffrement à faible cryptage.

- Sélectionnez une suite de chiffrement disponible avec le protocole sélectionné correspondant. Une configuration non valide peut entraîner l'échec de certaines fonctionnalités.
- Pour connaître la syntaxe correcte de la chaîne de chiffrement, reportez-vous à ["page chiffrement"](#) la section sur OpenSSL (publiée par la base logicielle OpenSSL). Depuis ONTAP 9.9.1 et les versions ultérieures, il n'est plus nécessaire de redémarrer manuellement tous les nœuds après avoir modifié la configuration de sécurité.

Renforcement de la sécurité SSH et TLS

L'administration SSH de ONTAP 9 nécessite un client OpenSSH 5.7 ou une version ultérieure. Les clients SSH doivent négocier avec l'algorithme de clé publique ECDSA (Elliptic Curve Digital Signature Algorithm) pour que la connexion réussisse.

Pour renforcer la sécurité TLS, activez uniquement TLS 1.2 et utilisez des suites de chiffrement capables de traiter le secret PFS (Perfect Forward Secret). PFS est une méthode d'échange de clés qui, lorsqu'elle est utilisée en combinaison avec des protocoles de chiffrement tels que TLS 1.2, empêche un attaquant de déchiffrer toutes les sessions réseau entre un client et un serveur.

Activez les suites de chiffrement compatibles TLSv1.2 et PFS

Pour activer uniquement les suites de chiffrement compatibles TLS 1.2 et PFS, utilisez la `security config modify` commande du niveau de privilège avancé.



Avant de modifier la configuration de l'interface SSL, assurez-vous que le client prend en charge les chiffrements DHE et ECDHE lors de la connexion à ONTAP pour maintenir la connectivité avec ONTAP.

Exemple

```
cluster1::*> security config modify -interface SSL -supported-protocols  
TLSv1.2 -supported-cipher-suites  
PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

Confirmez `y` pour chaque invite. Pour plus d'informations sur PFS, voir ["Blog NetApp"](#).

Informations associées

["Norme fédérale de traitement de l'information \(FIPS\) publication 140"](#)

Créez un certificat numérique signé par une autorité de certification

Pour de nombreuses organisations, le certificat numérique auto-signé pour l'accès au Web ONTAP n'est pas conforme à leurs politiques InfoSec. Sur les systèmes de production, il est recommandé d'installer un certificat numérique signé par une autorité de certification pour l'authentification du cluster ou du SVM en tant que serveur SSL pour NetApp.

Vous pouvez utiliser `security certificate generate-csr` la commande pour générer une requête de signature de certificat (CSR) et la `security certificate install` commande pour installer le certificat que vous recevez de l'autorité de certification.

Étapes

1. Pour créer un certificat numérique signé par l'autorité de certification de l'organisation, procédez comme suit :
 - a. Générer une RSC.
 - b. Suivez la procédure de votre organisation pour demander un certificat numérique à l'aide de la RSC auprès de l'autorité de certification de votre organisation. Par exemple, à l'aide de l'interface Web Microsoft Active Directory Certificate Services, accédez à <CA_server_name>/certsrv et demandez un certificat.
 - c. Installez le certificat numérique dans ONTAP.

Protocole d'état du certificat en ligne

Le protocole OCSP (Online Certificate Status Protocol) permet aux applications ONTAP qui utilisent des communications TLS ou LDAP de recevoir le statut du certificat numérique lorsque OCSP est activé. L'application reçoit une réponse signée indiquant que le certificat demandé est valide, révoqué ou inconnu.

OCSP permet de déterminer le statut actuel d'un certificat numérique sans nécessiter de listes de révocation de certificats.

Par défaut, la vérification du statut du certificat OCSP est désactivée. Il peut être activé à l'aide de la commande `security config ocsp enable -app name`, où le nom de l'application peut être `autosupport`, `audit_log`, `fabricpool`, `ems`, `knip`, `ldap_ad`, `ldap_nis`, `namemap`, ou `all`. La commande nécessite un niveau de privilège avancé.

Gestion SSHv2

``security ssh modify`` La commande remplace les configurations existantes des algorithmes d'échange de clés SSH, des chiffrements ou des algorithmes MAC pour le cluster ou un SVM par les paramètres de configuration que vous spécifiez.

Recommandation NetApp :



- Utilisez des mots de passe pour les sessions utilisateur.
- Utiliser une clé publique pour accéder à la machine.

Chiffrements et échanges de clés pris en charge

Chiffrement	Échange de clés
aes256-ctr	diffie-hellman-group-Exchange-sha256 (SHA-2)
aes192-ctr	diffie-hellman-Group-Exchange-sha1 (SHA-1)
aes128-ctr	diffie-hellman-groupe14-sha1 (SHA-1)
aes256-cbc	diffie-hellman-groupe1-sha1 (SHA-1)
aes192-cbc	-

Chiffrement	Échange de clés
aes128-cbc	-
aes128-gcm	-
aes256-gcm	-
3des-cbc	-

Cryptage symétrique AES et 3DES pris en charge

ONTAP prend également en charge les types de chiffrement symétrique AES et 3DES suivants (également appelés chiffrement) :

- hmac-sha1
- hmac-sha1-96
- hmac-md5
- hmac-md5-96
- hmac-ripemd160
- umac-64
- umac-64
- umac-128
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1-etm
- hmac-sha1-96-etm
- hmac-sha2-256-etm
- hmac-sha2-512-etm
- hmac-md5-etm
- hmac-md5-96-etm
- hmac-ripemd160-etm
- umac-64-etm
- umac-128-etm



La configuration de gestion SSH s'applique à ONTAP et au contrôleur BMC de la plate-forme.

NetApp AutoSupport

La fonction AutoSupport de ONTAP vous permet de contrôler de manière proactive l'état de votre système et d'envoyer automatiquement des messages et des détails au support technique NetApp, à l'équipe de support interne de votre entreprise ou à un partenaire de support. Par défaut, les messages AutoSupport envoyés au support technique NetApp sont activés lorsque le système de stockage est configuré pour la première fois. De plus, AutoSupport commence à envoyer des messages au support technique NetApp 24

heures après son activation. Cette période de 24 heures est configurable. Pour tirer parti de la communication avec l'équipe de support interne d'une entreprise, la configuration de l'hôte de messagerie doit être effectuée.

Seul l'administrateur du cluster peut effectuer la gestion AutoSupport (configuration). L'administrateur du SVM n'a pas accès à AutoSupport. La fonction AutoSupport peut être désactivée. Toutefois, NetApp recommande de l'activer, car AutoSupport accélère l'identification et la résolution des problèmes en cas de problème sur le système de stockage. Par défaut, le système collecte les informations AutoSupport et les stocke localement même si vous désactivez AutoSupport.

Pour plus d'informations sur les messages AutoSupport, notamment sur ce qui se trouve dans les différents messages et sur l'emplacement d'envoi des différents types de messages, reportez-vous à la ["Conseiller digital NetApp Active IQ"](#) documentation.

Les messages AutoSupport contiennent des données sensibles, notamment, mais sans s'y limiter, les éléments suivants :

- Fichiers journaux
- Données contextuelles concernant des sous-systèmes spécifiques
- Données de configuration et d'état
- Les données de performance

AutoSupport prend en charge les protocoles de transport HTTPS, HTTP et SMTP. En raison des nature sensibles des messages AutoSupport, NetApp recommande fortement d'utiliser HTTPS comme protocole de transport par défaut pour l'envoi des messages AutoSupport au support NetApp.

De plus, vous devez utiliser `system node autosupport modify` la commande pour spécifier les cibles des données AutoSupport (par exemple, le support technique NetApp, les opérations internes d'une entreprise ou les partenaires). Cette commande vous permet également d'indiquer quelles informations AutoSupport spécifiques envoyer (par exemple, données de performances, fichiers journaux, etc.).

Pour désactiver entièrement AutoSupport, utilisez `system node autosupport modify -state disable` la commande.

Protocole de temps réseau

Bien que ONTAP vous permette de définir manuellement le fuseau horaire, la date et l'heure sur le cluster, vous devez configurer les serveurs NTP (Network Time Protocol) afin de synchroniser l'heure du cluster avec au moins trois serveurs NTP externes.

Les problèmes peuvent survenir lorsque l'heure du cluster est incorrecte. Bien que ONTAP vous permette de définir manuellement le fuseau horaire, la date et l'heure sur le cluster, vous devez configurer les serveurs NTP (Network Time Protocol) afin de synchroniser l'heure du cluster avec les serveurs NTP externes.

Depuis ONTAP 9.5, vous pouvez configurer votre serveur NTP avec une authentification symétrique.

Vous pouvez associer un maximum de 10 serveurs NTP externes à l'aide de la `cluster time-service ntp server create` commande. Pour la redondance et la qualité du service de temps, vous devez associer au moins trois serveurs NTP externes au cluster.

Pour plus de détails sur la configuration de NTP dans ONTAP, reportez-vous à la section ["Gestion de l'heure du cluster \(administrateurs du cluster uniquement\)"](#).

Comptes locaux du système de fichiers NAS (groupe de travail CIFS)

L'authentification des clients de groupe de travail offre une couche de sécurité supplémentaire à la solution ONTAP, qui est conforme à une posture d'authentification de domaine traditionnelle. Utilisez `vserver cifs session show` la commande pour afficher de nombreuses informations relatives au positionnement, notamment les informations IP, le mécanisme d'authentification, la version du protocole et le type d'authentification.

À partir de ONTAP 9, vous pouvez configurer un serveur CIFS dans un groupe de travail avec des clients CIFS qui s'authentifient auprès du serveur à l'aide d'utilisateurs et de groupes définis localement. L'authentification des clients de groupe de travail offre une couche de sécurité supplémentaire à la solution ONTAP, qui est conforme à une posture d'authentification de domaine traditionnelle. Pour configurer le serveur CIFS, utilisez `vserver cifs create` la commande. Une fois le serveur CIFS créé, vous pouvez le joindre à un domaine CIFS ou le joindre à un groupe de travail. Pour rejoindre un groupe de travail, utilisez le `-workgroup` paramètre. Voici un exemple de configuration :

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSEVER1  
-workgroup Sales
```



Un serveur CIFS en mode groupe de travail prend uniquement en charge l'authentification Windows NT LAN Manager (NTLM) et ne prend pas en charge l'authentification Kerberos.

NetApp recommande d'utiliser la fonction d'authentification NTLM avec des groupes de travail CIFS pour maintenir la sécurité de votre entreprise. Pour valider la posture de sécurité CIFS, NetApp recommande d'utiliser la `vserver cifs session show` commande pour afficher de nombreuses informations relatives au positionnement, notamment les informations IP, le mécanisme d'authentification, la version du protocole et le type d'authentification.

Audit du système de fichiers NAS

Les systèmes de fichiers NAS occupent une place de plus en plus importante dans le paysage actuel des menaces. Les fonctions d'audit sont essentielles pour assurer la visibilité des menaces.

La sécurité nécessite une validation. ONTAP 9 propose davantage d'événements d'audit et de détails dans l'ensemble de la solution. Dans la mesure où les menaces pèsent aujourd'hui sur les systèmes de fichiers NAS, les fonctions d'audit jouent un rôle essentiel pour assurer la visibilité. Grâce aux fonctionnalités d'audit améliorées de ONTAP 9, les informations d'audit CIFS sont plus que jamais abondantes. Les détails clés, y compris les suivants, sont consignés avec les événements créés :

- Accès aux fichiers, aux dossiers et au partage
- Fichiers créés, modifiés ou supprimés
- Accès en lecture du fichier réussi
- Échec des tentatives de lecture ou d'écriture des fichiers
- Modification des autorisations sur les dossiers

Créer une configuration d'audit

Vous devez activer l'audit CIFS pour générer des événements d'audit. Utiliser `vserver audit create` la commande pour créer une configuration d'audit. Par défaut, le journal d'audit utilise une méthode de rotation basée sur la taille. Vous pouvez utiliser une option de rotation basée sur le temps si elle est spécifiée dans le champ Paramètres de rotation. Les détails supplémentaires de la configuration de rotation de l'audit de journal incluent le planning de rotation, les limites de rotation, les jours de rotation de la semaine et la taille de rotation. Le texte suivant fournit un exemple de configuration d'audit utilisant une rotation mensuelle planifiée pour tous les jours de la semaine à 12:30.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule
-hour 12 -rotate-schedule-minute 30
```

Événements d'audit CIFS

Les événements d'audit CIFS sont les suivants :

- **Partage de fichiers** : génère un événement d'audit lorsqu'un partage réseau CIFS est ajouté, modifié ou supprimé à l'aide des commandes associées `vserver cifs share`.
- **Changement de stratégie d'audit** : génère un événement d'audit lorsque la stratégie d'audit est désactivée, activée ou modifiée à l'aide des commandes associées `vserver audit`.
- **Compte utilisateur** : génère un événement d'audit lorsqu'un utilisateur CIFS ou UNIX local est créé ou supprimé ; un compte utilisateur local est activé, désactivé ou modifié ; ou un mot de passe est réinitialisé ou modifié. Cet événement utilise la `vserver cifs users-and-groups local-group` commande ou la commande associée `vserver services name-service unix-user`.
- **Groupe de sécurité** : génère un événement d'audit lorsqu'un groupe de sécurité local CIFS ou UNIX est créé ou supprimé à l'aide de la `vserver cifs users-and-groups local-group` commande ou de la commande associée `vserver services name-service unix-group`.
- **Changement de stratégie d'autorisation** : génère un événement d'audit lorsque des droits sont accordés ou révoqués pour un utilisateur CIFS ou un groupe CIFS à l'aide de la `vserver cifs users-and-groups privilege` commande.



Cette fonctionnalité est basée sur la fonction d'audit du système, qui permet à un administrateur de vérifier ce que le système autorise et exécute du point de vue d'un utilisateur de données.

Effet des API REST sur l'audit NAS

ONTAP permet aux comptes d'administrateur d'accéder aux fichiers SMB/CIFS ou NFS et de les manipuler à l'aide d'API REST. Bien que les API REST puissent uniquement être exécutées par les administrateurs ONTAP, les commandes de l'API REST contournent le journal d'audit NAS du système. En outre, les administrateurs ONTAP peuvent également ignorer les autorisations liées aux fichiers lors de l'utilisation des API REST. Cependant, les actions de l'administrateur avec les API REST sur les fichiers sont capturées dans le journal de l'historique des commandes du système.

Créez un rôle d'API REST sans accès

Vous pouvez empêcher les administrateurs ONTAP d'utiliser des API REST pour l'accès aux fichiers en créant un rôle d'API REST qui n'a pas accès aux volumes ONTAP via REST. Pour configurer ce rôle, procédez

comme suit.

Étapes

1. Créez un nouveau rôle REST qui n'a pas accès aux volumes de stockage mais qui dispose de tout autre accès API REST.

```
cluster1::> security login rest-role create nofiles -vserver cluster1  
"/api/storage/volumes" -access none  
cluster1::> security login rest-role create nofiles -vserver cluster1  
"/api" -access all
```

2. Attribuez le compte administrateur au nouveau rôle d'API REST que vous avez créé à l'étape précédente.

```
cluster1::> security login modify -user-or-group-name user1 -application  
http -authentication-method password -vserver cluster1 -role nofile
```



Pour empêcher le compte d'administrateur de cluster ONTAP intégré d'utiliser les API REST pour accéder aux fichiers, vous devez d'abord ["créez un nouveau compte administrateur et désactivez ou supprimez le compte intégré"](#).

Configuration et activation de la signature et du chiffrement SMB CIFS

Vous pouvez configurer et activer la signature SMB qui protège la sécurité de la Data Fabric en veillant à ce que le trafic entre les systèmes de stockage et les clients ne soit pas compromis par des attaques par réexécution ou des attaques de l'homme du milieu. La signature SMB assure la protection en vérifiant que les messages SMB ont une signature valide.

Description de la tâche

Le protocole SMB constitue un vecteur de menaces courant pour les systèmes de fichiers et les architectures. Pour résoudre ce problème, la solution ONTAP 9 utilise la signature et le chiffrement SMB standard. La signature SMB protège la sécurité du maillage Data Fabric en s'assurant que le trafic entre les systèmes de stockage et les clients n'est pas compromis par des attaques par réexécution ou des attaques de l'homme du milieu. Il vérifie que les messages SMB ont une signature valide.

Bien que la signature SMB soit désactivée par défaut dans l'intérêt des performances, NetApp vous recommande fortement de l'activer. En outre, la solution ONTAP prend en charge le chiffrement SMB. Cette approche permet le transport sécurisé des données partage par partage. Le chiffrement SMB est désactivé par défaut. Cependant, NetApp vous recommande d'activer le chiffrement SMB.

La signature et le chiffrement LDAP sont désormais pris en charge dans SMB 2.0 et versions ultérieures. La signature (protection contre toute falsification) et le chiffrement (chiffrement) assurent une communication sécurisée entre les SVM et les serveurs Active Directory. Le chiffrement accéléré des nouvelles instructions AES (Intel AES ni) est désormais pris en charge par SMB 3.0 et les versions ultérieures. Intel AES ni améliore l'algorithme AES et accélère le chiffrement des données pour toute la gamme de processeurs compatibles.

Étapes

1. Pour configurer et activer la signature SMB, utilisez `vserver cifs security modify` la commande et vérifiez que le `-is-signing-required` paramètre est défini sur `true`. Voir l'exemple de configuration suivant :

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -is-signing-required true
```

2. Pour configurer et activer le chiffrement SMB et le chiffrement, utilisez `vserver cifs security modify` la commande et vérifiez que le `-is-smb-encryption-required` paramètre est défini sur `true`. Voir l'exemple de configuration suivant :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-----  -----
vs1      true
```

Sécurisation NFS

Les règles d'exportation sont les éléments fonctionnels d'une export-policy. Les règles d'exportation correspondent aux demandes d'accès client d'un volume par rapport à des paramètres spécifiques que vous configurez pour déterminer comment gérer les demandes d'accès client. Une export-policy doit contenir au moins une règle d'exportation pour permettre l'accès aux clients. Si une export-policy contient plusieurs règles, celles-ci sont traitées dans l'ordre dans lequel elles apparaissent dans l'export-policy.

Le contrôle d'accès est essentiel au maintien d'une posture de sécurité. Par conséquent, ONTAP utilise la fonctionnalité export policy pour limiter l'accès au volume NFS aux clients correspondant à des paramètres spécifiques. Les export-policy contiennent une ou plusieurs règles d'exportation qui traitent chaque requête d'accès client. Une export policy est associée à chaque volume afin de configurer l'accès client au volume. Le résultat de ce processus détermine si le client est autorisé ou refusé (avec un message d'autorisation refusée) à accéder au volume. Ce processus détermine également le niveau d'accès fourni au volume.



Pour que les clients puissent accéder aux données, une export policy doit exister sur un SVM. Un SVM peut contenir plusieurs export policies.

L'ordre des règles est dicté par le numéro d'index des règles. Si une règle correspond à un client, les autorisations de cette règle sont utilisées et aucune autre règle n'est traitée. Si aucune règle ne correspond, l'accès au client est refusé.

Les règles d'exportation déterminent les autorisations d'accès client en appliquant les critères suivants :

- Protocole d'accès aux fichiers utilisé par le client qui envoie la requête (par exemple, NFSv4 ou SMB)
- Un identifiant client (par exemple, le nom d'hôte ou l'adresse IP)
- Type de sécurité utilisé par le client pour l'authentification (par exemple, Kerberos v5, NTLM ou AUTH_SYS)

Si une règle spécifie plusieurs critères et que le client ne correspond pas à un ou plusieurs d'entre eux, la règle ne s'applique pas.

Un exemple de export-policy contient une règle d'export avec les paramètres suivants :

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Le type de sécurité détermine le niveau d'accès qu'un client reçoit. Les trois niveaux d'accès sont lecture seule, lecture-écriture et superutilisateur (pour les clients avec l'ID utilisateur 0). Comme le niveau d'accès déterminé par le type de sécurité est évalué dans cet ordre, vous devez respecter les règles répertoriées :

Règles pour les paramètres de niveau d'accès dans les règles d'exportation

Pour qu'un client obtienne les niveaux d'accès suivants	Ces paramètres d'accès doivent correspondre au type de sécurité du client
Lecture seule normale par l'utilisateur	Lecture seule (<code>-rorule</code>)
Lecture-écriture utilisateur normale	Lecture seule (<code>-rorule</code>) et lecture-écriture (<code>-rwrule</code>)
Super-utilisateur en lecture seule	Lecture seule (<code>-rorule</code>) et <code>-superuser</code>
Super-utilisateur lecture-écriture	Lecture seule (<code>-rorule</code>) et lecture-écriture (<code>-rwrule</code>) et <code>-superuser</code>


Les types de sécurité suivants sont valides pour chacun de ces trois paramètres d'accès :

- Toutes
- Aucune
- Jamais

Ces types de sécurité ne peuvent pas être utilisés avec le `-superuser` paramètre :

- `krb5`
- `ntlm`
- `system`

Règles pour les résultats des paramètres d'accès

Si le type de sécurité du client ...	Alors ...
Correspond à un type de sécurité spécifié dans le paramètre d'accès.	Le client reçoit l'accès pour ce niveau avec son propre ID utilisateur.
Ne correspond pas à un type de sécurité spécifié, mais le paramètre d'accès inclut l'option <code>none</code> .	Le client reçoit l'accès pour ce niveau et reçoit l'utilisateur anonyme avec l'ID utilisateur spécifié par le <code>-anon</code> paramètre.
Ne correspond pas à un type de sécurité spécifié et le paramètre d'accès n'inclut pas l'option <code>none</code> .	<div><div>Le client ne reçoit aucun accès pour ce niveau.</div><div> Cette restriction ne s'applique pas au <code>-superuser</code> paramètre car ce paramètre n'inclut toujours aucune, même si elle n'est pas spécifiée.</div></div>

Kerberos 5 et Krb5p

À partir de ONTAP 9, l'authentification Kerberos 5 avec service Privacy (krb5p) est prise en charge. Le mode d'authentification `krb5p` est sécurisé et offre une protection contre la falsification et l'espionnage des données. Il utilise des checksums pour chiffrer l'ensemble du trafic entre le client et le serveur. La solution ONTAP prend en charge le chiffrement AES 128 bits et 256 bits pour Kerberos. Le service de confidentialité comprend la vérification de l'intégrité des données reçues, l'authentification des utilisateurs et le cryptage des données avant leur transmission.

L'option `krb5p` est la plus présente dans la fonctionnalité `export policy`, où elle est définie comme option de cryptage. La méthode d'authentification `krb5p` peut être utilisée comme paramètre d'authentification, comme illustré dans l'exemple suivant :

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method krb5p -protocol nfs3
-access- type read
```

Activez la signature et le chiffrement du protocole d'accès aux répertoires légers

La signature et le chiffrement sont pris en charge pour permettre la sécurité des sessions lors de requêtes vers un serveur LDAP. Cette approche offre une alternative à la sécurité des sessions LDAP-over-TLS.

La signature valide l'intégrité des données LDAP à l'aide d'une technologie à clé secrète. Le chiffrement crypte les données LDAP afin de ne pas transmettre de données sensibles en clair. Les paramètres de sécurité de session sur un SVM correspondent à ceux disponibles sur le serveur LDAP. Par défaut, la signature et le chiffrement LDAP sont désactivés.

Étapes

1. Pour activer cette fonction, exécutez la `vserver cifs security modify` commande avec le `session-security-for-ad-ldap` paramètre.

Options des fonctions de sécurité LDAP :

- **Aucun** : par défaut, pas de signature ou de chiffrement
- **Sign** : signer le trafic LDAP
- **Sceau** : signer et crypter le trafic LDAP



Les paramètres de signe et de sceau sont cumulatifs, ce qui signifie que si l'option de signe est utilisée, le résultat est LDAP avec signature. Cependant, si l'option de joint est utilisée, le résultat est à la fois signé et joint. En outre, si aucun paramètre n'est spécifié pour cette commande, la valeur par défaut est aucun.

Voici un exemple de configuration :

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -session-security-for-ad-ldap seal
```

Créez et utilisez un NetApp FPolicy

Vous pouvez créer et utiliser un composant d'infrastructure FPolicy de la solution ONTAP, qui permet à des applications partenaires de surveiller et définir les autorisations d'accès aux fichiers. L'une des applications les plus puissantes est Storage Workload Security, une application SaaS NetApp qui offre une visibilité et un contrôle centralisés sur tous les accès aux données de l'entreprise dans les environnements de cloud hybride afin d'assurer la conformité et la sécurité.

Le contrôle d'accès est un concept de sécurité clé. La visibilité des accès aux fichiers et des opérations sur fichiers ainsi que la possibilité d'y réagir sont critiques pour maintenir le niveau de sécurité requis. Pour fournir cette visibilité et ce contrôle d'accès aux fichiers, la solution ONTAP utilise la fonction NetApp FPolicy.

Les règles peuvent être définies en fonction des types de fichiers. FPolicy détermine la façon dont le système de stockage gère les requêtes de chaque système client pour des opérations telles que les créations, ouvertures, renommages et suppressions. Depuis ONTAP 9, le système de notification d'accès aux fichiers FPolicy possède des commandes de filtrage et supporte de brèves coupures de réseau.

Étapes

1. Pour exploiter la fonction FPolicy, vous devez d'abord créer la règle FPolicy avec la `vserver fpolicy policy create` commande.



En outre, utilisez le `-events` paramètre si vous utilisez FPolicy pour la visibilité et la collecte des événements. La granularité supplémentaire fournie par ONTAP permet de filtrer les données et d'accéder au niveau de contrôle par nom d'utilisateur. Pour contrôler les privilèges et l'accès avec des noms d'utilisateur, spécifiez le `-privilege-user-name` paramètre.

Le texte suivant fournit un exemple de création FPolicy :


```
cluster1::> vserver fpolicy policy create -vserver vs1.example.com
-policy-name vs1_pol -events cserver_evt,vle1 -engine native -is
-mandatory true -allow-privileged-access no -is-passthrough-read-enabled
false
```

2. Une fois que vous avez créé la règle FPolicy, vous devez l'activer avec `vserver fpolicy enable` la commande. Cette commande définit également la priorité ou la séquence de l'entrée FPolicy.



La séquence FPolicy est importante car, si plusieurs règles ont souscrit au même événement d'accès aux fichiers, la séquence détermine l'ordre dans lequel l'accès est accordé ou refusé.

Le texte suivant fournit un exemple de configuration pour l'activation de la règle FPolicy et la validation de la configuration avec la `vserver fpolicy show` commande :

```
cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
vs2_pol -sequence-number 5

cluster1::> vserver fpolicy show
Vserver                Policy Name                Sequence  Status
Engine
-----
vs1.example.com        vs1_pol
vs2.example.com        vs2_pol
external
2 entries were displayed.
```

Améliorations de FPolicy

ONTAP 9 inclut les améliorations de FPolicy décrites dans les sections suivantes.

Filtrage des contrôles

De nouveaux filtres sont disponibles pour `SetAttr` et pour la suppression de notifications sur les activités d'annuaire.

Résilience asynchrone

Lorsqu'un serveur FPolicy fonctionnant en mode asynchrone est en panne du réseau, les notifications FPolicy générées lors de la panne sont stockées sur le nœud de stockage. Lorsque le serveur FPolicy est de nouveau en ligne, il est averti des notifications stockées et peut les récupérer du nœud de stockage. La durée pendant laquelle les notifications peuvent être stockées en cas de panne peut être configurée pendant 10 minutes.

Sécurité de LIF

Une LIF est une adresse IP ou un nom de port mondial (WWPN) avec des

caractéristiques associées, telles qu'un rôle, un port d'attache, un nœud d'attache, une liste de ports à basculer et une politique de pare-feu. Vous pouvez configurer les LIF sur les ports sur lesquels le cluster envoie et reçoit des communications sur le réseau. Il est essentiel de comprendre les caractéristiques de sécurité de chaque rôle de LIF.


Rôles LIF

Les rôles LIF peuvent être les suivants :

- **Data LIF** : une LIF associée à un SVM et utilisée pour communiquer avec les clients.
- **Cluster LIF** : une LIF utilisée pour transporter le trafic intracluster entre les nœuds d'un cluster.
- **Node management LIF** : une LIF qui fournit une adresse IP dédiée pour la gestion d'un nœud particulier dans un cluster.
- **Cluster management LIF** : une LIF qui fournit une interface de gestion unique pour l'ensemble du cluster.
- **Intercluster LIF** : une LIF utilisée pour la communication, la sauvegarde et la réplication entre clusters.

Caractéristiques de sécurité de chaque rôle de LIF

	LIF de données	LIF Cluster	FRV de gestion des nœuds	LIF de gestion de cluster	FRV InterCluster
Nécessite un sous-réseau IP privé ?	Non	Oui.	Non	Non	Non
Nécessite un réseau sécurisé ?	Non	Oui.	Non	Non	Oui.
Politique de pare-feu par défaut	Très restrictif	Entièrement ouvert	Moyen	Moyen	Très restrictif
Le pare-feu est-il personnalisable ?	Oui.	Non	Oui.	Oui.	Oui.

- 
- La LIF de cluster étant complètement ouverte sans règle de pare-feu configurable, elle doit se trouver sur un sous-réseau IP privé sur un réseau isolé et sécurisé.
 - Les rôles LIF ne doivent en aucun cas être exposés à Internet.

Pour en savoir plus sur la sécurisation des LIF, consultez le ["Configuration des politiques de pare-feu pour les LIF"](#).

Protocole et sécurité des ports

Outre les opérations et fonctions de sécurité intégrées, le renforcement d'une solution doit également inclure des mécanismes de sécurité externe. L'utilisation de dispositifs d'infrastructure supplémentaires, tels que des pare-feu, des systèmes de prévention des intrusions et d'autres dispositifs de sécurité, pour filtrer et limiter l'accès à ONTAP constitue un moyen efficace d'établir et de maintenir une stratégie de sécurité rigoureuse. Ces informations sont un élément clé pour filtrer et limiter l'accès à l'environnement et à ses ressources.

Protocoles et ports couramment utilisés

Service	Port/Protocole	Description
SSH	22/TCP	Connexion SSH
telnet	23/TCP	Connexion à distance
Domain	53/TCP	Serveur de noms de domaine
HTTP	80/TCP 80/UDP	HTTP
rpcbind	111/TCP 111/UDP	Appel de procédure à distance
NTP	123/UDP	Protocole de temps réseau
msrpc	135/UDP	Appel de procédure à distance Microsoft
Netbios-name	137/TCP 137/UDP	Service de noms NetBIOS
netbios-ssn	139/TCP	Session de service NetBIOS
SNMP	161/UDP	SNMP
HTTPS	443/TCP	Lien sécurisé :http
microsoft-ds	445/TCP	Services d'annuaire Microsoft
IPsec	500/UDP	Sécurité du protocole Internet
mount	635/UDP	Montage NFS
named	953/UDP	Nom démon
NFS	2049/UDP 2049/TCP	Démon du serveur NFS
nrv	2050/TCP	Protocole de volume distant NetApp
iscsi	3260/TCP	Port cible iSCSI
Lockd	4045/TCP 4045/UDP	Démon de verrouillage NFS
NFS	4046/TCP	Protocole de montage NFS
acp-proto	4046/UDP	Protocole de comptabilité
rquotad	4049/UDP	Protocole NFS rquotad
krb524	4444/UDP	Kerberos 524
IPsec	4500/UDP	Sécurité du protocole Internet
acp	5125/UDP 5133/UDP 5144/TCP	Autre port de contrôle pour le disque
Mdns	5353/UDP	DNS multicast
HTTPS	5986/UDP	Port HTTPS : protocole binaire d'écoute

Service	Port/Protocole	Description
TELNET	8023/TCP	Nœud-portée Telnet
HTTPS	8443/TCP	Outil 7MTT avec interface graphique via lien:HTTPS
RSH	8514/TCP	Portée du nœud RSH
KMIP	9877/TCP	Port client KMIP (hôte local interne uniquement)
ndmp	10000/TCP	NDMP
cifs port de témoin	40001/TCP	Port témoin CIFS
TLS	50000/TCP	Sécurité de la couche de transport
Iscsi	65200/TCP	Port iSCSI
SSH	65502/TCP	Coque sécurisée
vsun	65503/TCP	vsun

Ports internes NetApp

Port/Protocole	Description
900	RPC de cluster NetApp
902	RPC de cluster NetApp
904	RPC de cluster NetApp
905	RPC de cluster NetApp
910	RPC de cluster NetApp
911	RPC de cluster NetApp
913	RPC de cluster NetApp
914	RPC de cluster NetApp
915	RPC de cluster NetApp
918	RPC de cluster NetApp
920	RPC de cluster NetApp
921	RPC de cluster NetApp
924	RPC de cluster NetApp
925	RPC de cluster NetApp
927	RPC de cluster NetApp
928	RPC de cluster NetApp
929	RPC de cluster NetApp
931	RPC de cluster NetApp
932	RPC de cluster NetApp

Port/Protocole	Description
933	RPC de cluster NetApp
934	RPC de cluster NetApp
935	RPC de cluster NetApp
936	RPC de cluster NetApp
937	RPC de cluster NetApp
939	RPC de cluster NetApp
940	RPC de cluster NetApp
951	RPC de cluster NetApp
954	RPC de cluster NetApp
955	RPC de cluster NetApp
956	RPC de cluster NetApp
958	RPC de cluster NetApp
961	RPC de cluster NetApp
963	RPC de cluster NetApp
964	RPC de cluster NetApp
966	RPC de cluster NetApp
967	RPC de cluster NetApp
7810	RPC de cluster NetApp
7811	RPC de cluster NetApp
7812	RPC de cluster NetApp
7813	RPC de cluster NetApp
7814	RPC de cluster NetApp
7815	RPC de cluster NetApp
7816	RPC de cluster NetApp
7817	RPC de cluster NetApp
7818	RPC de cluster NetApp
7819	RPC de cluster NetApp
7820	RPC de cluster NetApp
7821	RPC de cluster NetApp
7822	RPC de cluster NetApp
7823	RPC de cluster NetApp
7824	RPC de cluster NetApp

Ressources de sécurité

Pour en savoir plus sur les informations décrites dans cette documentation de sécurité ONTAP, consultez les informations supplémentaires et concepts de sécurité suivants.

Pour plus d'informations sur le signalement de vulnérabilités et d'incidents, les réponses de sécurité NetApp et la confidentialité des clients, consultez le ["Portail de sécurité NetApp"](#).

- ["Notes de mise à jour de ONTAP 9"](#)
- ["Références des commandes ONTAP"](#)
- ["Administration de système"](#)
- ["Authentification administrateur et RBAC"](#)
- ["Chiffrement NetApp"](#)
- ["Tr-4647 : authentification multifacteur dans ONTAP 9.3"](#)
- ["Chiffrements OPENSSL"](#)
- ["CryptoMod FIPS-140-2 de niveau 1"](#)
- ["Authentification basée sur certificat avec le SDK de gestion NetApp pour ONTAP"](#)
- ["Gestion du réseau"](#)

Audit des événements NAS sur les SVM

Audit et suivi de sécurité SMB et NFS

Grâce à ONTAP, vous pouvez utiliser les fonctions d'audit de l'accès aux fichiers disponibles pour les protocoles SMB et NFS, comme l'audit natif et la gestion des règles de fichiers via FPolicy.

Vous devez concevoir et implémenter l'audit des événements d'accès aux fichiers SMB et NFS dans les circonstances suivantes :

- L'accès de base aux fichiers des protocoles SMB et NFS a été configuré.
- Vous souhaitez créer et gérer une configuration d'audit à l'aide de l'une des méthodes suivantes :
 - Fonctionnalité ONTAP native
 - Serveurs FPolicy externes

Audit des événements NAS sur les SVM

L'audit des événements NAS est une mesure de sécurité qui vous permet de suivre et de consigner certains événements SMB et NFS sur des serveurs virtuels de stockage (SVM). Cela vous permet de suivre les problèmes de sécurité potentiels et de prouver toute violation de la sécurité. Vous pouvez également définir et auditer les stratégies d'accès central Active Directory pour voir quel serait le résultat de leur mise en œuvre.

Événements SMB

Vous pouvez auditer les événements suivants :

- Événements d'accès aux fichiers et aux dossiers SMB

Vous pouvez auditer les événements d'accès aux fichiers et aux dossiers SMB sur des objets stockés sur des volumes FlexVol appartenant aux SVM activés à l'audit.

- Événements de connexion et de déconnexion SMB

Vous pouvez auditer les événements de connexion et de déconnexion SMB des serveurs SMB sur les SVM.

- Événements d'activation de stratégie d'accès central

Vous pouvez auditer l'accès effectif des objets sur les serveurs SMB à l'aide des autorisations appliquées à l'aide des règles d'accès centrales proposées. L'audit par la mise en place de stratégies d'accès central vous permet de voir quels sont les effets des stratégies d'accès central avant leur déploiement.

L'audit du staging des règles d'accès central est configuré à l'aide des GPO Active Directory. Cependant, la configuration d'audit du SVM doit être configurée pour auditer les événements de staging des règles d'accès central.

Bien que vous puissiez activer le staging de stratégie d'accès central dans la configuration d'audit sans activer le contrôle d'accès dynamique sur le serveur SMB, les événements de staging de stratégie d'accès central ne sont générés que si le contrôle d'accès dynamique est activé. Le contrôle d'accès dynamique est activé par le biais d'une option de serveur SMB. Elle n'est pas activée par défaut.

Événements NFS

Vous pouvez auditer les événements de fichier et de répertoire à l'aide des ACL NFSv4 sur des objets stockés sur les SVM.

Fonctionnement de l'audit

Concepts d'audit de base

Pour comprendre l'audit dans ONTAP, vous devez connaître certains concepts d'audit de base.

- **Fichiers de transfert**

Les fichiers binaires intermédiaires sur les nœuds individuels où les enregistrements d'audit sont stockés avant la consolidation et la conversion. Les fichiers de staging sont contenus dans des volumes de staging.

- **Volume de transfert**

Volume dédié créé par ONTAP pour stocker les fichiers de transfert. Il existe un volume intermédiaire par agrégat. Les volumes de sauvegarde sont partagés par toutes les machines virtuelles de stockage (SVM) activées par les audits, ce qui permet de stocker des enregistrements d'audit de l'accès aux données pour les volumes de données de cet agrégat particulier. Les enregistrements d'audit de chaque SVM sont stockés dans un répertoire distinct dans le volume intermédiaire.

Les administrateurs de cluster peuvent afficher des informations sur les volumes intermédiaires, mais la plupart des autres opérations de volume ne sont pas autorisées. Seul ONTAP peut créer des volumes intermédiaires. ONTAP attribue automatiquement un nom aux volumes intermédiaires. Tous les noms de volumes de staging commencent par MDV_aud_ Suivi par l'UUID de l'agrégat contenant ce volume intermédiaire (par exemple : MDV_aud_1d0131843d4811e296fc123478563412.)

- **Volumes système**

Un volume FlexVol qui contient des métadonnées spéciales, telles que les métadonnées pour les journaux d'audit des services de fichiers. Le SVM d'administration possède des volumes système qui sont visibles sur l'ensemble du cluster. Les volumes de staging sont un type de volume système.

- **Tâche de consolidation**

Tâche créée lorsque l'audit est activé. Cette tâche longue durée sur chaque SVM enregistre les enregistrements d'audit dans des fichiers intermédiaires dans les nœuds membres de la SVM. Cette tâche fusionne les enregistrements d'audit dans un ordre chronologique trié, puis les convertit en un format de journal d'événements lisible par l'utilisateur spécifié dans la configuration d'audit, soit au format de fichier EVTX soit au format XML. Les journaux d'événements convertis sont stockés dans le répertoire du journal des événements d'audit spécifié dans la configuration d'audit du SVM.

Fonctionnement du processus d'audit ONTAP

Le processus d'audit de ONTAP est différent du processus d'audit de Microsoft. Avant de configurer l'audit, vous devez comprendre le fonctionnement du processus d'audit ONTAP.

Les enregistrements d'audit sont initialement stockés dans des fichiers intermédiaires binaires sur des nœuds individuels. En cas d'audit sur un SVM, chaque nœud membre conserve les fichiers temporaires pour ce SVM. Ils sont régulièrement consolidés et convertis en journaux d'événements lisibles par l'utilisateur, qui sont stockés dans le répertoire du journal des événements d'audit de la SVM.

Processus lors de l'audit sur un SVM

L'audit peut uniquement être activé sur les SVM. Lorsque l'administrateur du stockage active l'audit sur le SVM, le sous-système d'audit vérifie si les volumes intermédiaires sont présents. Un volume de transfert doit exister pour chaque agrégat qui contient des volumes de données détenus par le SVM. Le sous-système d'audit crée tous les volumes de staging nécessaires s'ils n'existent pas.

Le sous-système d'audit effectue également d'autres tâches préalables avant l'activation de l'audit :

- Le sous-système d'audit vérifie que le chemin du répertoire des journaux est disponible et ne contient pas de symlinks.

Le répertoire log doit déjà exister sous la forme d'un chemin au sein du namespace du SVM. Il est recommandé de créer un nouveau volume ou qtree pour conserver les fichiers journaux d'audit. Le sous-système d'audit n'affecte pas d'emplacement de fichier journal par défaut. Si le chemin d'accès au répertoire du journal spécifié dans la configuration d'audit n'est pas un chemin valide, la création de la configuration d'audit échoue avec le `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` erreur.

La création de la configuration échoue si le répertoire existe mais contient des symlinks.

- L'audit planifie la tâche de consolidation.

Une fois cette tâche planifiée, l'audit est activé. La configuration d'audit du SVM et les fichiers journaux sont conservés lors d'un redémarrage ou si les serveurs NFS ou SMB sont arrêtés ou redémarrés.

Consolidation du journal des événements

La consolidation des journaux est une tâche planifiée qui s'exécute régulièrement jusqu'à ce que l'audit soit désactivé. Lorsque l'audit est désactivé, la tâche de consolidation vérifie que tous les journaux restants sont consolidés.

Audit garanti

L'audit est garanti par défaut. ONTAP garantit l'enregistrement de tous les événements d'accès aux fichiers vérifiables (tels que spécifiés par les ACL de règles d'audit configurées), même si un nœud n'est pas disponible. Une opération de fichier demandé ne peut pas être effectuée tant que l'enregistrement d'audit pour cette opération n'est pas enregistré dans le volume intermédiaire du stockage persistant. Si les enregistrements d'audit ne peuvent pas être archivés sur le disque dans les fichiers de transfert, soit en raison d'un espace insuffisant, soit en raison d'autres problèmes, les opérations client sont refusées.



Un administrateur ou un utilisateur de compte disposant d'un niveau de privilège peut contourner l'opération de journalisation d'audit de fichiers en utilisant le SDK de gestion NetApp ou les API REST. Vous pouvez déterminer si des actions ont été effectuées à l'aide du SDK de gestion NetApp ou des API REST en consultant les journaux de l'historique des commandes stockés dans le `audit.log` fichier.

Pour plus d'informations sur les journaux d'audit de l'historique des commandes, reportez-vous à la section « gestion de la journalisation d'audit pour les activités de gestion » du ["Administration du système"](#).

Processus de consolidation lorsqu'un nœud n'est pas disponible

Si un nœud contenant des volumes appartenant à un SVM dont l'audit est activé n'est pas disponible, le comportement de la tâche de consolidation d'audit dépend si le partenaire SFO (ou le partenaire HA dans le cas d'un cluster à deux nœuds) est disponible :

- Si le volume intermédiaire est disponible via le partenaire SFO, les volumes intermédiaires déclarés en dernier sur le nœud sont analysés et la consolidation s'effectue normalement.
- Si le partenaire SFO n'est pas disponible, la tâche crée un fichier journal partiel.

Lorsqu'un nœud est inaccessible, la tâche de consolidation consolide les enregistrements d'audit depuis les autres nœuds disponibles de ce SVM. Pour identifier qu'elle n'est pas terminée, la tâche ajoute le suffixe `.partial` au nom du fichier consolidé.

- Une fois le nœud indisponible disponible, les enregistrements d'audit de ce nœud sont consolidés avec les enregistrements d'audit des autres nœuds à ce moment-là.
- Tous les enregistrements d'audit sont conservés.

Rotation du journal des événements

Les fichiers journaux d'événements d'audit sont pivotés lorsqu'ils atteignent une taille de journal de seuil configurée ou dans une planification configurée. Lorsqu'un fichier journal d'événements est pivoté, la tâche de consolidation planifiée renomme d'abord le fichier actif converti en fichier d'archive horodaté, puis crée un nouveau fichier journal d'événements converti actif.

Processus lorsque l'audit est désactivé sur le SVM

Lorsque l'audit est désactivé sur le SVM, la tâche de consolidation est déclenchée une dernière fois. Tous les enregistrements d'audit en attente et enregistrés sont consignés dans un format lisible par l'utilisateur. Les

journaux d'événements stockés dans le répertoire du journal des événements ne sont pas supprimés lorsque l'audit est désactivé sur le SVM et sont disponibles pour l'affichage.

Une fois que tous les fichiers de données intermédiaires existants pour ce SVM sont consolidés, la tâche de consolidation est supprimée de la planification. La désactivation de la configuration d'audit de la SVM ne supprime pas la configuration d'audit. Un administrateur du stockage peut réactiver les audits à tout moment.

La tâche de consolidation d'audit, qui est créée lorsque l'audit est activé, surveille la tâche de consolidation et la recrée si la tâche de consolidation se ferme en raison d'une erreur. Les utilisateurs ne peuvent pas supprimer le travail de consolidation d'audit.

Exigences et considérations relatives à l'audit

Avant de configurer et d'activer l'audit sur votre serveur virtuel de stockage (SVM), vous devez connaître certaines exigences et considérations.

- Le nombre maximal de SVM pouvant être auditer dépend de votre version de ONTAP :

Version ONTAP	Maximum
9.8 et versions antérieures	50
9.9.1 et versions ultérieures	400

- L'audit n'est pas lié aux licences SMB ou NFS.

Vous pouvez configurer et activer l'audit même si les licences SMB et NFS ne sont pas installées sur le cluster.

- L'audit NFS prend en charge les ACE de sécurité (type U).
- Pour l'audit NFS, il n'y a pas de mappage entre les bits de mode et les ACE d'audit.

Lors de la conversion des ACL en bits de mode, les ACE d'audit sont ignorés. Lors de la conversion des bits de mode en listes de contrôle d'accès, les ACE d'audit ne sont pas générés.

- Le répertoire spécifié dans la configuration d'audit doit exister.

S'il n'existe pas, la commande de création de la configuration d'audit échoue.

- Le répertoire spécifié dans la configuration d'audit doit satisfaire aux exigences suivantes :
 - Le répertoire ne doit pas contenir de liens symboliques.

Si le répertoire spécifié dans la configuration d'audit contient des liens symboliques, la commande permettant de créer la configuration d'audit échoue.

- Vous devez spécifier le répertoire à l'aide d'un chemin d'accès absolu.

Vous ne devez pas spécifier de chemin relatif, par exemple, /vs1/. . /.

- L'audit dépend de l'espace disponible dans les volumes de transfert.

Vous devez connaître et planifier l'espace suffisant pour les volumes intermédiaires des agrégats contenant des volumes audités.

- L'audit dépend de l'espace disponible dans le volume contenant le répertoire dans lequel les journaux d'événements convertis sont stockés.

Vous devez connaître et disposer d'un plan vous assurant que l'espace disponible dans les volumes utilisés pour stocker les journaux d'événements est suffisant. Vous pouvez spécifier le nombre de journaux d'événements à conserver dans le répertoire d'audit en utilisant le `-rotate-limit` paramètre lors de la création d'une configuration d'audit, qui peut vous aider à vérifier que l'espace disponible pour les journaux d'événements du volume est suffisant.

- Bien que vous puissiez activer le staging de stratégie d'accès central dans la configuration d'audit sans activer le contrôle d'accès dynamique sur le serveur SMB, le contrôle d'accès dynamique doit être activé pour générer des événements de staging de stratégie d'accès central.

Le contrôle d'accès dynamique n'est pas activé par défaut.

Considérations relatives à l'espace des agrégats lors de l'activation des audits

Lorsqu'une configuration d'audit est créée et que l'audit est activé sur au moins une machine virtuelle de stockage (SVM) du cluster, le sous-système d'audit crée des volumes intermédiaires sur tous les agrégats existants et sur tous les nouveaux agrégats créés. Vous devez tenir compte de certaines considérations relatives à l'espace des agrégats lorsque vous activez l'audit sur le cluster.

La création d'un volume de transfert peut échouer en raison de l'absence de disponibilité de l'espace dans un agrégat. Cela peut se produire si vous créez une configuration d'audit et que les agrégats existants ne disposent pas d'espace suffisant pour contenir le volume d'activation.

Assurez-vous de disposer de suffisamment d'espace sur les agrégats existants pour les volumes intermédiaires avant d'activer l'audit sur une SVM.

Restrictions quant à la taille des enregistrements d'audit sur les fichiers intermédiaires

La taille d'un enregistrement d'audit sur un fichier temporaire ne peut pas être supérieure à 32 Ko.

Lorsque de grands enregistrements d'audit peuvent se produire

De grands enregistrements d'audit peuvent se produire lors de l'audit de gestion dans l'un des scénarios suivants :

- Ajout ou suppression d'utilisateurs à ou à partir de groupes comportant un grand nombre d'utilisateurs.
- Ajout ou suppression d'une liste de contrôle d'accès de partage de fichiers (ACL) sur un partage de fichiers avec un grand nombre d'utilisateurs de partage de fichiers.
- Autres scénarios.

Désactivez l'audit de gestion pour éviter ce problème. Pour ce faire, modifiez la configuration de l'audit et supprimez ce qui suit de la liste des types d'événements d'audit :

- partage de fichiers
- compte utilisateur
- groupe-de-sécurité

- autorisation-stratégie-modification

Après suppression, ils ne seront pas audités par le sous-système d'audit des services de fichiers.

Les effets des enregistrements d'audit trop importants

- Si la taille d'un enregistrement d'audit est trop importante (plus de 32 Ko), l'enregistrement d'audit n'est pas créé et le sous-système d'audit génère un message de système de gestion des événements (EMS) similaire à ce qui suit :

```
File Services Auditing subsystem failed the operation or truncated an audit
record because it was greater than max_audit_record_size value. Vserver
UUID=%s, event_id=%u, size=%u
```

Si l'audit est garanti, l'opération de fichier échoue car son enregistrement d'audit ne peut pas être créé.

- Si la taille de l'enregistrement d'audit est supérieure à 9,999 octets, le même message EMS est affiché. Un enregistrement d'audit partiel est créé avec une valeur de clé plus élevée manquante.
- Si l'enregistrement d'audit dépasse 2,000 caractères, le message d'erreur suivant s'affiche au lieu de la valeur réelle :

```
The value of this field was too long to display.
```

Formats du journal des événements d'audit pris en charge

Les formats de fichiers pris en charge pour les journaux d'événements d'audit convertis sont EVTX et XML formats de fichiers.

Vous pouvez spécifier le type de format de fichier lorsque vous créez la configuration d'audit. Par défaut, ONTAP convertit les journaux binaires en EVTX format de fichier.

Affiche les journaux d'événements d'audit

Vous pouvez utiliser les journaux d'événements d'audit pour déterminer si vous disposez de la sécurité adéquate des fichiers et si des tentatives d'accès incorrectes aux fichiers et aux dossiers ont été effectuées. Vous pouvez afficher et traiter les journaux d'événements d'audit enregistrés dans le EVTX ou XML formats de fichiers.

- EVTX format de fichier

Vous pouvez ouvrir le converti EVTX L'événement d'audit se connecte en tant que fichiers enregistrés à l'aide de Microsoft Event Viewer.

Vous pouvez utiliser deux options pour afficher les journaux d'événements à l'aide de l'Observateur d'événements :

- Vue générale

Les informations communes à tous les événements sont affichées pour l'enregistrement d'événement. Dans cette version de ONTAP, les données spécifiques à l'événement pour l'enregistrement d'événement ne sont pas affichées. Vous pouvez utiliser la vue détaillée pour afficher des données

spécifiques à un événement.

- Vue détaillée

Une vue conviviale et une vue XML sont disponibles. La vue conviviale et la vue XML affichent à la fois les informations communes à tous les événements et les données spécifiques à l'événement pour l'enregistrement d'événement.

- XML format de fichier

Vous pouvez afficher et traiter XML auditer les journaux d'événements sur des applications tierces prenant en charge le XML format de fichier. Les outils de visualisation XML peuvent être utilisés pour afficher les journaux d'audit à condition que vous ayez le schéma XML et des informations sur les définitions des champs XML. Pour plus d'informations sur le schéma XML et les définitions, reportez-vous au "[Référence de schéma d'audit ONTAP](#)".

Mode d'affichage des journaux d'audit actifs à l'aide de l'Observateur d'événements

Si le processus de consolidation d'audit est exécuté sur le cluster, le processus de consolidation ajoute de nouveaux enregistrements au fichier journal d'audit actif pour les serveurs virtuels de stockage (SVM) activés par audit. Ce journal d'audit actif est accessible et ouvert via un partage SMB dans Microsoft Event Viewer.

En plus d'afficher les enregistrements d'audit existants, Event Viewer dispose d'une option de rafraîchissement qui vous permet d'actualiser le contenu dans la fenêtre de la console. Si les journaux nouvellement ajoutés peuvent être consultés dans l'Observateur d'événements, cela dépend de l'activation ou non des oplocks sur le partage utilisé pour accéder au journal d'audit actif.

Paramètre oplocks sur le partage	Comportement
Activé	Event Viewer ouvre le journal qui contient les événements qui y sont écrits jusqu'à ce point dans le temps. L'opération d'actualisation n'actualise pas le journal avec de nouveaux événements ajoutés par le processus de consolidation.
Désactivé	Event Viewer ouvre le journal qui contient les événements qui y sont écrits jusqu'à ce point dans le temps. L'opération d'actualisation actualise le journal avec de nouveaux événements ajoutés par le processus de consolidation.



Ces informations ne s'appliquent que pour EVT_X journaux d'événements. XML Les journaux d'événements peuvent être affichés via SMB dans un navigateur ou via NFS à l'aide d'un éditeur ou d'un visualiseur XML.

Événements SMB pouvant être audités

Événements SMB pouvant être audités

ONTAP peut auditer certains événements SMB, notamment certains événements d'accès aux fichiers et aux dossiers, certains événements de connexion et de déconnexion, et des événements d'activation des règles d'accès central. Savoir quels événements

d'accès peuvent être audités est utile pour interpréter les résultats des journaux d'événements.

Les événements SMB supplémentaires suivants peuvent être audités dans ONTAP 9.2 et versions ultérieures :

ID D'ÉVÉNEMENT (EVT/EVTX)	Événement	Description	Catégorie
4670	Les autorisations d'objet ont été modifiées	ACCÈS AUX OBJETS : autorisations modifiées.	Accès aux fichiers
4907	Les paramètres d'audit d'objet ont été modifiés	ACCÈS À L'OBJET : paramètres d'audit modifiés.	Accès aux fichiers
4913	La stratégie d'accès à Object Central a été modifiée	ACCÈS À L'OBJET : BOUCHON MODIFIÉ.	Accès aux fichiers

Les événements SMB suivants peuvent être audités dans ONTAP 9.0 et versions ultérieures :

ID D'ÉVÉNEMENT (EVT/EVTX)	Événement	Description	Catégorie
540/4624	Un compte a été connecté avec succès	CONNEXION/DÉCONNEXION : connexion réseau (SMB).	Connexion et déconnexion
529/4625	Impossible de se connecter à un compte	CONNEXION/DÉCONNEXION : nom d'utilisateur inconnu ou mot de passe incorrect.	Connexion et déconnexion
530/4625	Impossible de se connecter à un compte	OUVERTURE/FERMETURE de SESSION : restriction de l'heure de connexion au compte.	Connexion et déconnexion
531/4625	Impossible de se connecter à un compte	CONNEXION/DÉCONNEXION : compte actuellement désactivé.	Connexion et déconnexion
532/4625	Impossible de se connecter à un compte	OUVERTURE/FERMETURE DE SESSION : le compte utilisateur a expiré.	Connexion et déconnexion
533/4625	Impossible de se connecter à un compte	OUVERTURE/FERMETURE DE SESSION : l'utilisateur ne peut pas se connecter à cet ordinateur.	Connexion et déconnexion
534/4625	Impossible de se connecter à un compte	OUVERTURE DE SESSION/DÉCONNEXION : l'utilisateur n'a pas accordé de type de connexion ici.	Connexion et déconnexion

535/4625	Impossible de se connecter à un compte	OUVERTURE/FERMETURE DE SESSION : le mot de passe de l'utilisateur a expiré.	Connexion et déconnexion
537/4625	Impossible de se connecter à un compte	OUVERTURE/FERMETURE de SESSION : la connexion a échoué pour des raisons autres que ci-dessus.	Connexion et déconnexion
539/4625	Impossible de se connecter à un compte	OUVERTURE DE SESSION/DÉCONNEXION : compte verrouillé.	Connexion et déconnexion
538/4634	Un compte a été déconnecté	OUVERTURE/FERMETURE DE SESSION : déconnexion de l'utilisateur local ou réseau.	Connexion et déconnexion
560/4656	Ouvrir objet/Créer objet	ACCÈS EN MODE OBJET : objet (fichier ou répertoire) ouvert.	Accès aux fichiers
563/4659	Ouvrez l'objet avec l'intention de supprimer	ACCÈS AUX OBJETS : un descripteur d'objet (fichier ou répertoire) a été demandé avec l'intention de supprimer.	Accès aux fichiers
564/4660	Supprimer l'objet	ACCÈS OBJET : supprimer l'objet (fichier ou répertoire). ONTAP génère cet événement lorsqu'un client Windows tente de supprimer l'objet (fichier ou répertoire).	Accès aux fichiers
567/4663	Lire objet/Ecrire objet/obtenir attributs d'objet/définir attributs d'objet	ACCÈS AUX OBJETS : tentative d'accès aux objets (lecture, écriture, obtenir l'attribut, définir l'attribut). Remarque : pour cet événement, ONTAP vérifie uniquement la première opération de lecture SMB et la première opération d'écriture SMB (succès ou échec) sur un objet. Cela empêche ONTAP de créer un nombre excessif d'entrées de journal lorsqu'un seul client ouvre un objet et effectue de nombreuses opérations de lecture ou d'écriture successives sur le même objet.	Accès aux fichiers
NA/4664	Lien dur	ACCÈS À L'OBJET : tentative de création d'un lien dur.	Accès aux fichiers

NA/4818	La politique d'accès central proposée n'accorde pas les mêmes autorisations d'accès que la politique d'accès central actuelle	ACCÈS AUX OBJETS : transfert de la stratégie d'accès central.	Accès aux fichiers
Na/NA - ID d'événement Data ONTAP 9999	Renommer l'objet	ACCÈS OBJET : objet renommé. Il s'agit d'un événement ONTAP. Windows ne prend actuellement pas en charge cet événement en tant qu'événement unique.	Accès aux fichiers
Na/NA Data ONTAP ID d'événement 9998	Dissocier l'objet	ACCÈS AUX OBJETS : objet non lié. Il s'agit d'un événement ONTAP. Windows ne prend actuellement pas en charge cet événement en tant qu'événement unique.	Accès aux fichiers

Informations supplémentaires sur l'événement 4656

Le `HandleID` dans l'audit XML event contient le descripteur de l'objet (fichier ou répertoire) accédé. Le `HandleID` La balise de l'événement EVT 4656 contient des informations différentes selon que l'événement ouvert permet de créer un nouvel objet ou d'ouvrir un objet existant :

- Si l'événement ouvert est une demande ouverte pour créer un nouvel objet (fichier ou répertoire), le `HandleID` La balise dans l'événement XML d'audit affiche un vide `HandleID` (par exemple : `<Data Name="HandleID">0000000000000000;00;00000000;00000000</Data>`).

Le `HandleID` Est vide car la demande OUVERTE (pour la création d'un nouvel objet) est auditée avant la création réelle de l'objet et avant qu'un descripteur n'existe. Les événements audités suivants pour le même objet ont le bon descripteur d'objet dans le `HandleID` balise :

- Si l'événement ouvert est une demande ouverte d'ouverture d'un objet existant, l'événement d'audit aura le descripteur affecté à cet objet dans le `HandleID` balise (par exemple : `<Data Name="HandleID">000000000000401;00;000000ea;00123ed4</Data>`).

Déterminez le chemin complet de l'objet vérifié

Le chemin d'accès de l'objet imprimé dans `<ObjectName>` la balise d'un enregistrement d'audit contient le nom du volume (entre parenthèses) et le chemin relatif de la racine du volume contenant. Si vous voulez déterminer le chemin complet de l'objet vérifié, y compris le chemin de jonction, il y a certaines étapes que vous devez suivre.

Étapes

1. Déterminez ce que correspond le nom du volume et le chemin relatif de l'objet vérifié en consultant le `<ObjectName>` balise dans l'événement d'audit.

Dans cet exemple, le nom du volume est "data1" et le chemin relatif vers le fichier est `/dir1/file.txt`:


```
<Data Name="ObjectName"> (data1);/dir1/file.txt </Data>
```

2. En utilisant le nom du volume déterminé à l'étape précédente, déterminez ce qu'est la Junction path du volume contenant l'objet vérifié :

Dans cet exemple, le nom du volume est "data1" et le chemin de jonction du volume contenant l'objet vérifié est /data/data1:

```
volume show -junction -volume data1
```

		Junction		Junction	
Vserver	Volume	Language	Active	Junction Path	Path Source
vs1	data1	en_US.UTF-8	true	/data/data1	RW_volume

3. Déterminez le chemin d'accès complet à l'objet vérifié en ajoutant le chemin d'accès relatif trouvé dans le <ObjectName> marquez la junction path du volume.

Dans cet exemple la Junction path du volume :

```
/data/data1/dir1/file.txt
```

Considérations relatives à l'audit des liens symlinks et des liens matériels

Il y a certaines considérations que vous devez garder à l'esprit lors de l'audit des liens symlinks et des liens matériels.

Un enregistrement d'audit contient des informations sur l'objet en cours d'audit, y compris le chemin d'accès à l'objet vérifié, qui est identifié dans le `ObjectName` balise : Vous devez savoir comment les chemins pour les liens symlinks et les liens rigides sont enregistrés dans le `ObjectName` balise :

Symlinks

Un symlink est un fichier avec un inode séparé qui contient un pointeur vers l'emplacement d'un objet de destination, appelé cible. Lors de l'accès à un objet via une symlink, ONTAP interprète automatiquement la symlink et suit le chemin canonique réel de protocole indépendant vers l'objet cible dans le volume.

Dans l'exemple de sortie suivant, il y a deux symlinks, tous deux pointant vers un fichier nommé `target.txt`. Un des symlinks est un symlink relatif et un est un symlink absolu. Si l'un des symlinks est vérifié, le `ObjectName` la balise de l'événement d'audit contient le chemin d'accès au fichier `target.txt`:

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

Liens matériels

Un lien dur est une entrée de répertoire qui associe un nom à un fichier existant sur un système de fichiers. Le lien matériel pointe vers l'emplacement d'inode du fichier d'origine. De la même manière que ONTAP interprète les symlinks, ONTAP interprète le lien rigide et suit le chemin canonique réel vers l'objet cible dans le volume. Lorsque l'accès à un objet de lien rigide est vérifié, l'événement d'audit enregistre ce chemin canonique absolu dans l' `ObjectName` marquez plutôt que le chemin du lien dur.

Points à prendre en compte lors de l'audit des autres flux de données NTFS

Vous devez garder à l'esprit certaines considérations lors de l'audit des fichiers avec les autres flux de données NTFS.

L'emplacement d'un objet vérifié est enregistré dans un enregistrement d'événement à l'aide de deux balises, le `ObjectName` tag (le chemin) et le `HandleID` étiquette (la poignée). Pour identifier correctement les demandes de flux en cours de journalisation, vous devez connaître les enregistrements ONTAP dans ces champs pour les flux de données alternatifs NTFS :

- EVTX ID : 4656 événements (ouvrir et créer des événements d'audit)
 - Le chemin du flux de données secondaire est enregistré dans le `ObjectName` balise :
 - La poignée du flux de données alternatif est enregistrée dans le `HandleID` balise :
- EVTX ID : 4663 événements (tous les autres événements d'audit, tels que lecture, écriture, getattr, etc.)
 - Le chemin du fichier de base, et non le flux de données secondaire, est enregistré dans le `ObjectName` balise :
 - La poignée du flux de données alternatif est enregistrée dans le `HandleID` balise :

Exemple

L'exemple suivant illustre comment identifier EVTX ID : 4663 événements pour d'autres flux de données à l'aide de l' `HandleID` balise : Même si le `ObjectName` la balise (chemin) enregistrée dans l'événement d'audit de lecture correspond au chemin du fichier de base, le `HandleID` la balise peut être utilisée pour identifier l'événement comme enregistrement d'audit pour le flux de données secondaire.

Les noms des fichiers de flux prennent le format `base_file_name:stream_name`. Dans cet exemple, le `dir1` le répertoire contient un fichier de base avec un autre flux de données ayant les chemins suivants :

```
/dir1/file1.txt  
/dir1/file1.txt:stream1
```



La sortie dans l'exemple d'événement suivant est tronquée comme indiqué ; la sortie n'affiche pas toutes les balises de sortie disponibles pour les événements.

Pour un EVTX ID 4656 (événement d'audit ouvert), la sortie de l'enregistrement d'audit du flux de données secondaire enregistre le nom du flux de données alternatif dans le `ObjectName` tag :

```

- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
</System>
- <EventData>
  [...]
  **<Data Name="ObjectType">Stream</Data>
  <Data Name="HandleID">00000000000401;00;000001e4;00176767</Data>
  <Data Name="ObjectName">\(data1\);/dir1/file1.txt:stream1</Data>
  **
  [...]
</EventData>
</Event>
- <Event>

```

Pour un EVT-X ID 4663 (lecture d'événement d'audit), la sortie de l'enregistrement d'audit du même flux de données alternatif enregistre le nom du fichier de base dans le `ObjectName` marqué, cependant, la poignée dans le `HandleID` tag est la poignée du flux de données alternatif et peut être utilisé pour mettre en corrélation cet événement avec l'autre flux de données :

```

- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
</System>
- <EventData>
  [...]
  **<Data Name="ObjectType">Stream</Data>
  <Data Name="HandleID">00000000000401;00;000001e4;00176767</Data>
  <Data Name="ObjectName">\(data1\);/dir1/file1.txt</Data> **
  [...]
</EventData>
</Event>
- <Event>

```

Les événements d'accès aux fichiers et aux répertoires NFS pouvant être vérifiés

ONTAP peut auditer certains événements d'accès aux fichiers et aux répertoires NFS. Savoir quels événements d'accès peuvent être audités est utile lors de l'interprétation

des résultats des journaux d'événements d'audit convertis.

Vous pouvez auditer les événements d'accès au répertoire et aux fichiers NFS suivants :

- LECTURE
- LA TRANSPARENCE
- FERMER
- READDIR
- ÉCRITURE
- DÉFINIR
- CRÉATION
- LIEN
- OPENATTR
- DÉPOSER
- GETATTR
- LA VÉRIFICATION
- NVÉRIFIER
- RENOMMER

Pour effectuer un audit fiable des événements DE RENOMMAGE NFS, vous devez définir des ACE d'audit sur les répertoires au lieu de fichiers car les autorisations de fichier ne sont pas vérifiées pour une opération DE RENOMMAGE si les autorisations de répertoire sont suffisantes.

Planification de la configuration d'audit

Avant de configurer l'audit sur les SVM (Storage Virtual machines), vous devez connaître les options de configuration disponibles et planifier les valeurs à définir pour chaque option. Ces informations peuvent vous aider à configurer la configuration d'audit qui répond aux besoins de votre entreprise.

Certains paramètres de configuration sont communs à toutes les configurations d'audit.

En outre, certains paramètres peuvent être utilisés pour spécifier les méthodes utilisées lors de la rotation des journaux d'audit consolidés et convertis. Vous pouvez spécifier l'une des trois méthodes suivantes lorsque vous configurez l'audit :

- Rotation des journaux en fonction de la taille du journal

Il s'agit de la méthode par défaut utilisée pour faire pivoter les journaux.

- Rotation des journaux en fonction d'un planning
- Rotation des journaux en fonction de la taille du journal et du planning (quel que soit l'événement qui se produit en premier)



Au moins une des méthodes de rotation du log doit toujours être définie.

Paramètres communs à toutes les configurations d'audit

Vous devez spécifier deux paramètres requis lors de la création de la configuration d'audit. Il existe également trois paramètres facultatifs que vous pouvez spécifier :

Type d'information	Option	Obligatoire	Inclure	Vos valeurs
<i>Nom du SVM</i> Nom du SVM sur lequel créer la configuration d'audit. Le SVM doit déjà exister.	<code>-vserver vserver_name</code>	Oui.	Oui.	
<i>Chemin de destination du journal</i> Spécifie le répertoire dans lequel les journaux d'audit convertis sont stockés, généralement un volume dédié ou un qtree. Le chemin doit déjà exister dans le namespace du SVM. Le chemin d'accès peut comporter jusqu'à 864 caractères et doit avoir des autorisations de lecture/écriture. Si le chemin n'est pas valide, la commande audit de configuration échoue. Si le SVM est une source de reprise après incident du SVM, le chemin de destination du journal ne peut pas se trouver sur le volume root. En effet, le contenu du volume racine n'est pas répliqué vers la destination de reprise après incident. Vous ne pouvez pas utiliser un volume FlexCache comme destination du journal (ONTAP 9.7 et versions ultérieures).	<code>-destination text</code>	Oui.	Oui.	

<p><i>Catégories d'événements à auditer</i></p> <p>Spécifie les catégories d'événements à auditer. Les catégories d'événements suivantes peuvent être auditées :</p> <ul style="list-style-type: none"> • Événements d'accès aux fichiers (SMB et NFSv4) • Événements de connexion et de déconnexion SMB • Événements d'activation de stratégie d'accès central <p>Les événements de transfert de stratégie d'accès central sont disponibles à partir des domaines Active Directory de Windows 2012.</p> <ul style="list-style-type: none"> • Événements de catégorie de partage de fichiers • Audit des événements de modification de règle • Événements locaux de gestion de compte utilisateur • Événements de gestion de groupe de sécurité • Événements de modification de la politique d'autorisation <p>La valeur par défaut consiste à auditer l'accès aux fichiers et les événements de connexion et de déconnexion SMB.</p> <p>Remarque : avant de pouvoir spécifier <code>cap-staging</code> En tant que catégorie d'événement, un serveur SMB doit exister sur le SVM. Bien que vous puissiez activer le staging de stratégie d'accès central dans la configuration d'audit sans activer le contrôle d'accès dynamique sur le serveur SMB, les événements de staging de stratégie d'accès central ne sont générés que si le contrôle d'accès dynamique est activé. Le contrôle d'accès dynamique est activé par le biais d'une option de serveur SMB. Elle n'est pas activée par défaut.</p>	<p><code>-events {file-ops</code></p>	<p><code>cifs- logon- logoff</code></p>	<p><code>cap- staging</code></p>	<p><code>file- share</code></p>
---	---------------------------------------	---	--------------------------------------	-------------------------------------

audit-policy-change	user-account	security-group	authorization-policy-change}	Non
		<p><i>Format de sortie du fichier journal</i></p> <p>Déterminez le format de sortie des journaux d'audit. Le format de sortie peut être spécifique à ONTAP XML Ou Microsoft Windows EVTX format du journal. Par défaut, le format de sortie est EVTX.</p>	-format {xml	evtx}

Non			<p><i>Limite de rotation des fichiers journaux</i></p> <p>Déterminer le nombre de fichiers journaux d'audit à conserver avant de faire pivoter le fichier journal le plus ancien vers l'extérieur. Par exemple, si vous saisissez une valeur de 5, les cinq derniers fichiers journaux sont conservés.</p> <p>Valeur de 0 indique que tous les fichiers journaux sont conservés. La valeur par défaut est 0.</p>	<p>-rotate -limit integer</p>
-----	--	--	--	---------------------------------------

Paramètres utilisés pour déterminer quand faire pivoter les journaux d'événements d'audit

Faire pivoter les journaux en fonction de la taille du journal

La valeur par défaut consiste à faire pivoter les journaux d'audit en fonction de la taille.

- La taille du journal par défaut est de 100 Mo
- Si vous souhaitez utiliser la méthode de rotation du journal par défaut et la taille du journal par défaut, vous n'avez pas besoin de configurer de paramètres spécifiques pour la rotation du journal.
- Si vous souhaitez faire pivoter les journaux d'audit en fonction d'une taille de journal seule, utilisez la commande suivante pour annuler la définition du `-rotate-schedule-minute` paramètre : `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

Si vous ne souhaitez pas utiliser la taille de journal par défaut, vous pouvez configurer le `-rotate-size` paramètre pour spécifier une taille de journal personnalisée :

Type d'information	Option	Obligatoire	Inclure	Vos valeurs
<i>Limite de taille du fichier journal</i> Détermine la limite de taille du fichier journal d'audit.	<code>-rotate-size {integer}[KO</code>	MO	GO	TO

Faire pivoter les journaux en fonction d'un horaire

Si vous choisissez de faire pivoter les journaux d'audit en fonction d'un planning, vous pouvez programmer la rotation du journal en utilisant les paramètres de rotation basés sur le temps dans n'importe quelle combinaison.

- Si vous utilisez une rotation basée sur le temps, le `-rotate-schedule-minute` paramètre obligatoire.
- Tous les autres paramètres de rotation basés sur le temps sont facultatifs.
- Le planning de rotation est calculé en utilisant toutes les valeurs liées au temps.

Par exemple, si vous spécifiez uniquement le `-rotate-schedule-minute` paramètre, les fichiers journaux d'audit sont pivotés en fonction des minutes spécifiées pour tous les jours de la semaine, pendant toutes les heures sur tous les mois de l'année.

- Si vous spécifiez uniquement un ou deux paramètres de rotation basés sur le temps (par exemple, `-rotate-schedule-month` et `-rotate-schedule-minutes`), les fichiers journaux pivotent en fonction des valeurs de minutes que vous avez spécifiées tous les jours de la semaine, pendant toutes les heures, mais seulement pendant les mois spécifiés.

Par exemple, vous pouvez préciser que le journal d'audit doit être tourné pendant les mois janvier, mars et août tous les lundis, mercredis et samedis à 10 h 30

- Si vous spécifiez des valeurs pour les deux `-rotate-schedule-dayofweek` et `-rotate-schedule-day`, ils sont considérés indépendamment.

Par exemple, si vous spécifiez `-rotate-schedule-dayofweek` Comme vendredi et `-rotate-schedule-day` Comme 13, les registres de vérification seront ensuite tournés tous les vendredis et les 13ème jours du mois spécifié, pas seulement tous les vendredis du 13ème.

- Si vous souhaitez faire pivoter les journaux d'audit en fonction d'une planification seule, utilisez la commande suivante pour annuler la définition du `-rotate-size` paramètre : `vserver audit modify -vserver vs0 -destination / -rotate-size -`

Vous pouvez utiliser la liste suivante de paramètres d'audit disponibles pour déterminer les valeurs à utiliser pour configurer un planning pour les rotations du journal d'événements d'audit :

Type d'information	Option	Obligatoire	Inclure	Vos valeurs
<p><i>Horaires de rotation du journal : mois</i></p> <p>Détermine le calendrier mensuel de rotation des journaux d'audit.</p> <p>Les valeurs valides sont January à December, et all. Par exemple, vous pouvez indiquer que le journal d'audit doit être pivoté pendant les mois janvier, mars et août.</p>	<p><code>-rotate-schedule-month</code> <code>chron_month</code></p>	Non		
<p><i>Horaires de rotation du journal : jour de la semaine</i></p> <p>Détermine le calendrier quotidien (jour de la semaine) pour la rotation des journaux d'audit.</p> <p>Les valeurs valides sont Sunday à Saturday, et all. Par exemple, vous pouvez préciser que le journal d'audit doit être tourné le mardi et le vendredi, ou pendant tous les jours d'une semaine.</p>	<p><code>-rotate-schedule</code> <code>-dayofweek</code> <code>chron_dayofweek</code></p>	Non		
<p><i>Horaires de rotation du journal : jour</i></p> <p>Détermine le jour du mois de la rotation du journal d'audit.</p> <p>Les valeurs valides vont de 1 à 31. Par exemple, vous pouvez indiquer que le journal d'audit doit être tourné les 10e et 20e jours d'un mois, ou tous les jours d'un mois.</p>	<p><code>-rotate-schedule-day</code> <code>chron_dayofmonth</code></p>	Non		

<p><i>Horaires de rotation du journal : heure</i></p> <p>Détermine le planning horaire pour la rotation du journal d'audit.</p> <p>Les valeurs valides vont de 0 de minuit à 23 (11 h 00). Spécification <code>all</code> fait pivoter les journaux d'audit toutes les heures. Par exemple, vous pouvez spécifier que le journal d'audit doit être tourné à 6 (6 h) et 18 (6 h).</p>	<p><code>-rotate-schedule-hour</code> <code>chron_hour</code></p>	Non		
<p><i>Horaires de rotation du journal : minute</i></p> <p>Détermine la planification des minutes pour la rotation du journal d'audit.</p> <p>Les valeurs valides vont de 0 à 59. Par exemple, vous pouvez indiquer que le journal d'audit doit être pivoté à la 30e minute.</p>	<p><code>-rotate-schedule-minute</code> <code>chron_minute</code></p>	Oui, si vous configurez une rotation de journal basée sur un planning, sinon non		

Faire pivoter les journaux en fonction de la taille du journal et de l'horaire

Vous pouvez choisir de faire pivoter les fichiers journaux en fonction de la taille du journal et d'une planification en définissant les deux `-rotate-size` paramètre et paramètres de rotation basés sur le temps dans n'importe quelle combinaison. Par exemple : si `-rotate-size` Est défini sur 10 Mo et `-rotate-schedule-minute` Est défini sur 15, les fichiers journaux pivotent lorsque la taille du fichier journal atteint 10 Mo ou la 15e minute de chaque heure (selon la première éventualité).

Créer une configuration d'audit de fichier et de répertoire sur les SVM

Créez la configuration d'audit

La création d'une configuration d'audit de fichier et de répertoire sur votre SVM (Storage Virtual machine) comprend les options de configuration disponibles, la planification de la configuration, puis la configuration et l'activation de la configuration. Vous pouvez ensuite afficher des informations sur la configuration d'audit pour confirmer que la configuration résultante est la configuration souhaitée.

Avant de pouvoir commencer l'audit des événements de fichiers et de répertoires, vous devez créer une configuration d'audit sur la machine virtuelle de stockage (SVM).

Avant de commencer

Si vous prévoyez de créer une configuration d'audit pour la mise en attente des règles d'accès central, un serveur SMB doit exister sur le SVM.



- Bien que vous puissiez activer le staging de stratégie d'accès central dans la configuration d'audit sans activer le contrôle d'accès dynamique sur le serveur SMB, les événements de staging de stratégie d'accès central ne sont générés que si le contrôle d'accès dynamique est activé.

Le contrôle d'accès dynamique est activé par le biais d'une option de serveur SMB. Elle n'est pas activée par défaut.

- Si les arguments d'un champ d'une commande ne sont pas valides, par exemple des entrées non valides pour les champs, des entrées dupliquées et des entrées non existantes, la commande échoue avant la phase d'audit.

Ces échecs ne génèrent pas d'enregistrement d'audit.

Description de la tâche

Si le SVM est une source de reprise d'activité du SVM, le chemin de destination ne peut pas se trouver sur le volume root.

Étape

1. À l'aide des informations de la fiche de planification, créez la configuration d'audit pour faire pivoter les journaux d'audit en fonction de la taille du journal ou d'une planification :

Si vous souhaitez faire pivoter les journaux d'audit en...	Entrer...
Taille du journal	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]]`
Un planning	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

Exemples

L'exemple suivant crée une configuration d'audit qui vérifie les opérations de fichiers et les événements de connexion et de déconnexion SMB (par défaut) à l'aide de la rotation basée sur la taille. Le format du journal est EVTX (valeur par défaut). Les journaux sont stockés dans le `/audit_log` répertoire. La taille limite du fichier journal est de 200 MB. Les journaux pivotent lorsqu'ils atteignent 200 Mo de taille :

```
cluster1::> vservers audit create -vservers vs1 -destination /audit_log  
-rotate-size 200MB
```

L'exemple suivant crée une configuration d'audit qui vérifie les opérations de fichiers et les événements de connexion et de déconnexion SMB (par défaut) à l'aide de la rotation basée sur la taille. Le format du journal est EVTX (valeur par défaut). Les journaux sont stockés dans le `/cifs_event_logs` répertoire. La taille limite du fichier journal est de 100 MB (valeur par défaut) et la limite de rotation du journal est 5:

```
cluster1::> vservers audit create -vservers vs1 -destination  
/cifs_event_logs -rotate-limit 5
```

L'exemple suivant crée une configuration d'audit qui audite les opérations de fichiers, les événements de connexion et de déconnexion CIFS, ainsi que les événements d'activation de stratégie d'accès central à l'aide d'une rotation basée sur le temps. Le format du journal est EVTX (valeur par défaut). Les journaux d'audit sont pivotés tous les mois, à 12:30 tous les jours de la semaine. La limite de rotation du log est de 5:

```
cluster1::> vservers audit create -vservers vs1 -destination /audit_log  
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-  
account,security-group,authorization-policy-change,cap-staging -rotate  
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour  
12 -rotate-schedule-minute 30 -rotate-limit 5
```

Informations associées

- ["Activation de l'audit sur le SVM"](#)
- ["Vérifiez la configuration de l'audit"](#)

Activation de l'audit sur le SVM

Une fois la configuration d'audit terminée, vous devez activer l'audit sur la machine virtuelle de stockage (SVM).

Avant de commencer

La configuration d'audit SVM doit déjà exister.

Description de la tâche

Lorsqu'une configuration SVM Disaster Recovery ID rebuter est démarrée en premier (une fois l'initialisation de SnapMirror terminée) et que le SVM dispose d'une configuration d'audit, ONTAP désactive automatiquement la configuration d'audit. L'audit est désactivé sur le SVM en lecture seule pour empêcher le remplissage des volumes de transit. Vous pouvez activer l'audit uniquement après la rupture de la relation SnapMirror et la SVM est read-write.

Étapes

1. Activer l'audit sur le SVM :

```
vservers audit enable -vservers vservers_name
```

```
vserver audit enable -vserver vs1
```

Informations associées

- ["Créez la configuration d'audit"](#)
- ["Vérifiez la configuration de l'audit"](#)

Vérifiez la configuration de l'audit

Une fois la configuration d'audit terminée, vous devez vérifier que l'audit est correctement configuré et activé.

Étapes

1. Vérifiez la configuration de l'audit :

```
vserver audit show -instance -vserver vserver_name
```

La commande suivante s'affiche sous forme de liste toutes les informations de configuration d'audit pour la machine virtuelle de stockage (SVM) vs1 :

```
vserver audit show -instance -vserver vs1
```

```
Vserver: vs1
Auditing state: true
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
Log Format: evt
Log File Size Limit: 200MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 0
```

Informations associées

- ["Créez la configuration d'audit"](#)
- ["Activation de l'audit sur le SVM"](#)

Configuration des règles d'audit des fichiers et des dossiers

Configuration des règles d'audit des fichiers et des dossiers

L'implémentation de l'audit sur les événements d'accès aux fichiers et aux dossiers est un processus en deux étapes. Vous devez d'abord créer et activer une configuration d'audit sur les serveurs virtuels de stockage (SVM). Ensuite, vous devez configurer des

stratégies d'audit sur les fichiers et dossiers que vous souhaitez surveiller. Vous pouvez configurer des stratégies d'audit pour surveiller les tentatives d'accès réussies et échouées.

Vous pouvez configurer les règles d'audit SMB et NFS. Les règles d'audit SMB et NFS diffèrent entre les exigences de configuration et les fonctionnalités d'audit.

Si les stratégies d'audit appropriées sont configurées, ONTAP surveille les événements d'accès SMB et NFS comme spécifié dans les règles d'audit uniquement si les serveurs SMB ou NFS sont exécutés.

Configurez les règles d'audit sur les répertoires et les fichiers de style de sécurité NTFS

Avant de pouvoir auditer les opérations de fichiers et de répertoires, vous devez configurer des stratégies d'audit sur les fichiers et répertoires pour lesquels vous souhaitez collecter les informations d'audit. Cela permet en plus de configurer et d'activer la configuration d'audit. Vous pouvez configurer les stratégies d'audit NTFS en utilisant l'onglet sécurité Windows ou l'interface de ligne de commande ONTAP.

Configuration des stratégies d'audit NTFS à l'aide de l'onglet sécurité de Windows

Vous pouvez configurer les stratégies d'audit NTFS sur les fichiers et les répertoires en utilisant l'onglet **sécurité Windows** de la fenêtre Propriétés Windows. Il s'agit de la même méthode utilisée lors de la configuration de stratégies d'audit sur des données résidant sur un client Windows, qui vous permet d'utiliser la même interface graphique que celle que vous êtes habitué à utiliser.

Avant de commencer

L'audit doit être configuré sur la machine virtuelle de stockage (SVM) qui contient les données auxquelles vous appliquez des listes de contrôle d'accès système (SACL).

Description de la tâche

La configuration des stratégies d'audit NTFS se fait en ajoutant des entrées aux SACL NTFS associées à un descripteur de sécurité NTFS. Le descripteur de sécurité est ensuite appliqué aux fichiers et répertoires NTFS. Ces tâches sont traitées automatiquement par l'interface graphique de Windows. Le descripteur de sécurité peut contenir des listes de contrôle d'accès discrétionnaire (DACL) pour l'application d'autorisations d'accès aux fichiers et aux dossiers, des listes SACL pour l'audit des fichiers et des dossiers, ou des listes SACL et des listes DACL.

Pour définir les stratégies d'audit NTFS à l'aide de l'onglet sécurité Windows, procédez comme suit sur un hôte Windows :

Étapes

1. Dans le menu **Tools** de l'Explorateur Windows, sélectionnez **Map network drive**.
2. Complétez la boîte **Map Network Drive** :
 - a. Sélectionnez une lettre **lecteur**.
 - b. Dans la zone **Folder**, saisissez le nom du serveur SMB qui contient le partage, en tenant les données à auditer et le nom du partage.

Vous pouvez indiquer l'adresse IP de l'interface de données du serveur SMB au lieu du nom du serveur SMB.

Si votre nom de serveur SMB est "SMB_SERVER" et que votre partage est nommé "share1", vous

devez entrer \\SMB_SERVER\share1.

c. Cliquez sur **Terminer**.

Le lecteur sélectionné est monté et prêt avec la fenêtre de l'Explorateur Windows affichant les fichiers et dossiers contenus dans le partage.

3. Sélectionnez le fichier ou le répertoire pour lequel vous souhaitez activer l'accès d'audit.
4. Cliquez avec le bouton droit de la souris sur le fichier ou le répertoire, puis sélectionnez **Propriétés**.
5. Sélectionnez l'onglet **sécurité**.
6. Cliquez sur **Avancé**.
7. Sélectionnez l'onglet **Audit**.
8. Effectuez les opérations souhaitées :

Si vous voulez	Procédez comme suit
Configuration de l'audit pour un nouvel utilisateur ou un nouveau groupe	<ol style="list-style-type: none">a. Cliquez sur Ajouter.b. Dans la zone entrer le nom de l'objet à sélectionner, saisissez le nom de l'utilisateur ou du groupe que vous souhaitez ajouter.c. Cliquez sur OK.
Supprimer l'audit d'un utilisateur ou d'un groupe	<ol style="list-style-type: none">a. Dans la zone entrer le nom de l'objet à sélectionner, sélectionnez l'utilisateur ou le groupe que vous souhaitez supprimer.b. Cliquez sur Supprimer.c. Cliquez sur OK.d. Ignorer le reste de cette procédure.
Modifier l'audit d'un utilisateur ou d'un groupe	<ol style="list-style-type: none">a. Dans la zone entrer le nom de l'objet à sélectionner, sélectionnez l'utilisateur ou le groupe que vous souhaitez modifier.b. Cliquez sur Modifier.c. Cliquez sur OK.

Si vous configurez l'audit sur un utilisateur ou un groupe ou si vous modifiez l'audit sur un utilisateur ou un groupe existant, la zone entrée d'audit pour <objet> s'ouvre.

9. Dans la case **appliquer à**, sélectionnez la façon dont vous souhaitez appliquer cette entrée d'audit.

Vous pouvez sélectionner l'une des options suivantes :

- **Ce dossier, sous-dossiers et fichiers**
- **Ce dossier et sous-dossiers**
- **Ce dossier uniquement**
- **Ce dossier et fichiers**
- **Sous-dossiers et fichiers uniquement**

- **Sous-dossiers uniquement**

- **Fichiers uniquement**

Si vous configurez l'audit sur un seul fichier, la case **appliquer à** n'est pas active. Le paramètre de case **appliquer à** est défini par défaut sur **cet objet uniquement**.



Étant donné que l'audit utilise les ressources de l'SVM, sélectionnez uniquement le niveau minimal qui fournit les événements d'audit qui répondent à vos exigences de sécurité.

10. Dans la case **Access**, sélectionnez ce que vous voulez auditer et si vous voulez auditer les événements réussis, les événements d'échec, ou les deux.

- Pour auditer les événements réussis, cochez la case succès.
- Pour auditer les événements d'échec, cochez la case échec.

Sélectionnez uniquement les actions à surveiller pour répondre à vos exigences de sécurité. Pour plus d'informations sur ces événements auditable, consultez votre documentation Windows. Vous pouvez auditer les événements suivants :

- **Contrôle total**
- **Dossier traverse / fichier d'exécution**
- **Liste de dossiers / lecture de données**
- **Lire les attributs**
- **Lire les attributs étendus**
- **Créer des fichiers / écrire des données**
- **Créer des dossiers / ajouter des données**
- **Ecrire des attributs**
- **Ecrire des attributs étendus**
- **Supprimer des sous-dossiers et des fichiers**
- **Supprimer**
- **Autorisations de lecture**
- **Modifier les autorisations**
- * Prendre possession*

11. Si vous ne souhaitez pas que le paramètre d'audit se propage aux fichiers et dossiers suivants du conteneur d'origine, sélectionnez la case **appliquer ces entrées d'audit aux objets et/ou aux conteneurs dans ce conteneur uniquement**.

12. Cliquez sur **appliquer**.

13. Une fois que vous avez terminé d'ajouter, de supprimer ou de modifier des entrées d'audit, cliquez sur **OK**.

La zone entrée d'audit pour <objet> se ferme.

14. Dans la zone **Audit**, sélectionnez les paramètres d'héritage de ce dossier.

Sélectionnez uniquement le niveau minimal qui fournit les événements d'audit qui répondent à vos exigences de sécurité. Vous pouvez choisir l'une des options suivantes :

- Sélectionnez l'option inclure les entrées d'audit héritées de la boîte parent de cet objet.

- Sélectionnez remplacer toutes les entrées d'audit héritées sur tous les descendants avec des entrées d'audit héritées de cet objet.
- Sélectionnez les deux cases.
- Sélectionnez aucune case.
Si vous définissez des SACLS sur un seul fichier, la boîte remplacer toutes les entrées d'audit héritées sur tous les descendants avec des entrées d'audit héritables de cet objet n'est pas présente dans la zone Audit.

15. Cliquez sur **OK**.

La zone Audit se ferme.

Configuration des règles d'audit NTFS à l'aide de l'interface de ligne de commande ONTAP

Vous pouvez configurer des stratégies d'audit sur des fichiers et des dossiers à l'aide de l'interface de ligne de commande ONTAP. Cela vous permet de configurer les stratégies d'audit NTFS sans avoir à vous connecter aux données à l'aide d'un partage SMB sur un client Windows.

Vous pouvez configurer les règles d'audit NTFS en utilisant le `vserver security file-directory` famille de commande.

Vous pouvez uniquement configurer les SACLS NTFS à l'aide de l'interface de ligne de commande. La configuration des SACLS NFSv4 n'est pas prise en charge avec cette famille de commandes ONTAP. Consultez les pages man pour plus d'informations sur l'utilisation de ces commandes pour configurer et ajouter des CLS NTFS aux fichiers et dossiers.

Configurer l'audit pour les fichiers et répertoires de style de sécurité UNIX

Vous configurez l'audit des répertoires et des fichiers de style de sécurité UNIX en ajoutant des ACE d'audit aux listes de contrôle d'accès NFSv4.x. Cela vous permet de surveiller certains événements d'accès aux fichiers et aux répertoires NFS à des fins de sécurité.

Description de la tâche

Pour NFSv4.x, les ACE discrétionnaires et système sont tous deux stockés dans la même liste de contrôle d'accès. Ils ne sont pas stockés dans des listes de contrôle d'accès (DACL) et des listes de contrôle d'accès (SALC) distinctes. Par conséquent, vous devez faire preuve de prudence lorsque vous ajoutez des ACE d'audit à une liste de contrôle d'accès existante pour éviter d'écraser et de perdre une liste de contrôle d'accès existante. L'ordre dans lequel vous ajoutez les ACE d'audit à une liste de contrôle d'accès existante n'a aucune importance.

Étapes

1. Récupérez la liste de contrôle d'accès existante pour le fichier ou le répertoire à l'aide de la `nfs4_getfacl` ou une commande équivalente.

Pour plus d'informations sur la manipulation des listes de contrôle d'accès, consultez les pages de manuels de votre client NFS.

2. Ajoutez les ACE d'audit souhaités.
3. Appliquez la liste de contrôle d'accès mise à jour au fichier ou au répertoire à l'aide de la `nfs4_setfacl` ou une commande équivalente.

Affiche des informations sur les stratégies d'audit appliquées aux fichiers et aux répertoires

Affiche des informations sur les stratégies d'audit à l'aide de l'onglet sécurité Windows

Vous pouvez afficher des informations sur les stratégies d'audit qui ont été appliquées aux fichiers et aux répertoires à l'aide de l'onglet sécurité de la fenêtre Propriétés de Windows. Cette méthode est identique à celle utilisée pour les données résidant sur un serveur Windows. Elle permet aux clients d'utiliser la même interface graphique qu'ils sont habitués.

Description de la tâche

L'affichage des informations sur les stratégies d'audit appliquées aux fichiers et aux répertoires vous permet de vérifier que les listes de contrôle d'accès système (SACL) appropriées sont définies sur les fichiers et dossiers spécifiés.

Pour afficher des informations sur les listes de contrôle d'application qui ont été appliquées aux fichiers et dossiers NTFS, procédez comme suit sur un hôte Windows.

Étapes

1. Dans le menu **Tools** de l'Explorateur Windows, sélectionnez **Map network drive**.
2. Renseignez la boîte de dialogue **Map Network Drive** :
 - a. Sélectionnez une lettre **lecteur**.
 - b. Dans la zone **Folder**, saisissez l'adresse IP ou le nom du serveur SMB de la machine virtuelle de stockage (SVM) contenant le partage contenant à la fois les données que vous souhaitez auditer et le nom du partage.

Si votre nom de serveur SMB est "SMB_SERVER" et que votre partage est nommé "share1", vous devez entrer \\SMB_SERVER\share1.



Vous pouvez indiquer l'adresse IP de l'interface de données du serveur SMB au lieu du nom du serveur SMB.

- c. Cliquez sur **Terminer**.

Le lecteur sélectionné est monté et prêt avec la fenêtre de l'Explorateur Windows affichant les fichiers et dossiers contenus dans le partage.

3. Sélectionnez le fichier ou le répertoire pour lequel vous affichez les informations d'audit.
4. Cliquez avec le bouton droit de la souris sur le fichier ou le répertoire et sélectionnez **Propriétés**.
5. Sélectionnez l'onglet **sécurité**.
6. Cliquez sur **Avancé**.
7. Sélectionnez l'onglet **Audit**.
8. Cliquez sur **Continuer**.

La boîte de dialogue Audit s'ouvre. La boîte de dialogue **Auditing Entries** affiche un récapitulatif des utilisateurs et des groupes auxquels des SACL sont appliquées.

9. Dans la zone **Auditing Entries**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez afficher les

entrées SACL.

10. Cliquez sur **Modifier**.

L'entrée Audit pour <Object> s'ouvre.

11. Dans la zone **Access**, affichez les CLS actuelles appliquées à l'objet sélectionné.

12. Cliquez sur **Annuler** pour fermer l'entrée **Audit pour <objet>**.

13. Cliquez sur **Annuler** pour fermer la case **Audit**.

Affiche des informations sur les règles d'audit NTFS sur les volumes FlexVol à l'aide de l'interface de ligne de commande

Vous pouvez afficher des informations sur les stratégies d'audit NTFS sur les volumes FlexVol, notamment les styles de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les listes de contrôle d'accès système. Vous pouvez utiliser ces informations pour valider votre configuration de sécurité ou résoudre les problèmes d'audit.

Description de la tâche

L'affichage des informations sur les stratégies d'audit appliquées aux fichiers et aux répertoires vous permet de vérifier que les listes de contrôle d'accès système (SACL) appropriées sont définies sur les fichiers et dossiers spécifiés.

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux fichiers ou dossiers dont vous souhaitez afficher les informations d'audit. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Les volumes et les qtrees de style de sécurité NTFS utilisent uniquement des listes de contrôle d'accès au système NTFS pour les stratégies d'audit.
- Les règles d'audit NTFS peuvent être appliquées aux fichiers et dossiers d'un volume de style de sécurité mixte avec la sécurité efficace NTFS.

Les volumes et qtrees de style de sécurité mixtes peuvent contenir certains fichiers et répertoires qui utilisent des autorisations de fichier UNIX, soit les bits de mode, soit les ACL NFSv4, ainsi que certains fichiers et répertoires utilisant les autorisations de fichier NTFS.

- Le niveau supérieur d'un volume de style de sécurité mixte peut avoir une sécurité efficace sous UNIX ou NTFS et peut-être ne pas contenir des CLS NTFS.
- Étant donné que la sécurité de Storage-Level Access Guard peut être configurée sur un volume mixte de style de sécurité, même si le style de sécurité efficace de la racine du volume ou de qtree est UNIX, La sortie d'un chemin de volume ou qtree dans lequel Storage-Level Access Guard est configuré peut afficher à la fois le fichier régulier et le dossier SACLs NFSv4 et les SACLs NTFS Storage-Level Access Guard.
- Si le chemin entré dans la commande est celui des données avec la sécurité effective NTFS, la sortie affiche également des informations sur les ACE de contrôle d'accès dynamique si le contrôle d'accès dynamique est configuré pour le chemin d'accès au fichier ou au répertoire donné.
- Lorsque vous affichez des informations de sécurité sur les fichiers et les dossiers avec la sécurité efficace NTFS, les champs de sortie liés à UNIX contiennent des informations d'autorisation de fichier UNIX en affichage uniquement.

Les fichiers et dossiers de style de sécurité NTFS utilisent uniquement les autorisations de fichier NTFS et les utilisateurs et groupes Windows lors de la détermination des droits d'accès aux fichiers.

- Les valeurs de sortie ACL s'affichent uniquement pour les fichiers et les dossiers disposant de la sécurité NTFS ou NFSv4.

Ce champ est vide pour les fichiers et les dossiers utilisant la sécurité UNIX qui n'ont que des autorisations de bit de mode appliquées (pas de listes de contrôle d'accès NFSv4).

- Les champs de sortie propriétaire et groupe de la sortie ACL ne s'appliquent que dans le cas des descripteurs de sécurité NTFS.

Étape

1. Afficher les paramètres de stratégie d'audit de fichier et de répertoire avec le niveau de détail souhaité :

Pour afficher les informations...	Saisissez la commande suivante...
Sous forme récapitulative	<code>vserver security file-directory show -vserver vserver_name -path path</code>
En tant que liste détaillée	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Exemples

L'exemple suivant affiche les informations de la stratégie d'audit pour le chemin `/corp` Au SVM `vs1`. Le chemin dispose d'une sécurité NTFS efficace. Le descripteur de sécurité NTFS contient à la fois une entrée RACL RÉUSSIE/ÉCHEC.

```

cluster::> vserver security file-directory show -vserver vs1 -path /corp
      Vserver: vs1
      File Path: /corp
      File Inode Number: 357
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8014
            Owner:DOMAIN\Administrator
            Group:BUILTIN\Administrators
            SACL - ACEs
                  ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                  SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
            DACL - ACEs
                  ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                  ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                  ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI

```

L'exemple suivant affiche les informations de la stratégie d'audit pour le chemin /datavol1 Au SVM vs1. Le chemin contient à la fois des fichiers standard et des SACL de dossier et des SALC de Storage-Level Access Guard.

```

cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

      Vserver: vs1
      File Path: /datavol1
      File Inode Number: 77
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xaa14
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            SACL - ACEs
                  AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
            DACL - ACEs
                  ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                  ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

      Storage-Level Access Guard security
      SACL (Applies to Directories):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

Moyens d'afficher des informations sur la sécurité des fichiers et les stratégies d'audit

Vous pouvez utiliser le caractère générique (*) pour afficher des informations sur la sécurité des fichiers et les stratégies d'audit de tous les fichiers et répertoires sous un

chemin donné ou un volume racine.

Le caractère générique (*) peut être utilisé comme dernier sous-composant d'un chemin d'accès de répertoire donné, sous lequel vous souhaitez afficher les informations de tous les fichiers et répertoires.

Si vous souhaitez afficher les informations d'un fichier ou d'un répertoire particulier nommé "", vous devez fournir le chemin complet à l'intérieur des guillemets doubles (" ").

Exemple

La commande suivante avec le caractère générique affiche les informations relatives à tous les fichiers et répertoires sous le chemin d'accès /1/ Du SVM vs1 :


```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*

      Vserver: vs1
      File Path: /1/1
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8514
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

      Vserver: vs1
      File Path: /1/1/abc
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8404
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

La commande suivante affiche les informations d'un fichier nommé "" sous le chemin d'accès /vol1/a Du SVM vs1. Le chemin est entouré de guillemets doubles (" ").

```
cluster::> vservers security file-directory show -vservers vs1 -path  
"/vol1/a/*"
```

```
      Vserver: vs1  
      File Path: "/vol1/a/*"  
      Security Style: mixed  
      Effective Style: unix  
      DOS Attributes: 10  
      DOS Attributes in Text: ----D---  
      Expanded Dos Attributes: -  
          Unix User Id: 1002  
          Unix Group Id: 65533  
          Unix Mode Bits: 755  
      Unix Mode Bits in Text: rwxr-xr-x  
          ACLs: NFSV4 Security Descriptor  
              Control:0x8014  
              SACL - ACEs  
                  AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA  
              DACL - ACEs  
                  ALLOW-EVERYONE@-0x1f00a9-FI|DI  
                  ALLOW-OWNER@-0x1f01ff-FI|DI  
                  ALLOW-GROUP@-0x1200a9-IG
```

Les événements de modification de l'interface de ligne de commande peuvent être audités

Les événements de modification de la CLI pouvant être audités

ONTAP peut auditer certains événements de modification de l'interface de ligne de commandes, notamment certains événements de partage SMB, certains événements de stratégie d'audit, certains événements de groupe de sécurité local, des événements de groupe d'utilisateurs locaux et des événements de politique d'autorisation. Il est utile de savoir quels événements de modification peuvent être audités lors de l'interprétation des résultats des journaux d'événements.

Vous pouvez gérer les événements de modification de l'interface de ligne de commande d'audit des machines virtuelles de stockage (SVM) en faisant tourner manuellement les journaux d'audit, en activant ou désactivant l'audit, en affichant des informations sur l'audit des événements de modification, en modifiant l'audit des événements et en supprimant les événements d'audit des modifications.

En tant qu'administrateur, si vous exécutez une commande pour modifier la configuration relative aux événements SMB-share, local user-group, local Security-group, autorisation-policy et audit-policy, un enregistrement génère et l'événement correspondant est vérifié :

Catégorie d'audit	Événements	ID d'événement	Exécuter cette commande...
-------------------	------------	----------------	----------------------------

Audit Mhost	modification de règles	[4719] Configuration d'audit modifiée	`vserver audit disable
enable	modify`	partage de fichiers	[5142] le partage réseau a été ajouté
vserver cifs share create	[5143] le partage réseau a été modifié	vserver cifs share modify `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] partage réseau supprimé	vserver cifs share delete
Audit	compte utilisateur	[4720] utilisateur local créé	vserver cifs users-and-groups local-user create vserver services name-service unix-user create
[4722] utilisateur local activé	`vserver cifs users-and-groups local-user create	modify`	[4724] Réinitialisation du mot de passe de l'utilisateur local
vserver cifs users-and-groups local-user set-password	[4725] utilisateur local désactivé	`vserver cifs users-and-groups local-user create	modify`
[4726] utilisateur local supprimé	vserver cifs users-and-groups local-user delete vserver services name-service unix-user delete	[4738] modification de l'utilisateur local	vserver cifs users-and-groups local-user modify vserver services name-service unix-user modify
[4781] utilisateur local Renommer	vserver cifs users-and-groups local-user rename	groupe-de-sécurité	[4731] Groupe de sécurité local créé
vserver cifs users-and-groups local-group create vserver services name-service unix-group create	[4734] Groupe de sécurité local supprimé	vserver cifs users-and-groups local-group delete vserver services name-service unix-group delete	[4735] Groupe de sécurité local modifié

<code>`vserver cifs users-and-groups local-group rename</code>	<code>modify` vserver services name-service unix-group modify</code>	[4732] utilisateur ajouté au groupe local	<code>vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser</code>
[4733] utilisateur supprimé du groupe local	<code>vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser</code>	autorisation-stratégie-modification	[4704] droits d'utilisateur attribués
<code>vserver cifs users-and-groups privilege add-privilege</code>	[4705] droits d'utilisateur supprimés	<code>`vserver cifs users-and-groups privilege remove-privilege</code>	<code>reset-privilege`</code>

Gérer un événement de partage de fichiers

Lorsqu'un événement de partage de fichiers est configuré pour un SVM (Storage Virtual machine) et qu'un audit est activé, des événements d'audit sont générés. Les événements de partage de fichiers sont générés lorsque le partage réseau SMB est modifié à l'aide de `vserver cifs share` commandes associées

Les événements de partage de fichiers avec les id-événements 5142, 5143 et 5144 sont générés lorsqu'un partage réseau SMB est ajouté, modifié ou supprimé pour la SVM. La configuration du partage réseau SMB est modifiée à l'aide du `cifs share access control create|modify|delete` commandes.

L'exemple suivant affiche un événement de partage de fichiers avec l'ID 5143 est généré lorsqu'un objet de partage appelé « `audit_dest` » est créé :

```

netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
    [ Name]   NetApp-Security-Auditing
    [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
    EventID 5142
    EventName Share Object Added
    ...
    ...
    ShareName audit_dest
    SharePath /audit_dest
    ShareProperties oplocks;browsable;changenotify;show-previous-versions;
    SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;;FA;;;WD)

```

Gestion de l'événement audit-policy-change

Lorsqu'un événement d'audit-policy-change est configuré pour une machine virtuelle de stockage (SVM) et qu'un audit est activé, des événements d'audit sont générés. Les événements audit-règle-modification sont générés lorsqu'une règle d'audit est modifiée à l'aide de `vserver audit` commandes associées

L'événement audit-policy-change avec l'ID-événement 4719 est généré chaque fois qu'une stratégie d'audit est désactivée, activée ou modifiée et aide à identifier quand un utilisateur tente de désactiver l'audit pour couvrir les pistes. Il est configuré par défaut et requiert un privilège de diagnostic pour être désactivé.

L'exemple suivant montre un événement de modification de règle d'audit avec l'ID 4719 généré lorsqu'un audit est désactivé :

```

netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
    [ Name]   NetApp-Security-Auditing
    [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
    EventID 4719
    EventName Audit Disabled
    ...
    ...
    SubjectUserName admin
    SubjectUserSid 65533-1001
    SubjectDomainName ~
    SubjectIP console
    SubjectPort

```

Gérer un événement de compte utilisateur

Lorsqu'un événement de compte utilisateur est configuré pour une machine virtuelle de stockage (SVM) et qu'un audit est activé, des événements d'audit sont générés.

Les événements du compte utilisateur avec les id-événements 4720, 4722, 4724, 4725, 4726, 4738 et 4781 sont générés lorsqu'un utilisateur SMB ou NFS local est créé ou supprimé du système, le compte d'utilisateur local est activé, désactivé ou modifié et le mot de passe de l'utilisateur SMB local est réinitialisé ou modifié. Les événements du compte utilisateur sont générés lorsqu'un compte utilisateur est modifié à l'aide de `vserver cifs users-and-groups <local user>` et `vserver services name-service <unix user>` commandes.

L'exemple suivant montre un événement de compte d'utilisateur avec l'ID 4720 généré lors de la création d'un utilisateur SMB local :

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
EventID 4720
EventName Local Cifs User Created
...
...
TargetUserName testuser
TargetDomainName NETAPP-CLUS1
TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
TargetType CIFS
DisplayName testuser
PasswordLastSet 1472662216
AccountExpires NO
PrimaryGroupId 513
UserAccountControl %%0200
SidHistory ~
PrivilegeList ~
```

L'exemple suivant affiche un événement de compte utilisateur avec l'ID 4781 généré lorsque l'utilisateur SMB local créé dans l'exemple précédent est renommé :

```

netapp-clus1::*> vservers cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4781
  EventName Local Cifs User Renamed
  ...
  ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~

```

Gérer l'événement de groupe de sécurité

Lorsqu'un événement de groupe de sécurité est configuré pour une machine virtuelle de stockage (SVM) et qu'un audit est activé, des événements d'audit sont générés.

Les événements du groupe de sécurité avec les id-événements 4731, 4732, 4733, 4734 et 4735 sont générés lorsqu'un groupe SMB ou NFS local est créé ou supprimé du système et que l'utilisateur local est ajouté ou supprimé du groupe. Les événements groupe-sécurité sont générés lorsqu'un compte utilisateur est modifié à l'aide de `vservers cifs users-and-groups <local-group>` et `vservers services name-service <unix-group>` commandes.

L'exemple suivant montre un événement de groupe de sécurité avec l'ID 4731 généré lors de la création d'un groupe de sécurité UNIX local :

```

netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4731
  EventName Local Unix Security Group Created
  ...
  ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~

```

Gérer l'événement autorisation-stratégie-modification

Lorsque l'événement autorisation-policy-change est configuré pour une machine virtuelle de stockage (SVM) et qu'un audit est activé, des événements d'audit sont générés.

Les événements autorisation-policy-change avec les id-événements 4704 et 4705 sont générés chaque fois que les droits d'autorisation sont accordés ou révoqués pour un utilisateur SMB et un groupe SMB. Les événements autorisation-stratégie-modification sont générés lorsque les droits d'autorisation sont affectés ou révoqués à l'aide de `vserver cifs users-and-groups privilege` commandes associées

L'exemple suivant affiche un événement de stratégie d'autorisation avec l'ID 4704 généré lorsque les droits d'autorisation d'un groupe d'utilisateurs SMB sont affectés :


```

netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID   4704
  EventName User Right Assigned
  ...
  ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
  SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS

```

Gérer les configurations d'audit

Rotation manuelle des journaux d'événements d'audit

Avant de pouvoir afficher les journaux d'événements d'audit, ils doivent être convertis en formats lisibles par l'utilisateur. Si vous souhaitez afficher les journaux des événements d'une machine virtuelle de stockage (SVM) spécifique avant que ONTAP ne fasse automatiquement pivoter le journal, vous pouvez faire tourner manuellement les journaux des événements d'audit sur un SVM.

Étape

1. Faites pivoter les journaux d'événements d'audit à l'aide de `vserver audit rotate-log` commande.

```
vserver audit rotate-log -vserver vs1
```

Le journal des événements d'audit est enregistré dans le répertoire du journal des événements d'audit SVM au format spécifié par la configuration d'audit (XML ou EVTX), et peut être consulté à l'aide de l'application appropriée.

Activation et désactivation de l'audit sur les SVM

Vous pouvez activer ou désactiver l'audit sur les serveurs virtuels de stockage (SVM). Vous pouvez désactiver l'audit des fichiers et des répertoires temporairement. Vous pouvez activer l'audit à tout moment (si une configuration d'audit existe).

Ce dont vous avez besoin

Avant de pouvoir activer l'audit sur le SVM, la configuration d'audit du SVM doit déjà exister.

"Créez la configuration d'audit"

Description de la tâche

La désactivation de l'audit ne supprime pas la configuration d'audit.

Étapes

1. Exécutez la commande appropriée :

Si vous voulez que l'audit soit...	Entrez la commande...
Activé	<code>vserver audit enable -vserver vserver_name</code>
Désactivé	<code>vserver audit disable -vserver vserver_name</code>

2. Vérifiez que l'audit est dans l'état souhaité :

```
vserver audit show -vserver vserver_name
```

Exemples

L'exemple suivant permet l'audit du SVM vs1 :

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                Vserver: vs1
            Auditing state: true
        Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtX
            Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
            Rotation Schedules: -
        Log Files Rotation Limit: 10
```

L'exemple suivant désactive l'audit pour SVM vs1 :

```
cluster1::> vserver audit disable -vserver vs1
```

```

                Vserver: vs1
            Auditing state: false
        Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtX
            Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
            Log Rotation Schedule: Day: -
            Log Rotation Schedule: Hour: -
        Log Rotation Schedule: Minute: -
                Rotation Schedules: -
            Log Files Rotation Limit: 10
```

Affiche des informations sur les configurations d'audit

Vous pouvez afficher des informations sur les configurations d'audit. Les informations peuvent vous aider à déterminer si la configuration est celle que vous souhaitez mettre en place pour chaque SVM. Les informations affichées vous permettent également de vérifier si une configuration d'audit est activée.

Description de la tâche

Vous pouvez afficher des informations détaillées sur les configurations d'audit sur tous les SVM. Vous pouvez également personnaliser les informations affichées dans le résultat en spécifiant des paramètres facultatifs. Si vous ne spécifiez aucun des paramètres facultatifs, les éléments suivants s'affichent :

- Nom du SVM auquel s'applique la configuration d'audit
- État d'audit, qui peut être `true` ou `false`

Si l'état d'audit est `true`, l'audit est activé. Si l'état d'audit est `false`, l'audit est désactivé.

- Catégories d'événements à vérifier
- Format du journal d'audit
- Répertoire cible dans lequel le sous-système d'audit stocke les journaux d'audit consolidés et convertis

Étape

1. Affiche des informations sur la configuration d'audit à l'aide du `vserver audit show` commande.

Pour plus d'informations sur l'utilisation de la commande, consultez les pages de manuels.

Exemples

L'exemple suivant affiche un résumé de la configuration d'audit de tous les SVM :

```
cluster1::> vserver audit show
```

Vserver	State	Event Types	Log Format	Target Directory
vs1	false	file-ops	evtx	/audit_log

L'exemple suivant affiche, sous forme de liste, toutes les informations de configuration d'audit de tous les SVM :

```
cluster1::> vserver audit show -instance
```


```

                Vserver: vs1
            Auditing state: true
        Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
            Log Format: evtx
        Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
            Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
            Rotation Schedules: -
        Log Files Rotation Limit: 0
```

Commandes permettant de modifier les configurations d'audit

Si vous souhaitez modifier un paramètre d'audit, vous pouvez modifier la configuration actuelle à tout moment, notamment modifier le chemin d'accès du journal et le format du journal, modifier les catégories d'événements à auditer, enregistrer automatiquement les fichiers journaux et spécifier le nombre maximal de fichiers journaux à enregistrer.

Les fonctions que vous recherchez...	Utilisez cette commande...
Modifiez le chemin de destination du journal	<code>vserver audit modify</code> avec le <code>-destination</code> paramètre

Modifier la catégorie d'événements à auditer	vserver audit modify avec le <code>-events</code> paramètre <div>  <div> Pour auditer les événements de transfert des règles d'accès central, l'option du serveur SMB Dynamic Access Control (DAC) doit être activée sur le serveur SVM (Storage Virtual machine). </div> </div>
Modifiez le format du journal	vserver audit modify avec le <code>-format</code> paramètre
Activation des sauvegardes automatiques en fonction de la taille du fichier journal interne	vserver audit modify avec le <code>-rotate-size</code> paramètre
Activation des sauvegardes automatiques en fonction d'un intervalle de temps	vserver audit modify avec le <code>-rotate-schedule-month</code> , <code>-rotate-schedule-dayofweek</code> , <code>-rotate-schedule-day</code> , <code>-rotate-schedule-hour</code> , et <code>-rotate-schedule-minute</code> paramètres
Spécification du nombre maximal de fichiers journaux enregistrés	vserver audit modify avec le <code>-rotate-limit</code> paramètre

Supprimer une configuration d'audit

Vous ne souhaitez plus auditer les événements de fichier et de répertoire sur la machine virtuelle de stockage (SVM) et ne souhaitez pas conserver une configuration d'audit sur la SVM, vous pouvez supprimer la configuration d'audit.

Étapes

1. Désactivez la configuration d'audit :

```
vserver audit disable -vserver vserver_name
```

```
vserver audit disable -vserver vs1
```

2. Supprimer la configuration d'audit :

```
vserver audit delete -vserver vserver_name
```

```
vserver audit delete -vserver vs1
```

Comprenez les implications du rétablissement du cluster

Si vous prévoyez de restaurer le cluster, sachez que le processus de restauration suivi par la ONTAP est exécuté lors de l'audit de serveurs virtuels de stockage (SVM) dans le

cluster. Vous devez effectuer certaines actions avant de revenir en retour.

Restauration vers une version d'ONTAP qui ne prend pas en charge l'audit des événements de connexion et de déconnexion SMB et des événements de mise en attente des règles d'accès central

La prise en charge de l'audit des événements de connexion et de déconnexion SMB et de l'activation des règles d'accès central commence avec clustered Data ONTAP 8.3. Si vous rétablissez une version de ONTAP qui ne prend pas en charge ces types d'événements et que vous disposez de configurations d'audit qui surveillent ces types d'événements, vous devez modifier la configuration d'audit de ces SVM activés par audit avant de procéder à un rétablissement. Vous devez modifier la configuration de manière à ce que seuls les événements file-op soient audités.

Dépanner les problèmes d'espace des volumes liés à l'audit et au staging

Des problèmes peuvent survenir lorsqu'il n'y a pas suffisamment d'espace sur les volumes d'activation ou sur le volume contenant les journaux d'événements d'audit. Si l'espace est insuffisant, les nouveaux enregistrements d'audit ne peuvent pas être créés, ce qui empêche les clients d'accéder aux données et les demandes d'accès échouent. Vous devez savoir comment résoudre ces problèmes d'espace de volume.

Résolution des problèmes d'espace liés aux volumes du journal des événements

Si les volumes contenant des fichiers journaux d'événements sont à court d'espace, l'audit ne peut pas convertir les enregistrements de journal en fichiers journaux. Cela entraîne des échecs d'accès client. Vous devez savoir comment résoudre les problèmes d'espace liés aux volumes des journaux d'événements.

- En affichant les informations sur l'utilisation et la configuration des volumes et des agrégats, les administrateurs du cluster et des serveurs virtuels de stockage peuvent déterminer si l'espace disponible est insuffisant.
- En cas de manque d'espace dans les volumes contenant les journaux d'événements, les administrateurs du SVM et du cluster peuvent résoudre ces problèmes d'espace en supprimant certains fichiers journaux d'événements ou en augmentant la taille du volume.



Si l'agrégat contenant le volume du journal des événements est plein, la taille de l'agrégat doit être augmentée avant que vous puissiez augmenter la taille du volume. Seul un administrateur de cluster peut augmenter la taille d'un agrégat.

- Le chemin de destination des fichiers journaux d'événements peut être modifié en répertoire sur un autre volume en modifiant la configuration d'audit.



L'accès aux données est refusé dans les cas suivants :

- Le répertoire de destination est supprimé.
- La limite de fichier d'un volume, qui héberge le répertoire de destination, atteint son niveau maximal.

En savoir plus sur :

- ["Afficher des informations sur les volumes et augmenter leur taille"](#).
- ["Afficher des informations sur les agrégats et la gestion des agrégats"](#).

Résoudre les problèmes d'espace liés aux volumes de transfert

Si l'un des volumes contenant des fichiers de transfert de votre machine virtuelle de stockage (SVM) manque d'espace, l'audit ne peut pas écrire les enregistrements des journaux dans les fichiers intermédiaires. Cela entraîne des échecs d'accès client. Pour résoudre ce problème, vous devez déterminer si certains volumes de transit utilisés dans le SVM sont pleins en affichant des informations sur l'utilisation du volume.

Si le volume contenant les fichiers journaux d'événements consolidés dispose de suffisamment d'espace, mais que l'espace occupé par les clients est insuffisant, les volumes intermédiaires risquent de manquer d'espace. L'administrateur du SVM doit vous contacter pour déterminer si l'espace des volumes intermédiaires contenant des fichiers de transfert pour la SVM est insuffisant. Le sous-système d'audit génère un événement EMS si les événements d'audit ne peuvent pas être générés en raison d'un espace insuffisant dans un volume de staging. Le message suivant s'affiche : `No space left on device`. Seul vous pouvez afficher les informations relatives aux volumes de transfert ; les administrateurs du SVM ne le peuvent pas.

Tous les noms de volumes de staging commencent par `MDV_aud_` Suivi par l'UUID de l'agrégat contenant ce volume intermédiaire. L'exemple suivant montre quatre volumes système sur le SVM admin, qui ont été automatiquement créés lors de la création d'une configuration d'audit des services de fichiers pour un SVM de données dans le cluster :

```
cluster1::> volume show -vserver cluster1
```

Vserver	Volume	Aggregate	State	Type	Size	Available
cluster1	MDV_aud_1d0131843d4811e296fc123478563412	aggr0	online	RW	5GB	4.75GB
cluster1	MDV_aud_8be27f813d7311e296fc123478563412	root_vs0	online	RW	5GB	4.75GB
cluster1	MDV_aud_9dc4ad503d7311e296fc123478563412	aggr1	online	RW	5GB	4.75GB
cluster1	MDV_aud_a4b887ac3d7311e296fc123478563412	aggr2	online	RW	5GB	4.75GB

4 entries were displayed.

Si l'espace disponible dans les volumes de transfert est insuffisant, vous pouvez résoudre les problèmes d'espace en augmentant la taille du volume.



Si l'agrégat contenant le volume intermédiaire est saturé, vous devez augmenter la taille de l'agrégat avant de pouvoir augmenter la taille du volume. Seul vous pouvez augmenter la taille d'un agrégat. Les administrateurs du SVM ne le peuvent pas.

Si un ou plusieurs agrégats ont un espace disponible inférieur à 2 Go (dans ONTAP 9.14.1 et versions antérieures) ou 5 Go (à partir de ONTAP 9.15.1), la création de l'audit du SVM échoue. Lorsque la création d'un audit SVM échoue, les volumes de transit qui ont été créés sont supprimés.

Utilisez FPolicy pour le contrôle et la gestion des fichiers sur SVM

Analysez FPolicy

De quoi sont les deux parties de la solution FPolicy

FPolicy est un système de notification d'accès aux fichiers qui permet de surveiller et de gérer les événements d'accès aux fichiers sur les machines virtuelles de stockage (SVM) à l'aide de solutions partenaires. Les solutions de partenaires vous aident à prendre en charge divers cas d'utilisation tels que la gouvernance et la conformité des données, la protection contre les ransomwares et la mobilité des données.

Les solutions partenaires incluent à la fois les solutions tierces prises en charge par NetApp et les produits NetApp sécurité des workloads et Cloud Data Sense.

Une solution FPolicy possède deux parties. La structure ONTAP FPolicy gère les activités sur le cluster et envoie des notifications à l'application partenaire (ou serveurs externes FPolicy). Les serveurs externes FPolicy traitent les notifications envoyées par ONTAP FPolicy pour répondre aux cas d'utilisation des clients.

Le framework ONTAP crée et gère la configuration FPolicy, surveille les événements de fichier et envoie des notifications aux serveurs FPolicy externes. ONTAP FPolicy fournit l'infrastructure qui permet la communication entre les serveurs FPolicy externes et les nœuds de machine virtuelle de stockage (SVM).

La structure FPolicy se connecte aux serveurs FPolicy externes et envoie des notifications pour certains événements du système de fichiers aux serveurs FPolicy lorsque ces événements se produisent suite à l'accès client. Les serveurs FPolicy externes traitent les notifications et renvoient les réponses au nœud. Ce qui se produit à la suite du traitement des notifications dépend de l'application et si la communication entre le nœud et les serveurs externes est asynchrone ou synchrone.

Quelles sont les notifications synchrones et asynchrones

FPolicy envoie des notifications aux serveurs FPolicy externes par le biais de l'interface FPolicy. Les notifications sont envoyées en mode synchrone ou asynchrone. Le mode de notification détermine le rôle de ONTAP après l'envoi de notifications aux serveurs FPolicy.

- **Notifications asynchrones**

Grâce aux notifications asynchrones, le nœud n'attend pas de réponse du serveur FPolicy, ce qui améliore le débit global du système. Ce type de notification est adapté aux applications où le serveur FPolicy n'exige aucune action résultant de l'évaluation des notifications. Par exemple, les notifications asynchrones sont utilisées lorsque l'administrateur de la machine virtuelle de stockage (SVM) souhaite surveiller et auditer l'activité d'accès aux fichiers.

Lorsqu'un serveur FPolicy fonctionnant en mode asynchrone est en panne du réseau, les notifications FPolicy générées lors de la panne sont stockées sur le nœud de stockage. Lorsque le serveur FPolicy est de nouveau en ligne, il est averti des notifications stockées et peut les récupérer du nœud de stockage. La durée pendant laquelle les notifications peuvent être stockées en cas de panne peut être configurée pendant 10 minutes.

À partir de ONTAP 9.14.1, FPolicy permet de configurer un magasin persistant pour capturer les

événements d'accès aux fichiers pour des règles asynchrones non obligatoires dans la SVM. Les magasins persistants peuvent aider à découpler le traitement des E/S client du traitement des notifications FPolicy afin de réduire la latence du client. Les configurations obligatoires synchrones (obligatoires ou non) et asynchrones ne sont pas prises en charge.

- **Notifications synchrones**

Lorsqu'il est configuré pour s'exécuter en mode synchrone, le serveur FPolicy doit accuser réception de chaque notification avant que l'opération client ne puisse continuer. Ce type de notification est utilisé lorsqu'une action est requise en fonction des résultats de l'évaluation des notifications. Par exemple, les notifications synchrones sont utilisées lorsque l'administrateur du SVM souhaite autoriser ou refuser des requêtes en fonction de critères spécifiés sur le serveur FPolicy externe.

Applications synchrones et asynchrones

Il existe de nombreuses utilisations possibles pour les applications FPolicy, asynchrone et synchrone.

Les applications asynchrones sont celles où le serveur FPolicy externe n'affecte pas l'accès aux fichiers ou aux répertoires ou ne modifie pas les données du SVM. Par exemple :

- Journalisation des audits et des accès aux fichiers
- Gestion des ressources de stockage

Les applications synchrones sont celles dont l'accès aux données est modifié ou quand le serveur FPolicy externe. Par exemple :

- La gestion des quotas
- Blocage de l'accès aux fichiers
- Archivage des fichiers et gestion du stockage hiérarchisé
- Services de cryptage et de décryptage
- Services de compression et de décompression

Les magasins persistants FPolicy

Les magasins persistants peuvent aider à découpler le traitement des E/S client du traitement des notifications FPolicy afin de réduire la latence du client. Depuis la version ONTAP 9.14.1, vous pouvez configurer un magasin persistant FPolicy pour capturer les événements d'accès aux fichiers pour des règles asynchrones non obligatoires dans la SVM. Les configurations obligatoires synchrones (obligatoires ou non) et asynchrones ne sont pas prises en charge.

Cette fonctionnalité est uniquement disponible en mode externe FPolicy. L'application partenaire que vous utilisez doit prendre en charge cette fonctionnalité. Vous devez collaborer avec votre partenaire pour vous assurer que cette configuration FPolicy est prise en charge.

À partir de ONTAP 9.15.1, la configuration du stockage persistant FPolicy est simplifiée. Le `persistent-store create` Automatise la création de volume pour la SVM et configure le volume avec les bonnes pratiques de stockage persistant.

Pour plus d'informations sur les meilleures pratiques en matière de stockage persistant, reportez-vous à la section ["D'exigences, de considérations et de meilleures pratiques pour la configuration de FPolicy"](#).

Pour plus d'informations sur l'ajout de magasins persistants, reportez-vous à la section "[Créez des magasins persistants](#)".

Types de configuration FPolicy

Il existe deux types de configuration de base pour les serveurs FPolicy. Une seule configuration utilise des serveurs FPolicy externes pour traiter les notifications et agir. L'autre configuration n'utilise pas de serveurs FPolicy externes. Il utilise à la place le serveur FPolicy interne et natif ONTAP pour bloquer simplement les fichiers en fonction des extensions.

- **Configuration de serveur FPolicy externe**

La notification est envoyée au serveur FPolicy qui présente la requête et applique des règles pour déterminer si le nœud doit autoriser l'opération de fichier demandée. Pour les règles synchrones, le serveur FPolicy envoie ensuite une réponse au nœud pour autoriser ou bloquer l'opération de fichier demandée.

- **Configuration de serveur FPolicy native**

La notification est tramée en interne. La requête est autorisée ou refusée en fonction des paramètres d'extension de fichier configurés dans le cadre FPolicy.

Remarque : les demandes d'extension de fichier refusées ne sont pas consignées.

Quand créer une configuration FPolicy native

Les configurations FPolicy natives utilisent le moteur FPolicy interne de ONTAP pour surveiller et bloquer les opérations basées sur l'extension du fichier. Cette solution ne nécessite pas de serveurs FPolicy externes (serveurs FPolicy). L'utilisation d'une configuration native de blocage de fichiers est appropriée lorsque cette solution simple est tout ce qui est nécessaire.

Le blocage de fichiers natif vous permet de surveiller toutes les opérations de fichiers qui correspondent aux événements de filtrage et d'opération configurés, puis de refuser l'accès aux fichiers avec des extensions particulières. Il s'agit de la configuration par défaut.

Cette configuration permet de bloquer l'accès aux fichiers en fonction de l'extension du fichier uniquement. Par exemple, pour bloquer les fichiers contenant mp3 extensions, vous configurez une stratégie pour fournir des notifications pour certaines opérations avec des extensions de fichier cible de mp3. La règle est configurée pour refuser mp3 demandes de fichiers pour les opérations qui génèrent des notifications.

Les configurations FPolicy natives sont les suivantes :

- Le blocage de fichiers natif est également pris en charge par le filtrage de fichiers basé sur serveur FPolicy.
- Les applications natives de blocage de fichiers et de filtrage de fichiers sur serveur FPolicy peuvent être configurées simultanément.

Pour ce faire, vous pouvez configurer deux règles FPolicy distinctes pour la machine virtuelle de stockage (SVM), une configurée pour le blocage natif des fichiers et une configurée pour le filtrage des fichiers basé sur serveur FPolicy.

- La fonctionnalité native de blocage de fichiers ne permet d'afficher que les fichiers basés sur les

extensions et non sur le contenu du fichier.

- Dans le cas de liens symboliques, le blocage de fichiers natif utilise l'extension de fichier du fichier racine.

En savoir plus sur "[FPolicy : blocage de fichiers natif](#)".

Quand créer une configuration utilisant des serveurs FPolicy externes

Les configurations FPolicy qui utilisent des serveurs FPolicy externes pour traiter et gérer les notifications proposent des solutions fiables pour les cas d'utilisation où il est nécessaire de bloquer simplement des fichiers en fonction de l'extension des fichiers.

Pour ce faire, vous devez créer une configuration qui utilise des serveurs FPolicy externes lorsque vous souhaitez effectuer des tâches telles que la surveillance et l'enregistrement des événements d'accès aux fichiers, fournir des services de quotas, exécuter des blocages de fichiers selon des critères autres que les extensions de fichiers simples, fournir des services de migration des données à l'aide d'applications de gestion du stockage hiérarchisé. Vous pouvez également proposer un ensemble de règles à très grande granularité qui contrôlent uniquement un sous-ensemble de données du serveur virtuel de stockage (SVM).

Rôles liés aux composants du cluster avec l'implémentation FPolicy

Le cluster, les SVM contenant les machines virtuelles de stockage et les LIF de données jouent tous un rôle dans l'implémentation d'une FPolicy.

- **cluster**

Le cluster contient le framework de gestion FPolicy. Il gère et gère les informations relatives à toutes les configurations FPolicy du cluster.

- **SVM**

Une configuration FPolicy est définie au niveau de la SVM. L'étendue de la configuration est le SVM, et ne fonctionne que sur les ressources SVM. Une configuration SVM ne peut pas surveiller et envoyer de notifications pour les demandes d'accès aux fichiers effectuées pour les données résidant sur une autre SVM.

Les configurations FPolicy peuvent être définies sur le SVM d'administration. Une fois les configurations définies sur le SVM d'administration, elles peuvent être consultées et utilisées dans tous les SVM.

- **LIF de données**

Les connexions aux serveurs FPolicy sont effectuées via les LIF de données appartenant au SVM avec la configuration FPolicy. Les LIF de données utilisées pour ces connexions peuvent basculer de la même manière que les LIF de données utilisées pour un accès client normal.

Fonctionnement de FPolicy avec des serveurs FPolicy externes

Une fois FPolicy configuré et activé sur le SVM, FPolicy s'exécute sur chaque nœud auquel le SVM participe. FPolicy est chargé de l'établissement et de la maintenance des connexions avec des serveurs FPolicy externes (serveurs FPolicy), pour le traitement des notifications, ainsi que pour la gestion des messages de notification vers et depuis des serveurs FPolicy.

Dans le cadre de la gestion des connexions, FPolicy possède également les responsabilités suivantes :

- Garantit que la notification des fichiers circule via le LIF correct vers le serveur FPolicy.
- Garantit que lorsque plusieurs serveurs FPolicy sont associés à une règle, l'équilibrage de la charge est réalisé lors de l'envoi de notifications aux serveurs FPolicy.
- Tentatives de rétablissement de la connexion en cas de panne de la connexion à un serveur FPolicy.
- Envoie les notifications aux serveurs FPolicy par le biais d'une session authentifiée.
- Gère la connexion de données de type passthrough établie par le serveur FPolicy pour le traitement des requêtes client lorsque la lecture-passe est activée.

Mode d'utilisation des canaux de contrôle pour les communications FPolicy

FPolicy initie une connexion du canal de contrôle à un serveur FPolicy externe à partir des LIFs de données de chaque nœud participant sur un SVM (Storage Virtual machine). FPolicy utilise des canaux de contrôle pour la transmission des notifications de fichiers. Par conséquent, un serveur FPolicy peut voir plusieurs connexions de canaux de contrôle basées sur la topologie SVM.

Utilisation des canaux privilégiés d'accès aux données pour la communication synchrone

Dans le cas d'une utilisation synchrone, le serveur FPolicy accède aux données résidant sur la machine virtuelle de stockage (SVM) via un chemin d'accès privilégié aux données. L'accès via le chemin privilégié expose l'ensemble du système de fichiers au serveur FPolicy. Elle peut accéder aux fichiers de données afin de collecter des informations, de scanner des fichiers, de lire des fichiers ou d'écrire dans des fichiers.

Étant donné que le serveur FPolicy externe peut accéder à l'intégralité du système de fichiers à partir de la racine de la SVM via le canal de données privilégié, la connexion de canal de données privilégié doit être sécurisée.

Comment les identifiants de connexion FPolicy sont utilisés avec les canaux d'accès aux données privilégiés

Le serveur FPolicy établit des connexions privilégiées aux données avec les nœuds du cluster grâce à des informations d'identification Windows spécifiques enregistrées avec la configuration FPolicy. SMB est le seul protocole pris en charge pour établir une connexion de canal avec accès aux données privilégié.

Si le serveur FPolicy nécessite un accès privilégié aux données, les conditions suivantes doivent être remplies :

- Une licence SMB doit être activée sur le cluster.
- Le serveur FPolicy doit fonctionner avec les identifiants configurés dans la configuration FPolicy.

Lors de la connexion à un canal de données, FPolicy utilise les informations d'identification du nom d'utilisateur Windows spécifié. Les données sont accessibles via le partage ONTAP_ADMIN\$ par l'administrateur.

L'attribution d'informations d'identification de super utilisateur pour l'accès privilégié aux données signifie

ONTAP utilise la combinaison de l'adresse IP et des identifiants de l'utilisateur configurés dans la configuration FPolicy pour attribuer les identifiants des super utilisateurs au serveur FPolicy.

Lorsque le serveur FPolicy accède aux données, l'état du super utilisateur accorde les privilèges suivants :

- Évitez les contrôles d'autorisation

L'utilisateur évite les vérifications de l'accès aux fichiers et aux répertoires.

- Privilèges de verrouillage spéciaux

ONTAP permet l'accès en lecture, en écriture ou en modification à n'importe quel fichier, indépendamment des verrous existants. Si le serveur FPolicy possède des verrous de plage d'octets sur le fichier, il entraîne la suppression immédiate des verrouillages existants sur ce dernier.

- Évitez les vérifications FPolicy

L'accès ne génère aucune notification FPolicy.

Gestion du traitement des règles par FPolicy

Il peut y avoir plusieurs règles FPolicy attribuées à votre SVM (Storage Virtual machine) ; chacune avec une priorité différente. Pour créer une configuration FPolicy appropriée sur le SVM, il est important de comprendre la façon dont FPolicy gère le traitement des règles.

Chaque requête d'accès aux fichiers est initialement évaluée afin de déterminer les règles qui surveillent cet événement. S'il s'agit d'un événement surveillé, les informations relatives à l'événement surveillé et les politiques intéressées sont transmises à FPolicy où il est évalué. Chaque stratégie est évaluée par ordre de priorité attribuée.

Lors de la configuration des règles, vous devez tenir compte des recommandations suivantes :

- Lorsque vous voulez qu'une règle soit toujours évaluée avant d'autres règles, configurez-la avec une priorité plus élevée.
- Si le succès de l'opération d'accès aux fichiers demandée sur un événement contrôlé est une condition préalable à une demande de fichier évaluée par rapport à une autre stratégie, donnez à la stratégie qui contrôle le succès ou l'échec de l'opération de premier fichier une priorité plus élevée.

Par exemple, si l'une des règles gère la fonctionnalité d'archivage et de restauration des fichiers FPolicy, et une seconde gère les opérations d'accès aux fichiers sur le fichier en ligne, la règle de gestion de la restauration des fichiers doit avoir une priorité plus élevée afin que le fichier soit restauré avant que l'opération gérée par la seconde stratégie puisse être autorisée.

- Si vous souhaitez évaluer toutes les règles pouvant s'appliquer à une opération d'accès aux fichiers, donnez une priorité inférieure aux règles synchrones.

Vous pouvez réorganiser les priorités de stratégie pour les stratégies existantes en modifiant le numéro de séquence de stratégie. Toutefois, pour que FPolicy évalue les règles en fonction de l'ordre de priorité modifié, vous devez désactiver et réactiver cette règle avec le numéro de séquence modifié.

Ce que est le processus de communication nœud à serveur FPolicy

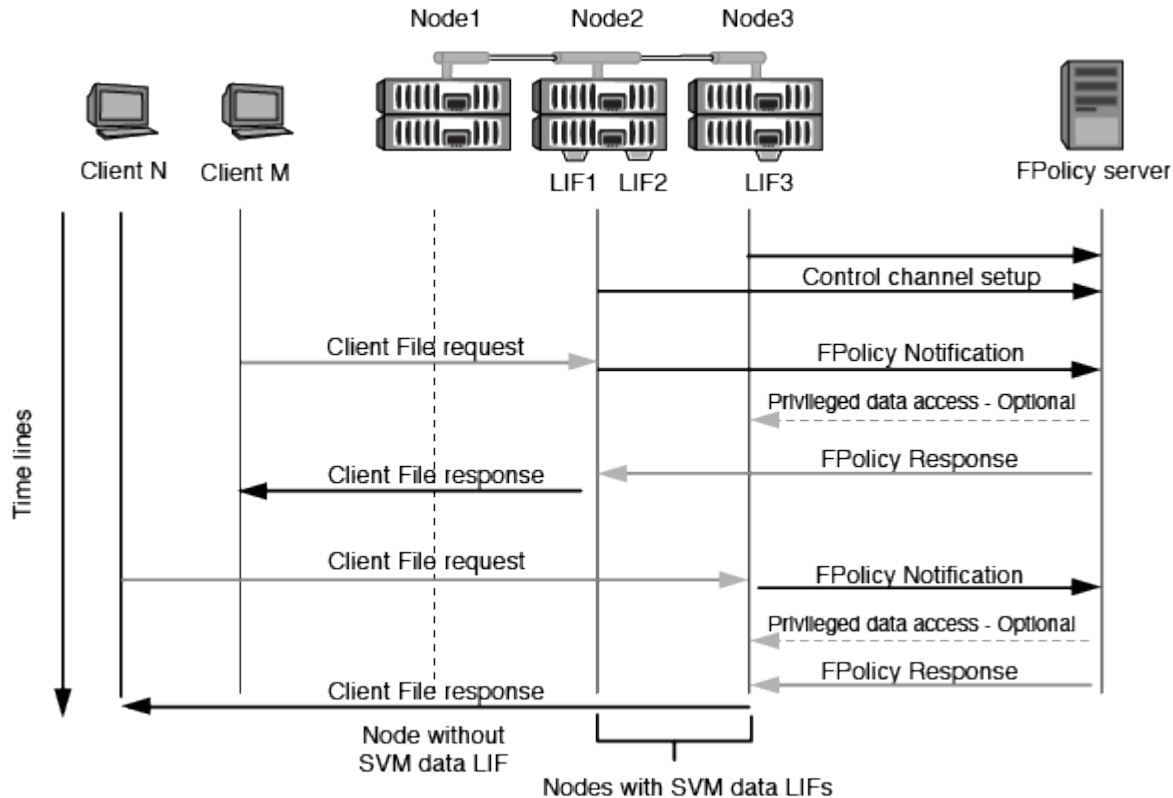
Pour planifier correctement la configuration de FPolicy, vous devez comprendre le processus de communication nœud à serveur FPolicy externe.

Chaque nœud qui participe sur chaque machine virtuelle de stockage (SVM) établit une connexion avec un serveur FPolicy externe (serveur FPolicy) à l'aide du protocole TCP/IP. Les connexions aux serveurs FPolicy sont configurées à l'aide des LIF de données du nœud. Par conséquent, un nœud participant ne peut établir une connexion que si le nœud possède une LIF de données opérationnelles pour le SVM.

Chaque processus FPolicy sur les nœuds participants tente d'établir une connexion avec le serveur FPolicy lorsque cette règle est activée. Il utilise l'adresse IP et le port du moteur externe FPolicy spécifiés dans la configuration des règles.

Cette connexion établit un canal de contrôle depuis chaque nœud participant sur chaque SVM vers le serveur FPolicy via la LIF de données. En outre, si des adresses LIF de données IPv4 et IPv6 sont présentes sur le même nœud participant, FPolicy tente d'établir des connexions pour IPv4 et IPv6. Par conséquent, dans un scénario où le SVM s'étend sur plusieurs nœuds ou si des adresses IPv4 et IPv6 sont présentes, le serveur FPolicy doit être prêt à traiter plusieurs requêtes de configuration de canal de contrôle provenant du cluster après l'activation de la politique FPolicy sur le SVM.

Par exemple, si un cluster possède trois nœuds—Node1, Node2 et nœud3- ainsi que les LIF de données du SVM se répartissent uniquement sur Node2 et nœud3, les canaux de contrôle sont lancés uniquement sur le nœud2 et celui du nœud3, indépendamment de la répartition des volumes de données. Supposons que Node2 possède deux LIF de données—LIF1 et LIF2—qui appartiennent à la SVM et que la connexion initiale est de LIF1. En cas d'échec de LIF1, FPolicy tente d'établir un canal de contrôle à partir de LIF2.



Comment FPolicy gère la communication externe lors de la migration ou du basculement de LIF

Les LIFs de données peuvent être migrées sur des ports data qui se trouvent sur le même nœud ou vers des ports data sur un nœud distant.

Lorsqu'une LIF de données subit une panne ou est migrée, une nouvelle connexion de canal de contrôle est établie vers le serveur FPolicy. FPolicy peut ensuite réessayer les requêtes des clients SMB et NFS ayant dépassé le délai d'attente. En conséquence, de nouvelles notifications sont envoyées aux serveurs FPolicy externes. Le nœud rejette les réponses du serveur FPolicy aux requêtes SMB et NFS d'origine avec temporisation.

Comment FPolicy gère la communication externe lors du basculement de nœud

Si le nœud de cluster qui héberge les ports de données utilisés pour la communication FPolicy tombe en panne, ONTAP interrompt la connexion entre le serveur FPolicy et le nœud.

Vous pouvez atténuer l'impact du basculement de cluster sur le serveur FPolicy en configurant la règle de

basculement pour migrer le port de données utilisé dans la communication FPolicy vers un autre nœud actif. Une fois la migration terminée, une nouvelle connexion est établie à l'aide du nouveau port de données.

Si la règle de basculement n'est pas configurée pour migrer le port de données, le serveur FPolicy doit attendre l'apparition du nœud défaillant. Une fois le nœud activé, une nouvelle connexion est lancée à partir de ce nœud avec un nouvel ID de session.



Le serveur FPolicy détecte les connexions interrompues avec le message du protocole de maintien de la disponibilité. Le délai d'expiration pour la purge de l'ID de session est déterminé lors de la configuration de FPolicy. Le délai de mise en veille par défaut est de deux minutes.

Fonctionnement des services FPolicy sur les espaces de noms des SVM

ONTAP offre un espace de noms de machine virtuelle de stockage unifié. Les volumes du cluster sont regroupés par des jonctions pour fournir un système de fichiers unique et logique. Le serveur FPolicy connaît la topologie de l'espace de noms et fournit des services FPolicy à l'échelle de l'espace de noms.

Le namespace est spécifique et contenu au sein du SVM ; par conséquent, vous pouvez voir le namespace uniquement depuis le contexte SVM. Les espaces de noms présentent les caractéristiques suivantes :

- Un nom d'espace unique existe dans chaque SVM, la racine de l'espace de noms étant le volume root, représenté dans le namespace par la barre oblique (/).
- Tous les autres volumes ont des points de jonction sous la racine (/).
- Les jonctions des volumes sont transparentes pour les clients.
- Une exportation NFS unique peut donner accès à l'espace de noms complet, sinon les export policy peuvent exporter des volumes spécifiques.
- Les partages SMB peuvent être créés sur le volume, dans des qtrees au sein du volume, ou sur n'importe quel répertoire dans le namespace.
- L'architecture d'espace de noms est flexible.

Voici quelques exemples d'architectures d'espaces de noms classiques :

- Un espace de noms avec une seule branche à la racine
- Un espace de noms avec plusieurs branches à la racine
- Un namespace avec plusieurs volumes non ramifiés en dehors de la racine

La fonctionnalité de gestion du stockage hiérarchique de FPolicy permet d'améliorer la facilité d'utilisation de la gestion hiérarchique du stockage

La fonctionnalité Passthrough Read permet au serveur FPolicy (fonctionnant comme serveur HSM (gestion hiérarchique du stockage)) de fournir un accès en lecture aux fichiers hors ligne sans avoir à rappeler le fichier du système de stockage secondaire au système de stockage primaire.

Lorsqu'un serveur FPolicy est configuré pour fournir HSM les fichiers stockés sur un serveur SMB, la migration de fichiers basée sur des règles se produit lorsque les fichiers sont stockés hors ligne sur le stockage secondaire et qu'un seul fichier stub reste sur le stockage primaire. Même si un fichier stub apparaît comme un fichier normal pour les clients, il s'agit en fait d'un fichier parse de la même taille que le fichier d'origine. Le

fichier sparse a le jeu de bits hors ligne SMB et pointe vers le fichier réel qui a été migré vers le stockage secondaire.

En général, lorsqu'une demande de lecture pour un fichier hors ligne est reçue, le contenu demandé doit être rappelé dans le stockage principal, puis accessible par le biais du stockage principal. Le besoin de rappeler des données dans le stockage primaire a plusieurs effets indésirables. L'augmentation de la latence aux demandes des clients, due à la nécessité de rappeler le contenu avant de répondre à la demande et l'augmentation de la consommation d'espace nécessaire pour les fichiers rappelés sur l'infrastructure de stockage primaire, soit un effet indésirable.

La fonctionnalité de passerelle FPolicy permet au serveur HSM (serveur FPolicy) de fournir un accès en lecture aux fichiers migrés hors ligne sans avoir à rappeler le fichier du système de stockage secondaire au système de stockage primaire. Au lieu de rappeler les fichiers dans le stockage primaire, les demandes de lecture peuvent être traitées directement depuis le système de stockage secondaire.



La fonction de déchargement des copies (ODX) n'est pas prise en charge par l'opération de lecture intermédiaire FPolicy.

La fonctionnalité Passthrough Read améliore la convivialité en offrant les avantages suivants :

- Les demandes de lecture peuvent être traitées même si l'espace de stockage primaire n'est pas suffisant pour récupérer les données demandées dans le stockage primaire.
- Meilleure gestion de la capacité et des performances lorsqu'une poussée de récupération des données peut se produire, par exemple si un script ou une solution de sauvegarde doit accéder à de nombreux fichiers hors ligne.
- Les demandes de lecture de fichiers hors ligne des copies Snapshot peuvent être traitées.

Étant donné que les copies Snapshot sont en lecture seule, le serveur FPolicy ne peut pas restaurer le fichier d'origine si le fichier stub est situé dans une copie Snapshot. L'utilisation de la lecture passthrough élimine ce problème.

- Des règles peuvent être définies pour définir ce contrôle lorsque les demandes de lecture sont traitées par l'accès au fichier sur le système de stockage secondaire et lorsqu'un fichier hors ligne doit être rappelé sur le système de stockage principal.

Par exemple, il est possible de créer une règle sur le serveur HSM qui spécifie le nombre d'accès au fichier hors ligne pendant une période donnée avant que le fichier ne soit remigré vers le stockage principal. Ce type de stratégie évite de rappeler les fichiers rarement utilisés.

Mode de gestion des requêtes de lecture lors de l'activation du mode de gestion FPolicy

Vous devez comprendre comment les requêtes de lecture sont gérées lorsque le mode de lecture intermédiaire FPolicy est activé afin de pouvoir configurer de manière optimale la connectivité entre le SVM et les serveurs FPolicy.

Lorsque la fonction de lecture intermédiaire FPolicy est activée et que le SVM reçoit une demande de fichier hors ligne, FPolicy envoie une notification au serveur FPolicy (serveur HSM) par l'intermédiaire du canal de connexion standard.

Après avoir reçu la notification, le serveur FPolicy lit les données du chemin de fichier envoyé dans la notification et envoie les données demandées à la SVM via la connexion de données privilégiée par lecture-intermédiaire établie entre le SVM et le serveur FPolicy.

Une fois les données envoyées, le serveur FPolicy répond à la demande de lecture comme ALLOW ou DENY. En fonction de l'autorisation ou du refus de la demande de lecture, ONTAP envoie les informations demandées ou envoie un message d'erreur au client.

Planification de la configuration FPolicy

D'exigences, de considérations et de meilleures pratiques pour la configuration de FPolicy

Avant de créer et de configurer des configurations FPolicy sur vos machines virtuelles de stockage (SVM), vous devez connaître certaines exigences, considérations et meilleures pratiques relatives à la configuration de FPolicy.

Les fonctionnalités FPolicy sont configurées soit via l'interface de ligne de commandes soit via l'API REST.

Conditions requises pour la configuration de FPolicy

Avant de configurer et d'activer FPolicy sur votre machine virtuelle de stockage (SVM), vous devez connaître certaines exigences.

- Tous les nœuds du cluster doivent exécuter une version de ONTAP qui prend en charge FPolicy.
- Si vous n'utilisez pas le moteur FPolicy natif ONTAP, vous devez installer des serveurs FPolicy externes (serveurs FPolicy).
- Les serveurs FPolicy doivent être installés sur un serveur accessible depuis les LIFs de données du SVM sur lequel les règles FPolicy sont activées.



Depuis la version ONTAP 9.8, ONTAP fournit un service LIF client pour les connexions FPolicy sortantes avec l'ajout du `data-fpolicy-client` service. ["En savoir plus sur les LIF et les règles de service"](#).

- L'adresse IP du serveur FPolicy doit être configurée en tant que serveur principal ou secondaire dans la configuration du moteur externe de la politique FPolicy.
- Si les serveurs FPolicy accèdent aux données sur un canal de données privilégié, les exigences supplémentaires suivantes doivent être respectées :
 - SMB doit être sous licence sur le cluster.

Un accès privilégié aux données se fait à l'aide de connexions SMB.

- Les informations d'identification utilisateur doivent être configurées pour accéder aux fichiers via le canal de données privilégié.
- Le serveur FPolicy doit fonctionner avec les identifiants configurés dans la configuration FPolicy.
- Toutes les LIFs de données utilisées pour communiquer avec les serveurs FPolicy doivent être configurées de sorte à avoir `cifs` comme l'un des protocoles autorisés.

Cela inclut les LIFs utilisées pour les connexions passthrough-read.

Meilleures pratiques et recommandations lors de la configuration de FPolicy

Lors de la configuration de FPolicy sur des machines virtuelles de stockage (SVM), familiarisez-vous avec les bonnes pratiques et recommandations générales de configuration pour garantir que votre configuration FPolicy offre des performances de contrôle fiables et des résultats qui répondent à vos besoins.

Pour obtenir des instructions spécifiques relatives aux performances, au dimensionnement et à la configuration, utilisez votre application partenaire FPolicy.

Magasins persistants

À partir de ONTAP 9.14.1, FPolicy permet de configurer un magasin persistant pour capturer les événements d'accès aux fichiers pour des règles asynchrones non obligatoires dans la SVM. Les magasins persistants peuvent aider à découpler le traitement des E/S client du traitement des notifications FPolicy afin de réduire la latence du client. Les configurations obligatoires synchrones (obligatoires ou non) et asynchrones ne sont pas prises en charge.

- Avant d'utiliser la fonction de stockage persistant, assurez-vous que vos applications partenaires prennent en charge cette configuration.
- Vous avez besoin d'un magasin persistant pour chaque SVM sur lequel FPolicy est activé.
 - Il n'est possible de configurer qu'un seul magasin persistant sur chaque SVM. Ce magasin persistant unique doit être utilisé pour toutes les configurations FPolicy de cette SVM, même si les règles proviennent de différents partenaires.
- ONTAP 9.15.1 ou version ultérieure :
 - Le magasin persistant, son volume et sa configuration de volume sont gérés automatiquement lorsque vous créez le magasin persistant.
- ONTAP 9.14.1 :
 - Le magasin persistant, son volume et sa configuration de volume sont gérés manuellement.
- Créez le volume de stockage persistant sur le nœud avec les LIF qui veulent que le trafic maximal soit surveillé par FPolicy.
 - ONTAP 9.15.1 ou version ultérieure : les volumes sont automatiquement créés et configurés lors de la création du magasin persistant.
 - ONTAP 9.14.1 : les administrateurs de cluster doivent créer et configurer un volume pour le magasin persistant sur chaque SVM sur lequel FPolicy est activé.
- Si les notifications accumulées dans le magasin persistant dépassent la taille du volume provisionné, FPolicy commence à supprimer la notification entrante avec les messages EMS appropriés.
 - ONTAP 9.15.1 ou version ultérieure : en plus du `size` paramètre, le `autosize-mode` peut aider le volume à croître ou à diminuer en fonction de la quantité d'espace utilisé.
 - ONTAP 9.14.1 : le `size` le paramètre est configuré lors de la création du volume pour fournir une limite maximale.
- Définissez la règle de snapshot sur `none` pour le volume de stockage persistant au lieu de `default`. Cela permet de s'assurer qu'il n'y a pas de restauration accidentelle de l'instantané, ce qui entraîne la perte des événements actuels et d'empêcher le traitement des événements en double.
 - ONTAP 9.15.1 ou version ultérieure : le `snapshot-policy` le paramètre est automatiquement configuré sur `none` lors de la création du magasin persistant.
 - ONTAP 9.14.1 : le `snapshot-policy` le paramètre est configuré sur `none` lors de la création du volume.
- Rendre le volume de stockage persistant inaccessible pour l'accès au protocole utilisateur externe (CIFS/NFS) afin d'éviter toute corruption accidentelle ou suppression des enregistrements d'événements persistants.
 - ONTAP 9.15.1 ou version ultérieure : ONTAP bloque automatiquement le volume depuis l'accès aux protocoles utilisateur externes (CIFS/NFS) lors de la création du magasin persistant.

- ONTAP 9.14.1 : une fois FPolicy activé, démontez le volume dans ONTAP pour supprimer la Junction path. Cela le rend inaccessible pour l'accès au protocole utilisateur externe (CIFS/NFS).

Pour plus d'informations, reportez-vous à la section "[Les magasins persistants FPolicy](#)" et "[Créez des magasins persistants](#)".

Basculement et rétablissement du magasin persistant

Le stockage persistant reste tel qu'il était au moment de la réception du dernier événement, en cas de redémarrage inattendu ou lorsque FPolicy est désactivé et réactivé. Après une opération de basculement, les nouveaux événements sont stockés et traités par le nœud partenaire. Après une opération de rétablissement, le magasin persistant reprend le traitement de tout événement non traité qui pourrait rester en provenance de lorsque le basculement du nœud s'est produit. Les événements en direct seraient prioritaires sur les événements non traités.

Si le volume du magasin persistant passe d'un nœud à un autre dans la même SVM, les notifications qui ne sont pas encore traitées sont également déplacées vers le nouveau nœud. Vous devez exécuter à nouveau le `fpolicy persistent-store create` sur l'un des nœuds après le déplacement du volume, afin de garantir que les notifications en attente sont envoyées au serveur externe.

Configuration des règles

La configuration du moteur externe FPolicy, les événements et l'étendue des SVM peuvent améliorer votre expérience et votre sécurité globale.

- Configuration du moteur externe FPolicy pour les SVM :
 - Le renforcement de la sécurité implique des coûts de performance. L'activation de la communication SSL (Secure Sockets Layer) a un effet sur les performances lors de l'accès aux partages.
 - Le moteur externe FPolicy doit être configuré avec plusieurs serveurs FPolicy de manière à fournir la résilience et la haute disponibilité du traitement des notifications du serveur FPolicy.
- Configuration des événements FPolicy pour les SVM :

La surveillance des opérations de fichiers influence votre expérience globale. Par exemple, le filtrage des opérations de fichiers indésirables côté stockage améliore votre expérience. NetApp recommande de configurer les éléments suivants :

- Surveillance des types minimaux d'opérations de fichiers et activation du nombre maximal de filtres sans rompre le cas d'utilisation.
 - Utilisation de filtres pour les opérations `getattr`, lecture, écriture, ouverture et fermeture. La part des environnements de home Directory SMB et NFS est élevée.
- Configuration du périmètre FPolicy pour les SVM :

Limitez l'étendue des règles aux objets de stockage concernés, tels que les partages, les volumes et les exportations, au lieu de les activer sur l'ensemble du SVM. NetApp recommande de vérifier les extensions de répertoire. Si le `is-file-extension-check-on-directories-enabled` le paramètre est défini sur `true`, les objets de répertoire sont soumis aux mêmes vérifications d'extension que les fichiers ordinaires.

Configuration du réseau

La connectivité réseau entre le serveur FPolicy et le contrôleur doit présenter une faible latence. NetApp recommande de séparer le trafic FPolicy du trafic client en utilisant un réseau privé.

De plus, vous devez placer des serveurs externes FPolicy (serveurs FPolicy) à proximité immédiate du cluster avec une connectivité à large bande passante afin d'obtenir une latence minimale et une connectivité à large bande passante.



Si la LIF du trafic FPolicy est configurée sur un port différent de la LIF pour le trafic client, la LIF FPolicy peut basculer vers l'autre nœud en raison d'une défaillance de port. Par conséquent, le serveur FPolicy devient inaccessible depuis le nœud ce qui provoque l'échec des notifications FPolicy pour les opérations de fichier sur le nœud. Pour éviter ce problème, vérifiez que le serveur FPolicy peut être accessible via au moins une LIF du nœud afin de traiter les requêtes FPolicy pour les opérations de fichiers effectuées sur ce nœud.

Configuration matérielle

Vous pouvez avoir le serveur FPolicy sur un serveur physique ou virtuel. Si le serveur FPolicy se trouve dans un environnement virtuel, vous devez allouer des ressources dédiées (CPU, réseau et mémoire) au serveur virtuel.

Le taux nœud/serveur FPolicy du cluster doit être optimisé pour s'assurer que les serveurs FPolicy ne sont pas surchargés et peuvent introduire des latences lorsque le SVM répond aux demandes du client. Le ratio optimal dépend de l'application partenaire pour laquelle le serveur FPolicy est utilisé. NetApp recommande de faire équipe avec ses partenaires pour déterminer la valeur appropriée.

Configuration à règles multiples

La règle FPolicy pour le blocage natif a la priorité la plus élevée, quel que soit le numéro de séquence, et les règles qui modifient la décision ont une priorité plus élevée que les autres. La priorité de la règle dépend de l'utilisation. NetApp recommande de faire équipe avec ses partenaires pour déterminer la priorité appropriée.

Considérations de taille

FPolicy effectue un contrôle en ligne des opérations SMB et NFS, envoie des notifications au serveur externe et attend une réponse, selon le mode de communication externe du moteur (synchrone ou asynchrone). Ce processus affecte les performances des accès SMB et NFS ainsi que des ressources CPU.

Pour résoudre tout problème, NetApp recommande de travailler avec ses partenaires pour évaluer et dimensionner l'environnement avant d'activer FPolicy. Les performances sont affectées par plusieurs facteurs, notamment le nombre d'utilisateurs, les caractéristiques de la charge de travail, tels que les opérations par utilisateur et la taille des données, la latence du réseau et les défaillances ou la lenteur du serveur.

Contrôle des performances

FPolicy est un système basé sur les notifications. Les notifications sont envoyées à un serveur externe pour traitement et pour générer une réponse à ONTAP. Ce processus aller-retour augmente la latence pour l'accès client.

La surveillance des compteurs de performances sur le serveur FPolicy et dans ONTAP vous permet d'identifier les goulets d'étranglement dans la solution et de configurer les paramètres nécessaires pour une solution optimale. Par exemple, une augmentation de la latence FPolicy a un effet en cascade sur la latence d'accès SMB et NFS. Par conséquent, vous devez contrôler à la fois la charge de travail (SMB et NFS) et la latence FPolicy. En outre, vous pouvez utiliser des règles de qualité de service dans ONTAP pour configurer une charge de travail pour chaque volume ou SVM activé pour FPolicy.

NetApp recommande d'exécuter `statistics show -object workload` commande permettant d'afficher les statistiques des charges de travail. De plus, vous devez surveiller les paramètres suivants :

- Latences moyennes, en lecture et en écriture
- Nombre total d'opérations
- Compteurs de lecture et d'écriture

Vous pouvez contrôler les performances des sous-systèmes FPolicy à l'aide des compteurs FPolicy suivants.



Vous devez être en mode diagnostic pour collecter les statistiques relatives à FPolicy.

Étapes

1. Collectez les compteurs FPolicy :

- `statistics start -object fpolicy -instance instance_name -sample-id ID`
- `statistics start -object fpolicy_policy -instance instance_name -sample-id ID`

2. Afficher les compteurs FPolicy :

- `statistics show -object fpolicy -instance instance_name -sample-id ID`
- `statistics show -object fpolicy_server -instance instance_name -sample-id ID`

Le `fpolicy` et `fpolicy_server` les compteurs fournissent des informations sur plusieurs paramètres de performances décrits dans le tableau suivant.

Compteurs	Description
• compteurs « fpolicy »*	demandes_abandonnées
Nombre de demandes d'écran pour lesquelles le traitement est abandonné sur le SVM	nombre_événements
Liste des événements entraînant une notification	latence_demande_max
Latence maximale des demandes d'écran	demandes_en_attente
Nombre total de demandes d'écran en cours de traitement	requêtes_traitées
Nombre total de requêtes d'écran effectuées via le traitement fpolicy sur la SVM	liste_latence_de_la_demande
Histogramme de latence pour les demandes d'écran	taux_envoyé_demandes

Compteurs	Description
Nombre de demandes d'écran envoyées par seconde	taux_de_réception_demandes
Nombre de demandes d'écran reçues par seconde	<ul style="list-style-type: none"> compteurs « fpolicy_server »*
latence_demande_max	Latence maximale pour une demande d'écran
demandes_en_attente	Nombre total de demandes d'écran en attente de réponse
latence_de_la_demande	Latence moyenne pour une demande d'écran
liste_latence_de_la_demande	Histogramme de latence pour les demandes d'écran
taux_envoyé_demande	Nombre de requêtes d'écran envoyées au serveur FPolicy par seconde
taux_de_réception_réponse	Nombre de réponses d'écran reçues du serveur FPolicy par seconde

Gérer le flux de travail FPolicy et la dépendance vis-à-vis d'autres technologies

NetApp recommande de désactiver une règle FPolicy avant d'apporter toute modification de la configuration. Par exemple, si vous souhaitez ajouter ou modifier une adresse IP dans le moteur externe configuré pour la stratégie activé, désactivez d'abord la stratégie.

Si vous configurez FPolicy pour surveiller les volumes NetApp FlexCache, NetApp vous recommande de ne pas configurer FPolicy pour surveiller les opérations de lecture et de fichier getattr. La surveillance de ces opérations dans ONTAP nécessite la récupération des données I2P (inode-to-path). Les données I2P ne pouvant pas être récupérées à partir de volumes FlexCache, elles doivent être récupérées à partir du volume d'origine. Le contrôle de ces opérations élimine donc les avantages de performance que FlexCache peut offrir.

Lorsque FPolicy et une solution antivirus externe sont déployés, la solution antivirus reçoit d'abord les notifications. Le traitement FPolicy démarre uniquement une fois l'analyse antivirus terminée. Il est important de dimensionner correctement les solutions antivirus, car une analyse antivirus lente peut affecter les performances globales.

Considérations relatives à la mise à niveau en lecture directe et au rétablissement

Vous devez connaître certaines considérations relatives à la mise à niveau et à la restauration avant de procéder à une mise à niveau vers une version de ONTAP qui prend en charge la lecture d'un mot de passe-passe ou avant de restaurer une version qui ne prend pas en charge la lecture d'un fichier passthrough.

Mise à niveau

Une fois que tous les nœuds sont mis à niveau vers une version de ONTAP qui prend en charge le mode de lecture intermédiaire FPolicy, le cluster est capable d'utiliser la fonctionnalité de lecture intermédiaire. Cependant, la lecture du mot de passe est désactivée par défaut sur les configurations FPolicy existantes. Pour utiliser la lecture passerelle sur les configurations FPolicy existantes, vous devez désactiver la règle FPolicy et modifier la configuration, puis réactiver la configuration.

Rétablissement

Avant de revenir à une version de ONTAP qui ne prend pas en charge la lecture passthrough FPolicy, vous devez remplir les conditions suivantes :

- Désactivez toutes les stratégies à l'aide de passthrough-read, puis modifiez les configurations affectées pour qu'elles n'utilisent pas passthrough-read.
- Désactivez la fonctionnalité FPolicy sur le cluster en désactivant chaque politique FPolicy sur le cluster.

Avant de revenir à une version de ONTAP qui ne prend pas en charge les magasins persistants, assurez-vous qu'aucune des règles FPolicy ne dispose d'un magasin persistant configuré. Si un magasin persistant est configuré, la restauration échouera.

Quelles sont les étapes de configuration d'une configuration FPolicy

Avant de pouvoir surveiller l'accès aux fichiers, FPolicy doit être créé et activé sur la machine virtuelle de stockage (SVM) pour laquelle les services FPolicy sont requis.

Les étapes de configuration et d'activation d'une configuration FPolicy sur le SVM sont les suivantes :

1. Créer un moteur externe FPolicy.

Le moteur externe FPolicy identifie les serveurs FPolicy externes associés à une configuration FPolicy spécifique. Si le moteur interne FPolicy « natif » est utilisé pour créer une configuration native de blocage de fichiers, il n'est pas nécessaire de créer un moteur externe FPolicy.

À partir de ONTAP 9.15.1, vous pouvez utiliser le `protobuf` format du moteur. Lorsqu'il est réglé sur `protobuf`, Les messages de notification sont codés sous forme binaire à l'aide de Google Protobuf. Avant de régler le format du moteur sur `protobuf`, Assurez-vous que le serveur FPolicy prend également en charge `protobuf` désérialisation. Pour plus d'informations, voir "[Planification de la configuration du moteur externe FPolicy](#)"

2. Créez un événement FPolicy.

Un événement FPolicy décrit ce que la règle FPolicy doit surveiller. Les événements consistent en des protocoles et des opérations de fichiers à surveiller et peuvent contenir une liste de filtres. Les événements utilisent des filtres pour restreindre la liste des événements surveillés pour lesquels le moteur externe FPolicy doit envoyer des notifications. Les événements spécifient également si la règle surveille les opérations de volume.

3. Créez un magasin persistant FPolicy (en option).

À partir de ONTAP 9.14.1, FPolicy vous permet de configurer votre système "[magasins persistants](#)" Pour capturer les événements d'accès aux fichiers pour les politiques asynchrones non obligatoires dans la SVM. Les configurations obligatoires synchrones (obligatoires ou non) et asynchrones ne sont pas prises en charge.

Les magasins persistants peuvent aider à découpler le traitement des E/S client du traitement des notifications FPolicy afin de réduire la latence du client.

À partir de ONTAP 9.15.1, la configuration du stockage persistant FPolicy est simplifiée. Le `persistent-store-create` Automatise la création de volume pour le SVM et configure le volume pour le magasin persistant.

4. Créez une règle FPolicy.

Il incombe à la politique FPolicy d'associer, au périmètre approprié, l'ensemble des événements à surveiller et pour lesquels des notifications d'événements surveillés doivent être envoyées au serveur FPolicy désigné (ou au moteur natif si aucun serveur FPolicy n'est configuré). Cette politique définit également si le serveur FPolicy possède des droits d'accès privilégiés aux données pour lesquelles il reçoit des notifications. Un serveur FPolicy a besoin d'un accès privilégié si le serveur doit accéder aux données. Les cas d'utilisation classiques où un accès privilégié est nécessaire comprennent le blocage de fichiers, la gestion des quotas et la gestion hiérarchique du stockage. C'est l'endroit où vous spécifiez si la configuration de cette règle utilise un serveur FPolicy ou le serveur FPolicy interne « natif ».

Une stratégie spécifie si le filtrage est obligatoire. Si le filtrage est obligatoire et que tous les serveurs FPolicy sont en panne ou qu'aucune réponse n'est reçue des serveurs FPolicy dans une période de temporisation définie, l'accès aux fichiers est refusé.

Les limites d'une politique sont le SVM. Une politique ne peut s'appliquer à plusieurs SVM. Cependant, un SVM spécifique peut avoir plusieurs règles FPolicy, avec chacune des combinaisons de périmètre, d'événements et de configurations de serveur externes mêmes ou différentes.

5. Configuration de la portée de la règle

Le périmètre FPolicy détermine quels volumes, partages ou règles d'exportation agissent ou excluent par la surveillance. L'étendue détermine également quelles extensions de fichier doivent être incluses ou exclues de la surveillance FPolicy.



Les listes d'exclusion ont priorité sur les listes d'inclusion.

6. Activez la règle FPolicy.

Lorsque la stratégie est activée, les canaux de contrôle et, éventuellement, les canaux de données privilégiés sont connectés. Le processus FPolicy dédié aux nœuds sur lesquels le SVM participe à la surveillance de l'accès aux fichiers et aux dossiers. Pour les événements correspondant aux critères configurés, il envoie des notifications aux serveurs FPolicy (ou au moteur natif si aucun serveur FPolicy n'est configuré).



Si la stratégie utilise un blocage de fichiers natif, un moteur externe n'est pas configuré ou associé à la stratégie.

Planification de la configuration du moteur externe FPolicy

Planification de la configuration du moteur externe FPolicy

Avant de configurer le moteur externe FPolicy, vous devez comprendre la signification de la création d'un moteur externe et les paramètres de configuration disponibles. Ces informations vous aident à déterminer les valeurs à définir pour chaque paramètre.

Informations définies lors de la création du moteur externe FPolicy

La configuration de moteur externe définit les informations dont FPolicy a besoin pour établir et gérer des connexions aux serveurs externes FPolicy, notamment :

- Nom du SVM

- Nom du moteur
- Les adresses IP des serveurs FPolicy principaux et secondaires et le numéro de port TCP à utiliser lors de la connexion aux serveurs FPolicy
- Indique si le type de moteur est asynchrone ou synchrone
- Indique si le format du moteur est `xml` ou `protobuf`

À partir de ONTAP 9.15.1, vous pouvez utiliser le `protobuf` format du moteur. Lorsqu'il est réglé sur `protobuf`, Les messages de notification sont codés sous forme binaire à l'aide de Google Protobuf. Avant de régler le format du moteur sur `protobuf`, Assurez-vous que le serveur FPolicy prend également en charge `protobuf` désérialisation.

Étant donné que le format `protobuf` est pris en charge à partir de ONTAP 9.15.1, vous devez prendre en compte le format du moteur externe avant de revenir à une version antérieure de ONTAP. Si vous restaurez une version antérieure à ONTAP 9.15.1, contactez votre partenaire FPolicy pour :

- Modifiez chaque format de moteur de `protobuf` à `xml`
- Supprimer les moteurs avec un format de moteur de `protobuf`
- Authentification de la connexion entre le nœud et le serveur FPolicy

Si vous choisissez de configurer l'authentification SSL mutuelle, vous devez également configurer les paramètres qui fournissent les informations de certificat SSL.

- Comment gérer la connexion à l'aide de divers paramètres de privilèges avancés

Cela inclut des paramètres qui définissent des éléments tels que les valeurs de temporisation, les valeurs de relance, les valeurs de maintien de la vie, les valeurs maximales de demande, les valeurs de taille de tampon de réception et d'envoi, ainsi que les valeurs de temporisation de la session.

Le `vserver fpolicy policy external-engine create` Permet de créer un moteur externe FPolicy.

Quels sont les paramètres externes de base du moteur

Pour planifier la configuration, vous pouvez utiliser le tableau suivant des paramètres de configuration de base de FPolicy :

Type d'information	Option
<p>SVM</p> <p>Spécifie le nom du SVM que vous souhaitez associer à ce moteur externe.</p> <p>Chaque configuration FPolicy est définie au sein d'un seul SVM. Le moteur externe, l'événement de politique, l'étendue des règles et la politique associés pour créer une configuration de politique FPolicy doivent tous être associés au même SVM.</p>	<p><code>-vserver vserver_name</code></p>

<p><i>Nom du moteur</i></p> <p>Spécifie le nom à attribuer à la configuration du moteur externe. Vous devez spécifier le nom du moteur externe ultérieurement lors de la création de la règle FPolicy. Ceci associe le moteur externe à la politique.</p> <p>Le nom peut comporter jusqu'à 256 caractères.</p> <div data-bbox="167 401 220 457" data-label="Image"> </div> <p>Le nom doit comporter jusqu'à 200 caractères si vous configurez le nom du moteur externe dans une configuration de reprise après incident de MetroCluster ou de SVM.</p> <p>Le nom peut contenir n'importe quelle combinaison des caractères ASCII suivants :</p> <ul style="list-style-type: none"> • a à z • A à Z • 0 à 9 • «»_», «»-", and ".» 	<p>-engine-name engine_name</p>
<p><i>Serveurs FPolicy primaires</i></p> <p>Spécifie les serveurs FPolicy principaux vers lesquels le nœud envoie des notifications pour une règle FPolicy donnée. La valeur est indiquée comme une liste d'adresses IP délimitée par des virgules.</p> <p>Si plusieurs adresses IP de serveur principal sont spécifiées, chaque nœud sur lequel le SVM participe crée une connexion de contrôle à chaque serveur FPolicy principal spécifié au moment de l'activation de la règle. Si vous configurez plusieurs serveurs FPolicy principaux, des notifications sont envoyées selon une séquence périodique aux serveurs FPolicy.</p> <p>Si le moteur externe est utilisé dans une configuration de reprise sur incident de MetroCluster ou de SVM, indiquez les adresses IP des serveurs FPolicy du site source en tant que serveurs principaux. Les adresses IP des serveurs FPolicy du site de destination doivent être spécifiées en tant que serveurs secondaires.</p>	<p>-primary-servers IP_address,...</p>
<p><i>Numéro de port</i></p> <p>Spécifie le numéro de port du service FPolicy.</p>	<p>-port integer</p>

<p><i>Serveurs FPolicy secondaires</i></p> <p>Spécifie les serveurs FPolicy secondaires vers lesquels envoyer les événements d'accès aux fichiers pour une politique FPolicy donnée. La valeur est indiquée comme une liste d'adresses IP délimitée par des virgules.</p> <p>Les serveurs secondaires sont utilisés uniquement lorsqu'aucun des serveurs primaires n'est accessible. Les connexions aux serveurs secondaires sont établies lorsque la stratégie est activée, mais les notifications sont envoyées aux serveurs secondaires uniquement si aucun des serveurs primaires n'est accessible. Si vous configurez plusieurs serveurs secondaires, des notifications sont envoyées aux serveurs FPolicy de manière périodique.</p>	<p>-secondary-servers IP_address,...</p>
<p><i>Type de moteur externe</i></p> <p>Indique si le moteur externe fonctionne en mode synchrone ou asynchrone. Par défaut, FPolicy fonctionne en mode synchrone.</p> <p>Lorsqu'il est réglé sur <code>synchronous</code>, Le traitement des requêtes de fichier envoie une notification au serveur FPolicy, mais ne se poursuit qu'après avoir reçu une réponse du serveur FPolicy. À ce stade, le flux de demande continue ou le traitement génère un déni, selon que la réponse du serveur FPolicy permet l'action demandée.</p> <p>Lorsqu'il est réglé sur <code>asynchronous</code>, Le traitement des requêtes de fichier envoie une notification au serveur FPolicy, puis continue.</p>	<p>-extern-engine-type external_engine_type La valeur de ce paramètre peut être l'une des suivantes :</p> <ul style="list-style-type: none"> • synchronous • asynchronous
<p><i>Format de moteur externe</i></p> <p>Spécifiez si le format du moteur externe est xml ou protobuf.</p> <p>À partir de ONTAP 9.15.1, vous pouvez utiliser le format du moteur protobuf. Lorsqu'ils sont définis sur protobuf, les messages de notification sont codés sous forme binaire à l'aide de Google Protobuf. Avant de définir le format du moteur sur protobuf, assurez-vous que le serveur FPolicy prend également en charge la désérialisation des protobuf.</p>	<p>- extern-engine-format {protobuf ou xml}</p>

<p><i>Option SSL pour la communication avec le serveur FPolicy</i></p> <p>Spécifie l'option SSL pour la communication avec le serveur FPolicy. Ce paramètre est obligatoire. Vous pouvez choisir l'une des options en fonction des informations suivantes :</p> <ul style="list-style-type: none"> Lorsqu'il est réglé sur <code>no-auth</code>, aucune authentification n'a lieu. <p>La liaison de communication est établie sur TCP.</p> <ul style="list-style-type: none"> Lorsqu'il est réglé sur <code>server-auth</code>, Le SVM authentifie le serveur FPolicy à l'aide de l'authentification du serveur SSL. Lorsqu'il est réglé sur <code>mutual-auth</code>, L'authentification mutuelle a lieu entre le SVM et le serveur FPolicy ; le SVM authentifie le serveur FPolicy et le serveur FPolicy authentifie le SVM. <p>Si vous choisissez de configurer l'authentification SSL mutuelle, vous devez également configurer l' <code>-certificate-common-name</code>, <code>-certificate-serial</code>, et <code>-certificate-ca</code> paramètres.</p>	<p><code>-ssl-option {no-auth</code></p>
<p><code>server-auth</code></p>	<p><code>mutual-auth}</code></p>
<p><i>FQDN du certificat ou nom commun personnalisé</i></p> <p>Spécifie le nom du certificat utilisé si l'authentification SSL entre le SVM et le serveur FPolicy est configurée. Vous pouvez spécifier le nom du certificat en tant que FQDN ou en tant que nom commun personnalisé.</p> <p>Si vous spécifiez <code>mutual-auth</code> pour le <code>-ssl-option</code> paramètre, vous devez spécifier une valeur pour le <code>-certificate-common-name</code> paramètre.</p>	<p><code>-certificate-common-name text</code></p>
<p><i>Numéro de série du certificat</i></p> <p>Spécifie le numéro de série du certificat utilisé pour l'authentification si l'authentification SSL entre le SVM et le serveur FPolicy est configurée.</p> <p>Si vous spécifiez <code>mutual-auth</code> pour le <code>-ssl-option</code> paramètre, vous devez spécifier une valeur pour le <code>-certificate-serial</code> paramètre.</p>	<p><code>-certificate-serial text</code></p>
<p><i>Autorité de certification</i></p> <p>Spécifie le nom de l'autorité de certification du certificat utilisé pour l'authentification si l'authentification SSL entre le SVM et le serveur FPolicy est configurée.</p> <p>Si vous spécifiez <code>mutual-auth</code> pour le <code>-ssl-option</code> paramètre, vous devez spécifier une valeur pour le <code>-certificate-ca</code> paramètre.</p>	<p><code>-certificate-ca text</code></p>

Quelles sont les options avancées du moteur externe

Vous pouvez utiliser le tableau suivant des paramètres de configuration avancée FPolicy pour personnaliser ou non votre configuration avec des paramètres avancés. Ces paramètres permettent de modifier le comportement de communication entre les nœuds du cluster et les serveurs FPolicy :

Type d'information	Option
<p><i>Délai d'annulation d'une demande</i></p> <p>Spécifie l'intervalle de temps en heures (h), minutes (m), ou secondes (s) Que le nœud attend une réponse du serveur FPolicy.</p> <p>Si l'intervalle de temporisation passe, le nœud envoie une requête d'annulation au serveur FPolicy. Le nœud envoie ensuite la notification à un autre serveur FPolicy. Ce délai aide à gérer un serveur FPolicy qui ne répond pas, ce qui peut améliorer la réponse des clients SMB/NFS. Par ailleurs, l'annulation des demandes après une période de temporisation peut faciliter la libération des ressources système, car la demande de notification est déplacée d'un serveur FPolicy défaillant/défectueux vers un autre serveur FPolicy.</p> <p>La plage de cette valeur est de 0 à 100. Si la valeur est définie sur 0, L'option est désactivée et les messages de requête d'annulation ne sont pas envoyés au serveur FPolicy. La valeur par défaut est 20s.</p>	<p>-reqs-cancel-timeout integer[h</p>
m	s]
<p><i>Délai d'attente pour l'abandon d'une demande</i></p> <p>Spécifie le délai d'expiration en heures (h), minutes (m), ou secondes (s) pour l'abandon d'une demande.</p> <p>La plage de cette valeur est de 0 à 200.</p>	<p>-reqs-abort-timeout `integer[h</p>
m	s]
<p><i>Intervalle pour l'envoi de demandes d'état</i></p> <p>Spécifie l'intervalle en heures (h), minutes (m), ou secondes (s) Après quoi une requête d'état est envoyée au serveur FPolicy.</p> <p>La plage de cette valeur est de 0 à 50. Si la valeur est définie sur 0, L'option est désactivée et les messages de requête d'état ne sont pas envoyés au serveur FPolicy. La valeur par défaut est 10s.</p>	<p>-status-req-interval integer[h</p>
m	s]

<p><i>Nombre maximal de requêtes en attente sur le serveur FPolicy</i></p> <p>Spécifie le nombre maximal de requêtes en attente pouvant être mises en file d'attente sur le serveur FPolicy.</p> <p>La plage de cette valeur est de 1 à 10000. La valeur par défaut est 500.</p>	<p><code>-max-server-reqs integer</code></p>
<p><i>Timeout pour la déconnexion d'un serveur FPolicy non réactif</i></p> <p>Spécifie l'intervalle de temps en heures (h), minutes (m), ou secondes (s) Après quoi la connexion au serveur FPolicy est interrompue.</p> <p>La connexion est interrompue après le délai d'expiration uniquement si la file d'attente du serveur FPolicy contient le nombre maximal de requêtes autorisées et qu'aucune réponse n'est reçue dans le délai d'expiration. Le nombre maximal de demandes est de 50 (valeur par défaut) ou le numéro spécifié par le <code>max-server-reqs</code> paramètre.</p> <p>La plage de cette valeur est de 1 à 100. La valeur par défaut est 60s.</p>	<p><code>-server-progress</code> <code>-timeout integer[h</code></p>
m	s]
<p><i>Intervalle d'envoi de messages de maintien de la disponibilité au serveur FPolicy</i></p> <p>Spécifie l'intervalle de temps en heures (h), minutes (m), ou secondes (s) À laquelle les messages de maintien de la disponibilité sont envoyés au serveur FPolicy.</p> <p>Les messages de maintien de la vie détectent les connexions à demi-ouverture.</p> <p>La plage de cette valeur est de 10 à 600. Si la valeur est définie sur 0, L'option est désactivée et les messages de maintien en service ne peuvent pas être envoyés aux serveurs FPolicy. La valeur par défaut est 120s.</p>	<p><code>-keep-alive-interval-integer[h</code></p>
m	s]
<p><i>Tentatives de reconnexion maximales</i></p> <p>Spécifie le nombre maximal de fois que le SVM tente de se reconnecter au serveur FPolicy une fois la connexion interrompue.</p> <p>La plage de cette valeur est de 0 à 20. La valeur par défaut est 5.</p>	<p><code>-max-connection-retries integer</code></p>

<p><i>Taille du tampon de réception</i></p> <p>Spécifie la taille du tampon de réception du socket connecté pour le serveur FPolicy.</p> <p>La valeur par défaut est 256 kilo-octets (Ko). Lorsque la valeur est définie sur 0, la taille du tampon de réception est définie sur une valeur définie par le système.</p> <p>Par exemple, si la taille par défaut de la mémoire tampon de réception du socket est de 65536 octets, en définissant la valeur ajustable sur 0, la taille de la mémoire tampon de socket est définie sur 65536 octets. Vous pouvez utiliser n'importe quelle valeur autre que celle par défaut pour définir la taille (en octets) du tampon de réception.</p>	<p><code>-recv-buffer-size</code> integer</p>
<p><i>Envoyer la taille du tampon</i></p> <p>Spécifie la taille du tampon d'envoi du socket connecté pour le serveur FPolicy.</p> <p>La valeur par défaut est 256 kilo-octets (Ko). Lorsque la valeur est définie sur 0, la taille du tampon d'envoi est définie sur une valeur définie par le système.</p> <p>Par exemple, si la taille par défaut du tampon d'envoi du socket est définie sur 65536 octets, en définissant la valeur ajustable sur 0, la taille de la mémoire tampon du socket est définie sur 65536 octets. Vous pouvez utiliser n'importe quelle valeur autre que celle par défaut pour définir la taille (en octets) du tampon d'envoi.</p>	<p><code>-send-buffer-size</code> integer</p>
<p><i>Délai de purge d'un ID de session pendant la reconnexion</i></p> <p>Spécifie l'intervalle en heures (h), minutes (m), ou secondes (s) Après quoi un nouvel ID de session est envoyé au serveur FPolicy pendant les tentatives de reconnexion.</p> <p>Si la connexion entre le contrôleur de stockage et le serveur FPolicy est interrompue et la reconnexion est effectuée au sein du <code>-session -timeout</code> Intervalle, l'ancien ID de session est envoyé au serveur FPolicy pour qu'il puisse envoyer les réponses aux anciennes notifications.</p> <p>La valeur par défaut est définie sur 10 secondes.</p>	<p><code>-session-timeout</code> [integerh][integerm][integer s]</p>

Informations supplémentaires sur la configuration des moteurs externes FPolicy pour utiliser les connexions authentifiées SSL

Vous devez connaître des informations supplémentaires pour configurer le moteur externe FPolicy de façon à utiliser le protocole SSL lors de la connexion aux serveurs FPolicy.

Authentification de serveur SSL

Si vous choisissez de configurer le moteur externe FPolicy pour l'authentification du serveur SSL, vous devez installer le certificat public de l'autorité de certification (CA) qui a signé le certificat du serveur FPolicy avant de créer le moteur externe.

Authentification mutuelle

Si vous configurez les moteurs externes FPolicy pour utiliser l'authentification mutuelle SSL lors du raccordement des LIF de données des machines virtuelles de stockage aux serveurs FPolicy externes, avant de créer le moteur externe, Vous devez installer le certificat public de l'autorité de certification qui a signé le certificat du serveur FPolicy avec le certificat public et le fichier de clé pour l'authentification de la SVM. Vous ne devez pas supprimer ce certificat lorsque des règles FPolicy utilisent le certificat installé.

Si le certificat est supprimé pendant que FPolicy l'utilise pour l'authentification mutuelle lors de la connexion à un serveur FPolicy externe, vous ne pouvez pas réactiver une règle FPolicy désactivée qui utilise ce certificat. La politique FPolicy ne peut pas être réactivée dans ce cas, même si un nouveau certificat avec les mêmes paramètres est créé et installé sur le SVM.

Si le certificat a été supprimé, vous devez installer un nouveau certificat, créer de nouveaux moteurs externes FPolicy utilisant le nouveau certificat et associer les nouveaux moteurs externes à la politique FPolicy que vous souhaitez réactiver en modifiant la règle FPolicy.

Installer les certificats pour SSL

Le certificat public de l'autorité de certification utilisé pour signer le certificat du serveur FPolicy est installé à l'aide du `security certificate install` commande avec `-type` paramètre défini sur `client-ca`. La clé privée et le certificat public requis pour l'authentification de la SVM sont installés à l'aide de `security certificate install` commande avec `-type` paramètre défini sur `server`.

Les certificats ne sont pas répliqués dans les relations de SVM de reprise après incident avec une configuration sans ID-preserve

Les certificats de sécurité utilisés pour l'authentification SSL lors des connexions aux serveurs FPolicy ne répliquent pas les données vers des destinations de reprise après incident des SVM avec des configurations sans ID-preserve. Bien que la configuration du moteur externe FPolicy sur le SVM soit répliquée, les certificats de sécurité ne sont pas répliqués. Vous devez installer manuellement les certificats de sécurité sur la destination.

Lorsque vous configurez la relation de SVM Disaster Recovery, la valeur que vous sélectionnez pour le `-identity-preserve` de la `snapmirror create` La commande détermine les détails de configuration répliqués dans le SVM de destination.

Si vous définissez le `-identity-preserve` option à `true` (ID-preserve), tous les détails de la configuration FPolicy sont répliqués, y compris les informations du certificat de sécurité. Vous devez installer les certificats de sécurité sur la destination uniquement si vous définissez l'option sur `false` (Non-ID-preserve).

Restrictions liées aux moteurs externes FPolicy avec configurations de reprise après incident MetroCluster et SVM

Vous pouvez créer un moteur externe FPolicy à étendue du cluster en attribuant la machine virtuelle de stockage du cluster (SVM) au moteur externe. Cependant, lors de la création d'un moteur externe « cluster-scoped » dans une configuration de reprise après incident de MetroCluster ou de SVM, il existe certaines restrictions lors du choix de la

méthode d'authentification utilisée par le SVM pour la communication externe avec le serveur FPolicy.

Il existe trois options d'authentification que vous pouvez choisir lors de la création de serveurs FPolicy externes : aucune authentification, authentification de serveur SSL et authentification mutuelle SSL. Bien qu'il n'y ait aucune restriction lors du choix de l'option d'authentification si le serveur FPolicy externe est affecté à un SVM de données, il existe des restrictions lors de la création d'un moteur externe FPolicy d'étendue au cluster :

Configuration	Autorisé ?
Reprise après incident de MetroCluster ou SVM et moteur externe FPolicy à étendue du cluster sans authentification (le protocole SSL n'est pas configuré)	Oui.
Reprise après incident de MetroCluster ou SVM et moteur externe FPolicy à étendue du cluster avec serveur SSL ou authentification mutuelle SSL	Non

- En cas d'existence d'un moteur externe FPolicy avec authentification SSL et que vous souhaitez créer une configuration de reprise après incident MetroCluster ou SVM, vous devez modifier ce moteur externe afin qu'il n'utilise aucune authentification ou supprimer le moteur externe avant de créer la configuration de reprise après incident MetroCluster ou SVM.
- Si la configuration de reprise après incident de MetroCluster ou SVM existe déjà, ONTAP vous empêche de créer un moteur externe FPolicy à étendue du cluster avec l'authentification SSL.

Remplir la fiche de configuration du moteur externe FPolicy

Vous pouvez utiliser cette fiche technique pour enregistrer les valeurs nécessaires lors du processus de configuration du moteur externe FPolicy. Si une valeur de paramètre est requise, vous devez déterminer la valeur à utiliser pour ces paramètres avant de configurer le moteur externe.

Informations concernant la configuration de base d'un moteur externe

Vous devez indiquer si vous souhaitez inclure chaque paramètre dans la configuration du moteur externe, puis enregistrer la valeur des paramètres que vous souhaitez inclure.

Type d'information	Obligatoire	Inclure	Vos valeurs
Nom de la machine virtuelle de stockage (SVM)	Oui.	Oui.	
Nom du moteur	Oui.	Oui.	
Serveurs FPolicy principaux	Oui.	Oui.	
Numéro de port	Oui.	Oui.	
Serveurs FPolicy secondaires	Non		

Type de moteur externe	Non		
Option SSL pour la communication avec le serveur FPolicy externe	Oui.	Oui.	
Nom de domaine complet du certificat ou nom commun personnalisé	Non		
Numéro de série du certificat	Non		
Autorité de certification	Non		

Informations relatives aux paramètres avancés du moteur externe

Pour configurer un moteur externe avec des paramètres avancés, vous devez saisir la commande de configuration en mode Advanced Privilege.

Type d'information	Obligatoire	Inclure	Vos valeurs
Délai d'annulation d'une demande	Non		
Délai d'abandon d'une demande	Non		
Intervalle d'envoi des demandes d'état	Non		
Nombre maximal de requêtes en attente sur le serveur FPolicy	Non		
Délai de déconnexion d'un serveur FPolicy non réactif	Non		
Intervalle d'envoi de messages de sauvegarde au serveur FPolicy	Non		
Nombre maximal de tentatives de reconnexion	Non		
Taille de la mémoire tampon de réception	Non		
Taille de la mémoire tampon d'envoi	Non		
Délai de purge d'un ID de session pendant la reconnexion	Non		

Planification de la configuration des événements FPolicy

Planifier l’présentation de la configuration des événements FPolicy

Avant de configurer des événements FPolicy, vous devez comprendre ce qu’il signifie pour créer un événement FPolicy. Vous devez déterminer les protocoles à surveiller, les événements à surveiller et les filtres d’événements à utiliser. Ces informations vous aident à planifier les valeurs que vous souhaitez définir.

Ce qu’il signifie pour créer un événement FPolicy

La création de l’événement FPolicy consiste à définir les informations nécessaires au processus FPolicy pour déterminer les opérations d’accès aux fichiers à surveiller et pour lesquelles des notifications d’événements surveillés doivent être envoyées au serveur FPolicy externe. La configuration des événements FPolicy définit les informations de configuration suivantes :

- Nom de la machine virtuelle de stockage (SVM)
- Nom de l’événement
- Les protocoles à surveiller

FPolicy peut surveiller les opérations d’accès aux fichiers SMB, NFSv3 et NFSv4, et, à partir de ONTAP 9.15.1, NFSv4.1.

- Quelles opérations de fichier surveiller

Toutes les opérations de fichier ne sont pas valides pour chaque protocole.

- Les filtres de fichier à configurer

Seules certaines combinaisons d’opérations de fichier et de filtres sont valides. Chaque protocole dispose de son propre ensemble de combinaisons prises en charge.

- Contrôler le montage et le démontage de volumes



Il y a une dépendance avec trois des paramètres (`-protocol`, `-file-operations`, `-filters`). Les combinaisons suivantes sont valides pour les trois paramètres :

- Vous pouvez spécifier le `-protocol` et `-file-operations` paramètres.
- Vous pouvez spécifier les trois paramètres.
- Vous ne pouvez spécifier aucun des paramètres.

Contenu de la configuration des événements FPolicy

Pour vous aider à planifier votre configuration, vous pouvez utiliser la liste suivante de paramètres de configuration des événements FPolicy disponibles :

Type d’information	Option
--------------------	--------

<p>SVM</p> <p>Spécifie le nom du SVM que vous souhaitez associer à cet événement FPolicy.</p> <p>Chaque configuration FPolicy est définie au sein d'un seul SVM. Le moteur externe, l'événement de politique, l'étendue des règles et la politique associés pour créer une configuration de politique FPolicy doivent tous être associés au même SVM.</p>	<p><code>-vserver vserver_name</code></p>
<p>Nom de l'événement</p> <p>Spécifie le nom à attribuer à l'événement FPolicy. Lorsque vous créez la politique FPolicy, vous associez l'événement FPolicy à la règle à l'aide du nom de l'événement.</p> <p>Le nom peut comporter jusqu'à 256 caractères.</p> <div data-bbox="167 751 220 808" data-label="Image"></div> <p>Le nom doit comporter jusqu'à 200 caractères si vous configurez l'évènement dans une configuration de reprise d'activité de MetroCluster ou de SVM.</p> <p>Le nom peut contenir n'importe quelle combinaison des caractères ASCII suivants :</p> <ul style="list-style-type: none"> • a à z • A à Z • 0 à 9 • « _ ", "' -, and ". » 	<p><code>-event-name event_name</code></p>
<p>Protocole</p> <p>Spécifie le protocole à configurer pour l'événement FPolicy. La liste pour <code>-protocol</code> peut inclure l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> • cifs • nfsv3 • nfsv4 <div data-bbox="167 1633 220 1690" data-label="Image"></div> <p>Si vous spécifiez <code>-protocol</code>, vous devez alors spécifier une valeur valide dans l' <code>-file-operations</code> paramètre. Au fur et à mesure que la version du protocole change, les valeurs valides peuvent changer.</p> <div data-bbox="167 1791 220 1848" data-label="Image"></div> <p>À partir de ONTAP 9.15.1, nfsv4 vous permet de capturer les événements NFSv4.0 et NFSv4.1.</p>	<p><code>-protocol protocol</code></p>

Opérations_fichier

Spécifie la liste des opérations sur les fichiers pour l'événement FPolicy.

L'événement vérifie les opérations spécifiées dans cette liste à partir de toutes les demandes client utilisant le protocole spécifié dans `-protocol` paramètre. Vous pouvez lister une ou plusieurs opérations de fichier à l'aide d'une liste délimitée par des virgules. La liste pour `-file-operations` peut inclure une ou plusieurs des valeurs suivantes :

- `close` pour les opérations de fermeture de fichier
- `create` pour les opérations de création de fichier
- `create-dir` pour les opérations de création de répertoire
- `delete` pour les opérations de suppression de fichier
- `delete_dir` pour les opérations de suppression de répertoire
- `getattr` pour obtenir les opérations d'attribut
- `link` pour les opérations de liaison
- `lookup` pour les opérations de recherche
- `open` pour les opérations d'ouverture de fichier
- `read` pour les opérations de lecture de fichiers
- `write` pour les opérations d'écriture de fichiers
- `rename` pour les opérations de renommage de fichiers
- `rename_dir` pour les opérations de renommage de répertoire
- `setattr` pour les opérations de définition d'attribut
- `symlink` pour les opérations de lien symbolique



Si vous spécifiez `-file-operations`, vous devez alors spécifier un protocole valide dans l' `-protocol` paramètre.

`-file-operations`
`file_operations,...`

Filtres

-filters filter, ...

Spécifie la liste des filtres pour une opération de fichier donnée pour le protocole spécifié. Les valeurs dans le `-filters` paramètre utilisé pour filtrer les demandes client. La liste peut comprendre un ou plusieurs des éléments suivants :



Si vous spécifiez le `-filters` paramètre, vous devez ensuite spécifier également des valeurs valides pour le `-file-operations` et `-protocol` paramètres.

- `monitor-ads` option permettant de filtrer la demande client pour un autre flux de données.
- `close-with-modification` option permettant de filtrer la demande client pour fermer avec modification.
- `close-without-modification` option permettant de filtrer la demande client pour la fermeture sans modification.
- `first-read` option permettant de filtrer la demande client pour la première lecture.
- `first-write` option permettant de filtrer la demande client pour la première écriture.
- `offline-bit` option permettant de filtrer la demande client pour le jeu de bits hors ligne.

La configuration de ce filtre permet au serveur FPolicy de recevoir une notification uniquement lorsque des fichiers hors ligne sont utilisés.

- `open-with-delete-intent` option permettant de filtrer la demande client pour ouvrir avec l'intention de suppression.

La configuration de ce filtre entraîne la réception d'une notification sur le serveur FPolicy uniquement lorsqu'une tentative est effectuée pour ouvrir un fichier avec l'intention de le supprimer. Ceci est utilisé par les systèmes de fichiers lorsque `FILE_DELETE_ON_CLOSE` l'indicateur est spécifié.

- `open-with-write-intent` option permettant de filtrer la demande client pour ouvrir avec une intention d'écriture.

La configuration de ce filtre entraîne la réception d'une notification sur le serveur FPolicy uniquement lorsqu'une tentative est effectuée pour ouvrir un fichier avec l'intention d'y écrire un objet.

- `write-with-size-change` option permettant de filtrer la demande d'écriture client avec changement de taille.
- `setattr-with-owner-change` option permettant de filtrer les demandes `setattr` du client pour changer le propriétaire d'un fichier ou d'un répertoire.
- `setattr-with-group-change` option permettant de filtrer les demandes `setattr` du client pour changer le groupe d'un fichier ou d'un répertoire.

<p><i>Est une opération de volume requise</i></p> <p>Spécifie si une surveillance est requise pour les opérations de montage et de démontage de volumes. La valeur par défaut est <code>false</code>.</p>	<pre>-volume-operation {true</pre>
<pre>false} -filters filter, ...</pre>	<p><i>Notifications de refus d'accès FPolicy</i></p> <p>À partir de ONTAP 9.13.1, les utilisateurs peuvent recevoir des notifications en cas d'échec des opérations sur les fichiers en raison d'un manque d'autorisations. Ces notifications sont précieuses pour la sécurité, la protection contre les ransomware et la gouvernance. Des notifications seront générées pour l'opération de fichier ayant échoué en raison d'un manque d'autorisation, notamment :</p> <ul style="list-style-type: none"> • Défaillances dues aux autorisations NTFS. • Échecs dus aux bits de mode Unix. • Défaillances dues à des ACL NFSv4.
<pre>-monitor-fileop-failure {true</pre>	<pre>false}</pre>

• **exclude-directory-option** permettant de filtrer les demandes client pour les opérations d'annuaire.

Lorsque vous configurez votre événement FPolicy, vous devez savoir que seules certaines combinaisons d'opérations et de filtres sont prises en charge pour la surveillance des opérations d'accès aux fichiers SMB.

Le tableau suivant fournit la liste des combinaisons d'opérations de fichiers et de filtres prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers SMB :

Opérations de fichiers prises en charge	Filtres pris en charge
fermer	surveillance-ads, hors ligne-bit, fermeture-avec-modification, fermeture-sans-modification, gros-avec-lecture, exclure-répertoire
création	surveillance-ads, hors ligne-bit

dir_de_création	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
supprimer	surveillance-ads, hors ligne-bit
dir_de_suppression	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
getattr	offline-bit, exclude-dir
la transparence	monitor-ads, offline-bit, open-with-delete-intentionnel, open-with-write-intentions, exclude-dir
lecture	surveillance-ads, hors-ligne-bit, première lecture
écriture	surveillance-ads, hors-ligne-bit, première-écriture, écriture-avec-changement de taille
renommer	surveillance-ads, hors ligne-bit
rename_dir	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
définir	monitor-ads, offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_creation_time_change, setattr_with_size_change, setattr_with_allocation_size_change, exclude_directory

À partir de ONTAP 9.13.1, les utilisateurs peuvent recevoir des notifications en cas d'échec des opérations sur les fichiers en raison d'un manque d'autorisations. Le tableau suivant répertorie les combinaisons de filtres et d'opérations de fichiers refusés d'accès pris en charge pour la surveillance FPolicy des événements d'accès aux fichiers SMB :

Opération de fichier d'accès refusé prise en charge	Filtres pris en charge
la transparence	NA

Opérations de fichiers et combinaisons de filtres prises en charge pouvant être moniteurs par FPolicy pour NFSv3

Lorsque vous configurez votre événement FPolicy, vous devez savoir que seules certaines combinaisons d'opérations sur les fichiers et de filtres sont prises en charge pour surveiller les opérations d'accès aux fichiers NFSv3.

Le tableau suivant répertorie les opérations de fichiers et les combinaisons de filtres prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers NFSv3 :

Opérations de fichiers prises en charge	Filtres pris en charge
création	bit hors ligne
dir_de_création	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
supprimer	bit hors ligne
dir_de_suppression	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
lien	bit hors ligne
recherche	offline-bit, exclude-dir
lecture	bit hors ligne, première lecture
écriture	bit hors ligne, première écriture, écriture avec changement de taille
renommer	bit hors ligne
rename_dir	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
définir	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modif_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
symlink	bit hors ligne

À partir de ONTAP 9.13.1, les utilisateurs peuvent recevoir des notifications en cas d'échec des opérations sur les fichiers en raison d'un manque d'autorisations. Le tableau suivant répertorie les combinaisons de filtres et d'opérations de fichiers refusés d'accès prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers NFSv3 :

Opération de fichier d'accès refusé prise en charge	Filtres pris en charge
l'accès	NA
création	NA
dir_de_création	NA
supprimer	NA
dir_de_suppression	NA

lien	NA
lecture	NA
renommer	NA
rename_dir	NA
définir	NA
écriture	NA

Opérations de fichiers et combinaisons de filtres prises en charge que FPolicy peut surveiller pour NFSv4

Lorsque vous configurez votre événement FPolicy, vous devez savoir que seules certaines combinaisons d'opérations et de filtres sont prises en charge pour surveiller les opérations d'accès aux fichiers NFSv4.

À partir de ONTAP 9.15.1, FPolicy prend en charge le protocole NFSv4.1.

La liste des opérations de fichiers et des combinaisons de filtres prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers NFSv4 ou NFSv4.1 est fournie dans le tableau suivant :

Opérations de fichiers prises en charge	Filtres pris en charge
fermer	bit hors ligne, répertoire d'exclusion
création	bit hors ligne
dir_de_création	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
supprimer	bit hors ligne
dir_de_suppression	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
getattr	bit hors ligne, répertoire d'exclusion
lien	bit hors ligne
recherche	bit hors ligne, répertoire d'exclusion
la transparence	bit hors ligne, répertoire d'exclusion
lecture	bit hors ligne, première lecture

écriture	bit hors ligne, première écriture, écriture avec changement de taille
renommer	bit hors ligne
rename_dir	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
définir	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
symlink	bit hors ligne

À partir de ONTAP 9.13.1, les utilisateurs peuvent recevoir des notifications en cas d'échec des opérations sur les fichiers en raison d'un manque d'autorisations. La liste des combinaisons de filtres et d'opérations de fichiers refusés d'accès prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers NFSv4 ou NFSv4.1 est fournie dans le tableau suivant :

Opération de fichier d'accès refusé prise en charge	Filtres pris en charge
l'accès	NA
création	NA
dir_de_création	NA
supprimer	NA
dir_de_suppression	NA
lien	NA
la transparence	NA
lecture	NA
renommer	NA
rename_dir	NA
définir	NA
écriture	NA

Remplissez la fiche de configuration des événements FPolicy

Vous pouvez utiliser cette fiche pour enregistrer les valeurs nécessaires lors du processus de configuration des événements FPolicy. Si une valeur de paramètre est requise, vous devez déterminer la valeur à utiliser pour ces paramètres avant de configurer l'événement FPolicy.

Vous devez indiquer si vous souhaitez inclure chaque paramètre dans la configuration des événements FPolicy, puis noter la valeur des paramètres que vous souhaitez inclure.

Type d'information	Obligatoire	Inclure	Vos valeurs
Nom de la machine virtuelle de stockage (SVM)	Oui.	Oui.	
Nom de l'événement	Oui.	Oui.	
Protocole	Non		
Opérations sur les fichiers	Non		
Filtres	Non		
Opération de volume	Non		
Événements d'accès refusé (Support à partir de ONTAP 9.13)	Non		

Planifiez la configuration de la règle FPolicy

Planifier l'présentation de la configuration de la règle FPolicy

Avant de configurer la règle FPolicy, vous devez comprendre les paramètres requis lors de la création de la règle ainsi que les raisons pour lesquelles vous pouvez vouloir configurer certains paramètres facultatifs. Ces informations vous aident à déterminer les valeurs à définir pour chaque paramètre.


Lors de la création d'une politique FPolicy, vous associez cette règle à ce qui suit :

- Le serveur virtuel de stockage (SVM)
- Un ou plusieurs événements FPolicy
- Moteur externe FPolicy

Vous pouvez également configurer plusieurs paramètres de stratégie facultatifs.

Contenu de la configuration des règles FPolicy

Vous pouvez utiliser la liste suivante de règles FPolicy disponibles et de paramètres facultatifs pour vous aider à planifier votre configuration :

Type d'information	Option	Obligatoire	Valeur par défaut
<p><i>Nom du SVM</i></p> <p>Spécifie le nom du SVM sur lequel vous souhaitez créer une politique FPolicy.</p>	<p>-vserver vserver_name</p>	Oui.	Aucune
<p><i>Nom de la politique</i></p> <p>Spécifie le nom de la politique FPolicy.</p> <p>Le nom peut comporter jusqu'à 256 caractères.</p> <div>  <p>Le nom doit comporter jusqu'à 200 caractères si la stratégie est configurée dans une configuration de reprise après incident de MetroCluster ou de SVM.</p> </div> <p>Le nom peut contenir n'importe quelle combinaison des caractères ASCII suivants :</p> <ul style="list-style-type: none"> • a à z • A à Z • 0 à 9 • « » _ , « » - " , and " . » 	<p>-policy-name policy_name</p>	Oui.	Aucune
<p><i>Noms d'événements</i></p> <p>Spécifie une liste d'événements séparés par des virgules à associer à la politique FPolicy.</p> <ul style="list-style-type: none"> • Vous pouvez associer plusieurs événements à une stratégie. • Un événement est spécifique à un protocole. • Vous pouvez utiliser une seule stratégie pour surveiller les événements d'accès aux fichiers pour plusieurs protocoles en créant un événement pour chaque protocole que la stratégie doit surveiller, puis en associant les événements à la stratégie. • Les événements doivent déjà exister. 	<p>-events event_name, ...</p>	Oui.	Aucune

<p><i>Magasin permanent</i></p> <p>Depuis la version ONTAP 9.14.1, ce paramètre spécifie le magasin persistant qui capture les événements d'accès aux fichiers pour des politiques asynchrones non obligatoires dans la SVM.</p>	<p>-persistent -store persistent_store_name</p>	<p>Non</p>	<p>Aucune</p>
<p><i>Nom du moteur externe</i></p> <p>Spécifie le nom du moteur externe à associer à la politique FPolicy.</p> <ul style="list-style-type: none"> • Un moteur externe contient les informations requises par le nœud pour envoyer des notifications à un serveur FPolicy. • Vous pouvez configurer FPolicy de façon à utiliser le moteur externe natif ONTAP pour simplifier le blocage des fichiers ou à utiliser un moteur externe configuré pour utiliser des serveurs FPolicy externes (serveurs FPolicy) pour obtenir des fonctions plus sophistiquées de blocage et de gestion des fichiers. • Si vous souhaitez utiliser le moteur externe natif, vous ne pouvez pas spécifier de valeur pour ce paramètre ou vous pouvez le spécifier <code>native</code> comme valeur. • Si vous souhaitez utiliser des serveurs FPolicy, la configuration du moteur externe doit déjà exister. 	<p>-engine engine_name</p>	<p>Oui (à moins que la politique n'utilise le moteur natif ONTAP interne)</p>	<p>native</p>

<p><i>Est un screening obligatoire</i></p> <p>Indique si un filtrage d'accès aux fichiers obligatoire est requis.</p> <ul style="list-style-type: none"> • Le paramètre de filtrage obligatoire détermine quelle action est prise en cas d'incident d'accès aux fichiers lorsque tous les serveurs principaux et secondaires sont en panne ou qu'aucune réponse n'est reçue des serveurs FPolicy au cours d'une période de temporisation donnée. • Lorsqu'il est réglé sur <code>true</code>, les événements d'accès aux fichiers sont refusés. • Lorsqu'il est réglé sur <code>false</code>, les événements d'accès aux fichiers sont autorisés. 	<p><code>-is-mandatory</code> <code>{true</code></p>	<p><code>false}</code></p>	<p>Non</p>
--	--	----------------------------	------------

true	<p><i>Autoriser l'accès privilégié</i></p> <p>Indique si vous souhaitez que le serveur FPolicy possède un accès privilégié aux fichiers et dossiers surveillés à l'aide d'une connexion de données privilégiée.</p> <p>S'ils sont configurés, les serveurs FPolicy peuvent accéder aux fichiers à partir de la racine de l'SVM contenant les données surveillées à l'aide de la connexion de données privilégiée.</p> <p>Pour l'accès privilégié aux données, SMB doit être sous licence sur le cluster et toutes les LIFs de données utilisées pour se connecter aux serveurs FPolicy doivent être configurées de ce fait <code>cifs</code> comme l'un des protocoles autorisés.</p> <p>Si vous souhaitez configurer la policy pour autoriser les accès privilégiés, vous devez également spécifier le nom d'utilisateur du compte que vous souhaitez que le serveur FPolicy utilise pour cet accès privilégié.</p>	<p>-allow -privileged -access {yes</p>	no}
------	--	--	-----

Non (sauf si la lecture passthrough est activée)	no	<p><i>Nom d'utilisateur privilégié</i></p> <p>Spécifie le nom d'utilisateur du compte que les serveurs FPolicy utilisent pour l'accès aux données privilégié.</p> <ul style="list-style-type: none"> • La valeur de ce paramètre doit utiliser le format "daomain\user name". • Si -allow -privileged -access est défini sur no, toute valeur définie pour ce paramètre est ignorée. 	<p>-privileged</p> <p>-user-name</p> <p>user_name</p>
--	----	--	---

Non (sauf si l'accès privilégié est activé)	Aucune	<p><i>Autoriser la lecture_passthrough</i></p> <p>Spécifie si les serveurs FPolicy peuvent fournir des services de passe-lecture pour les fichiers qui ont été archivés sur le stockage secondaire (fichiers hors ligne) par les serveurs FPolicy :</p> <ul style="list-style-type: none"> • Passthrough-read est un moyen de lire les données pour les fichiers hors ligne sans restaurer les données dans le stockage primaire. <p>La lecture Passthrough réduit les latences de réponse. Les fichiers ne sont donc pas rappelés dans le stockage primaire, ce qui évite de l'avoir à remonter pour répondre à la demande de lecture. De plus, la lecture intermédiaire optimise l'efficacité du stockage puisque vous n'avez plus besoin d'utiliser l'espace de stockage principal avec des fichiers rappelés uniquement pour satisfaire les demandes de lecture.</p>	<p>-is-passthrough -read-enabled {true</p>
---	--------	---	--

Condition pour les configurations de l'étendue FPolicy si la politique FPolicy utilise le moteur natif

Si vous configurez la règle FPolicy pour utiliser le moteur natif, il existe une condition spécifique à la définition du périmètre FPolicy configuré pour la règle.

Le périmètre FPolicy définit les limites de la règle FPolicy s'applique, par exemple, si la FPolicy s'applique à des volumes ou des partages spécifiés. Un certain nombre de paramètres limitent davantage l'étendue à laquelle la politique FPolicy s'applique. L'un de ces paramètres, `-is-file-extension-check-on-directories-enabled` indique s'il faut vérifier les extensions de fichier sur les répertoires. La valeur par défaut est `false`, ce qui signifie que les extensions de fichiers des répertoires ne sont pas vérifiées.

Lorsqu'une politique de FPolicy utilisant le moteur natif est activée sur un partage ou un volume et sur `-is-file-extension-check-on-directories-enabled` le paramètre est défini sur `false` pour le périmètre de la politique, l'accès au répertoire est refusé. Avec cette configuration, car les extensions de fichier ne sont pas vérifiées pour les répertoires, toute opération de répertoire est refusée si elle relève de la portée de la stratégie.

Pour vous assurer que l'accès au répertoire a réussi lors de l'utilisation du moteur natif, vous devez définir le `-is-file-extension-check-on-directories-enabled` paramètre à `true` lors de la création de la portée.

Avec ce paramètre défini sur `true`, Les contrôles d'extension se produisent pour les opérations d'annuaire et la décision d'autoriser ou de refuser l'accès est prise en fonction des extensions incluses ou exclues dans la configuration du périmètre FPolicy.

Remplissez la fiche de règles FPolicy

Vous pouvez utiliser cette fiche pour enregistrer les valeurs nécessaires lors du processus de configuration de la politique FPolicy. Il est important d'enregistrer si vous souhaitez inclure chaque paramètre dans la configuration de la règle FPolicy, puis d'enregistrer la valeur des paramètres à inclure.

Type d'information	Inclure	Vos valeurs
Nom de la machine virtuelle de stockage (SVM)	Oui.	
Nom de la règle	Oui.	
Noms des événements	Oui.	
Stockage persistant		
Nom du moteur externe		
Un screening obligatoire est-il requis ?		
Autoriser l'accès privilégié		
Nom d'utilisateur privilégié		

Planification de la configuration du cadre FPolicy

Planifier l'présentation de la configuration du cadre FPolicy

Avant de configurer le cadre FPolicy, vous devez comprendre ce qu'il signifie. Vous devez comprendre le contenu de la configuration du périmètre. Vous devez également comprendre les règles de priorité de la portée. Ces informations peuvent vous aider à planifier les valeurs que vous souhaitez définir.

Ce qu'il signifie pour créer une étendue FPolicy

La création du périmètre FPolicy consiste à définir les limites de la règle FPolicy. Le serveur virtuel de stockage (SVM) est la limite de base. Lorsque vous créez un cadre pour une politique FPolicy, vous devez définir la politique FPolicy à laquelle elle s'applique, et vous devez désigner la SVM à laquelle vous souhaitez appliquer le périmètre.

Un certain nombre de paramètres limitent davantage la portée au sein de la SVM spécifiée. Vous pouvez restreindre la portée en spécifiant ce qui doit être inclus dans la portée ou en spécifiant ce qui à exclure de la portée. Après avoir appliqué une portée à une stratégie activée, les vérifications d'événements de stratégie sont appliquées à la portée définie par cette commande.

Des notifications sont générées pour les événements d'accès aux fichiers où des correspondances sont trouvées dans les options « inclure ». Les notifications ne sont pas générées pour les événements d'accès aux fichiers où des correspondances sont trouvées dans les options « exclure ».

La configuration du périmètre FPolicy définit les informations de configuration suivantes :

- Nom du SVM
- Nom de la règle
- Les partages à inclure ou à exclure de ce qui est surveillé
- Les règles d'exportation à inclure ou à exclure de ce qui est surveillé
- Les volumes à inclure ou à exclure de ce qui est surveillé
- Les extensions de fichier à inclure ou exclure de ce qui est surveillé
- Vérification de l'extension de fichier sur les objets de répertoire



Il existe des considérations spéciales à prendre en compte pour ce qui est des règles FPolicy de cluster. La politique de FPolicy de cluster est une règle que l'administrateur du cluster crée pour le SVM d'admin. Si l'administrateur du cluster crée également le périmètre de cette politique FPolicy de cluster, l'administrateur du SVM ne peut pas créer de étendue pour cette même politique. Toutefois, si l'administrateur du cluster ne crée pas de périmètre pour la politique de FPolicy de cluster, tout administrateur du SVM peut créer le périmètre de cette politique. Si l'administrateur SVM crée un périmètre pour cette politique FPolicy de cluster, l'administrateur du cluster ne peut pas créer par la suite une étendue de cluster pour cette même policy de cluster. En effet, l'administrateur du cluster ne peut pas remplacer la portée de la même politique de cluster.

Les règles de priorité de la portée


Les règles de priorité suivantes s'appliquent aux configurations du périmètre :

- Lorsqu'un partage est inclus dans le `-shares-to-include` le paramètre et le volume parent du partage sont inclus dans le `-volumes-to-exclude` paramètre, `-volumes-to-exclude` a priorité sur `-shares-to-include`.
- Lorsqu'une export-policy est incluse dans le `-export-policies-to-include` et le volume parent de la export policy est inclus dans le `-volumes-to-exclude` paramètre, `-volumes-to-exclude` a priorité sur `-export-policies-to-include`.
- Un administrateur peut spécifier les deux `-file-extensions-to-include` et `-file-extensions-to-exclude` listes.

Le `-file-extensions-to-exclude` le paramètre est vérifié avant le `-file-extensions-to-include` le paramètre est vérifié.

Contenu de la configuration de l'étendue FPolicy

Pour planifier votre configuration, vous pouvez utiliser la liste suivante des paramètres de configuration du périmètre FPolicy disponibles :



Lors de la configuration des partages, des règles d'exportation, des volumes et des extensions de fichiers à inclure ou à exclure du périmètre, les paramètres d'inclusion et d'exclusion peuvent inclure des métacaractères tels que «`»?`» and «`»*`». L'utilisation d'expressions régulières n'est pas prise en charge.

Type d'information	Option
<p>SVM</p> <p>Spécifie le nom du SVM sur lequel vous souhaitez créer une étendue FPolicy.</p> <p>Chaque configuration FPolicy est définie au sein d'un seul SVM. Le moteur externe, l'événement de politique, l'étendue des règles et la politique associés pour créer une configuration de politique FPolicy doivent tous être associés au même SVM.</p>	<p><code>-vserver vserver_name</code></p>
<p>Nom de la politique</p> <p>Spécifie le nom de la politique FPolicy à laquelle vous souhaitez associer le périmètre. La politique FPolicy doit déjà exister.</p>	<p><code>-policy-name policy_name</code></p>
<p>Actions à inclure</p> <p>Spécifie une liste de partages délimitée par des virgules pour contrôler la politique FPolicy à laquelle le périmètre est appliqué.</p>	<p><code>-shares-to-include share_name, ...</code></p>

<p><i>Actions à exclure</i></p> <p>Spécifie une liste de partages délimitée par des virgules, à exclure de la surveillance de la politique FPolicy à laquelle le périmètre est appliqué.</p>	<pre>-shares-to-exclude share_name, ...</pre>
<p><i>Volumes à inclure</i> Spécifie une liste de volumes séparés par des virgules à surveiller pour la politique FPolicy à laquelle le périmètre est appliqué.</p>	<pre>-volumes-to-include volume_name, ...</pre>
<p><i>Volumes à exclure</i></p> <p>Spécifie une liste de volumes séparés par des virgules à exclure de la surveillance de la politique FPolicy à laquelle le périmètre est appliqué.</p>	<pre>-volumes-to-exclude volume_name, ...</pre>
<p><i>Exporter les stratégies à inclure</i></p> <p>Spécifie une liste des règles d'exportation séparées par des virgules pour surveiller la politique FPolicy à laquelle le périmètre est appliqué.</p>	<pre>-export-policies-to-include export_policy_name, ...</pre>
<p><i>Exporter des stratégies à exclure</i></p> <p>Spécifie une liste de règles d'exportation séparées par des virgules afin d'exclure de la surveillance de la politique FPolicy à laquelle le périmètre est appliqué.</p>	<pre>-export-policies-to-exclude export_policy_name, ...</pre>
<p><i>Extensions de fichier à inclure</i></p> <p>Spécifie une liste d'extensions de fichiers délimitée par des virgules pour surveiller la politique FPolicy à laquelle le périmètre est appliqué.</p>	<pre>-file-extensions-to-include file_extensions, ...</pre>
<p><i>Extension de fichier à exclure</i></p> <p>Spécifie une liste d'extensions de fichiers délimitée par des virgules à exclure de la surveillance de la politique FPolicy à laquelle le périmètre est appliqué.</p>	<pre>-file-extensions-to-exclude file_extensions, ...</pre>
<p><i>La vérification de l'extension de fichier sur le répertoire est-elle activée ?</i></p> <p>Indique si les vérifications d'extension de nom de fichier s'appliquent également aux objets de répertoire. Si ce paramètre est défini sur <code>true</code>, les objets de répertoire sont soumis aux mêmes contrôles d'extension que les fichiers normaux. Si ce paramètre est défini sur <code>false</code>, les noms de répertoire ne correspondent pas pour les postes et les notifications sont envoyées pour les répertoires même si leurs extensions de nom ne correspondent pas.</p> <p>Si la politique FPolicy à laquelle l'étendue est affectée est configurée pour utiliser le moteur natif, ce paramètre doit être défini sur <code>true</code>.</p>	<pre>-is-file-extension-check-on-directories-enabled {true</pre>
<p><code>false</code></p>	<pre>}</pre>

Remplissez la fiche de l'étendue FPolicy

Vous pouvez utiliser cette fiche pour enregistrer les valeurs nécessaires lors du processus de configuration du périmètre FPolicy. Si une valeur de paramètre est requise, vous devez déterminer la valeur à utiliser pour ces paramètres avant de configurer l'étendue FPolicy.

Vous devez indiquer si vous souhaitez inclure chaque paramètre dans la configuration de l'étendue FPolicy, puis noter la valeur des paramètres que vous souhaitez inclure.

Type d'information	Obligatoire	Inclure	Vos valeurs
Nom de la machine virtuelle de stockage (SVM)	Oui.	Oui.	
Nom de la règle	Oui.	Oui.	
Partages à inclure	Non		
Partages à exclure	Non		
Volumes à inclure	Non		
Volumes à exclure	Non		
Export-policy à inclure	Non		
Exporter les règles à exclure	Non		
Extensions de fichier à inclure	Non		
Extension de fichier à exclure	Non		
La vérification de l'extension de fichier sur le répertoire est-elle activée ?	Non		

Créer la configuration FPolicy

Créez le moteur externe FPolicy

Vous devez créer un moteur externe pour commencer à créer une configuration FPolicy. Le moteur externe définit la façon dont FPolicy établit et gère les connexions aux serveurs FPolicy externes. Si votre configuration utilise le moteur ONTAP interne (moteur externe natif) pour le blocage simple des fichiers, vous n'avez pas besoin de configurer un moteur externe FPolicy distinct et n'avez pas besoin de réaliser cette étape.

Ce dont vous avez besoin

Le "moteur externe" la fiche doit être remplie.

Description de la tâche

Si le moteur externe est utilisé dans une configuration MetroCluster, indiquez les adresses IP des serveurs FPolicy du site source en tant que serveurs primaires. Les adresses IP des serveurs FPolicy du site de destination doivent être spécifiées en tant que serveurs secondaires.

Étapes

- 1. Créez le moteur externe FPolicy à l'aide de `vserver fpolicy policy external-engine create` commande.

La commande suivante crée un moteur externe sur une machine virtuelle de stockage (SVM) `vs1.example.com`. Aucune authentification n'est requise pour les communications externes avec le serveur FPolicy.

```
vserver fpolicy policy external-engine create -vserver-name vs1.example.com
-engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
no-auth
```

- 2. Vérifiez la configuration du moteur externe FPolicy à l'aide du `vserver fpolicy policy external-engine show` commande.

Les informations d’affichage de la commande suivante concernant tous les moteurs externes configurés sur le SVM `vs1.example.com` :

```
vserver fpolicy policy external-engine show -vserver vs1.example.com
```

		Primary	Secondary		
External					
Vserver	Engine	Servers	Servers	Port	Engine
Type					
-----	-----	-----	-----	-----	

vs1.example.com	engine1	10.1.1.2,	-	6789	
synchronous		10.1.1.3			

La commande suivante affiche des informations détaillées sur le moteur externe nommé « moteur1 » sur le SVM `vs1.example.com` :

```
vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
-name engine1
```



```
Vserver: vs1.example.com
Engine: engine1
Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
Port Number of FPolicy Service: 6789
Secondary FPolicy Servers: -
External Engine Type: synchronous
SSL Option for External Communication: no-auth
FQDN or Custom Common Name: -
Serial Number of Certificate: -
Certificate Authority: -
```

Créez l'événement FPolicy

Dans le cadre de la configuration de règles FPolicy, vous devez créer un événement FPolicy. Lors de sa création, vous associez l'événement à la politique FPolicy. Un événement définit le protocole à surveiller et les événements d'accès aux fichiers à surveiller et à filtrer.

Avant de commencer

Vous devez terminer l'événement FPolicy ["feuille de calcul"](#).

Créez l'événement FPolicy

1. Créez l'événement FPolicy à l'aide de `vserver fpolicy policy event create` commande.

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name
event1 -protocol cifs -file-operations open,close,read,write
```

2. Vérifiez la configuration d'événement FPolicy à l'aide de `vserver fpolicy policy event show` commande.

```
vserver fpolicy policy event show -vserver vs1.example.com
```

Vserver	Event Name	File Protocols	File Operations	Filters	Is Volume Operation
vs1.example.com	event1	cifs	open, close, read, write	-	false

Créez les événements de refus d'accès FPolicy

À partir de ONTAP 9.13.1, les utilisateurs peuvent recevoir des notifications en cas d'échec des opérations sur les fichiers en raison d'un manque d'autorisations. Ces notifications sont précieuses pour la sécurité, la protection contre les ransomware et la gouvernance.

1. Créez l'événement FPolicy à l'aide de `vserver fpolicy policy event create` commande.

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name  
event1 -protocol cifs -monitor-fileop-failure true -file-operations open
```

Créez des magasins persistants FPolicy

Les magasins persistants peuvent aider à découpler le traitement des E/S client du traitement des notifications FPolicy afin de réduire la latence du client. À partir de ONTAP 9.14.1, FPolicy vous permet de configurer votre système "**magasins persistants**". Pour capturer les événements d'accès aux fichiers pour les politiques asynchrones non obligatoires dans la SVM. Les configurations obligatoires synchrones (obligatoires ou non) et asynchrones ne sont pas prises en charge.

À partir de ONTAP 9.15.1, la configuration du stockage persistant FPolicy est simplifiée. Le `persistent-store create` Automatise la création de volume pour le SVM et configure le volume pour le magasin persistant.

Selon la version ONTAP, il existe deux façons de créer un magasin persistant :

- ONTAP 9.15.1 ou version ultérieure : lorsque vous créez le magasin persistant, ONTAP crée et configure automatiquement son volume en même temps. Cela simplifie la configuration du magasin persistant FPolicy et met en œuvre toutes les bonnes pratiques.
- ONTAP 9.14.1 : créez et configurez manuellement un volume, puis créez un magasin persistant pour le volume qui vient d'être créé.

Il n'est possible de configurer qu'un seul magasin persistant sur chaque SVM. Ce magasin persistant unique doit être utilisé pour toutes les configurations FPolicy de cette SVM, même si les règles proviennent de différents partenaires.

Création d'un magasin persistant (ONTAP 9.15.1 ou version ultérieure)

À partir de ONTAP 9.15.1, utilisez le `fpolicy persistent-store create` Commande permettant de créer le stockage persistant FPolicy avec création et configuration de volumes en ligne. ONTAP bloque automatiquement le volume pour l'accès aux protocoles utilisateur externes (CIFS/NFS).

Avant de commencer

- La SVM sur laquelle vous souhaitez créer le magasin persistant doit avoir au moins un agrégat.
- Vous devez avoir accès aux agrégats disponibles pour la SVM et disposer des autorisations suffisantes pour créer des volumes.

Étapes

1. Créez le magasin persistant, qui crée et configure automatiquement le volume :

```
vserver fpolicy persistent-store create -vserver <vserver> -persistent-store  
<name> -volume <volume_name> -size <size> -autosize-mode  
<off|grow|grow_shrink>
```

- Le `vserver` Paramètre est le nom du SVM.
- Le `persistent-store` paramètre est le nom du magasin persistant.

- Le `volume` paramètre est le nom du volume du magasin persistant.



Si vous souhaitez utiliser un volume existant vide, utilisez le `volume show` pour la rechercher et la spécifier dans le paramètre `volume`.

- Le `size` le paramètre est basé sur la durée pendant laquelle vous souhaitez conserver les événements qui ne sont pas transmis au serveur externe (application partenaire).

Par exemple, si vous souhaitez que 30 minutes d'événements se poursuivent dans un cluster avec une capacité de 30 000 notifications par seconde :

Taille du volume requis = $30000 \times 30 \times 60 \times 0,6$ Ko (taille moyenne des enregistrements de notification)
= 32400000 Ko = ~32 Go

Pour connaître le taux de notification approximatif, vous pouvez accéder à votre application partenaire FPolicy ou utiliser le compteur FPolicy `requests_dispatched_rate`.



Si vous utilisez un volume existant, le paramètre `size` est facultatif. Si vous indiquez une valeur pour le paramètre `size`, le volume sera modifié avec la taille que vous spécifiez.

- Le `autosize-mode` paramètre spécifie le mode de dimensionnement automatique du volume. Les modes de dimensionnement automatique pris en charge sont les suivants :

- Désactivé : la taille du volume n'augmente pas ou ne diminue pas en fonction de la quantité d'espace utilisé.
- Grow : le volume augmente automatiquement lorsque l'espace utilisé dans le volume dépasse le seuil Grow.
- Grow_Grow - la taille du volume augmente ou diminue en fonction de la quantité d'espace utilisé.

2. Créez la règle FPolicy et ajoutez le nom du stockage persistant à cette règle. Pour plus d'informations, voir ["Créez la règle FPolicy"](#).

Création d'un magasin persistant (ONTAP 9.14.1)

Vous pouvez créer un volume, puis créer un magasin persistant pour utiliser ce volume. Vous pouvez ensuite bloquer le nouveau volume créé à partir de l'accès au protocole utilisateur externe (CIFS/NFS).

Étapes

1. Créer sur le SVM un volume vide pouvant être provisionné pour le magasin persistant :

```
volume create -vserver <SVM Name> -volume <volume> -state <online> -policy
<default> -unix-permissions <777> -size <value> -aggregate <aggregate name>
-snapshot-policy <none>
```

Un utilisateur administrateur disposant de privilèges RBAC suffisants (pour créer un volume) crée un volume (à l'aide de la commande cli du volume ou de l'API REST) de la taille souhaitée et fournit le nom de ce volume en tant que `-volume`. Dans le magasin persistant, créez la commande CLI ou l'API REST.

- Le `vserver` Paramètre est le nom du SVM.
- Le `volume` paramètre est le nom du volume du magasin persistant.
- Le `state` le paramètre doit être défini sur `en ligne` afin que le volume soit disponible.

- Le `policy` Le paramètre est défini sur la stratégie de service FPolicy, si vous en avez déjà un configuré. Si ce n'est pas le cas, vous pouvez utiliser le `volume modify` plus tard, pour ajouter la règle.
- Le `unix-permissions` le paramètre est facultatif.
- Le `size` le paramètre est basé sur la durée pendant laquelle vous souhaitez conserver les événements qui ne sont pas transmis au serveur externe (application partenaire).

Par exemple, si vous souhaitez que 30 minutes d'événements se poursuivent dans un cluster avec une capacité de 30 000 notifications par seconde :

Taille du volume requis = 30000 x 30 x 60 x 0,6 Ko (taille moyenne des enregistrements de notification)
= 32400000 Ko = ~32 Go

Pour connaître le taux de notification approximatif, vous pouvez accéder à votre application partenaire FPolicy ou utiliser le compteur FPolicy `requests_dispatched_rate`.

- Le paramètre `aggregate` est nécessaire pour les volumes FlexVol, sinon il n'est pas requis.
- Le `snapshot-policy` le paramètre doit être défini sur aucun. Cela permet de s'assurer qu'il n'y a pas de restauration accidentelle de l'instantané, ce qui entraîne la perte des événements actuels et empêche le traitement des événements en double.

Si vous souhaitez utiliser un volume existant vide, utilisez le `volume show` pour le trouver et le `volume modify` commande permettant d'apporter les modifications nécessaires. Assurez-vous que la stratégie, la taille et `snapshot-policy` les paramètres sont définis correctement pour le magasin persistant.

2. Créez le magasin persistant :

```
vserver fpolicy persistent store create -vserver <SVM> -persistent-store
<PS_name> -volume <volume>
```

- Le `vserver` Paramètre est le nom du SVM.
- Le `persistent-store` paramètre est le nom du magasin persistant.
- Le `volume` paramètre est le nom du volume du magasin persistant.

3. Créez la règle FPolicy et ajoutez le nom du stockage persistant à cette règle. Pour plus d'informations, voir ["Créez la règle FPolicy"](#).

Créez la règle FPolicy

Lorsque vous créez la politique FPolicy, vous associez un moteur externe et un ou plusieurs événements à la règle. La politique spécifie également si un filtrage obligatoire est nécessaire, si les serveurs FPolicy ont un accès privilégié aux données sur la machine virtuelle de stockage (SVM) et si la lecture passe-automatique pour les fichiers hors ligne est activée.

Ce dont vous avez besoin

- La fiche de politique FPolicy doit être remplie.
- Si vous prévoyez de configurer la règle pour utiliser les serveurs FPolicy, le moteur externe doit exister.

- Il faut au moins un événement FPolicy que vous prévoyez d'associer à la règle FPolicy.
- Si vous souhaitez configurer l'accès aux données privilégié, un serveur SMB doit exister sur la SVM.
- Pour configurer un magasin persistant pour une stratégie, le type de moteur doit être **async** et la stratégie doit être **non obligatoire**.

Pour plus d'informations, voir "[Créez des magasins persistants](#)".

Étapes

1. Créez la règle FPolicy :

```
vserver fpolicy policy create -vserver-name vserver_name -policy-name
policy_name -engine engine_name -events event_name, [-persistent-store
PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-
privileged-user-name domain\user_name] [-is-passthrough-read-enabled
{true|false}]
```

- Vous pouvez ajouter un ou plusieurs événements à la règle FPolicy.
- Par défaut, le tramage obligatoire est activé.
- Si vous souhaitez autoriser l'accès privilégié en définissant l' `-allow-privileged-access` paramètre à `yes`, vous devez également configurer un nom d'utilisateur privilégié pour l'accès privilégié.
- Si vous souhaitez configurer Passthrough-read en définissant le paramètre `-is-passthrough-read-enabled` paramètre à `true`, vous devez également configurer l'accès privilégié aux données.

La commande suivante crée une politique nommée « politique 1 » qui est associée à l'événement « event1 » et au moteur externe « moteur1 ». Cette règle utilise des valeurs par défaut dans la configuration de la stratégie :

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1
-events event1 -engine engine1
```

La commande suivante crée une politique nommée « politique 2 » qui est associée à l'événement « event2 » et au moteur externe « moteur2 ». Cette stratégie est configurée pour utiliser l'accès privilégié à l'aide du nom d'utilisateur spécifié. La lecture passe-système est activée :

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
-events event2 -engine engine2 -allow-privileged-access yes -privileged-
user-name example\archive_acct -is-passthrough-read-enabled true
```

La commande suivante crée une politique nommée `""native1""` qui est associée à l'événement `""event3""`. Cette règle utilise le moteur natif et les valeurs par défaut dans la configuration de la règle :

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
-events event3 -engine native
```

2. Vérifiez la configuration de la politique FPolicy à l'aide de `vserver fpolicy policy show` commande.

La commande suivante affiche des informations sur les trois politiques FPolicy configurées, y compris les informations suivantes :

- SVM associé à la politique

- Moteur externe associé à la politique
 - Événements associés à la politique
 - Indique si un screening obligatoire est requis
 - Si un accès privilégié est requis
- ```
vserver fpolicy policy show
```

| Vserver         | Policy Name | Events | Engine  | Is Mandatory | Privileged Access |
|-----------------|-------------|--------|---------|--------------|-------------------|
| -----           | -----       | -----  | -----   | -----        |                   |
| vs1.example.com | policy1     | event1 | engine1 | true         | no                |
| vs1.example.com | policy2     | event2 | engine2 | true         | yes               |
| vs1.example.com | native1     | event3 | native  | true         | no                |

## Créez le périmètre FPolicy

Après avoir créé la règle FPolicy, vous devez créer une étendue FPolicy. Lors de la création du périmètre, vous associez ce dernier à une règle FPolicy. Le périmètre définit les limites applicables à la politique FPolicy. Les portées peuvent inclure ou exclure des fichiers basés sur des partages, des règles d'exportation, des volumes et des extensions de fichier.

### Ce dont vous avez besoin

La fiche de l'étendue de FPolicy doit être remplie. La politique FPolicy doit exister avec un moteur externe associé (si cette règle est configurée pour utiliser des serveurs FPolicy externes) et doit avoir au moins un événement FPolicy associé.

### Étapes

1. Créez le cadre FPolicy à l'aide de `vserver fpolicy policy scope create` commande.

```
vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name policy1 -volumes-to-include datavol1,datavol2
```

2. Vérifiez la configuration du cadre FPolicy à l'aide du `vserver fpolicy policy scope show` commande.

```
vserver fpolicy policy scope show -vserver vs1.example.com -instance
```

```
Vserver: vs1.example.com
Policy: policy1
Shares to Include: -
Shares to Exclude: -
Volumes to Include: datavol1, datavol2
Volumes to Exclude: -
Export Policies to Include: -
Export Policies to Exclude: -
File Extensions to Include: -
File Extensions to Exclude: -
```

## Activez la règle FPolicy

Une fois que vous avez configuré une configuration de règles FPolicy, vous activez cette règle. L'activation de la stratégie définit sa priorité et lance la surveillance de l'accès aux fichiers pour la stratégie.

### Ce dont vous avez besoin

La politique FPolicy doit exister avec un moteur externe associé (si cette règle est configurée pour utiliser des serveurs FPolicy externes) et doit avoir au moins un événement FPolicy associé. Le cadre de la politique FPolicy doit exister et doit être attribué à la politique FPolicy.

### Description de la tâche

La priorité est utilisée lorsque plusieurs règles sont activées sur la machine virtuelle de stockage (SVM) et qu'une seule règle a souscrit au même événement d'accès aux fichiers. Les règles qui utilisent la configuration du moteur natif ont une priorité plus élevée que les règles pour tout autre moteur, quel que soit le numéro de séquence qui leur est attribué lors de l'activation de la stratégie.



Une policy ne peut pas être activée sur le SVM admin

### Étapes

1. Activez la politique FPolicy à l'aide de `vserver fpolicy enable` commande.

```
vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1
-sequence-number 1
```

2. Vérifiez que la politique FPolicy est activée à l'aide du `vserver fpolicy show` commande.

```
vserver fpolicy show -vserver vs1.example.com
```

| Vserver         | Policy Name | Sequence<br>Number | Status | Engine  |
|-----------------|-------------|--------------------|--------|---------|
| -----           | -----       | -----              | -----  | -----   |
| vs1.example.com | policy1     | 1                  | on     | engine1 |

## Gérer les configurations FPolicy

### Modifier les configurations FPolicy

#### Commandes permettant de modifier les configurations FPolicy

Vous pouvez modifier les configurations FPolicy en modifiant les éléments de la configuration. Vous pouvez modifier les moteurs externes, les événements FPolicy, les étendues FPolicy, les magasins persistants FPolicy et les règles FPolicy. Vous pouvez également activer ou désactiver les règles FPolicy. Lorsque vous désactivez la règle FPolicy, la surveillance des fichiers est interrompue.

Vous devez désactiver une règle FPolicy avant de modifier sa configuration.

| Si vous voulez modifier... | Utilisez cette commande...                                 |
|----------------------------|------------------------------------------------------------|
| Moteurs externes           | <code>vserver fpolicy policy external-engine modify</code> |
| Événements                 | <code>vserver fpolicy policy event modify</code>           |
| Étendues                   | <code>vserver fpolicy policy scope modify</code>           |
| Stockage persistant        | <code>vserver fpolicy persistent-store modify</code>       |
| Stratégies                 | <code>vserver fpolicy policy modify</code>                 |

Consultez les pages de manuels pour les commandes pour plus d'informations.

#### Activez ou désactivez les règles FPolicy

Vous pouvez activer les règles FPolicy une fois la configuration terminée. L'activation de la stratégie définit sa priorité et lance la surveillance de l'accès aux fichiers pour la stratégie. Vous pouvez désactiver les règles FPolicy pour arrêter la surveillance des accès aux fichiers correspondant à cette règle.

#### Ce dont vous avez besoin

La configuration FPolicy doit être réalisée avant l'activation des règles FPolicy.

#### Description de la tâche

- La priorité est utilisée lorsque plusieurs règles sont activées sur la machine virtuelle de stockage (SVM) et qu'une seule règle a souscrit au même événement d'accès aux fichiers.
- Les règles qui utilisent la configuration du moteur natif ont une priorité plus élevée que les règles pour tout autre moteur, quel que soit le numéro de séquence qui leur est attribué lors de l'activation de la stratégie.
- Pour modifier la priorité d'une règle FPolicy, vous devez la désactiver puis la réactiver à l'aide du nouveau numéro de séquence.

#### Étape



## 1. Effectuez l'action appropriée :

| Les fonctions que vous recherchez... | Saisissez la commande suivante...                                                                                |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Activez une règle FPolicy            | <code>vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer</code> |
| Désactiver une règle FPolicy         | <code>vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name</code>                         |

## Affiche des informations sur les configurations FPolicy

### Fonctionnement des commandes show

Il est utile lors de l'affichage d'informations sur la configuration FPolicy pour comprendre la `show` les commandes fonctionnent.

A `show` la commande sans paramètre supplémentaire affiche les informations sous forme récapitulative. De plus, chaque `show` la commande dispose des deux mêmes paramètres facultatifs mutuellement exclusifs. `-instance` et `-fields`.

Lorsque vous utilisez le `-instance` paramètre avec un `show` commande, la sortie de la commande affiche des informations détaillées au format de liste. Dans certains cas, le résultat détaillé peut être long et inclure plus d'informations que vous n'en avez besoin. Vous pouvez utiliser le `-fields fieldname[,fieldname...]` paramètre permettant de personnaliser la sortie afin qu'elle affiche les informations uniquement pour les champs que vous spécifiez. Vous pouvez définir les champs que vous pouvez spécifier en saisissant ? après le `-fields` paramètre.



La sortie d'un `show` commande avec `-fields` paramètre peut afficher d'autres champs pertinents et nécessaires associés aux champs demandés.

Toutes les `show` la commande comporte un ou plusieurs paramètres facultatifs qui filtrent la sortie et vous permettent de réduire la portée des informations affichées dans la sortie de la commande. Vous pouvez définir l'identité des paramètres facultatifs disponibles pour une commande en saisissant ? après le `show` commande.

Le `show` La commande prend en charge les motifs de style UNIX et les caractères génériques pour vous permettre de faire correspondre plusieurs valeurs dans les arguments de paramètres-commande. Par exemple, vous pouvez utiliser l'opérateur générique (\*), L'opérateur NOT (!), l'opérateur OR (|), l'opérateur Range (integer...integer), l'opérateur moins-que (<), l'opérateur plus grand-que (>), l'opérateur MOINS-égal ou égal à (<=) et l'opérateur supérieur ou égal à (>=) lors de la spécification de valeurs.

Pour plus d'informations sur l'utilisation de modèles de style UNIX et de caractères génériques, reportez-vous au [Utilisation de l'interface de ligne de commandes ONTAP](#).

### Commandes permettant d'afficher des informations sur les configurations FPolicy

Vous utilisez le `fpolicy show` Commandes permettant d'afficher des informations sur la configuration FPolicy, y compris les informations sur les moteurs, événements, étendues et règles FPolicy externes.

|                                               |                                                          |
|-----------------------------------------------|----------------------------------------------------------|
| Pour afficher des informations sur FPolicy... | Utilisez cette commande...                               |
| Moteurs externes                              | <code>vserver fpolicy policy external-engine show</code> |
| Événements                                    | <code>vserver fpolicy policy event show</code>           |
| Étendues                                      | <code>vserver fpolicy policy scope show</code>           |
| Stratégies                                    | <code>vserver fpolicy policy show</code>                 |

Consultez les pages de manuels pour les commandes pour plus d'informations.

#### Affiche des informations sur l'état des règles FPolicy

Vous pouvez afficher des informations sur le statut des règles FPolicy pour déterminer si une règle est activée, le moteur externe qu'elle est configuré à utiliser, le numéro de séquence correspondant à la règle et à quel serveur virtuel de stockage (SVM) la politique FPolicy est associée.

#### Description de la tâche

Si vous ne spécifiez aucun paramètre, la commande affiche les informations suivantes :

- Nom du SVM
- Nom de la règle
- Numéro de séquence de police
- Statut de la stratégie

Outre l'affichage des informations sur l'état des règles de FPolicy configurées sur le cluster ou un SVM spécifique, vous pouvez utiliser les paramètres de la commande pour filtrer les résultats de la commande par d'autres critères.

Vous pouvez spécifier le `-instance` paramètre pour afficher des informations détaillées sur les règles répertoriées. Vous pouvez également utiliser le `-fields` paramètre pour afficher uniquement les champs indiqués dans la sortie de la commande, ou `-fields ?` pour déterminer les champs que vous pouvez utiliser.

#### Étape

1. Afficher des informations filtrées sur l'état des règles FPolicy à l'aide de la commande appropriée :

|                                                             |                                                |
|-------------------------------------------------------------|------------------------------------------------|
| Pour afficher des informations d'état sur les stratégies... | Entrez la commande...                          |
| Sur le cluster                                              | <code>vserver fpolicy show</code>              |
| Dont le statut est spécifié                                 | <code>`vserver fpolicy show -status {on</code> |
| off}`                                                       | Sur un SVM spécifié                            |

|                                                  |                                          |
|--------------------------------------------------|------------------------------------------|
| vserver fpolicy show<br>-vserver vserver_name    | Avec le nom de la règle spécifiée        |
| vserver fpolicy show<br>-policy-name policy_name | Qui utilisent le moteur externe spécifié |

## Exemple

Les exemples suivants affichent les informations sur les règles FPolicy sur le cluster :

```
cluster1::> vserver fpolicy show
```

| Vserver         | Policy Name    | Sequence<br>Number | Status | Engine |
|-----------------|----------------|--------------------|--------|--------|
| FPolicy         | cserver_policy | -                  | off    | eng1   |
| vs1.example.com | v1p1           | -                  | off    | eng2   |
| vs1.example.com | v1p2           | -                  | off    | native |
| vs1.example.com | v1p3           | -                  | off    | native |
| vs1.example.com | cserver_policy | -                  | off    | eng1   |
| vs2.example.com | v1p1           | 3                  | on     | native |
| vs2.example.com | v1p2           | 1                  | on     | eng3   |
| vs2.example.com | cserver_policy | 2                  | on     | eng1   |

## Affiche des informations sur les règles FPolicy activées

Vous pouvez afficher des informations sur les règles FPolicy activées pour déterminer le moteur externe FPolicy à utiliser, la priorité de la règle et le SVM associé à la règle FPolicy.

### Description de la tâche

Si vous ne spécifiez aucun paramètre, la commande affiche les informations suivantes :

- Nom du SVM
- Nom de la règle
- Priorité de la stratégie

Vous pouvez utiliser les paramètres de la commande pour filtrer la sortie de la commande par critères spécifiés.

### Étape

1. Afficher des informations sur les règles FPolicy activées à l'aide de la commande appropriée :

|                                                                            |                       |
|----------------------------------------------------------------------------|-----------------------|
| Si vous souhaitez afficher des informations sur les stratégies activées... | Entrez la commande... |
|----------------------------------------------------------------------------|-----------------------|

|                                     |                                                                    |
|-------------------------------------|--------------------------------------------------------------------|
| Sur le cluster                      | <code>vserver fpolicy show-enabled</code>                          |
| Sur un SVM spécifié                 | <code>vserver fpolicy show-enabled -vserver vserver_name</code>    |
| Avec le nom de la règle spécifiée   | <code>vserver fpolicy show-enabled -policy-name policy_name</code> |
| Avec le numéro de séquence spécifié | <code>vserver fpolicy show-enabled -priority integer</code>        |

## Exemple

Les exemples suivants affichent les informations sur les règles FPolicy activées sur le cluster :

```
cluster1::> vserver fpolicy show-enabled
Vserver Policy Name Priority

vs1.example.com pol_native native
vs1.example.com pol_native2 native
vs1.example.com pol1 2
vs1.example.com pol2 4
```

## Gérez les connexions du serveur FPolicy

### Connectez-vous à des serveurs FPolicy externes

Pour activer le traitement de fichiers, vous devrez peut-être vous connecter manuellement à un serveur FPolicy externe si la connexion a déjà été interrompue. Une connexion est interrompue une fois le délai d'expiration du serveur atteint ou en raison d'une erreur. L'administrateur peut également mettre fin manuellement à une connexion.

### Description de la tâche

En cas d'erreur fatale, la connexion au serveur FPolicy peut être interrompue. Après avoir résolu le problème à l'origine de l'erreur fatale, vous devez vous reconnecter manuellement au serveur FPolicy.

### Étapes

1. Connectez-vous au serveur FPolicy externe à l'aide de `vserver fpolicy engine-connect` commande.

Pour plus d'informations sur la commande, consultez les pages de manuels.

2. Vérifiez que le serveur FPolicy externe est connecté à l'aide du `vserver fpolicy show-engine` commande.

Pour plus d'informations sur la commande, consultez les pages de manuels.

**Effectue la déconnexion des serveurs FPolicy externes**

Vous devrez peut-être vous déconnecter manuellement d'un serveur FPolicy externe. Cette opération peut être utile si le serveur FPolicy présente des problèmes avec le traitement des demandes de notification ou si vous devez effectuer une maintenance sur le serveur FPolicy.

**Étapes**

- 1. Déconnectez-vous du serveur FPolicy externe à l'aide de `vserver fpolicy engine-disconnect` commande.

Pour plus d'informations sur la commande, consultez les pages de manuels.

- 2. Vérifiez que le serveur FPolicy externe est déconnecté à l'aide de `vserver fpolicy show-engine` commande.

Pour plus d'informations sur la commande, consultez les pages de manuels.

**Affiche des informations sur les connexions aux serveurs FPolicy externes**

Vous pouvez afficher les informations d'état des connexions aux serveurs FPolicy externes pour le cluster ou pour une machine virtuelle de stockage (SVM) spécifiée. Ces informations peuvent vous aider à déterminer quels serveurs FPolicy sont connectés.

**Description de la tâche**

Si vous ne spécifiez aucun paramètre, la commande affiche les informations suivantes :

- Nom du SVM
- Nom du nœud
- Nom de la règle FPolicy
- Adresse IP du serveur FPolicy
- État du serveur FPolicy
- Type de serveur FPolicy

En plus d'afficher les informations relatives aux connexions FPolicy sur le cluster ou un SVM spécifique, vous pouvez utiliser les paramètres de la commande pour filtrer les résultats de la commande par d'autres critères.

Vous pouvez spécifier le `-instance` paramètre pour afficher des informations détaillées sur les règles répertoriées. Vous pouvez également utiliser le `-fields` paramètre pour afficher uniquement les champs indiqués dans la sortie de la commande. Vous pouvez entrer ? après le `-fields` paramètre pour déterminer les champs que vous pouvez utiliser.

**Étape**

- 1. Afficher des informations filtrées sur l'état de connexion entre le nœud et le serveur FPolicy à l'aide de la commande appropriée :

|                                                                                           |           |
|-------------------------------------------------------------------------------------------|-----------|
| Pour afficher les informations sur l'état des connexions à propos des serveurs FPolicy... | Entrer... |
|-------------------------------------------------------------------------------------------|-----------|

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Que vous spécifiez                               | <code>vserver fpolicy show-engine -server IP_address</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Pour un SVM spécifié                             | <code>vserver fpolicy show-engine -vserver vserver_name</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Associés à une politique spécifiée               | <code>vserver fpolicy show-engine -policy-name policy_name</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Avec l'état du serveur que vous spécifiez        | <p><code>vserver fpolicy show-engine -server-status status</code></p> <p>La liste ci-dessous répertorie les différents États du serveur :</p> <ul style="list-style-type: none"> <li>• <code>connected</code></li> <li>• <code>disconnected</code></li> <li>• <code>connecting</code></li> <li>• <code>disconnecting</code></li> </ul>                                                                                                                                                                                                                                                                                                                                      |
| Avec le type spécifié                            | <p><code>vserver fpolicy show-engine -server-type type</code></p> <p>Le type de serveur FPolicy peut être l'un des suivants :</p> <ul style="list-style-type: none"> <li>• <code>primary</code></li> <li>• <code>secondary</code></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Qui ont été déconnectés avec la raison spécifiée | <p><code>vserver fpolicy show-engine -disconnect-reason text</code></p> <p>La déconnexion peut être due à plusieurs raisons. Les raisons courantes de la déconnexion sont les suivantes :</p> <ul style="list-style-type: none"> <li>• <code>Disconnect command received from CLI.</code></li> <li>• <code>Error encountered while parsing notification response from FPolicy server.</code></li> <li>• <code>FPolicy Handshake failed.</code></li> <li>• <code>SSL handshake failed.</code></li> <li>• <code>TCP Connection to FPolicy server failed.</code></li> <li>• <code>The screen response message received from the FPolicy server is not valid.</code></li> </ul> |

### Exemple

Cet exemple affiche des informations sur les connexions des moteurs externes aux serveurs FPolicy du SVM vs1.example.com :

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
```

| FPolicy         |         |       |          | Server-      | Server- |
|-----------------|---------|-------|----------|--------------|---------|
| Vserver         | Policy  | Node  | Server   | status       | type    |
| -----           | -----   | ----- | -----    | -----        |         |
| vs1.example.com | policy1 | node1 | 10.1.1.2 | connected    | primary |
| vs1.example.com | policy1 | node1 | 10.1.1.3 | disconnected | primary |
| vs1.example.com | policy1 | node2 | 10.1.1.2 | connected    | primary |
| vs1.example.com | policy1 | node2 | 10.1.1.3 | disconnected | primary |

Cet exemple affiche des informations uniquement sur les serveurs FPolicy connectés :

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
```

| node  | vserver         | policy-name | server   |
|-------|-----------------|-------------|----------|
| ----- | -----           | -----       | -----    |
| node1 | vs1.example.com | policy1     | 10.1.1.2 |
| node2 | vs1.example.com | policy1     | 10.1.1.2 |

#### Affiche des informations sur l'état de la connexion de passerelle FPolicy

Vous pouvez afficher des informations sur l'état de la connexion de passage en lecture FPolicy à des serveurs FPolicy externes pour le cluster ou à un SVM spécifié. Ces informations peuvent vous aider à identifier les serveurs FPolicy dotés de connexions de données de type « passthrough read » et pour lesquels les serveurs FPolicy sont déconnectés.

#### Description de la tâche

Si vous ne spécifiez aucun paramètre, la commande affiche les informations suivantes :

- Nom du SVM
- Nom de la règle FPolicy
- Nom du nœud
- Adresse IP du serveur FPolicy
- État de la connexion de lecture intermédiaire FPolicy

En plus d'afficher les informations relatives aux connexions FPolicy sur le cluster ou un SVM spécifique, vous pouvez utiliser les paramètres de la commande pour filtrer les résultats de la commande par d'autres critères.

Vous pouvez spécifier le `-instance` paramètre pour afficher des informations détaillées sur les règles répertoriées. Vous pouvez également utiliser le `-fields` paramètre pour afficher uniquement les champs indiqués dans la sortie de la commande. Vous pouvez entrer ? après le `-fields` paramètre pour déterminer les champs que vous pouvez utiliser.

#### Étape

1. Afficher des informations filtrées sur l'état de connexion entre le nœud et le serveur FPolicy à l'aide de la commande appropriée :

|                                                                                         |                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pour afficher les informations sur l'état de la connexion...                            | Entrez la commande...                                                                                                                                                                                                                                            |
| État de la connexion de lecture « pashrough FPolicy » pour le cluster                   | <code>vserver fpolicy show-passthrough-read-connection</code>                                                                                                                                                                                                    |
| État de connexion de passerelle FPolicy pour un SVM spécifié                            | <code>vserver fpolicy show-passthrough-read-connection -vserver vserver_name</code>                                                                                                                                                                              |
| État de la connexion de lecture intermédiaire FPolicy pour une règle spécifiée          | <code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name</code>                                                                                                                                                                           |
| État détaillé de la connexion de lecture intermédiaire FPolicy pour une règle spécifiée | <code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance</code>                                                                                                                                                                 |
| État de la connexion de lecture intermédiaire FPolicy pour l'état que vous spécifiez    | <code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status</code> La liste ci-dessous répertorie les différents États du serveur : <ul style="list-style-type: none"><li>• connected</li><li>• disconnected</li></ul> |

**Exemple**

La commande suivante affiche des informations relatives aux connexions de lecture passerelle de tous les serveurs FPolicy du cluster :

```
cluster1::> vserver fpolicy show-passthrough-read-connection
```

| Vserver         | Policy Name | Node       | FPolicy Server | Server Status |
|-----------------|-------------|------------|----------------|---------------|
| vs2.example.com | pol_cifs_2  | FPolicy-01 | 2.2.2.2        | disconnected  |
| vs1.example.com | pol_cifs_1  | FPolicy-01 | 1.1.1.1        | connected     |

La commande suivante affiche des informations détaillées sur les connexions en lecture pasde serveurs FPolicy configurées dans la politique « Pol\_cifs\_1 » :



```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance
```

Node: FPolicy-01

Vserver: vs1.example.com

Policy: pol\_cifs\_1

Server: 1.1.1.1

Session ID of the Control Channel: 8cef052e-2502-11e3-  
88d4-123478563412

Server Status: connected

Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45

Time Passthrough Read Channel was Disconnected: -

Reason for Passthrough Read Channel Disconnection: none

## Vérifiez l'accès à l'aide du suivi de sécurité

### Fonctionnement des traces de sécurité

Vous pouvez ajouter des filtres de suivi des autorisations pour demander à ONTAP de consigner des informations sur la raison pour laquelle les serveurs SMB et NFS d'une machine virtuelle de stockage (SVM) autorise ou refuse la demande d'un client ou d'un utilisateur d'effectuer une opération. Cela peut être utile lorsque vous voulez vérifier que votre schéma de sécurité d'accès aux fichiers est approprié ou lorsque vous souhaitez résoudre les problèmes d'accès aux fichiers.

Les traces de sécurité vous permettent de configurer un filtre qui détecte les opérations client sur SMB et NFS sur le SVM et trace tous les contrôles d'accès correspondant à ce filtre. Vous pouvez alors afficher les résultats de la trace, ce qui fournit un résumé pratique de la raison pour laquelle l'accès a été autorisé ou refusé.

Lorsque vous voulez vérifier les paramètres de sécurité de l'accès SMB ou NFS sur des fichiers et dossiers de votre SVM ou si vous êtes confronté à un problème d'accès, vous pouvez rapidement ajouter un filtre pour activer le suivi des autorisations.

La liste suivante présente des faits importants sur le fonctionnement des traces de sécurité :

- ONTAP applique des traces de sécurité au niveau du SVM.
- Chaque requête entrante est criblée pour voir si elle correspond aux critères de filtrage des traces de sécurité activées.
- Des traces sont effectuées pour les demandes d'accès aux fichiers et aux dossiers.
- Les traces peuvent être filtrées en fonction des critères suivants :
  - Adresse IP du client
  - Chemin SMB ou NFS
  - Nom Windows
  - Nom UNIX

- Les demandes sont examinées pour les résultats des réponses *autorisé* et *refusé*.
- Chaque demande correspondant aux critères de filtrage des tracés activés est enregistrée dans le journal des résultats de suivi.
- L'administrateur du stockage peut configurer une temporisation sur un filtre pour la désactiver automatiquement.
- Si une demande correspond à plusieurs filtres, les résultats du filtre dont le numéro d'index est le plus élevé sont enregistrés.
- L'administrateur du stockage peut imprimer les résultats à partir du journal des résultats de suivi pour déterminer pourquoi une demande d'accès a été autorisée ou refusée.

## Types de contrôles d'accès surveillance des traces de sécurité

Les vérifications d'accès d'un fichier ou d'un dossier sont effectuées en fonction de plusieurs critères. Les traces de sécurité contrôlent les opérations sur tous ces critères.

Les types de vérifications d'accès que contrôle des traces de sécurité comprennent les éléments suivants :

- Méthode de sécurité volume et qtree
- Sécurité efficace du système de fichiers contenant les fichiers et les dossiers sur lesquels des opérations sont demandées
- Mappage d'utilisateurs
- Les autorisations de niveau partage
- Les autorisations de niveau exportation
- Les autorisations de niveau fichier
- Sécurité de la protection d'accès au niveau du stockage

## Considérations relatives à la création de traces de sécurité

Lorsque vous créez des traces de sécurité sur des machines virtuelles de stockage (SVM), tenez compte de plusieurs points à prendre en compte. Par exemple, vous devez savoir quels protocoles vous pouvez créer une trace, quels styles de sécurité sont pris en charge et quel est le nombre maximum de traces actives.

- Vous ne pouvez créer que des traces de sécurité sur des SVM.
- Chaque entrée de filtre de trace de sécurité est spécifique au SVM.

On doit spécifier le SVM sur lequel vous souhaitez exécuter le tracé.

- Vous pouvez ajouter des filtres de suivi des permissions pour les requêtes SMB et NFS.
- On doit configurer le serveur SMB ou NFS sur le SVM sur lequel vous souhaitez créer des filtres de trace.
- Vous pouvez créer des traces de sécurité pour les fichiers et les dossiers résidant sur NTFS, UNIX, ainsi que sur des volumes et des qtrees de type sécurité mixtes.
- Vous pouvez ajouter un maximum de 10 filtres de suivi des permissions par SVM.
- Vous devez spécifier un numéro d'index de filtre lors de la création ou de la modification d'un filtre.

Les filtres sont pris en compte dans l'ordre du numéro d'index. Les critères d'un filtre avec un numéro

d'index plus élevé sont pris en compte avant les critères avec un nombre d'index plus faible. Si la demande suivie correspond aux critères de plusieurs filtres activés, seul le filtre dont le numéro d'index est le plus élevé est déclenché.

- Une fois que vous avez créé et activé un filtre de trace de sécurité, vous devez exécuter des demandes de fichier ou de dossier sur un système client pour générer l'activité que le filtre de trace peut capturer et ouvrir une session dans le journal des résultats de trace.
- Vous devez ajouter des filtres de suivi des autorisations pour la vérification de l'accès aux fichiers ou le dépannage uniquement.

L'ajout de filtres de suivi des autorisations a un effet mineur sur les performances du contrôleur.

Lorsque vous avez terminé l'activité de vérification ou de dépannage, vous devez désactiver ou supprimer tous les filtres de suivi des autorisations. En outre, les critères de filtrage que vous sélectionnez doivent être aussi spécifiques que possible pour que ONTAP n'envoie pas un grand nombre de résultats de trace au journal.

## Exécuter des traces de sécurité

### Présenter les traces de sécurité

Une trace de sécurité implique la création d'un filtre de trace de sécurité, la vérification des critères de filtre, la génération de demandes d'accès sur un client SMB ou NFS qui correspondent aux critères de filtre, ainsi que l'affichage des résultats.

Une fois que vous avez terminé d'utiliser un filtre de sécurité pour capturer des informations de trace, vous pouvez modifier le filtre et le réutiliser ou le désactiver si vous n'en avez plus besoin. Après avoir affiché et analysé les résultats de trace du filtre, vous pouvez les supprimer s'ils ne sont plus nécessaires.

### Créer des filtres de trace de sécurité

Vous pouvez créer des filtres de trace de sécurité qui détectent les opérations des clients SMB et NFS sur les SVM (Storage Virtual machines) et vérifient tous les contrôles d'accès correspondant au filtre. Vous pouvez utiliser les résultats des tracés de sécurité pour valider votre configuration ou résoudre des problèmes d'accès.


### Description de la tâche

Il existe deux paramètres requis pour la commande `vserver Security trace filter create` :

| Paramètres requis                  | Description                                                                                                                                         |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-vserver vserver_name</code> | <i>Nom du SVM</i><br><br>Nom du SVM qui contient les fichiers ou les dossiers sur lesquels vous souhaitez appliquer le filtre de trace de sécurité. |

|                                  |                                                                                                                                                                                                                              |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-index index_number</code> | <p><i>Filtrer l'index numéro</i></p> <p>Le numéro d'index que vous souhaitez appliquer au filtre. Vous êtes limité à un maximum de 10 filtres de trace par SVM. Les valeurs autorisées pour ce paramètre sont de 1 à 10.</p> |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Un certain nombre de paramètres de filtre facultatifs vous permettent de personnaliser le filtre de trace de sécurité afin de réduire les résultats générés par le tracé de sécurité :

| Paramètre de filtre                                                                                                                                                                                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-client-ip IP_Address</code>                                                                                                                                                                                                    | Ce filtre spécifie l'adresse IP à partir de laquelle l'utilisateur accède au SVM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <code>-path path</code>                                                                                                                                                                                                               | <p>Ce filtre indique le chemin d'accès sur lequel appliquer le filtre de suivi des autorisations. La valeur pour <code>-path</code> peut utiliser l'un des formats suivants :</p> <ul style="list-style-type: none"> <li>• Le chemin complet, en commençant par la racine du partage ou de l'exportation</li> <li>• Chemin partiel, relatif à la racine du partage</li> </ul> <p>Vous devez utiliser les séparateurs de répertoire de style UNIX du répertoire de style NFS dans la valeur de chemin d'accès.</p>                                                                                                                                                                                 |
| <code>-windows-name win_user_name</code><br>ou <code>-unix</code><br><code>-name ``unix_user_name</code>                                                                                                                              | <p>Vous pouvez spécifier le nom d'utilisateur Windows ou le nom d'utilisateur UNIX dont vous souhaitez effectuer le suivi des demandes d'accès. La variable de nom d'utilisateur n'est pas sensible à la casse. Vous ne pouvez pas spécifier à la fois un nom d'utilisateur Windows et un nom d'utilisateur UNIX dans le même filtre.</p> <div>  <p>Même si vous pouvez suivre les événements d'accès SMB et NFS, il est possible d'utiliser l'utilisateur UNIX mappé et les groupes d'utilisateurs UNIX mappés lors des vérifications d'accès sur des données de style de sécurité UNIX ou mixtes.</p> </div> |
| <code>-trace-allow {yes</code>                                                                                                                                                                                                        | <code>no}</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Le suivi des événements de refus est toujours activé pour un filtre de trace de sécurité. Vous pouvez éventuellement suivre les événements. Pour suivre les événements d'autorisation, définissez ce paramètre sur <code>yes</code> . | <code>-enabled {enabled</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <code>disabled}</code>                                                                                                                                                                                                                | Vous pouvez activer ou désactiver le filtre de trace de sécurité. Par défaut, le filtre de trace de sécurité est activé.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|                       |                                                                                         |
|-----------------------|-----------------------------------------------------------------------------------------|
| -time-enabled integer | Vous pouvez spécifier un délai d'attente pour le filtre, après lequel il est désactivé. |
|-----------------------|-----------------------------------------------------------------------------------------|

### Étapes

#### 1. Créer un filtre de trace de sécurité :

```
vserver security trace filter create -vserver vserver_name -index
index_numberfilter_parameters
```

filter\_parameters est une liste des paramètres de filtre facultatifs.

Pour plus d'informations, consultez les pages de manuels relatives à la commande.

#### 2. Vérifiez l'entrée du filtre de trace de sécurité :

```
vserver security trace filter show -vserver vserver_name -index index_number
```

### Exemples

La commande suivante crée un filtre de trace de sécurité pour tout utilisateur accédant à un fichier avec un chemin de partage \\server\share1\dir1\dir2\file.txt À partir de l'adresse IP 10.10.10.7. Le filtre utilise un chemin complet pour le -path option. L'adresse IP du client utilisée pour accéder aux données est 10.10.10.7. Le filtre est sorti après 30 minutes :

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver Index Client-IP Path Trace-Allow
Windows-Name
----- -
vs1 1 10.10.10.7 /dir1/dir2/file.txt no -
```

La commande suivante crée un filtre de trace de sécurité utilisant un chemin relatif pour l' -path option. Le filtre trace l'accès pour un utilisateur Windows nommé « joe ». Joe accède à un fichier avec un chemin de partage \\server\share1\dir1\dir2\file.txt. Les traces de filtre autorisent et refusent les événements :

```
cluster1::> vservers security trace filter create -vservers vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vservers security trace filter show -vservers vs1 -index 2
Vserver: vs1
Filter Index: 2
Client IP Address to Match: -
Path: /dir1/dir2/file.txt
Windows User Name: mydomain\joe
UNIX User Name: -
Trace Allow Events: yes
Filter Enabled: enabled
Minutes Filter is Enabled: 60
```

### Affiche des informations sur les filtres de trace de sécurité

Vous pouvez afficher des informations sur les filtres de trace de sécurité configurés sur votre SVM (Storage Virtual machine). Cela vous permet de voir quels types d'événements d'accès chaque filtre trace.

#### Étape

1. Affiche des informations sur les entrées du filtre de trace de sécurité à l'aide de `vservers security trace filter show` commande.

Pour plus d'informations sur l'utilisation de cette commande, consultez les pages de manuels.

### Exemples

La commande suivante affiche des informations sur tous les filtres de trace de sécurité sur le SVM vs1 :

```
cluster1::> vservers security trace filter show -vservers vs1
```

| Vserver | Index | Client-IP | Path                | Trace-Allow | Windows-Name |
|---------|-------|-----------|---------------------|-------------|--------------|
| vs1     | 1     | -         | /dir1/dir2/file.txt | yes         | -            |
| vs1     | 2     | -         | /dir3/dir4/         | no          | mydomain\joe |

### Affiche les résultats du suivi de sécurité

Vous pouvez afficher les résultats de suivi de sécurité générés pour les opérations de fichiers qui correspondent aux filtres de trace de sécurité. Les résultats permettent de valider votre configuration de sécurité d'accès aux fichiers ou de résoudre les problèmes d'accès aux fichiers SMB et NFS.

## Ce dont vous avez besoin

Un filtre de trace de sécurité activé doit exister et des opérations doivent avoir été effectuées à partir d'un client SMB ou NFS correspondant au filtre de trace de sécurité pour générer les résultats de trace de sécurité.

## Description de la tâche

Vous pouvez afficher un récapitulatif de tous les résultats de la trace de sécurité ou personnaliser les informations affichées dans la sortie en spécifiant des paramètres facultatifs. Cela peut être utile lorsque les résultats du suivi de sécurité contiennent un grand nombre d'enregistrements.

Si vous ne spécifiez aucun des paramètres facultatifs, les éléments suivants s'affichent :

- Nom de la machine virtuelle de stockage (SVM)
- Nom du nœud
- Numéro d'index de trace de sécurité
- Style de sécurité
- Chemin
- Raison
- Nom d'utilisateur

Le nom d'utilisateur s'affiche en fonction de la configuration du filtre de trace :

| Si le filtre est configuré...     | Alors...                                                               |
|-----------------------------------|------------------------------------------------------------------------|
| Avec un nom d'utilisateur UNIX    | Le résultat du suivi de sécurité affiche le nom d'utilisateur UNIX.    |
| Avec un nom d'utilisateur Windows | Le résultat du suivi de sécurité affiche le nom d'utilisateur Windows. |
| Sans nom d'utilisateur            | Le résultat du suivi de sécurité affiche le nom d'utilisateur Windows. |

Vous pouvez personnaliser la sortie à l'aide de paramètres facultatifs. Voici certains des paramètres facultatifs que vous pouvez utiliser pour affiner les résultats renvoyés dans le résultat de la commande :

| Paramètre facultatif                 | Description                                                                                                                                                                                                                |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-fields field_name, ...</code> | Affiche la sortie sur les champs que vous choisissez. Vous pouvez utiliser ce paramètre seul ou en combinaison avec d'autres paramètres facultatifs.                                                                       |
| <code>-instance</code>               | Affiche des informations détaillées sur les événements de trace de sécurité. Utilisez ce paramètre avec d'autres paramètres facultatifs pour afficher des informations détaillées sur des résultats de filtre spécifiques. |
| <code>-node node_name</code>         | Affiche des informations uniquement sur les événements du nœud spécifié.                                                                                                                                                   |

|                                             |                                                                                                                                               |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-vserver vserver_name</code>          | Affiche des informations uniquement sur les événements du SVM spécifié.                                                                       |
| <code>-index integer</code>                 | Affiche des informations sur les événements survenus à la suite du filtre correspondant au numéro d'index spécifié.                           |
| <code>-client-ip IP_address</code>          | Affiche des informations sur les événements survenus à la suite de l'accès au fichier à partir de l'adresse IP du client spécifiée.           |
| <code>-path path</code>                     | Affiche des informations sur les événements qui se sont produits suite à l'accès au fichier au chemin spécifié.                               |
| <code>-user-name user_name</code>           | Affiche des informations sur les événements qui se sont produits à la suite de l'accès au fichier par l'utilisateur Windows ou UNIX spécifié. |
| <code>-security-style security_style</code> | Affiche des informations sur les événements survenus sur les systèmes de fichiers avec le style de sécurité spécifié.                         |

Pour plus d'informations sur les autres paramètres facultatifs que vous pouvez utiliser avec la commande, reportez-vous à la page `man`.

## Étape

1. Affiche les résultats du filtre de trace de sécurité à l'aide de l' `vserver security trace trace-result show` commande.

```
vserver security trace trace-result show -user-name domain\user
```

```
Vserver: vs1
```

| Node  | Index | Filter Details                                               | Reason                        |
|-------|-------|--------------------------------------------------------------|-------------------------------|
| ----- | ----- | -----                                                        | -----                         |
| node1 | 3     | User:domain\user<br>Security Style:mixed<br>Path:/dir1/dir2/ | Access denied by explicit ACE |
| node1 | 5     | User:domain\user<br>Security Style:unix<br>Path:/dir1/       | Access denied by explicit ACE |

## Modifier les filtres de trace de sécurité

Si vous souhaitez modifier les paramètres de filtre facultatifs utilisés pour déterminer les événements d'accès qui sont tracés, vous pouvez modifier les filtres de trace de sécurité existants.

## Description de la tâche



Vous devez identifier le filtre de trace de sécurité à modifier en précisant le nom de la machine virtuelle de stockage (SVM) sur laquelle le filtre est appliqué et le numéro d'index du filtre. Vous pouvez modifier tous les paramètres de filtre facultatifs.

## Étapes

### 1. Modifier un filtre de trace de sécurité :

```
vserver security trace filter modify -vserver vserver_name -index
index_numberfilter_parameters
```

- ° `vserver_name` Est le nom du SVM sur lequel vous souhaitez appliquer un filtre de trace de sécurité.
- ° `index_number` est le numéro d'index que vous souhaitez appliquer au filtre. Les valeurs autorisées pour ce paramètre sont de 1 à 10.
- ° `filter_parameters` est une liste des paramètres de filtre facultatifs.

### 2. Vérifiez l'entrée du filtre de trace de sécurité :

```
vserver security trace filter show -vserver vserver_name -index index_number
```

## Exemple

La commande suivante modifie le filtre de trace de sécurité avec l'index numéro 1. Le filtre trace les événements pour tout utilisateur accédant à un fichier avec un chemin de partage `\\server\share1\dir1\dir2\file.txt` À partir de n'importe quelle adresse IP. Le filtre utilise un chemin complet pour le `-path` option. Les traces de filtre autorisent et refusent les événements :

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
Vserver: vs1
Filter Index: 1
Client IP Address to Match: -
Path: /dir1/dir2/file.txt
Windows User Name: -
UNIX User Name: -
Trace Allow Events: yes
Filter Enabled: enabled
Minutes Filter is Enabled: 60
```

## Supprimer les filtres de trace de sécurité

Lorsque vous n'avez plus besoin d'une entrée de filtre de trace de sécurité, vous pouvez la supprimer. Étant donné que vous pouvez disposer d'un maximum de 10 filtres de suivi de sécurité par machine virtuelle de stockage (SVM), la suppression des filtres inutiles vous permet de créer de nouveaux filtres si vous avez atteint le maximum.

## Description de la tâche

Pour identifier de manière unique le filtre de trace de sécurité que vous souhaitez supprimer, vous devez spécifier les éléments suivants :

- Nom du SVM auquel le filtre de trace est appliqué
- Numéro d'index du filtre de trace

### Étapes

1. Identifiez le numéro d'index de filtre de l'entrée de filtre de trace de sécurité que vous souhaitez supprimer :

```
vserver security trace filter show -vserver vserver_name
```

```
vserver security trace filter show -vserver vs1
```

| Vserver      | Index | Client-IP | Path                | Trace-Allow |
|--------------|-------|-----------|---------------------|-------------|
| Windows-Name |       |           |                     |             |
| -----        | ----- | -----     | -----               | -----       |
| vs1          | 1     | -         | /dir1/dir2/file.txt | yes         |
| vs1          | 2     | -         | /dir3/dir4/         | no          |
| mydomain\joe |       |           |                     |             |

2. À l'aide des informations de numéro d'index de filtre de l'étape précédente, supprimez l'entrée de filtre :

```
vserver security trace filter delete -vserver vserver_name -index index_number
```

```
vserver security trace filter delete -vserver vs1 -index 1
```

3. Vérifiez que l'entrée du filtre de trace de sécurité est supprimée :

```
vserver security trace filter show -vserver vserver_name
```

```
vserver security trace filter show -vserver vs1
```

| Vserver      | Index | Client-IP | Path        | Trace-Allow |
|--------------|-------|-----------|-------------|-------------|
| Windows-Name |       |           |             |             |
| -----        | ----- | -----     | -----       | -----       |
| vs1          | 2     | -         | /dir3/dir4/ | no          |
| mydomain\joe |       |           |             |             |

### Supprimer les enregistrements de trace de sécurité

Une fois que vous avez terminé d'utiliser un enregistrement de suivi de filtre pour vérifier la sécurité d'accès aux fichiers ou pour résoudre les problèmes d'accès client SMB ou NFS, vous pouvez supprimer l'enregistrement de trace de sécurité du journal de suivi de sécurité.

## Description de la tâche

Avant de pouvoir supprimer un enregistrement de trace de sécurité, vous devez connaître le numéro de séquence de l'enregistrement.



Chaque machine virtuelle de stockage (SVM) peut stocker un maximum de 128 traces. Si le maximum est atteint sur la SVM, les anciens enregistrements de trace sont automatiquement supprimés au fur et à mesure de l'ajout de nouveaux enregistrements. Si vous ne souhaitez pas supprimer manuellement les enregistrements de trace sur ce SVM, vous pouvez laisser ONTAP supprimer automatiquement les plus anciens résultats de trace une fois que le maximum est atteint pour laisser place à de nouveaux résultats.

## Étapes

1. Identifiez le numéro de séquence de l'enregistrement à supprimer :

```
vserver security trace trace-result show -vserver vserver_name -instance
```

2. Supprimer l'enregistrement de trace de sécurité :

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name -seqnum integer
```

```
vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
999
```

- ° -node node\_name est le nom du nœud de cluster sur lequel l'événement de suivi des autorisations que vous souhaitez supprimer s'est produit.

Ce paramètre est obligatoire.

- ° -vserver vserver\_name Est le nom du SVM sur lequel l'événement de suivi des permissions que vous souhaitez supprimer s'est produit.

Ce paramètre est obligatoire.

- ° -seqnum integer est le numéro de séquence de l'événement de journal que vous souhaitez supprimer.

Ce paramètre est obligatoire.

## Supprimer tous les enregistrements de trace de sécurité

Si vous ne souhaitez pas conserver les enregistrements de trace de sécurité existants, vous pouvez supprimer tous les enregistrements d'un nœud à l'aide d'une seule commande.

### Étape

1. Supprimer tous les enregistrements de trace de sécurité :

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name *
```

- ° -node node\_name est le nom du nœud de cluster sur lequel l'événement de suivi des autorisations

que vous souhaitez supprimer s'est produit.

- `-vserver vserver_name` Est le nom de la machine virtuelle de stockage (SVM) sur laquelle l'événement de suivi des permissions que vous souhaitez supprimer s'est produit.

## Interpréter les résultats du suivi de sécurité

Les résultats du suivi de sécurité indiquent la raison pour laquelle une demande a été autorisée ou refusée. Sortie affiche le résultat sous la forme d'une combinaison de la raison d'autoriser ou de refuser l'accès et de l'emplacement dans le chemin de vérification d'accès où l'accès est autorisé ou refusé. Vous pouvez utiliser les résultats pour isoler et identifier les raisons pour lesquelles les actions sont ou ne sont pas autorisées.

### Recherche d'informations sur les listes de types de résultats et les détails du filtre

Vous pouvez trouver les listes de types de résultats et les détails de filtre qui peuvent être inclus dans les résultats de trace de sécurité dans les pages de manuel de `vserver security trace trace-result show` commande.

#### Exemple de sortie du Reason champ dans un Allow type de résultat

Voici un exemple de sortie du Reason champ qui apparaît dans les résultats de trace se connecte à un Allow type de résultat :

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

#### Exemple de sortie du Reason champ dans un Allow type de résultat

Voici un exemple de sortie du Reason champ qui apparaît dans le journal des résultats de trace dans un Deny type de résultat :

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

#### Exemple de sortie du Filter details légale

Voici un exemple de sortie du Filter details dans le journal des résultats de trace, qui répertorie le style de sécurité efficace du système de fichiers contenant des fichiers et des dossiers qui correspondent aux critères de filtre :

```
Security Style: MIXED and ACL
```

## Où trouver des informations complémentaires

Une fois que vous avez testé l'accès client SMB, vous pouvez effectuer une configuration SMB avancée ou ajouter un accès SAN. Après avoir testé l'accès client NFS avec succès, vous pouvez effectuer une configuration NFS avancée ou ajouter un accès SAN. Une fois les accès au protocole terminés, vous devez protéger le volume root du SVM.

### Configuration SMB

Vous pouvez configurer davantage l'accès SMB à l'aide des éléments suivants :

- ["Gestion SMB"](#)

Décrit la configuration et la gestion de l'accès aux fichiers à l'aide du protocole SMB.

- ["Rapport technique NetApp 4191 : guide des meilleures pratiques pour les services de fichiers Windows dans clustered Data ONTAP 8.2"](#)

Fournit une brève présentation de l'implémentation SMB et d'autres fonctionnalités des services de fichiers Windows avec des recommandations et des informations de dépannage de base pour ONTAP.

- ["Rapport technique NetApp 3740 : SMB 2 le protocole CIFS nouvelle génération dans Data ONTAP"](#)

Décrit les fonctionnalités, les détails de configuration et son implémentation de SMB 2 dans ONTAP.

### Configuration NFS

Vous pouvez configurer davantage l'accès NFS à l'aide des éléments suivants :

- ["Gestion NFS"](#)

Décrit comment configurer et gérer l'accès aux fichiers à l'aide du protocole NFS.

- ["Rapport technique NetApp 4067 : Guide des meilleures pratiques et de mise en œuvre de NFS"](#)

Sert de guide opérationnel NFSv3 et NFSv4 et présente le système d'exploitation ONTAP avec un point sur NFSv4.

- ["Rapport technique de NetApp 4668 : name Services Best Practices Guide \(Guide des meilleures pratiques des services de noms\)"](#)

Fournit une liste complète des meilleures pratiques, limites, recommandations et considérations relatives à la configuration des fichiers LDAP, NIS, DNS et utilisateurs et groupes locaux à des fins d'authentification.

- ["Rapport technique NetApp 4616 : NFS Kerberos dans ONTAP avec Microsoft Active Directory"](#)
- ["Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP"](#)
- ["Rapport technique NetApp 3580 : Guide des améliorations et des meilleures pratiques NFSv4 implémentation d'Data ONTAP"](#)

Décrit les meilleures pratiques à suivre lors de l'implémentation des composants NFSv4 sur des clients AIX, Linux ou Solaris reliés à des systèmes exécutant ONTAP.

## Protection du volume racine

Après avoir configuré les protocoles sur le SVM, il faut s'assurer que son volume root est protégé :

- "Protection des données"

Décrit la procédure de création d'un miroir de partage de charge pour protéger le volume racine du SVM, une pratique recommandée par NetApp pour les SVM compatibles avec NAS. Décrit également la procédure de restauration rapide en cas de défaillances ou de pertes de volumes en promouvant le volume racine du SVM à partir d'un miroir de partage de charge.

## Gestion du chiffrement avec System Manager



### Crypter les données stockées à l'aide du chiffrement logiciel

Utilisez le chiffrement de volume pour garantir que les données de volume ne peuvent pas être lues si le périphérique sous-jacent est requalifié, perdu ou volé. Le chiffrement de volume n'a pas besoin de disques spéciaux, il est compatible avec tous les disques durs et SSD.

Le chiffrement de volume requiert un gestionnaire de clés. Vous pouvez configurer le gestionnaire de clés intégré à l'aide de System Manager. Vous pouvez également utiliser un gestionnaire de clés externe, mais vous devez d'abord le configurer à l'aide de l'interface de ligne de commande de ONTAP.

Une fois le gestionnaire de clés configuré, les nouveaux volumes sont chiffrés par défaut.

#### Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Sous **Encryption**, cliquez sur  pour configurer le Gestionnaire de clés intégré pour la première fois.
3. Pour crypter les volumes existants, cliquez sur **Storage > volumes**.
4. Sur le volume souhaité, cliquez sur  puis sur **Modifier**.
5. Sélectionnez **Activer le cryptage**.



### Chiffrez les données stockées à l'aide de disques à autochiffrement

Le cryptage de disque garantit que toutes les données d'un niveau local ne peuvent pas être lues si l'équipement sous-jacent est requalifié, perdu ou volé. Le chiffrement de disque requiert des disques SSD ou des disques durs à autocryptage spéciaux.

Le chiffrement des disques requiert un gestionnaire de clés. Vous pouvez configurer le gestionnaire de clés intégré à l'aide de System Manager. Vous pouvez également utiliser un gestionnaire de clés externe, mais vous devez d'abord le configurer à l'aide de l'interface de ligne de commande de ONTAP.

Si ONTAP détecte des disques à autochiffrement, il vous invite à configurer le gestionnaire de clés intégré lorsque vous créez le niveau local.

#### Étapes

1. Sous **Encryption**, cliquez sur  pour configurer le gestionnaire de clés intégré.
2. Si vous voyez un message indiquant que les disques doivent être re-clés, cliquez sur , puis sur **Rekey**.

# Gestion du chiffrement via l'interface de ligne de commandes

## Présentation du chiffrement NetApp

NetApp propose des technologies de cryptage logicielles et matérielles qui permettent de garantir que les données au repos ne peuvent pas être lues si le support de stockage est requalifié, perdu ou volé.

- Le chiffrement logiciel associé à NetApp Volume Encryption (NVE) prend en charge le chiffrement des données sur un volume à la fois
- Le chiffrement matériel utilisant NetApp Storage Encryption (NSE) prend en charge le chiffrement de disque intégral (FDE) des données au moment de leur écriture.

## Configurez NetApp Volume Encryption

### Configurer la présentation de NetApp Volume Encryption

NetApp Volume Encryption (NVE) est une technologie logicielle de chiffrement des données au repos d'un volume à la fois. Une clé de chiffrement accessible uniquement au système de stockage garantit que les données du volume ne peuvent pas être lues si l'appareil sous-jacent est requalifié, perdu ou volé.

### Présentation de NVE

Avec NVE, les métadonnées et les données (y compris les copies Snapshot) sont chiffrées. L'accès aux données est donné par une clé XTS-AES-256 unique, une par volume. Un serveur de gestion externe des clés ou un gestionnaire de clés intégré (OKM) sert les clés pour les nœuds :

- Le serveur externe de gestion des clés est un système tiers de votre environnement de stockage qui transmet des clés aux nœuds à l'aide du protocole KMIP (Key Management Interoperability Protocol). Il est recommandé de configurer des serveurs de gestion externe des clés sur un système de stockage différent de vos données.
- Le gestionnaire de clés intégré est un outil intégré qui sert des clés aux nœuds du même système de stockage que vos données.

Depuis ONTAP 9.7, le chiffrement d'agrégat et de volume est activé par défaut si vous disposez d'une licence VE (Volume Encryption) et utilisez un gestionnaire de clés intégré ou externe. La licence VE est incluse avec "ONTAP One". Lorsqu'un gestionnaire de clés externe ou intégré est configuré, la configuration du chiffrement des données au repos est modifiée pour les nouveaux agrégats et les nouveaux volumes. Par défaut, NetApp Aggregate Encryption (NAE) sera activé dans les nouveaux agrégats. Par défaut, les nouveaux volumes qui ne font pas partie d'un agrégat NAE ont sur lequel le chiffrement de volume NetApp (NVE) est activé. Lorsqu'un serveur SVM (Data Storage Virtual machine) est configuré avec son propre gestionnaire de clés à l'aide d'une gestion mutualisée des clés, alors le volume créé pour ce SVM est automatiquement configuré avec NVE.

Vous pouvez activer le chiffrement sur un volume nouveau ou existant. NVE prend en charge la gamme complète de fonctionnalités d'efficacité du stockage, notamment la déduplication et la compression. À partir de ONTAP 9.14.1, vous pouvez [Activez NVE sur les volumes root du SVM existant](#).



Si vous utilisez SnapLock, vous pouvez activer le chiffrement uniquement sur les nouveaux volumes SnapLock vides. Vous ne pouvez pas activer le chiffrement sur un volume SnapLock existant.

Vous pouvez utiliser NVE sur n'importe quel type d'agrégat (HDD, SSD, hybride, LUN de baie), avec n'importe quel type RAID et dans n'importe quelle implémentation ONTAP prise en charge, y compris ONTAP Select. Vous pouvez également utiliser NVE avec le chiffrement matériel pour « chiffrer » les données sur des disques à autochiffrement.

Lorsque NVE est activé, le « core dump » est également chiffré.

### Chiffrement d'agrégat

En général, une clé unique est attribuée à chaque volume chiffré. Lorsque le volume est supprimé, la clé est supprimée.

Depuis ONTAP 9.6, il est possible d'utiliser *NetApp Aggregate Encryption (NAE)* pour attribuer des clés à l'agrégat contenant pour le chiffrement des volumes. Lors de la suppression d'un volume chiffré, les clés de l'agrégat sont préservées. Les clés sont supprimées si l'agrégat entier est supprimé.

Vous devez utiliser le chiffrement au niveau de l'agrégat pour procéder à la déduplication à la volée ou en arrière-plan au niveau de l'agrégat. NVE ne prend cependant pas en charge la déduplication au niveau de l'agrégat.

Depuis ONTAP 9.7, le chiffrement d'agrégat et de volume est activé par défaut si vous disposez d'une licence VE (Volume Encryption) et utilisez un gestionnaire de clés intégré ou externe.

Les volumes NVE et NAE peuvent coexister sur un même agrégat. Par défaut, les volumes NAE sont chiffrés avec un chiffrement au niveau des agrégats. Vous pouvez remplacer la valeur par défaut lorsque vous chiffrez le volume.

Vous pouvez utiliser le `volume move` Commande de conversion d'un volume NVE en volume NAE, et inversement. Vous pouvez répliquer un volume NAE sur un volume NVE.

Vous ne pouvez pas utiliser `secure purge` Commandes sur un volume NAE.

### Quand utiliser des serveurs externes de gestion des clés

Bien qu'il soit moins coûteux et généralement plus pratique d'utiliser le gestionnaire de clés intégré, vous devez configurer des serveurs KMIP si les conditions suivantes sont vraies :

- Votre solution de gestion des clés de chiffrement doit être conforme à la norme FIPS 140-2 (Federal Information Processing Standards) ou OASIS KMIP.
- Vous avez besoin d'une solution à plusieurs clusters et d'une gestion centralisée des clés de chiffrement.
- Votre entreprise exige que les clés d'authentification soient sécurisées sur un système ou à un emplacement différent de celui des données.

### Champ d'application de la gestion externe des clés

Le périmètre de la gestion externe des clés détermine si les serveurs de gestion des clés sécurisent tous les SVM dans le cluster ou bien uniquement les SVM sélectionnés :

- Vous pouvez utiliser une *cluster scope* pour configurer la gestion des clés externe pour tous les SVM du cluster. L'administrateur du cluster a accès à chaque clé stockée sur les serveurs.



- Depuis ONTAP 9.6, vous pouvez utiliser une *SVM scope* pour configurer la gestion externe des clés pour une SVM nommée dans le cluster. C'est le mieux adapté aux environnements mutualisés dans lesquels chaque locataire utilise un autre SVM (ou ensemble de SVM) pour transmettre les données. Seul l'administrateur du SVM pour un locataire donné peut accéder aux clés pour ce locataire.
- Vous pouvez utiliser ONTAP 9.10.1 depuis [Azure Key Vault](#) et [Google Cloud KMS](#) Protection des clés NVE uniquement pour les SVM de données. Ce dernier est disponible pour le KMS d'AWS à partir de la version 9.12.0.

Vous pouvez utiliser les deux étendues du même cluster. Si les serveurs de gestion des clés ont été configurés pour un SVM, ONTAP utilise uniquement ces serveurs pour sécuriser les clés. Sinon, ONTAP sécurise les clés avec les serveurs de gestion des clés configurés pour le cluster.

Une liste de gestionnaires de clés externes validés est disponible dans le "[Matrice d'interopérabilité NetApp \(IMT\)](#)". Pour trouver cette liste, entrez le terme « gestionnaires de clés » dans la fonction de recherche de l'IMT.

### Détails du support

Le tableau suivant présente les détails de la prise en charge de NVE :

| Ressource ou fonctionnalité | Détails du support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Plateformes                 | Une fonctionnalité de déchargement AES-ni est requise. Consultez la page <a href="#">Hardware Universe (HWU)</a> pour vérifier que NVE et NAE sont pris en charge pour votre plateforme.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Le cryptage                 | <p>Depuis ONTAP 9.7, les volumes et les agrégats nouvellement créés sont chiffrés par défaut lorsque vous ajoutez une licence VE (Volume Encryption) et qu'un gestionnaire de clés intégré ou externe est configuré. Si vous devez créer un agrégat non chiffré, utilisez la commande suivante :</p> <pre>storage aggregate create -encrypt-with-aggr-key false</pre> <p>Si vous avez besoin de créer un volume de texte brut, utilisez la commande suivante :</p> <pre>volume create -encrypt false</pre> <p>Le chiffrement n'est pas activé par défaut lorsque :</p> <ul style="list-style-type: none"> <li>• La licence VE n'est pas installée.</li> <li>• Le gestionnaire de clés n'est pas configuré.</li> <li>• La plateforme ou le logiciel ne prend pas en charge le chiffrement.</li> <li>• Le chiffrement matériel est activé.</li> </ul> |
| ONTAP                       | Toutes les implémentations de ONTAP. La prise en charge de ONTAP Cloud est disponible dans ONTAP 9.5 et versions ultérieures.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Périphériques               | HDD, SSD, hybride, LUN de baie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RAID                   | RAID0, RAID4, RAID-DP, RAID-TEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Volumes                | Volumes de données et volumes root SVM existants. Il n'est pas possible de chiffrer des données sur des volumes de métadonnées MetroCluster. Dans les versions de ONTAP antérieures à 9.14.1, vous ne pouvez pas chiffrer les données sur le volume racine du SVM avec NVE. À partir de ONTAP 9.14.1, ONTAP prend en charge <a href="#">NVE sur les volumes root du SVM</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Chiffrement d'agrégat  | <p>Depuis la version ONTAP 9.6, NVE prend en charge le chiffrement au niveau des agrégats (NAE) :</p> <ul style="list-style-type: none"> <li>• Vous devez utiliser le chiffrement au niveau de l'agrégat pour procéder à la déduplication à la volée ou en arrière-plan au niveau de l'agrégat.</li> <li>• Vous ne pouvez pas reKey un volume de chiffrement au niveau de l'agrégat.</li> <li>• La suppression sécurisée n'est pas prise en charge sur les volumes de chiffrement au niveau des agrégats.</li> <li>• Outre les volumes de données, NAE prend en charge le chiffrement des volumes root du SVM et du volume de métadonnées MetroCluster. NAE ne prend pas en charge le chiffrement du volume racine.</li> </ul>                                                                                                  |
| Étendue des SVM        | Depuis ONTAP 9.6, NVE prend en charge le périmètre des SVM pour la gestion externe des clés uniquement, et non pour le gestionnaire de clés intégré. MetroCluster est pris en charge à partir de ONTAP 9.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Efficacité du stockage | <p>Déduplication, compression, compaction, FlexClone.</p> <p>Les clones utilisent la même clé que le parent, même après le fractionnement du clone. Vous devez effectuer une <code>volume move</code> sur un clone divisé, après quoi le clone divisé aura une clé différente.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| La réplication         | <ul style="list-style-type: none"> <li>• Pour la réplication de volume, les volumes source et de destination peuvent avoir des paramètres de chiffrement différents. Le chiffrement peut être configuré pour la source et non configuré pour la destination, et inversement.</li> <li>• Pour la réplication SVM, le volume de destination est automatiquement chiffré, sauf si le nœud de destination ne contient pas de nœud qui prend en charge le chiffrement de volume, dans ce cas la réplication réussit, mais le volume de destination n'est pas chiffré.</li> <li>• Dans le cas de configurations MetroCluster, chaque cluster extrait les clés de gestion externes des serveurs de clés configurés. Les clés OKM sont répliquées vers le site partenaire par le service de réplication de la configuration.</li> </ul> |
| La conformité          | Depuis ONTAP 9.2, SnapLock est pris en charge en mode conformité et entreprise pour les nouveaux volumes uniquement. Vous ne pouvez pas activer le chiffrement sur un volume SnapLock existant.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

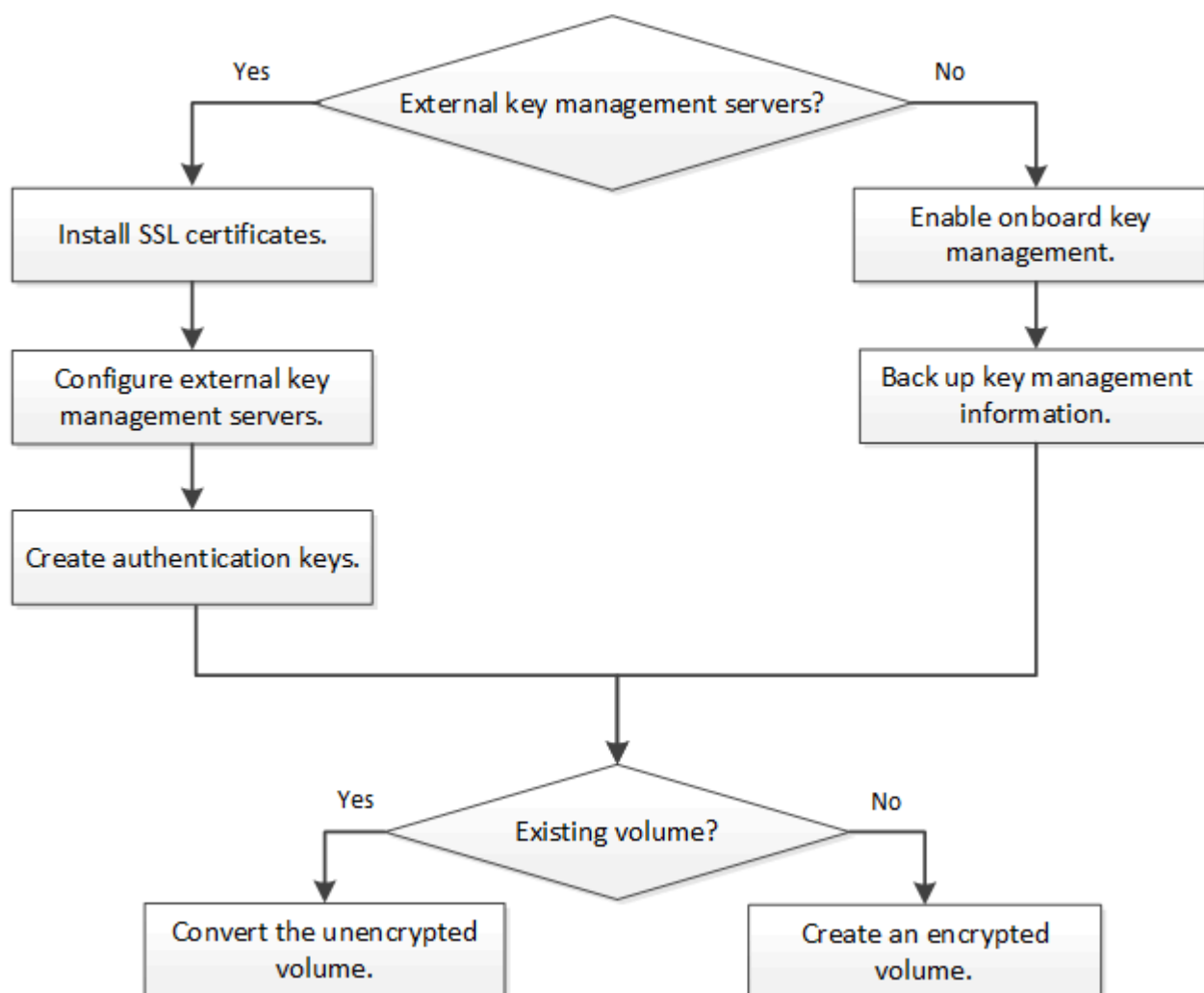
|                                     |                                                                                                                                                                                                                                                                 |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FlexGroups                          | FlexGroups est pris en charge à partir de ONTAP 9.2. Les agrégats de destination doivent être du même type que les agrégats source, au niveau des volumes ou de l'agrégat. ONTAP 9.5 prend en charge le renouvellement de clés des volumes FlexGroup sur place, |
| Transition depuis la version 7-mode | À partir de 7-mode transition Tool 3.3, vous pouvez utiliser l'interface de ligne de commandes de l'outil 7-mode transition Tool pour effectuer une transition basée sur les copies vers les volumes de destination NVE sur le système en cluster.              |

#### Informations associées

["FAQ : NetApp Volume Encryption et NetApp Aggregate Encryption"](#)

#### Flux de travail NetApp Volume Encryption

Vous devez configurer les services de gestion des clés avant d'activer le chiffrement de volume. Vous pouvez activer le chiffrement sur un nouveau volume ou sur un volume existant.



["Vous devez installer la licence VE"](#) Et configurez les services de gestion des clés avant de chiffrer les données avec NVE. Avant d'installer la licence, vous devez ["Déterminez si votre version de ONTAP prend en charge NVE"](#).

## Configurez NVE

### Déterminez si votre version de cluster prend en charge NVE

Vous devez déterminer si votre version de cluster prend en charge NVE avant d'installer la licence. Vous pouvez utiliser le `version` pour déterminer la version du cluster.

### Description de la tâche

La version en cluster est la version la plus basse d'ONTAP s'exécutant sur n'importe quel nœud du cluster.

### Étape

1. Déterminez si votre version de cluster prend en charge NVE :

```
version -v
```

NVE n'est pas pris en charge si la sortie de la commande affiche le texte « 1Ono-DARE » (pour « pas de chiffrement des données au repos »), ou si vous utilisez une plateforme non répertoriée dans le ["Détails du support"](#).

La commande suivante détermine si NVE est pris en charge sur `cluster1`.

```
cluster1::> version -v
NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
```

La sortie de `1Ono-DARE` Indique que NVE n'est pas pris en charge sur la version du cluster.

### Installez la licence

Une licence VE vous permet d'utiliser cette fonctionnalité sur tous les nœuds du cluster. Cette licence est requise avant de pouvoir chiffrer les données avec NVE. Il est inclus avec ["ONTAP One"](#).

Avant ONTAP One, la licence VE était incluse avec le pack de chiffrement. Le pack de chiffrement n'est plus proposé, mais reste valide. Bien qu'il ne soit pas actuellement requis, les clients existants peuvent choisir de ["Passez à ONTAP One"](#).

### Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez avoir reçu la clé de licence VE de votre représentant commercial ou avoir installé ONTAP One.

### Étapes

1. ["Vérifiez que la licence VE est installée"](#).

Le nom du package de licences VE est `VE`.

2. Si la licence n'est pas installée, ["Utilisez System Manager ou l'interface de ligne de commandes ONTAP pour l'installer"](#).

### Configurer la gestion externe des clés en vue d'ensemble

Vous pouvez utiliser un ou plusieurs serveurs externes de gestion des clés pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Un serveur externe de gestion des clés est un système tiers de votre environnement de stockage qui transmet des clés aux nœuds à l'aide du protocole KMIP (Key Management Interoperability Protocol).



Pour ONTAP 9.1 et les versions antérieures, les LIFs de node-management doivent être attribuées à des ports configurés avec le rôle de node-management avant de pouvoir utiliser le gestionnaire de clés externe.

NetApp Volume Encryption (NVE) prend en charge le gestionnaire de clés intégré dans ONTAP 9.1 et les versions ultérieures. Depuis la version ONTAP 9.3, NVE prend en charge le protocole KMIP (externe Key Management) et le gestionnaire de clés intégré. À partir de ONTAP 9.10.1, vous pouvez l'utiliser [Azure Key Vault](#) ou [Google Cloud Key Manager Service](#) Pour protéger vos clés NVE. À partir de ONTAP 9.11.1, vous pouvez configurer plusieurs gestionnaires de clés externes dans un cluster. Voir [Configurez les serveurs de clés en cluster](#).

### Gérez des gestionnaires de clés externes avec System Manager

À partir de la version ONTAP 9.7, vous pouvez stocker et gérer les clés d'authentification et de chiffrement à l'aide du gestionnaire de clés intégré. À partir de ONTAP 9.13.1, vous pouvez également utiliser des gestionnaires de clés externes pour stocker et gérer ces clés.

Le gestionnaire de clés intégré stocke et gère les clés dans une base de données sécurisée interne au cluster. L'étendue du cluster est celle-ci. Un gestionnaire de clés externe stocke et gère les clés à l'extérieur du cluster. Il peut s'agir du cluster ou de la VM de stockage. Un ou plusieurs gestionnaires de clés externes peuvent être utilisés. Les conditions suivantes s'appliquent :

- Si le gestionnaire de clés intégré est activé, un gestionnaire de clés externe ne peut pas être activé au niveau du cluster, mais il peut être activé au niveau de la VM de stockage.
- Si un gestionnaire de clés externe est activé au niveau du cluster, le gestionnaire de clés intégré ne peut pas être activé.

Lorsque vous utilisez des gestionnaires de clés externes, vous pouvez enregistrer jusqu'à quatre serveurs de clés principaux par machine virtuelle de stockage et par cluster. Chaque serveur de clés principal peut être mis en cluster avec jusqu'à trois serveurs de clés secondaires.



### Configurez un gestionnaire de clés externe


Pour ajouter un gestionnaire de clés externe à une VM de stockage, il est conseillé d'ajouter une passerelle en option lors de la configuration de l'interface réseau de la VM de stockage. Si la machine virtuelle de stockage a été créée sans la route réseau, vous devrez créer la route explicitement pour le gestionnaire de clés externe. Voir "[Créer une LIF \(interface réseau\)](#)".

#### Étapes

Vous pouvez configurer un gestionnaire de clés externe à partir de différents emplacements dans System Manager.

1. Pour configurer un gestionnaire de clés externe, effectuez l'une des étapes de démarrage suivantes.

| Flux de travail                                                                                       | Navigation                                           | Étape de départ                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configurer le gestionnaire de clés                                                                    | <b>Cluster &gt; Paramètres</b>                       | Accédez à la section <b>sécurité</b> . Sous <b>cryptage</b> , sélectionnez  . Sélectionnez <b>Gestionnaire de clés externe</b> .                 |
| Ajouter un niveau local                                                                               | <b>Stockage &gt; niveaux</b>                         | Sélectionnez <b>+ Ajouter un niveau local</b> . Cochez la case « configurer le gestionnaire de clés ». Sélectionnez <b>Gestionnaire de clés externe</b> .                                                                           |
| Préparez le stockage                                                                                  | <b>Tableau de bord</b>                               | Dans la section <b>capacité</b> , sélectionnez <b>préparer le stockage</b> . Sélectionnez ensuite « configurer le gestionnaire de clés ». Sélectionnez <b>Gestionnaire de clés externe</b> .                                        |
| Configuration du chiffrement (gestionnaire de clés dans le périmètre de la VM de stockage uniquement) | <b>Stockage &gt; machines virtuelles de stockage</b> | Sélectionnez la VM de stockage. Sélectionnez l'onglet <b>Paramètres</b> . Dans la section <b>cryptage</b> sous <b>sécurité</b> , sélectionnez  . |

2. Pour ajouter un serveur de clés principal, sélectionnez **+ Add** et renseignez les champs **adresse IP ou Nom d'hôte** et **Port**.
3. Les certificats installés existants sont répertoriés dans les champs **KMIP Server CA Certificates** et **KMIP client Certificate**. Vous pouvez effectuer l'une des actions suivantes :
  - Sélectionnez  cette option pour sélectionner les certificats installés que vous souhaitez mapper au gestionnaire de clés. (Plusieurs certificats d'autorité de certification de service peuvent être sélectionnés, mais un seul certificat client peut être sélectionné.)
  - Sélectionnez **Ajouter un nouveau certificat** pour ajouter un certificat qui n'a pas encore été installé et le mapper au gestionnaire de clés externe.
  - Sélectionnez **x** en regard du nom du certificat pour supprimer les certificats installés que vous ne souhaitez pas mapper au gestionnaire de clés externe.
4. Pour ajouter un serveur de clés secondaire, sélectionnez **Ajouter** dans la colonne **Secondary Key Servers** et fournissez ses détails.
5. Sélectionnez **Enregistrer** pour terminer la configuration.

## Modifier un gestionnaire de clés externe existant

Si vous avez déjà configuré un gestionnaire de clés externe, vous pouvez modifier ses paramètres.



### Étapes

1. Pour modifier la configuration d'un gestionnaire de clés externe, effectuez l'une des étapes de démarrage suivantes.

| Portée | Navigation | Étape de départ |
|--------|------------|-----------------|
|--------|------------|-----------------|

|                                                                            |                                                      |                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gestionnaire de clés externe de l'étendue du cluster                       | <b>Cluster &gt; Paramètres</b>                       | Accédez à la section <b>sécurité</b> . Sous <b>Encryption</b> , sélectionnez  , puis <b>Edit External Key Manager</b> .                                                                    |
| Périmètre de l'ordinateur virtuel de stockage gestionnaire de clés externe | <b>Stockage &gt; machines virtuelles de stockage</b> | Sélectionnez la VM de stockage. Sélectionnez l'onglet <b>Paramètres</b> . Dans la section <b>Encryption</b> sous <b>Security</b> , sélectionnez  , puis <b>Edit External Key Manager</b> . |

2. Les serveurs de clés existants sont répertoriés dans le tableau **Key Servers**. Vous pouvez effectuer les opérations suivantes :

- Ajoutez un nouveau serveur de clés en sélectionnant  **Add** .
- Supprimez un serveur de clés en sélectionnant  à la fin de la cellule de table contenant le nom du serveur de clés. Les serveurs de clés secondaires associés à ce serveur de clés principal sont également supprimés de la configuration.

## Supprimez un gestionnaire de clés externe

Un gestionnaire de clés externe peut être supprimé si les volumes sont non chiffrés.

### Étapes

1. Pour supprimer un gestionnaire de clés externe, effectuez l'une des opérations suivantes.

| Portée                                                                     | Navigation                                           | Étape de départ                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gestionnaire de clés externe de l'étendue du cluster                       | <b>Cluster &gt; Paramètres</b>                       | Accédez à la section <b>sécurité</b> . Sous <b>Encryption</b> , sélectionnez <b>SELECT</b>  , puis <b>Delete External Key Manager</b> .                                                      |
| Périmètre de l'ordinateur virtuel de stockage gestionnaire de clés externe | <b>Stockage &gt; machines virtuelles de stockage</b> | Sélectionnez la VM de stockage. Sélectionnez l'onglet <b>Paramètres</b> . Dans la section <b>Encryption</b> sous <b>Security</b> , sélectionnez  , puis <b>Delete External Key Manager</b> . |

## Migration des clés entre les gestionnaires de clés

Lorsque plusieurs gestionnaires de clés sont activés sur un cluster, les clés doivent être migrées d'un gestionnaire de clés vers un autre. System Manager effectue automatiquement ce processus.

- Si le gestionnaire de clés intégré ou un gestionnaire de clés externe est activé au niveau du cluster et que certains volumes sont chiffrés, Ensuite, lorsque vous configurez un gestionnaire de clés externe au niveau de la VM de stockage, les clés doivent être migrées du gestionnaire de clés intégré ou du gestionnaire de clés externe au niveau du cluster vers le gestionnaire de clés externe au niveau de la VM de stockage. System Manager effectue automatiquement ce processus.
- Si les volumes ont été créés sans chiffrement sur une machine virtuelle de stockage, les clés n'ont pas besoin d'être migrées.

## Installez les certificats SSL sur le cluster

Le cluster et le serveur KMIP utilisent des certificats SSL KMIP pour vérifier l'identité de l'autre et établir une connexion SSL. Avant de configurer la connexion SSL avec le serveur KMIP, vous devez installer les certificats SSL du client KMIP pour le cluster et le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP.

### Description de la tâche

Dans une paire haute disponibilité, les deux nœuds doivent utiliser les mêmes certificats SSL publics et privés KMIP. Si vous connectez plusieurs paires haute disponibilité au même serveur KMIP, tous les nœuds des paires haute disponibilité doivent utiliser les mêmes certificats SSL publics et privés.

### Avant de commencer

- L'heure doit être synchronisée sur le serveur qui crée les certificats, le serveur KMIP et le cluster.
- Vous devez avoir obtenu le certificat public du client SSL KMIP pour le cluster.
- Vous devez avoir obtenu la clé privée associée au certificat client SSL KMIP pour le cluster.
- Le certificat client SSL KMIP ne doit pas être protégé par un mot de passe.
- Vous devez avoir obtenu le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP.
- Dans un environnement MetroCluster, vous devez installer les mêmes certificats SSL KMIP sur les deux clusters.



Vous pouvez installer les certificats client et serveur sur le serveur KMIP avant ou après l'installation des certificats sur le cluster.

### Étapes

1. Installez les certificats client SSL KMIP pour le cluster :

```
security certificate install -vserver admin_svm_name -type client
```

Vous êtes invité à entrer les certificats SSL KMIP publics et privés.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Installez le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP :

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

### Gestion externe des clés dans ONTAP 9.6 et versions ultérieures (NVE)

Vous pouvez utiliser un ou plusieurs serveurs KMIP pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Depuis ONTAP 9.6, il est possible de configurer un gestionnaire de clés externe distinct pour sécuriser les clés utilisées par un SVM de données pour accéder aux données chiffrées.

À partir de ONTAP 9.11.1, vous pouvez ajouter jusqu'à 3 serveurs de clés secondaires par serveur de clés principal pour créer un serveur de clés en cluster. Pour plus d'informations, voir [Configurez les serveurs de clés externes en cluster](#).



## Description de la tâche

Vous pouvez connecter jusqu'à quatre serveurs KMIP à un cluster ou un SVM. Un minimum de deux serveurs est recommandé pour la redondance et la reprise après sinistre.

Le périmètre de la gestion externe des clés détermine si les serveurs de gestion des clés sécurisent tous les SVM dans le cluster ou bien uniquement les SVM sélectionnés :

- Vous pouvez utiliser une *cluster scope* pour configurer la gestion des clés externe pour tous les SVM du cluster. L'administrateur du cluster a accès à chaque clé stockée sur les serveurs.
- Depuis ONTAP 9.6, vous pouvez utiliser une *SVM scope* pour configurer la gestion externe des clés pour une SVM de données dans le cluster. C'est le mieux adapté aux environnements mutualisés dans lesquels chaque locataire utilise un autre SVM (ou ensemble de SVM) pour transmettre les données. Seul l'administrateur du SVM pour un locataire donné peut accéder aux clés pour ce locataire.
- Pour les environnements mutualisés, installez une licence pour *MT\_EK\_MGMT* à l'aide de la commande suivante :

```
system license add -license-code <MT_EK_MGMT license code>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page *man*.

Vous pouvez utiliser les deux étendues du même cluster. Si les serveurs de gestion des clés ont été configurés pour un SVM, ONTAP utilise uniquement ces serveurs pour sécuriser les clés. Sinon, ONTAP sécurise les clés avec les serveurs de gestion des clés configurés pour le cluster.

Vous pouvez configurer la gestion intégrée des clés au niveau du cluster et la gestion externe des clés au niveau de SVM. Vous pouvez utiliser le `security key-manager key migrate` Commande pour migrer les clés de la gestion intégrée des clés au périmètre du cluster vers des gestionnaires de clés externes au périmètre des SVM

## Avant de commencer

- Les certificats client SSL KMIP et serveur doivent avoir été installés.
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Si vous souhaitez activer la gestion externe des clés dans un environnement MetroCluster, MetroCluster doit être entièrement configuré avant d'activer la gestion externe des clés.
- Dans un environnement MetroCluster, vous devez installer le certificat SSL KMIP sur les deux clusters.

## Étapes

1. Configurer la connectivité du gestionnaire de clés pour le cluster :

```
security key-manager external enable -vserver admin_SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```



- Le `security key-manager external enable` la commande remplace le `security key-manager setup` commande. Si vous exécutez la commande à l'invite de connexion du cluster, *admin\_SVM* Par défaut au SVM admin du cluster actuel. Vous devez être l'administrateur du cluster pour configurer le périmètre du cluster. Vous pouvez exécuter le `security key-manager external modify` commande pour modifier la configuration de la gestion externe des clés.
- Dans un environnement MetroCluster, si vous configurez une gestion externe des clés pour le SVM admin, vous devez répéter l'opération `security key-manager external enable` commande sur le cluster partenaire.

La commande suivante active la gestion externe des clés pour `cluster1` avec trois serveurs de clés externes. Le premier serveur de clés est spécifié à l'aide de son nom d'hôte et de son port, le second est spécifié à l'aide d'une adresse IP et du port par défaut, et le troisième est spécifié à l'aide d'une adresse et d'un port IPv6 :

```
cluster1::> security key-manager external enable -vserver cluster1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

## 2. Configurer un SVM gestionnaire de clés :

```
security key-manager external enable -vserver SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```



- Si vous exécutez la commande à l'invite de connexion du SVM, *SVM* Par défaut au SVM actuel On doit être un administrateur de cluster ou de SVM pour configurer le cadre de la SVM. Vous pouvez exécuter le `security key-manager external modify` commande pour modifier la configuration de la gestion externe des clés.
- Dans un environnement MetroCluster, si vous configurez une gestion externe des clés pour une SVM de données, vous n'avez pas besoin de répéter le `security key-manager external enable` commande sur le cluster partenaire.

La commande suivante active la gestion externe des clés pour `svm1` avec un serveur à une seule clé qui écoute le port par défaut 5696 :

```
svm11::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

## 3. Répétez la dernière étape pour tout SVM supplémentaire.



Vous pouvez également utiliser le `security key-manager external add-servers` Commande permettant de configurer des SVM supplémentaires Le `security key-manager external add-servers` la commande remplace le `security key-manager add` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

#### 4. Vérifiez que tous les serveurs KMIP configurés sont connectés :

```
security key-manager external show-status -node node_name
```



Le `security key-manager external show-status` la commande remplace le `security key-manager show -status` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

```
cluster1::> security key-manager external show-status
```

| Node  | Vserver  | Key Server                                   | Status    |
|-------|----------|----------------------------------------------|-----------|
| ----- |          |                                              |           |
| node1 |          |                                              |           |
|       | svm1     | keyserver.svm1.com:5696                      | available |
|       | cluster1 | 10.0.0.10:5696                               | available |
|       |          | fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 | available |
|       |          | ks1.local:15696                              | available |
| node2 |          |                                              |           |
|       | svm1     | keyserver.svm1.com:5696                      | available |
|       | cluster1 | 10.0.0.10:5696                               | available |
|       |          | fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 | available |
|       |          | ks1.local:15696                              | available |

```
8 entries were displayed.
```

#### 5. Vous pouvez également convertir des volumes en texte brut en volumes chiffrés.

```
volume encryption conversion start
```

Un gestionnaire de clés externe doit être entièrement configuré avant la conversion des volumes. Dans un environnement MetroCluster, un gestionnaire de clés externe doit être configuré sur les deux sites.

### Activez la gestion externe des clés dans ONTAP 9.5 et versions antérieures

Vous pouvez utiliser un ou plusieurs serveurs KMIP pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous pouvez connecter jusqu'à quatre

serveurs KMIP à un nœud. Un minimum de deux serveurs est recommandé pour la redondance et la reprise après sinistre.

### Description de la tâche

ONTAP configure la connectivité du serveur KMIP pour tous les nœuds du cluster.

### Avant de commencer

- Les certificats client SSL KMIP et serveur doivent avoir été installés.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant de configurer un gestionnaire de clés externe.
- Dans un environnement MetroCluster, vous devez installer le certificat SSL KMIP sur les deux clusters.

### Étapes

1. Configurer la connectivité du gestionnaire de clés pour les nœuds du cluster :

```
security key-manager setup
```

La configuration du gestionnaire de clés démarre.



Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

2. Entrez la réponse appropriée à chaque invite.
3. Ajoutez un serveur KMIP :

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.1
```



Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

4. Ajoutez un serveur KMIP supplémentaire pour la redondance :

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.2
```



Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

5. Vérifiez que tous les serveurs KMIP configurés sont connectés :

```
security key-manager show -status
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> security key-manager show -status
```

| Node        | Port | Registered Key Manager | Status    |
|-------------|------|------------------------|-----------|
| -----       | ---- | -----                  | -----     |
| cluster1-01 | 5696 | 20.1.1.1               | available |
| cluster1-01 | 5696 | 20.1.1.2               | available |
| cluster1-02 | 5696 | 20.1.1.1               | available |
| cluster1-02 | 5696 | 20.1.1.2               | available |

6. Vous pouvez également convertir des volumes en texte brut en volumes chiffrés.

```
volume encryption conversion start
```

Un gestionnaire de clés externe doit être entièrement configuré avant la conversion des volumes. Dans un environnement MetroCluster, un gestionnaire de clés externe doit être configuré sur les deux sites.

### Gérer les clés avec un fournisseur cloud

À partir de ONTAP 9.10.1, vous pouvez l'utiliser ["Azure Key Vault \(AKV\)"](#) et ["Service de gestion des clés \(KMS cloud\) de Google Cloud Platform"](#) Pour protéger vos clés de chiffrement ONTAP dans une application hébergée dans le cloud. À partir de ONTAP 9.12.0, vous pouvez également protéger les clés NVE avec ["KMS D'AWS"](#).

Vous pouvez utiliser AWS KMS, AKV et Cloud KMS pour protéger les données ["Clés NetApp Volume Encryption \(NVE\)"](#) Uniquement pour les SVM de données.

### Description de la tâche

La gestion des clés avec un fournisseur cloud peut être activée via l'interface de ligne de commandes ou l'API REST ONTAP.

Lorsque vous utilisez un fournisseur cloud pour protéger vos clés, sachez que par défaut, une LIF de SVM de données communique avec le terminal de gestion des clés cloud. Un réseau de gestion de nœuds est utilisé pour communiquer avec les services d'authentification du fournisseur cloud (login.microsoftonline.com pour Azure ; oauth2.googleapis.com pour le Cloud KMS). Si le réseau de cluster n'est pas configuré correctement, le cluster n'utilisera pas correctement le service de gestion des clés.

Lorsque vous utilisez un service de gestion des clés de fournisseur cloud, vous devez connaître les limites suivantes :

- La gestion des clés du fournisseur cloud n'est pas disponible pour le chiffrement du stockage NetApp (NSE) et le chiffrement d'agrégat NetApp (NAE). ["KMIP externes"](#) peut être utilisé à la place.
- La gestion des clés du fournisseur cloud n'est pas disponible pour les configurations MetroCluster.
- La gestion des clés du fournisseur cloud peut uniquement être configurée sur un SVM de données.

### Avant de commencer

- Vous devez avoir configuré le KMS sur le fournisseur cloud approprié.
- Les nœuds du cluster ONTAP doivent prendre en charge NVE.
- ["Vous devez avoir installé les licences Volume Encryption \(VE\) et MTEKM \(Encryption Key Management\)"](#)

[multitenant](#)". Ces licences sont incluses avec "ONTAP One".

- Vous devez être administrateur du cluster ou du SVM.
- La SVM de données ne doit pas inclure de volumes chiffrés ni utiliser un gestionnaire de clés. Si le SVM de données inclut des volumes chiffrés, vous devez les migrer avant de configurer le KMS.

### **Activez la gestion externe des clés**

L'activation de la gestion externe des clés dépend du gestionnaire de clés que vous utilisez. Choisissez l'onglet du gestionnaire de clés et de l'environnement appropriés.

## AWS

### Avant de commencer

- Vous devez créer un octroi pour la clé KMS AWS qui sera utilisée par le rôle IAM gérant le chiffrement. Le rôle IAM doit inclure une politique permettant les opérations suivantes :
  - DescribeKey
  - Encrypt
  - Decrypt

Pour plus d'informations, consultez la documentation AWS pour "[subventions](#)".

### Activez AWS KMS sur un SVM ONTAP

1. Avant de commencer, procurez-vous l'ID de clé d'accès et la clé secrète sur votre serveur KMS AWS.
2. Définissez le niveau de privilège sur avancé :  
`set -priv advanced`
3. Activer AWS KMS :  
`security key-manager external aws enable -vserver svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. Lorsque vous y êtes invité, entrez la clé secrète.
5. Vérifiez que le KMS AWS a été correctement configuré :  
`security key-manager external aws show -vserver svm_name`

## Azure

### Activez Azure Key Vault sur un SVM ONTAP

1. Avant de commencer, vous devez obtenir les informations d'authentification appropriées à partir de votre compte Azure, soit un secret client, soit un certificat.  
Vous devez également vous assurer que tous les nœuds du cluster fonctionnent correctement. Vous pouvez le vérifier à l'aide de la commande `cluster show`.
2. Définissez le niveau privilégié sur avancé  
`set -priv advanced`
3. Activation de AKV sur le SVM  
`security key-manager external azure enable -client-id client_id -tenant-id tenant_id -name -key-id key_id -authentication-method {certificate|client-secret}`  
Lorsque vous y êtes invité, entrez le certificat client ou le secret client de votre compte Azure.
4. Vérifiez que la fonction AKV est activée correctement :  
`security key-manager external azure show vserver svm_name`  
Si l'accessibilité du service n'est pas OK, établir la connectivité au service de gestion des clés AKV via la LIF du SVM de données.

## Google Cloud

### Activez le serveur KMS cloud sur une SVM ONTAP

1. Avant de commencer, procurez-vous la clé privée du fichier de clé de compte Google Cloud KMS au format JSON. Elles sont disponibles dans votre compte GCP.  
Vous devez également vous assurer que tous les nœuds du cluster fonctionnent correctement. Vous pouvez le vérifier à l'aide de la commande `cluster show`.

2. Définir le niveau privilégié sur avancé :

```
set -priv advanced
```

3. Activation du KMS cloud sur le SVM

```
security key-manager external gcp enable -vserver svm_name -project-id
project_id-key-ring-name key_ring_name -key-ring-location key_ring_location
-key-name key_name
```

Lorsque vous y êtes invité, entrez le contenu du fichier JSON avec la clé privée du compte de service

4. Vérifiez que Cloud KMS est configuré avec les paramètres appropriés :

```
security key-manager external gcp show vservers svm_name
```

Le statut de `kms_wrapped_key_status` sera le cas "UNKNOWN" si aucun volume chiffré n'a été créé.

Si la accessibilité du service n'est pas satisfaisante, établissez la connectivité au service de gestion des clés GCP via LIF du SVM de données.

Si un ou plusieurs volumes chiffrés sont déjà configurés pour un SVM de données et que les clés NVE correspondantes sont gérées par le gestionnaire de clés intégré des SVM d'administration, ces clés doivent être migrées vers le service externe de gestion des clés. Pour ce faire via l'interface de ligne de commandes, lancer la commande :

```
security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM
```

Il n'est pas possible de créer de nouveaux volumes chiffrés pour le SVM de données du locataire tant que toutes les clés NVE du SVM de données ne sont pas migrées correctement.

### Informations associées

- ["Chiffrez les volumes avec les solutions de chiffrement NetApp pour Cloud Volumes ONTAP"](#)

### Intégrez la gestion des clés dans ONTAP 9.6 et versions ultérieures (NVE)

Vous pouvez utiliser le gestionnaire de clés intégré pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous devez activer le gestionnaire de clés intégré sur chaque cluster qui accède à un volume chiffré ou à un disque à chiffrement automatique.

### Description de la tâche

Vous devez exécuter le `security key-manager onboard sync` commande à chaque ajout d'un nœud au cluster.

Si vous avez une configuration MetroCluster, vous devez exécuter `security key-manager onboard enable` d'abord sur le cluster local, puis exécutez le `security key-manager onboard sync` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'entre eux. Lorsque vous exécutez le `security key-manager onboard enable` à partir du cluster local, puis effectuez une synchronisation sur le cluster distant. vous n'avez pas besoin d'exécuter le `enable` commandez à nouveau à partir du cluster distant.

Par défaut, vous n'êtes pas tenu de saisir la phrase de passe du gestionnaire de clés lors du redémarrage d'un nœud. Vous pouvez utiliser le `cc-mode-enabled=yes` option pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage.

Pour NVE, si vous définissez `cc-mode-enabled=yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées. Pour `volume create`, vous n'avez pas besoin de spécifier `-encrypt true`. Pour `volume move start`, vous n'avez pas besoin de spécifier



`-encrypt-destination true.`

Lors de la configuration du chiffrement des données ONTAP au repos, pour répondre aux exigences relatives aux solutions commerciales pour les données classées (CSfC), vous devez utiliser NSE avec NVE et vous assurer que le gestionnaire de clés intégré est activé en mode critères communs. Reportez-vous à la ["Description de la solution CSfC"](#) Pour en savoir plus sur CSfC.

Lorsque le gestionnaire de clés intégré est activé en mode critères communs (`cc-mode-enabled=yes`), le comportement du système est modifié de l'une des manières suivantes :

- Le système surveille les tentatives consécutives de mot de passe de cluster ayant échoué lorsqu'il fonctionne en mode critères communs.

Si vous ne saisissez pas la phrase secrète appropriée au démarrage, les volumes chiffrés ne sont pas montés. Pour corriger cette situation, vous devez redémarrer le nœud et saisir la phrase secrète correcte du cluster. Une fois démarré, le système peut saisir jusqu'à 5 tentatives consécutives de saisie de la phrase secrète du cluster dans une période de 24 heures pour toute commande nécessitant une phrase secrète comme paramètre. Si la limite est atteinte (par exemple, vous n'avez pas saisi correctement la phrase de passe du cluster 5 fois de suite) alors vous devez attendre l'expiration du délai de 24 heures ou redémarrer le nœud pour réinitialiser la limite.

- Les mises à jour d'images système utilisent le certificat de signature de code NetApp RSA-3072 avec des digests signés SHA-384 pour vérifier l'intégrité de l'image au lieu du certificat de signature de code RSA-2048 NetApp habituel et des digests signés par code SHA-256.

La commande de mise à niveau vérifie que le contenu de l'image n'a pas été modifié ou corrompu en vérifiant diverses signatures numériques. Le processus de mise à jour de l'image passe à l'étape suivante si la validation réussit ; sinon, la mise à jour de l'image échoue. Voir la `cluster image` pour plus d'informations sur les mises à jour système.

Le gestionnaire de clés intégré stocke les clés dans la mémoire volatile. Le contenu de la mémoire volatile est effacé lors du redémarrage ou de l'arrêt du système. Dans des conditions de fonctionnement normales, le contenu de la mémoire volatile est effacé dans les 30 secondes lorsqu'un système est arrêté.

### Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant de configurer le gestionnaire de clés intégré.

### Étapes

1. Lancez la configuration du gestionnaire de clés :

```
security key-manager onboard enable -cc-mode-enabled yes|no
```



Réglez `cc-mode-enabled=yes` pour demander aux utilisateurs de saisir la phrase de passe du gestionnaire de clés après un redémarrage. Pour NVE, si vous définissez `cc-mode-enabled=yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées. Le - `cc-mode-enabled` Cette option n'est pas prise en charge dans les configurations MetroCluster. Le `security key-manager onboard enable` la commande remplace le `security key-manager setup` commande.

L'exemple suivant démarre la commande Key Manager setup sur `cluster1` sans exiger la saisie de la phrase de passe après chaque redémarrage :

```
cluster1::> security key-manager onboard enable
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1":<32..256 ASCII characters long text>
Reenter the cluster-wide passphrase: <32..256 ASCII characters long
text>
```

2. À l'invite de phrase de passe, entrez une phrase de passe comprise entre 32 et 256 caractères, ou une phrase de passe entre 64 et 256 caractères pour « mode CC ».



Si la phrase de passe « CC-mode » spécifiée est inférieure à 64 caractères, il y a un délai de cinq secondes avant que l'opération de configuration du gestionnaire de clés n'affiche à nouveau l'invite de phrase de passe.

3. À l'invite de confirmation de la phrase de passe, saisissez à nouveau la phrase de passe.
4. Vérifiez que les clés d'authentification ont été créées :

```
security key-manager key query -key-type NSE-AK
```



Le `security key-manager key query` la commande remplace le `security key-manager query key` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant vérifie que les clés d'authentification ont été créées pour `cluster1`:

```
cluster1::> security key-manager key query -key-type NSE-AK
Node: node1
Vserver: cluster1
Key Manager: onboard
Key Manager Type: OKM
Key Manager Policy: -
```

| Key Tag                                                                                            | Key Type | Encryption | Restored |
|----------------------------------------------------------------------------------------------------|----------|------------|----------|
| node1                                                                                              | NSE-AK   | AES-256    | true     |
| Key ID:<br>00000000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000<br>00000000 |          |            |          |
| node1                                                                                              | NSE-AK   | AES-256    | true     |
| Key ID:<br>00000000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000<br>00000000 |          |            |          |

2 entries were displayed.

5. Vous pouvez également convertir des volumes en texte brut en volumes chiffrés.

```
volume encryption conversion start
```

Le gestionnaire de clés intégré doit être entièrement configuré avant de convertir les volumes. Dans un environnement MetroCluster, le gestionnaire de clés intégré doit être configuré sur les deux sites.

### Une fois que vous avez terminé

Copiez la phrase secrète dans un emplacement sécurisé à l'extérieur du système de stockage pour une utilisation ultérieure.

Chaque fois que vous configurez la phrase secrète Onboard Key Manager, vous devez également sauvegarder les informations manuellement dans un emplacement sécurisé en dehors du système de stockage afin de les utiliser en cas d'incident. Voir ["Sauvegardez manuellement les informations intégrées de gestion des clés"](#).

### Gestion intégrée des clés dans ONTAP 9.5 et versions antérieures (NVE)

Vous pouvez utiliser le gestionnaire de clés intégré pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous devez activer le gestionnaire de clés intégré sur chaque cluster qui accède à un volume chiffré ou à un disque auto-chiffré.

### Description de la tâche

Vous devez exécuter le `security key-manager setup` commande à chaque ajout d'un nœud au cluster.

Si vous disposez d'une configuration MetroCluster, consultez les consignes suivantes :

- Dans ONTAP 9.5, vous devez exécuter `security key-manager setup` sur le cluster local et `security key-manager setup -sync-metrocluster-config yes` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.
- Avant ONTAP 9.5, vous devez exécuter `security key-manager setup` sur le cluster local, attendez environ 20 secondes, puis exécutez `security key-manager setup` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.

Par défaut, vous n'êtes pas tenu de saisir la phrase de passe du gestionnaire de clés lors du redémarrage d'un nœud. À partir de ONTAP 9.4, vous pouvez utiliser le `-enable-cc-mode yes` option pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage.

Pour NVE, si vous définissez `-enable-cc-mode yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées. Pour `volume create`, vous n'avez pas besoin de spécifier `-encrypt true`. Pour `volume move start`, vous n'avez pas besoin de spécifier `-encrypt-destination true`.



Après une tentative de phrase de passe, vous devez redémarrer le nœud.

#### Avant de commencer

- Si vous utilisez NSE ou NVE avec un serveur de gestion externe des clés (KMIP), vous devez avoir supprimé la base de données du gestionnaire de clés externe.

["Transition vers la gestion intégrée des clés à partir d'une gestion externe des clés"](#)

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant de configurer le gestionnaire de clés intégré.

#### Étapes

1. Lancez la configuration du gestionnaire de clés :

```
security key-manager setup -enable-cc-mode yes|no
```



À partir de ONTAP 9.4, vous pouvez utiliser le `-enable-cc-mode yes` option permettant aux utilisateurs de saisir la phrase de passe du gestionnaire de clés après un redémarrage. Pour NVE, si vous définissez `-enable-cc-mode yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées.

L'exemple suivant commence à configurer le gestionnaire de clés sur le cluster 1 sans que la phrase de passe ne soit saisie après chaque redémarrage :

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase: <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase: <32..256 ASCII characters long
text>
```

2. Entrez `yes` à l'invite, configurez la gestion intégrée des clés.
3. À l'invite de phrase de passe, entrez une phrase de passe comprise entre 32 et 256 caractères, ou une phrase de passe entre 64 et 256 caractères pour « mode CC ».



Si la phrase de passe « CC-mode » spécifiée est inférieure à 64 caractères, il y a un délai de cinq secondes avant que l'opération de configuration du gestionnaire de clés n'affiche à nouveau l'invite de phrase de passe.

4. À l'invite de confirmation de la phrase de passe, saisissez à nouveau la phrase de passe.
5. Vérifier que les clés sont configurées pour tous les nœuds :

```
security key-manager key show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID Used By

0000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID Used By

0000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

6. Vous pouvez également convertir des volumes en texte brut en volumes chiffrés.

```
volume encryption conversion start
```

Le gestionnaire de clés intégré doit être entièrement configuré avant de convertir les volumes. Dans un environnement MetroCluster, le gestionnaire de clés intégré doit être configuré sur les deux sites.

### Une fois que vous avez terminé

Copiez la phrase secrète dans un emplacement sécurisé à l'extérieur du système de stockage pour une utilisation ultérieure.

Chaque fois que vous configurez la phrase secrète Onboard Key Manager, vous devez également sauvegarder les informations manuellement dans un emplacement sécurisé en dehors du système de stockage afin de les utiliser en cas d'incident. Voir ["Sauvegardez manuellement les informations intégrées de gestion des clés"](#).

### Activez la gestion intégrée des clés dans les nouveaux nœuds ajoutés

Vous pouvez utiliser le gestionnaire de clés intégré pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous devez activer le gestionnaire de clés intégré sur chaque cluster qui accède à un volume chiffré ou à un disque auto-chiffré.



Pour ONTAP 9.5 et les versions antérieures, vous devez exécuter le `security key-manager setup` commande à chaque ajout d'un nœud au cluster.

Pour ONTAP 9.6 et versions ultérieures, vous devez exécuter le `security key-manager sync` commande à chaque ajout d'un nœud au cluster.

Si vous ajoutez un nœud à un cluster dont la gestion intégrée des clés est configurée, vous exécutez cette commande pour actualiser les clés manquantes.

Si vous disposez d'une configuration MetroCluster, consultez les consignes suivantes :

- Avec ONTAP 9.6, vous devez exécuter `security key-manager onboard enable` sur le cluster local, puis s'exécute `security key-manager onboard sync` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.
- Dans ONTAP 9.5, vous devez exécuter `security key-manager setup` sur le cluster local et `security key-manager setup -sync-metrocluster-config yes` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.
- Avant ONTAP 9.5, vous devez exécuter `security key-manager setup` sur le cluster local, attendez environ 20 secondes, puis exécutez `security key-manager setup` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.

Par défaut, vous n'êtes pas tenu de saisir la phrase de passe du gestionnaire de clés lors du redémarrage d'un nœud. À partir de ONTAP 9.4, vous pouvez utiliser le `-enable-cc-mode yes` option pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage.

Pour NVE, si vous définissez `-enable-cc-mode yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées. Pour `volume create`, vous n'avez pas besoin de spécifier `-encrypt true`. Pour `volume move start`, vous n'avez pas besoin de spécifier `-encrypt-destination true`.



Après une tentative de phrase de passe, vous devez redémarrer le nœud.

## Chiffrement des données de volume avec NVE

### Chiffrement des données de volume avec NVE

Depuis ONTAP 9.7, le chiffrement de l'agrégat et du volume est activé par défaut lorsque vous disposez de la licence VE et de la gestion intégrée ou externe des clés. Pour ONTAP 9.6 et version antérieure, vous pouvez activer le chiffrement sur un nouveau volume ou sur un volume existant. Vous devez avoir installé la licence VE et activé la gestion des clés avant de pouvoir activer le chiffrement de volume. NVE est conforme à la norme FIPS-140-2 de niveau 1.

### Chiffrement au niveau de l'agrégat avec licence VE

Depuis la version ONTAP 9.7, les agrégats et volumes nouvellement créés sont chiffrés par défaut lorsque vous disposez de "[Licence VE](#)" et de la gestion des clés intégrée ou externe. Depuis ONTAP 9.6, vous pouvez utiliser le chiffrement au niveau de l'agrégat pour attribuer des clés à l'agrégat contenant afin de chiffrer les volumes.

### Description de la tâche

Vous devez utiliser le chiffrement au niveau de l'agrégat pour procéder à la déduplication à la volée ou en arrière-plan au niveau de l'agrégat. NVE ne prend cependant pas en charge la déduplication au niveau de l'agrégat.

Un agrégat activé pour le chiffrement au niveau de l'agrégat est appelé agrégat NAE (pour le chiffrement d'agrégat NetApp). Tous les volumes d'un agrégat NAE doivent être chiffrés avec un chiffrement NAE ou NVE. Grâce au chiffrement au niveau des agrégats, les volumes que vous créez dans l'agrégat sont chiffrés avec un chiffrement NAE par défaut. Vous pouvez remplacer le par défaut pour utiliser le chiffrement NVE.

Les volumes en texte brut ne sont pas pris en charge dans les agrégats NAE.

### Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

### Étapes

1. Activer ou désactiver le chiffrement au niveau des agrégats :

| Pour...                                                   | Utilisez cette commande...                                                                                         |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Créez un agrégat NAE avec ONTAP 9.7 ou version ultérieure | <pre>storage aggregate create -aggregate<br/>aggregate_name -node node_name</pre>                                  |
| Créez un agrégat NAE avec ONTAP 9.6                       | <pre>storage aggregate create -aggregate<br/>aggregate_name -node node_name -encrypt-with<br/>-aggr-key true</pre> |

|                                                |                                                                                                                             |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Conversion d'un agrégat non-NAE en agrégat NAE | <code>storage aggregate modify -aggregate <i>aggregate_name</i> -node <i>node_name</i> -encrypt-with -aggr-key true</code>  |
| Conversion d'un agrégat NAE en agrégat non-NAE | <code>storage aggregate modify -aggregate <i>aggregate_name</i> -node <i>node_name</i> -encrypt-with -aggr-key false</code> |

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

La commande suivante active le chiffrement au niveau de l'agrégat sur `aggr1`:

- ONTAP 9.7 ou version ultérieure :

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 ou version antérieure :

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

## 2. Vérifier que l'agrégat est activé pour le chiffrement :

```
storage aggregate show -fields encrypt-with-aggr-key
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

La commande suivante vérifie que `aggr1` est activé pour le chiffrement :

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate encrypt-aggr-key

aggr0_vsim4 false
aggr1 true
2 entries were displayed.
```

## Une fois que vous avez terminé

Exécutez le `volume create` commande permettant de créer les volumes chiffrés.

Si vous utilisez un serveur KMIP pour stocker les clés de cryptage d'un nœud, ONTAP « transfère » automatiquement une clé de cryptage vers le serveur lorsque vous chiffrez un volume.

## Activer le chiffrement sur un nouveau volume

Vous pouvez utiliser le `volume create` commande permettant d'activer le chiffrement



sur un nouveau volume.

### Description de la tâche

Vous pouvez chiffrer les volumes à l'aide de NetApp Volume Encryption (NVE) et, à partir de ONTAP 9.6, NetApp Aggregate Encryption (NAE). Pour en savoir plus sur NAE et NVE, consultez le [présentation du chiffrement de volume](#).

La procédure d'activation du chiffrement sur un nouveau volume dans ONTAP varie en fonction de la version de ONTAP que vous utilisez et de votre configuration spécifique :


- À partir de ONTAP 9.4, si vous l'activez `cc-mode` Lorsque vous configurez le gestionnaire de clés intégré, les volumes que vous créez avec le `volume create` la commande est automatiquement chiffrée, que vous spécifiez ou non `-encrypt true`.
- Dans ONTAP 9.6 et les versions antérieures, vous devez utiliser `-encrypt true` avec `volume create` commandes permettant d'activer le chiffrement (à condition que vous n'ayez pas activé `cc-mode`).
- Si vous voulez créer un volume NAE dans ONTAP 9.6, vous devez activer NAE au niveau des agrégats. Reportez-vous à la section [Activation du chiffrement au niveau de l'agrégat avec la licence VE](#) pour plus de détails sur cette tâche.
- Depuis la version ONTAP 9.7, les nouveaux volumes créés sont chiffrés par défaut lorsque vous disposez de "Licence VE" et de la gestion des clés intégrée ou externe. Par défaut, les nouveaux volumes créés dans un agrégat NAE seront de type NAE plutôt que NVE.
  - Dans ONTAP 9.7 et versions ultérieures, si vous ajoutez `-encrypt true` à la `volume create` Commande de création d'un volume dans un agrégat NAE, au lieu de NAE pour le volume le chiffrement NVE. Tous les volumes d'un agrégat NAE doivent être chiffrés avec NVE ou NAE.



Les volumes en texte brut ne sont pas pris en charge dans les agrégats NAE.

### Étapes

1. Créez un nouveau volume et spécifiez si le chiffrement est activé sur le volume. Si le nouveau volume se trouve dans un agrégat NAE, le volume en est par défaut un volume NAE :

| Pour créer...        | Utilisez cette commande...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Volume NAE           | <pre>volume create -vserver SVM_name -volume volume_name<br/>-aggregate aggregate_name</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Un volume NVE        | <pre>volume create -vserver SVM_name -volume volume_name<br/>-aggregate aggregate_name -encrypt true +</pre> <div><p>Dans les versions ONTAP 9.6 et antérieures, où NAE n'est pas pris en charge, <code>-encrypt true</code> Spécifie que le volume doit être chiffré avec NVE. Dans ONTAP 9.7 et versions ultérieures, où les volumes sont créés dans des agrégats NAE, <code>-encrypt true</code> Remplace le type de chiffrement par défaut de NAE pour créer un volume NVE.</p></div> |
| Volume de texte brut | <pre>volume create -vserver SVM_name -volume volume_name<br/>-aggregate aggregate_name -encrypt false</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

Pour obtenir la syntaxe complète de la commande, reportez-vous à la page de référence de la commande `LINK:https://docs.netapp.com/us-en/ontap-cli/volume-create.html[volume create^]`.

## 2. Vérifiez que les volumes sont activés pour le chiffrement :

```
volume show -is-encrypted true
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["Référence de commande ONTAP"](#).

### Résultat

Si vous utilisez un serveur KMIP pour stocker les clés de chiffrement d'un nœud, ONTAP « transmet automatiquement » une clé de chiffrement au serveur lorsque vous chiffrez un volume.

```
=
:allow-uri-read:
```

### Activez le chiffrement sur un volume existant

Vous pouvez utiliser le `volume move start` ou le `volume encryption conversion start` commande permettant d'activer le chiffrement sur un volume existant.

### Description de la tâche

- Vous pouvez utiliser ONTAP 9.3 à partir de `volume encryption conversion start` commande permettant de chiffrer un volume existant « à la place », sans avoir à déplacer le volume vers un autre emplacement. Vous pouvez également utiliser le `volume move start` commande.
- Pour ONTAP 9.2 et les versions antérieures, vous pouvez utiliser uniquement le `volume move start` commande permettant d'activer le chiffrement en déplaçant un volume existant.

### Activez le chiffrement sur un volume existant à l'aide de la commande `Volume Encryption conversion start`

Vous pouvez utiliser ONTAP 9.3 à partir de `volume encryption conversion start` commande permettant de chiffrer un volume existant « à la place », sans avoir à déplacer le volume vers un autre emplacement.

Une fois que vous avez lancé une opération de conversion, elle doit être terminée. Si vous rencontrez un problème de performances pendant l'opération, vous pouvez exécuter le `volume encryption conversion pause` commande pour mettre l'opération en pause, et le `volume encryption conversion resume` commande pour reprendre l'opération.



Vous ne pouvez pas utiliser `volume encryption conversion start` Pour convertir un volume SnapLock.

### Étapes

#### 1. Activer le chiffrement sur un volume existant :

```
volume encryption conversion start -vserver SVM_name -volume volume_name
```

Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

La commande suivante active le chiffrement sur un volume existant `vol1`:

```
cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
```

Le système crée une clé de chiffrement pour le volume. Les données du volume sont chiffrées.

2. Vérifiez l'état de l'opération de conversion :

```
volume encryption conversion show
```

Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

La commande suivante affiche le statut de l'opération de conversion :

```
cluster1::> volume encryption conversion show
```

| Vserver | Volume | Start Time         | Status                       |
|---------|--------|--------------------|------------------------------|
| -----   | -----  | -----              | -----                        |
| vs1     | vol1   | 9/18/2017 17:51:41 | Phase 2 of 2 is in progress. |

3. Une fois l'opération de conversion terminée, vérifiez que le volume est activé pour le chiffrement :

```
volume show -is-encrypted true
```

Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

La commande suivante affiche les volumes chiffrés sur `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State  | Type  | Size  | Available | Used  |
|---------|--------|-----------|--------|-------|-------|-----------|-------|
| -----   | -----  | -----     | -----  | ----- | ----- | -----     | ----- |
| vs1     | vol1   | aggr2     | online | RW    | 200GB | 160.0GB   | 20%   |

## Résultat

Si vous utilisez un serveur KMIP pour stocker les clés de cryptage d'un nœud, ONTAP « transfère » automatiquement une clé de cryptage vers le serveur lorsque vous chiffrez un volume.

## Activez le chiffrement sur un volume existant à l'aide de la commande `volume Move start`

Vous pouvez utiliser le `volume move start` commande permettant d'activer le chiffrement en déplaçant un volume existant. Vous devez utiliser `volume move start` Dans ONTAP 9.2 et versions antérieures. Vous pouvez utiliser le même agrégat ou un autre agrégat.

## Description de la tâche

- Vous pouvez utiliser ONTAP 9.8 depuis `volume move start` Pour activer le chiffrement sur un volume

SnapLock ou FlexGroup.

- Depuis ONTAP 9.4, si vous activez « cc-mode » lors de la configuration du gestionnaire de clés intégré, les volumes que vous créez avec le système `volume move start` la commande est automatiquement chiffrée. Vous n'avez pas besoin de spécifier `-encrypt-destination true`.
- Depuis ONTAP 9.6, il est possible d'utiliser le chiffrement au niveau de l'agrégat pour attribuer des clés à l'agrégat contenant afin de déplacer les volumes. Un volume chiffré avec une clé unique est appelé *volume NVE* (ce qui signifie qu'il utilise le chiffrement de volume NetApp). Un volume chiffré avec une clé au niveau de l'agrégat est appelé un volume NAE\_ (pour le chiffrement d'agrégat NetApp). Les volumes en texte brut ne sont pas pris en charge dans les agrégats NAE.
- À partir de ONTAP 9.14.1, vous pouvez chiffrer un volume root SVM avec NVE. Pour plus d'informations, voir [Configurer le chiffrement de volume NetApp sur un volume root SVM](#).

## Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche, ou un administrateur de SVM à qui l'administrateur du cluster a délégué des pouvoirs.

## "Délégation d'autorité pour exécuter la commande de déplacement de volume"

### Étapes

1. Déplacez un volume existant et spécifiez si le chiffrement est activé sur le volume :

| Pour convertir...                                                                                                                         | Utilisez cette commande...                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Volume en texte brut vers un volume NVE                                                                                                   | <code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true</code>                               |
| Un volume NVE ou en texte clair vers un volume NAE (en supposant que le chiffrement au niveau de l'agrégat est activé sur la destination) | <code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true</code>                             |
| Un volume NAE vers un volume NVE                                                                                                          | <code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false</code>                            |
| Volume NAE en volume en texte brut                                                                                                        | <code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false</code> |
| Un volume NVE vers un volume en texte brut                                                                                                | <code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false</code>                              |

Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

La commande suivante convertit un volume en texte brut nommé `vol1` Vers un volume NVE :

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

En supposant que le chiffrement au niveau de l'agrégat soit activé sur la destination, la commande suivante convertit un volume NVE ou en texte brut nommé `vol1` Pour un volume NAE :

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

La commande suivante convertit un volume NAE nommé `vol2` Vers un volume NVE :

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

La commande suivante convertit un volume NAE nommé `vol2` vers un volume en texte clair :

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

La commande suivante convertit un volume NVE nommé `vol2` vers un volume en texte clair :

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

## 2. Afficher le type de chiffrement des volumes du cluster :

```
volume show -fields encryption-type none|volume|aggregate
```

Le `encryption-type` Ce champ est disponible dans ONTAP 9.6 et versions ultérieures.

Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

La commande suivante affiche le type de cryptage des volumes dans `cluster2`:

```
cluster2::> volume show -fields encryption-type

vserver volume encryption-type
----- -
vs1 vol1 none
vs2 vol2 volume
vs3 vol3 aggregate
```

### 3. Vérifiez que les volumes sont activés pour le chiffrement :

```
volume show -is-encrypted true
```

Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

La commande suivante affiche les volumes chiffrés sur `cluster2`:

```
cluster2::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State  | Type  | Size  | Available | Used  |
|---------|--------|-----------|--------|-------|-------|-----------|-------|
| -----   | -----  | -----     | -----  | ----- | ----- | -----     | ----- |
| vs1     | vol1   | aggr2     | online | RW    | 200GB | 160.0GB   | 20%   |

#### Résultat

Si vous utilisez un serveur KMIP pour stocker les clés de chiffrement d'un nœud, ONTAP transmet automatiquement une clé de chiffrement au serveur lorsque vous chiffrez un volume.

#### Configurer le chiffrement de volume NetApp sur un volume root SVM

À partir de la version ONTAP 9.14.1, vous pouvez activer NetApp Volume Encryption (NVE) sur un volume racine de machine virtuelle de stockage (SVM). Avec NVE, le volume racine est chiffré avec une clé unique, pour renforcer la sécurité au niveau du SVM.

#### Description de la tâche

NVE sur un volume root SVM ne peut être activé qu'une fois le SVM créé.

#### Avant de commencer

- Le volume racine du SVM ne doit pas se trouver sur un agrégat chiffré avec le chiffrement d'agrégat NetApp (NAE).
- Vous devez avoir activé le chiffrement avec Onboard Key Manager ou un gestionnaire de clés externe.
- Vous devez exécuter ONTAP 9.14.1 ou une version ultérieure.
- Pour migrer un SVM contenant un volume racine chiffré avec NVE, vous devez convertir le volume racine du SVM en volume texte brut une fois la migration terminée, puis re-chiffrer le volume racine du SVM.
  - Si l'agrégat de destination de la migration du SVM utilise NAE, le volume racine hérite de NAE par défaut.
- Si la SVM est dans une relation de SVM DR :
  - Les paramètres de chiffrement d'un SVM en miroir ne sont pas copiés vers la destination. Si vous activez NVE sur la source ou la destination, vous devez activer NVE séparément sur le volume racine du SVM en miroir.
  - Si tous les agrégats du cluster de destination utilisent NAE, le volume racine du SVM utilisera NAE.

#### Étapes

Vous pouvez activer NVE sur un volume root SVM via l'interface de ligne de commandes ONTAP ou System Manager.

## CLI

Vous pouvez activer NVE sur le volume racine du SVM sans déplacement ou en déplaçant le volume entre les agrégats.

### Chiffrez le volume racine sur place

1. Convertir le volume root en volume chiffré :

```
volume encryption conversion start -vserver svm_name -volume volume
```

2. Confirmez que le chiffrement a réussi. Le `volume show -encryption-type volume` Affiche la liste de tous les volumes qui utilisent NVE.

### Chiffrer le volume root du SVM en le déplaçant


1. Lancer un déplacement de volume :

```
volume move start -vserver svm_name -volume volume -destination-aggregate aggregate -encrypt-with-aggr-key false -encrypt-destination true
```

Pour plus d'informations sur `volume move`, voir [Déplacer un volume](#).

2. Confirmez le `volume move` l'opération a réussi avec le `volume move show` commande. Le `volume show -encryption-type volume` Affiche la liste de tous les volumes qui utilisent NVE.

## System Manager

1. Accédez à **stockage > volumes**.
2. À côté du nom du volume root du SVM à crypter, sélectionner  puis **Edit**.
3. Sous l'en-tête **stockage et optimisation**, sélectionnez **Activer le cryptage**.
4. Sélectionnez **Enregistrer**.

### Activer le chiffrement de volume racine de nœud

Depuis ONTAP 9.8, vous pouvez utiliser NetApp Volume Encryption pour protéger le volume racine de votre nœud.



#### Description de la tâche

Cette procédure s'applique au volume racine du nœud. Elle ne s'applique pas aux volumes root du SVM. Les volumes root des SVM peuvent être protégés via le chiffrement au niveau des agrégats et [À partir de ONTAP 9.14.1, NVE](#).

Une fois le chiffrement du volume racine démarré, il doit être terminé. Vous ne pouvez pas interrompre l'opération. Une fois le cryptage terminé, vous ne pouvez pas attribuer de nouvelle clé au volume racine et vous ne pouvez pas effectuer de suppression sécurisée.

### Avant de commencer

- Votre système doit utiliser une configuration haute disponibilité.
- Le volume racine du nœud doit déjà être créé.
- Votre système doit disposer d'un gestionnaire de clés intégré ou d'un serveur de gestion des clés externe à l'aide du protocole KMIP (Key Management Interoperability Protocol).

## Étapes

1. Chiffrer le volume root :

```
volume encryption conversion start -vserver SVM_name -volume root_vol_name
```

2. Vérifiez l'état de l'opération de conversion :

```
volume encryption conversion show
```

3. Une fois l'opération de conversion terminée, vérifiez que le volume est crypté :

```
volume show -fields
```

Voici un exemple de sortie pour un volume chiffré.

```
::> volume show -vserver xyz -volume vol0 -fields is-encrypted
vserver volume is-encrypted

xyz vol0 true
```

## Configuration du chiffrement matériel NetApp

### Configuration de la présentation de NetApp Hardware-based Encryption

Le chiffrement matériel NetApp prend en charge le chiffrement de disque intégral (FDE) des données au fur et à mesure de leur écriture. Les données ne peuvent pas être lues si une clé de chiffrement est stockée sur le micrologiciel. La clé de chiffrement, à son tour, n'est accessible qu'à un nœud authentifié.

### Présentation du cryptage matériel NetApp

Un nœud s'authentifie auprès d'un disque auto-chiffré à l'aide d'une clé d'authentification extraite d'un serveur de gestion externe des clés ou d'un gestionnaire de clés intégré :

- Le serveur externe de gestion des clés est un système tiers de votre environnement de stockage qui transmet des clés aux nœuds à l'aide du protocole KMIP (Key Management Interoperability Protocol). Il est recommandé de configurer des serveurs de gestion externe des clés sur un système de stockage différent de vos données.
- Le gestionnaire de clés intégré est un outil intégré qui sert des clés d'authentification aux nœuds du même système de stockage que vos données.

Vous pouvez utiliser NetApp Volume Encryption avec chiffrement matériel pour « paramétrer la fonctionnalité de chiffrement » des données sur des disques à autochiffrement.

Lorsque les disques à chiffrement automatique sont activés, le « core dump » est également chiffré.





Si une paire haute disponibilité utilise des disques avec cryptage SAS ou NVMe (SED, NSE, FIPS), vous devez suivre les instructions de la rubrique [Retour d'un lecteur FIPS ou SED en mode non protégé](#) Pour tous les disques de la paire HA avant d'initialiser le système (options de démarrage 4 ou 9). Si vous ne le faites pas, vous risquez de subir des pertes de données si les disques sont requalifiés.

### Types de disques à autocryptage pris en charge

Deux types de disques à autocryptage sont pris en charge :

- Tous les systèmes FAS et AFF prennent en charge les disques SAS ou NVMe certifiés FIPS avec le chiffrement automatique. Ces unités, appelées unités *FIPS*, sont conformes aux exigences de la publication 140-2 de la norme fédérale de traitement des informations, niveau 2. Les fonctionnalités certifiées permettent d'ajouter des protections au chiffrement, comme la prévention d'attaques par déni de service sur le disque. Les disques FIPS ne peuvent pas être combinés avec d'autres types de disques sur le même nœud ou la même paire HA.
- Depuis ONTAP 9.6, les disques NVMe à autocryptage n'ayant pas encore été testés FIPS sont pris en charge sur des systèmes AFF A800, A320 et versions ultérieures. Ces disques, appelés *SED*, offrent les mêmes fonctionnalités de cryptage que les disques FIPS, mais peuvent être combinés avec des disques sans cryptage sur un même nœud ou une paire haute disponibilité.
- Tous les disques validés FIPS utilisent un module cryptographique de firmware qui a été validé par FIPS. Le module cryptographique du lecteur FIPS n'utilise aucune clé générée en dehors du disque (la phrase de passe d'authentification entrée dans le lecteur est utilisée par le module cryptographique du firmware du disque pour obtenir une clé de chiffrement).



Les disques sans chiffrement sont des disques qui ne sont pas des disques SED ou FIPS.



Si vous utilisez NSE sur un système doté d'un module Flash cache, vous devez également activer NVE ou NAE. NSE ne chiffre pas les données qui résident sur le module Flash cache.

### Quand utiliser la gestion externe des clés

Le gestionnaire de clés intégré est moins coûteux et généralement plus pratique, mais vous devez utiliser une gestion externe des clés si l'un des éléments suivants est vrai :

- La stratégie de votre entreprise nécessite une solution de gestion des clés qui utilise un module cryptographique FIPS 140-2 de niveau 2 (ou supérieur).
- Vous avez besoin d'une solution à plusieurs clusters et d'une gestion centralisée des clés de chiffrement.
- Votre entreprise exige que les clés d'authentification soient sécurisées sur un système ou à un emplacement différent de celui des données.

### Détails du support

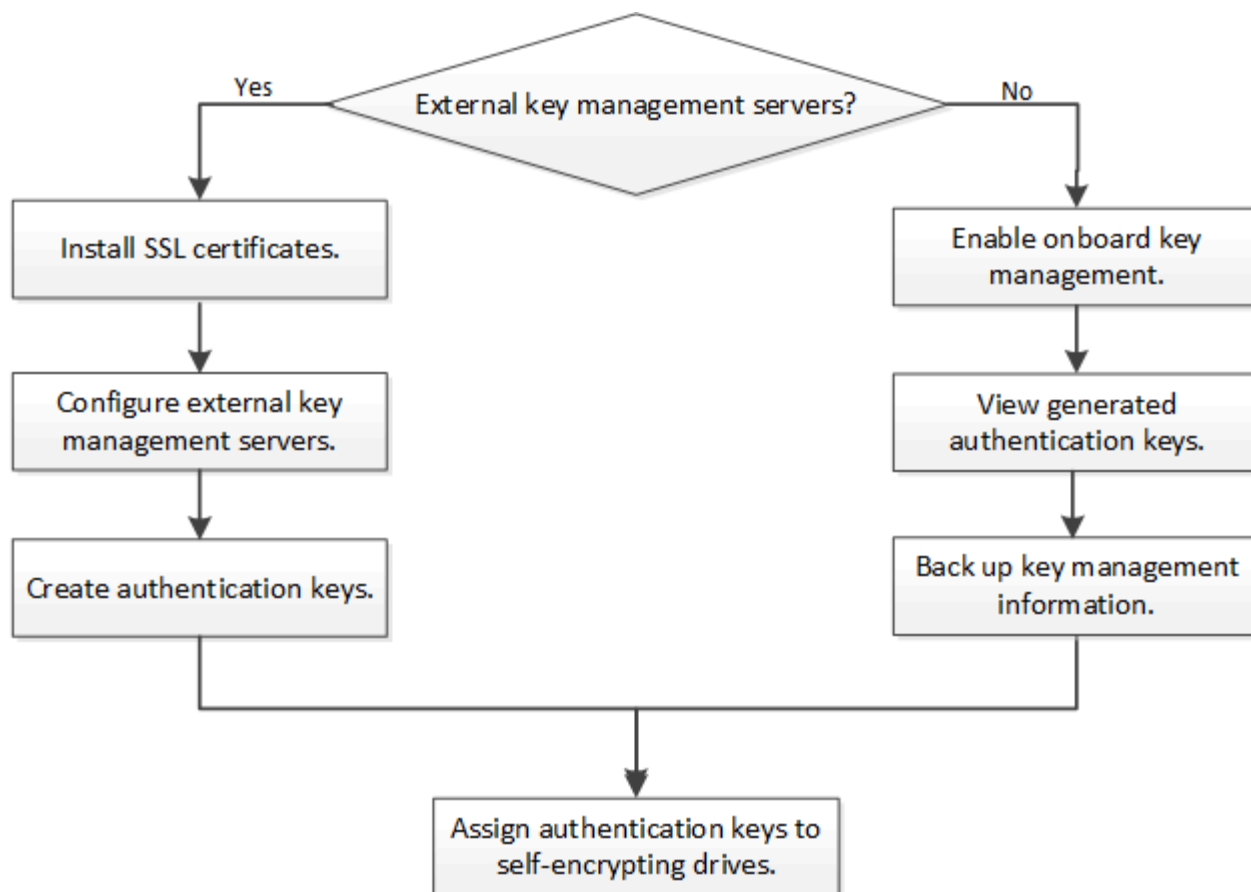
Le tableau suivant présente des détails importants sur la prise en charge du chiffrement matériel. Consultez la matrice d'interopérabilité pour obtenir les dernières informations sur les serveurs, les systèmes de stockage et les tiroirs disques KMIP pris en charge.

| Ressource ou fonctionnalité | Détails du support |
|-----------------------------|--------------------|
|-----------------------------|--------------------|

|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jeux de disques non homogènes                              | <ul style="list-style-type: none"> <li>• Les disques FIPS ne peuvent pas être combinés avec d'autres types de disques sur le même nœud ou la même paire HA. Les paires haute disponibilité conformes peuvent coexister avec des paires haute disponibilité non conformes dans le même cluster.</li> <li>• Les disques SED peuvent être combinés avec des disques sans cryptage sur un même nœud ou une même paire haute disponibilité.</li> </ul>                        |
| Type de disque                                             | <ul style="list-style-type: none"> <li>• Les disques FIPS peuvent être des disques SAS ou NVMe.</li> <li>• Les disques SED doivent être des disques NVMe.</li> </ul>                                                                                                                                                                                                                                                                                                     |
| Interfaces réseau de 10 Go                                 | Depuis ONTAP 9.3, les configurations de gestion des clés KMIP prennent en charge des interfaces réseau de 10 Gbit pour les communications avec des serveurs de gestion des clés externes.                                                                                                                                                                                                                                                                                |
| Ports de communication avec le serveur de gestion des clés | Depuis ONTAP 9.3, vous pouvez utiliser n'importe quel port du contrôleur de stockage pour la communication avec le serveur de gestion des clés. Dans le cas contraire, vous devez utiliser le port e0M pour la communication avec les serveurs de gestion des clés. Selon le modèle du contrôleur de stockage, certaines interfaces réseau peuvent ne pas être disponibles durant le processus de démarrage pour la communication avec les serveurs de gestion des clés. |
| MetroCluster (MCC)                                         | <ul style="list-style-type: none"> <li>• Les disques NVMe prennent en charge MCC.</li> <li>• Les disques SAS ne prennent pas en charge MCC.</li> </ul>                                                                                                                                                                                                                                                                                                                   |

#### Flux de production de cryptage matériel

Vous devez configurer les services de gestion des clés pour que le cluster puisse s'authentifier sur le disque auto-chiffré. Vous pouvez utiliser un serveur de gestion externe des clés ou un gestionnaire de clés intégré.



#### Informations associées

- ["NetApp Hardware Universe"](#)
- ["NetApp Volume Encryption et chiffrement d'agrégat NetApp"](#)

### Configurez la gestion externe des clés

#### Configurer la gestion externe des clés en vue d'ensemble

Vous pouvez utiliser un ou plusieurs serveurs externes de gestion des clés pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Un serveur externe de gestion des clés est un système tiers de votre environnement de stockage qui transmet des clés aux nœuds à l'aide du protocole KMIP (Key Management Interoperability Protocol).

Pour ONTAP 9.1 et les versions antérieures, les LIFs de node-management doivent être attribuées à des ports configurés avec le rôle de node-management avant de pouvoir utiliser le gestionnaire de clés externe.

NetApp Volume Encryption (NVE) peut être implémenté avec le gestionnaire de clés intégré dans ONTAP 9.1 et les versions ultérieures. Dans ONTAP 9.3 et versions ultérieures, NVE peut être implémenté avec une gestion des clés externe (KMIP) et un gestionnaire de clés intégré. À partir de ONTAP 9.11.1, vous pouvez configurer plusieurs gestionnaires de clés externes dans un cluster. Voir [Configurez les serveurs de clés en cluster](#).

Si vous utilisez ONTAP 9.2 ou une version antérieure, vous devez remplir la fiche de configuration du réseau avant d'activer la gestion externe des clés.



Depuis ONTAP 9.3, le système détecte automatiquement toutes les informations réseau nécessaires.

| Élément                                                            | Remarques                                                                                                                                                                                                                             | Valeur |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| Nom de l'interface réseau de gestion des clés                      |                                                                                                                                                                                                                                       |        |
| Adresse IP de l'interface réseau de gestion des clés               | Adresse IP de la LIF de node management, au format IPv4 ou IPv6                                                                                                                                                                       |        |
| Longueur du préfixe réseau IPv6 de gestion des clés                | Si vous utilisez IPv6, la longueur du préfixe réseau IPv6                                                                                                                                                                             |        |
| Masque de sous-réseau de l'interface réseau de gestion des clés    |                                                                                                                                                                                                                                       |        |
| Adresse IP de la passerelle d'interface réseau de gestion des clés |                                                                                                                                                                                                                                       |        |
| Adresse IPv6 pour l'interface réseau du cluster                    | Requis uniquement si vous utilisez IPv6 pour l'interface réseau de gestion des clés                                                                                                                                                   |        |
| Numéro de port pour chaque serveur KMIP                            | Facultatif. Le numéro de port doit être le même pour tous les serveurs KMIP. Si vous ne fournissez pas de numéro de port, il prend par défaut le port 5696, qui est le port attribué par Internet Numbers Authority (IANA) pour KMIP. |        |
| Nom de la balise clé                                               | Facultatif. Le nom de la balise clé est utilisé pour identifier toutes les clés appartenant à un nœud. Le nom de la balise par défaut est le nom du nœud.                                                                             |        |

#### Informations associées

["Rapport technique NetApp 3954 : exigences et procédures de préinstallation pour IBM Tivoli Lifetime Key Manager pour NetApp Storage Encryption"](#)

["Rapport technique NetApp 4074 : exigences et procédures de préinstallation pour NetApp Storage Encryption pour SafeNet KeySecure"](#)

## Installez les certificats SSL sur le cluster

Le cluster et le serveur KMIP utilisent des certificats SSL KMIP pour vérifier l'identité de l'autre et établir une connexion SSL. Avant de configurer la connexion SSL avec le serveur KMIP, vous devez installer les certificats SSL du client KMIP pour le cluster et le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP.

### Description de la tâche

Dans une paire haute disponibilité, les deux nœuds doivent utiliser les mêmes certificats SSL publics et privés KMIP. Si vous connectez plusieurs paires haute disponibilité au même serveur KMIP, tous les nœuds des paires haute disponibilité doivent utiliser les mêmes certificats SSL publics et privés.

### Avant de commencer

- L'heure doit être synchronisée sur le serveur qui crée les certificats, le serveur KMIP et le cluster.
- Vous devez avoir obtenu le certificat public du client SSL KMIP pour le cluster.
- Vous devez avoir obtenu la clé privée associée au certificat client SSL KMIP pour le cluster.
- Le certificat client SSL KMIP ne doit pas être protégé par un mot de passe.
- Vous devez avoir obtenu le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP.
- Dans un environnement MetroCluster, vous devez installer les mêmes certificats SSL KMIP sur les deux clusters.



Vous pouvez installer les certificats client et serveur sur le serveur KMIP avant ou après l'installation des certificats sur le cluster.

### Étapes

1. Installez les certificats client SSL KMIP pour le cluster :

```
security certificate install -vserver admin_svm_name -type client
```

Vous êtes invité à entrer les certificats SSL KMIP publics et privés.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Installez le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP :

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

### Activation de la gestion externe des clés dans ONTAP 9.6 et versions ultérieures (basée sur le matériel)

Vous pouvez utiliser un ou plusieurs serveurs KMIP pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous pouvez connecter jusqu'à quatre serveurs KMIP à un nœud. Un minimum de deux serveurs est recommandé pour la redondance et la reprise après sinistre.

À partir de ONTAP 9.11.1, vous pouvez ajouter jusqu'à 3 serveurs de clés secondaires par serveur de clés principal pour créer un serveur de clés en cluster. Pour plus d'informations, voir [Configurez les serveurs de clés externes en cluster](#).

## Avant de commencer

- Les certificats client SSL KMIP et serveur doivent avoir été installés.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant de configurer un gestionnaire de clés externe.
- Dans un environnement MetroCluster, vous devez installer le certificat SSL KMIP sur les deux clusters.

## Étapes

1. Configurer la connectivité du gestionnaire de clés pour le cluster :

```
security key-manager external enable -vserver admin_SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```



- Le `security key-manager external enable` la commande remplace le `security key-manager setup` commande. Vous pouvez exécuter le `security key-manager external modify` commande pour modifier la configuration de la gestion externe des clés. Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.
- Dans un environnement MetroCluster, si vous configurez une gestion externe des clés pour le SVM admin, vous devez répéter l'opération `security key-manager external enable` commande sur le cluster partenaire.

La commande suivante active la gestion externe des clés pour `cluster1` avec trois serveurs de clés externes. Le premier serveur de clés est spécifié à l'aide de son nom d'hôte et de son port, le second est spécifié à l'aide d'une adresse IP et du port par défaut, et le troisième est spécifié à l'aide d'une adresse et d'un port IPv6 :

```
cluster1::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. Vérifiez que tous les serveurs KMIP configurés sont connectés :

```
security key-manager external show-status -node node_name -vserver SVM -key
-server host_name|IP_address:port -key-server-status available|not-
responding|unknown
```



Le `security key-manager external show-status` la commande remplace le `security key-manager show -status` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> security key-manager external show-status
```

| Node  | Vserver  | Key Server                                   | Status    |
|-------|----------|----------------------------------------------|-----------|
| ----- |          |                                              |           |
| ----- |          |                                              |           |
| node1 |          |                                              |           |
|       | cluster1 |                                              |           |
|       |          | 10.0.0.10:5696                               | available |
|       |          | fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 | available |
|       |          | ks1.local:15696                              | available |
| node2 |          |                                              |           |
|       | cluster1 |                                              |           |
|       |          | 10.0.0.10:5696                               | available |
|       |          | fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 | available |
|       |          | ks1.local:15696                              | available |

```
6 entries were displayed.
```

#### Activez la gestion externe des clés dans ONTAP 9.5 et versions antérieures

Vous pouvez utiliser un ou plusieurs serveurs KMIP pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous pouvez connecter jusqu'à quatre serveurs KMIP à un nœud. Un minimum de deux serveurs est recommandé pour la redondance et la reprise après sinistre.

#### Description de la tâche

ONTAP configure la connectivité du serveur KMIP pour tous les nœuds du cluster.

#### Avant de commencer

- Les certificats client SSL KMIP et serveur doivent avoir été installés.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant de configurer un gestionnaire de clés externe.
- Dans un environnement MetroCluster, vous devez installer le certificat SSL KMIP sur les deux clusters.

#### Étapes

1. Configurer la connectivité du gestionnaire de clés pour les nœuds du cluster :

```
security key-manager setup
```

La configuration du gestionnaire de clés démarre.



Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

2. Entrez la réponse appropriée à chaque invite.

### 3. Ajoutez un serveur KMIP :

```
security key-manager add -address key_management_server_ipaddress
```



Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

### 4. Ajoutez un serveur KMIP supplémentaire pour la redondance :

```
security key-manager add -address key_management_server_ipaddress
```



Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

### 5. Vérifiez que tous les serveurs KMIP configurés sont connectés :

```
security key-manager show -status
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> security key-manager show -status
```

| Node        | Port | Registered Key Manager | Status    |
|-------------|------|------------------------|-----------|
| -----       | ---- | -----                  | -----     |
| cluster1-01 | 5696 | 20.1.1.1               | available |
| cluster1-01 | 5696 | 20.1.1.2               | available |
| cluster1-02 | 5696 | 20.1.1.1               | available |
| cluster1-02 | 5696 | 20.1.1.2               | available |

### 6. Vous pouvez également convertir des volumes en texte brut en volumes chiffrés.

```
volume encryption conversion start
```

Un gestionnaire de clés externe doit être entièrement configuré avant la conversion des volumes. Dans un environnement MetroCluster, un gestionnaire de clés externe doit être configuré sur les deux sites.

#### Configurez les serveurs de clés externes en cluster

À partir de ONTAP 9.11.1, il est possible de configurer la connectivité aux serveurs de gestion externe des clés en cluster sur un SVM. Avec des serveurs de clés en cluster, vous pouvez désigner des serveurs de clés principaux et secondaires sur une SVM. Lors



de l'enregistrement des clés, ONTAP essaie d'abord d'accéder à un serveur de clés principal avant de tenter d'accéder aux serveurs secondaires de manière séquentielle jusqu'à ce que l'opération s'effectue correctement, ce qui évite la duplication des clés.

Les serveurs de clés externes peuvent être utilisés pour les clés NSE, NVE, NAE et SED. Un SVM peut prendre en charge jusqu'à quatre principaux serveurs KMIP externes. Chaque serveur principal peut prendre en charge jusqu'à trois serveurs de clés secondaires.

### Avant de commencer

- ["La gestion des clés KMIP doit être activée pour le SVM"](#).
- Ce processus prend uniquement en charge les serveurs de clés qui utilisent KMIP. Pour obtenir la liste des serveurs de clés pris en charge, reportez-vous à la ["Matrice d'interopérabilité NetApp"](#).
- Tous les nœuds du cluster doivent exécuter ONTAP 9.11.1 ou une version ultérieure.
- L'ordre des serveurs répertorie les arguments dans `-secondary-key-servers` Paramètre correspond à l'ordre d'accès des serveurs de gestion externe des clés (KMIP).

### Créer un serveur de clés mis en cluster

La procédure de configuration varie selon que vous avez configuré ou non un serveur de clés principal.

#### Ajout de serveurs de clés primaires et secondaires à un SVM

1. Vérifier qu'aucune gestion des clés n'a été activée pour le cluster :  

```
security key-manager external show -vserver svm_name
```

Si le SVM possède déjà le maximum de quatre serveurs de clés principaux activés, vous devez supprimer l'un des serveurs de clés principaux existants avant d'en ajouter un nouveau.
2. Activez le gestionnaire de clés principal :  

```
security key-manager external enable -vserver svm_name -key-servers
server_ip -client-cert client_cert_name -server-ca-certs
server_ca_cert_names
```
3. Modifiez le serveur de clés principal pour ajouter des serveurs de clés secondaires. Le `-secondary-key-servers` paramètre accepte une liste séparée par des virgules de trois serveurs de clés au maximum.  

```
security key-manager external modify-server -vserver svm_name -key-servers
primary_key_server -secondary-key-servers list_of_key_servers
```

#### Ajoutez des serveurs de clés secondaires à un serveur de clés principal existant

1. Modifiez le serveur de clés principal pour ajouter des serveurs de clés secondaires. Le `-secondary-key-servers` paramètre accepte une liste séparée par des virgules de trois serveurs de clés au maximum.  

```
security key-manager external modify-server -vserver svm_name -key-servers
primary_key_server -secondary-key-servers list_of_key_servers
```

Pour plus d'informations sur les serveurs de clés secondaires, reportez-vous à la section [\[mod-secondary\]](#).

### Modifier les serveurs de clés en cluster

Vous pouvez modifier les clusters de serveurs de clés externes en modifiant l'état (principal ou secondaire) de

serveurs de clés spécifiques, en ajoutant et en supprimant des serveurs de clés secondaires ou en modifiant l'ordre d'accès des serveurs de clés secondaires.

## Conversion des serveurs de clés principaux et secondaires

Pour convertir un serveur de clés principal en serveur de clés secondaire, vous devez d'abord le supprimer de la SVM avec le `security key-manager external remove-servers` commande.

Pour convertir un serveur de clés secondaire en serveur de clés principal, vous devez d'abord supprimer le serveur de clés secondaire de son serveur de clés principal existant. Voir [\[mod-secondary\]](#). Si vous convertissez un serveur de clés secondaire en serveur principal lors de la suppression d'une clé existante, toute tentative d'ajout d'un nouveau serveur avant la suppression et la conversion peut entraîner la duplication des clés.

## Modifier les serveurs de clés secondaires

Les serveurs de clés secondaires sont gérés à l'aide du `-secondary-key-servers` paramètre du `security key-manager external modify-server` commande. Le `-secondary-key-servers` le paramètre accepte une liste séparée par des virgules. L'ordre spécifié des serveurs de clés secondaires dans la liste détermine la séquence d'accès des serveurs de clés secondaires. L'ordre d'accès peut être modifié en exécutant la commande `security key-manager external modify-server` les serveurs de clés secondaires étant entrés dans une séquence différente.

Pour supprimer un serveur de clés secondaire, le `-secondary-key-servers` les arguments doivent inclure les serveurs clés que vous voulez conserver lors de l'omission de celui à supprimer. Pour supprimer tous les serveurs de clés secondaires, utilisez l'argument `-`, indiquant aucun.

Pour plus d'informations, reportez-vous au `security key-manager external` dans le ["Référence de commande ONTAP"](#).

## Créez des clés d'authentification dans ONTAP 9.6 et versions ultérieures

Vous pouvez utiliser le `security key-manager key create` Commande permettant de créer les clés d'authentification d'un nœud et de les stocker sur les serveurs KMIP configurés.

### Description de la tâche

Si votre configuration de sécurité exige que vous utilisiez des clés différentes pour l'authentification des données et l'authentification FIPS 140-2, vous devez créer une clé distincte pour chacune d'elles. Si ce n'est pas le cas, vous pouvez utiliser la même clé d'authentification pour la conformité FIPS que pour l'accès aux données.

ONTAP crée des clés d'authentification pour tous les nœuds du cluster.

- Cette commande n'est pas prise en charge lorsque le gestionnaire de clés intégré est activé. Toutefois, deux clés d'authentification sont créées automatiquement lorsque le gestionnaire de clés intégré est activé. Les clés peuvent être affichées à l'aide de la commande suivante :

```
security key-manager key query -key-type NSE-AK
```

- Vous recevez un avertissement si les serveurs de gestion des clés configurés stockent déjà plus de 128 clés d'authentification.
- Vous pouvez utiliser le `security key-manager key delete` commande permettant de supprimer les

clés inutilisées. Le `security key-manager key delete` La commande échoue si la clé donnée est actuellement utilisée par ONTAP. (Vous devez avoir des privilèges supérieurs à « admin » pour utiliser cette commande.)



Dans un environnement MetroCluster, avant de supprimer une clé, veillez à ce que cette clé ne soit pas utilisée sur le cluster partenaire. Vous pouvez utiliser les commandes suivantes sur le cluster partenaire pour vérifier que la clé n'est pas utilisée :

- `storage encryption disk show -data-key-id key-id`
- `storage encryption disk show -fips-key-id key-id`

## Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

## Étapes

1. Créer les clés d'authentification pour les nœuds du cluster :

```
security key-manager key create -key-tag passphrase_label -prompt-for-key
true|false
```



Réglage `prompt-for-key=true` provoque l'invite de l'administrateur de cluster à utiliser la phrase secrète lors de l'authentification de disques cryptés. Dans le cas contraire, le système génère automatiquement une phrase de passe de 32 octets. Le `security key-manager key create` la commande remplace le `security key-manager create-key` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

L'exemple suivant crée les clés d'authentification pour `cluster1`, génération automatique d'une phrase de passe de 32 octets :

```
cluster1::> security key-manager key create
Key ID:
000000000000000002000000000001006268333f870860128fbe17d393e5083b00000000
00000000
```

2. Vérifiez que les clés d'authentification ont été créées :

```
security key-manager key query -node node
```



Le security key-manager key query la commande remplace le security key-manager query key commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man. L'ID de clé affiché dans la sortie est un identificateur utilisé pour faire référence à la clé d'authentification. Ce n'est pas la clé d'authentification ou la clé de chiffrement des données.

L'exemple suivant vérifie que les clés d'authentification ont été créées pour `cluster1`:

Node: node1

Restored

yes

```
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
```

yes

```
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

Node: node2

Restored

yes

```
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
```

yes

```
00000000000000000200000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

- Vous recevez un avertissement si les serveurs de gestion des clés configurés stockent déjà plus de 128 clés d'authentification.

Vous pouvez utiliser le logiciel du serveur de gestion des clés pour supprimer toutes les clés inutilisées, puis exécuter de nouveau la commande.

## Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

## Étapes

1. Créer les clés d'authentification pour les nœuds du cluster :

```
security key-manager create-key
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



L'ID de clé affiché dans la sortie est un identificateur utilisé pour faire référence à la clé d'authentification. Ce n'est pas la clé d'authentification ou la clé de chiffrement des données.

L'exemple suivant crée les clés d'authentification pour `cluster1`:

```
cluster1::> security key-manager create-key
(security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID: F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```

2. Vérifiez que les clés d'authentification ont été créées :

```
security key-manager query
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant vérifie que les clés d'authentification ont été créées pour `cluster1`:

```
cluster1::> security key-manager query

(security key-manager query)

 Node: cluster1-01
 Key Manager: 20.1.1.1
 Server Status: available

Key Tag Key Type Restored

cluster1-01 NSE-AK yes
 Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

 Node: cluster1-02
 Key Manager: 20.1.1.1
 Server Status: available

Key Tag Key Type Restored

cluster1-02 NSE-AK yes
 Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
```

#### Attribution d'une clé d'authentification de données à un lecteur FIPS ou SED (gestion de clés externe)

Vous pouvez utiliser le `storage encryption disk modify` Commande permettant d'attribuer une clé d'authentification de données à un lecteur FIPS ou SED. Les nœuds de cluster utilisent cette clé pour verrouiller ou déverrouiller des données chiffrées sur le disque.

#### Description de la tâche

Un disque à chiffrement automatique est protégé contre tout accès non autorisé uniquement si son ID de clé d'authentification est défini sur une valeur autre que celle par défaut. L'ID sécurisé du fabricant (MSID), qui possède l'ID de clé 0x0, est la valeur par défaut standard des lecteurs SAS. Pour les disques NVMe, la valeur standard par défaut est une clé nulle, représentée sous forme d'ID de clé vierge. Lorsque vous attribuez l'ID de clé à un disque auto-crypté, le système remplace son ID de clé d'authentification par une valeur autre que celle par défaut.

Cette procédure n'est pas perturbatrice.

#### Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

#### Étapes

1. Attribuez une clé d'authentification de données à un lecteur FIPS ou SED :

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Vous pouvez utiliser le `security key-manager query -key-type NSE-AK` Commande permettant d'afficher les ID de clés.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
```

```
Info: Starting modify on 14 disks.
 View the status of the operation by using the
 storage encryption disk show-status command.
```

2. Vérifiez que les clés d'authentification ont été attribuées :

```
storage encryption disk show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> storage encryption disk show
Disk Mode Data Key ID

0.0.0 data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1 data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
[...]
```

## Configurez la gestion intégrée des clés

### Activez la gestion intégrée des clés dans ONTAP 9.6 et versions ultérieures

Vous pouvez utiliser le gestionnaire de clés intégré pour authentifier les nœuds de cluster sur un lecteur FIPS ou SED. Le gestionnaire de clés intégré est un outil intégré qui sert des clés d'authentification aux nœuds du même système de stockage que vos données. Le gestionnaire de clés intégré est conforme à la norme FIPS-140-2 de niveau 1.

Vous pouvez utiliser le gestionnaire de clés intégré pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous devez activer le gestionnaire de clés intégré sur chaque cluster qui accède à un volume chiffré ou à un disque auto-chiffré.

### Description de la tâche

Vous devez exécuter le `security key-manager onboard enable` commande à chaque ajout d'un nœud au cluster. Dans les configurations MetroCluster, vous devez exécuter `security key-manager onboard enable` sur le cluster local, puis s'exécute `security key-manager onboard sync` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.

Par défaut, vous n'êtes pas tenu de saisir la phrase de passe du gestionnaire de clés lors du redémarrage d'un nœud. Sauf dans MetroCluster, vous pouvez utiliser `cc-mode-enabled=yes` option pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage.

Lorsque le gestionnaire de clés intégré est activé en mode critères communs (`cc-mode-enabled=yes`), le comportement du système est modifié de l'une des manières suivantes :

- Le système surveille les tentatives consécutives de mot de passe de cluster ayant échoué lorsqu'il fonctionne en mode critères communs.

Si NetApp Storage Encryption (NSE) est activé et que vous ne saisissez pas la phrase secrète appropriée au démarrage, le système ne peut pas s'authentifier sur ses disques et redémarre automatiquement. Pour corriger ce problème, vous devez saisir la phrase secrète correcte du cluster à l'invite de démarrage. Une fois démarré, le système peut saisir jusqu'à 5 tentatives consécutives de saisie de la phrase secrète du cluster dans une période de 24 heures pour toute commande nécessitant une phrase secrète comme paramètre. Si la limite est atteinte (par exemple, vous n'avez pas saisi correctement la phrase de passe du cluster 5 fois de suite) alors vous devez attendre l'expiration du délai de 24 heures ou redémarrer le nœud pour réinitialiser la limite.

- Les mises à jour d'images système utilisent le certificat de signature de code NetApp RSA-3072 avec des digests signés SHA-384 pour vérifier l'intégrité de l'image au lieu du certificat de signature de code RSA-2048 NetApp habituel et des digests signés par code SHA-256.

La commande de mise à niveau vérifie que le contenu de l'image n'a pas été modifié ou corrompu en vérifiant diverses signatures numériques. Le processus de mise à jour de l'image passe à l'étape suivante si la validation réussit ; sinon, la mise à jour de l'image échoue. Pour plus d'informations sur les mises à jour du système, reportez-vous à la page de manuel « image du cluster ».

Le gestionnaire de clés intégré stocke les clés dans la mémoire volatile. Le contenu de la mémoire volatile est effacé lors du redémarrage ou de l'arrêt du système. Dans des conditions de fonctionnement normales, le contenu de la mémoire volatile est effacé dans les 30 secondes lorsqu'un système est arrêté.

### Avant de commencer

- Si vous utilisez NSE avec un serveur de gestion externe des clés (KMIP), vous devez avoir supprimé la base de données de gestionnaire de clés externe.

#### "Transition vers la gestion intégrée des clés à partir d'une gestion externe des clés"

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant que le gestionnaire de clés intégré ne soit configuré.

### Étapes

1. Lancez la commande de configuration du gestionnaire de clés :



```
security key-manager onboard enable -cc-mode-enabled yes|no
```



Réglez `cc-mode-enabled=yes` pour demander aux utilisateurs de saisir la phrase de passe du gestionnaire de clés après un redémarrage. Le - `cc-mode-enabled` Cette option n'est pas prise en charge dans les configurations MetroCluster. Le `security key-manager onboard enable` la commande remplace le `security key-manager setup` commande.

L'exemple suivant démarre la commande Key Manager setup sur `cluster1` sans exiger la saisie de la phrase de passe après chaque redémarrage :

```
cluster1::> security key-manager onboard enable
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1":<32..256 ASCII characters long text>
Reenter the cluster-wide passphrase: <32..256 ASCII characters long
text>
```

2. À l'invite de phrase de passe, entrez une phrase de passe comprise entre 32 et 256 caractères, ou une phrase de passe entre 64 et 256 caractères pour « mode CC ».



Si la phrase de passe « CC-mode » spécifiée est inférieure à 64 caractères, il y a un délai de cinq secondes avant que l'opération de configuration du gestionnaire de clés n'affiche à nouveau l'invite de phrase de passe.

3. À l'invite de confirmation de la phrase de passe, saisissez à nouveau la phrase de passe.
4. Vérifiez que les clés d'authentification ont été créées :

```
security key-manager key query -node node
```



Le `security key-manager key query` la commande remplace le `security key-manager query key` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

L'exemple suivant vérifie que les clés d'authentification ont été créées pour `cluster1`:

```
cluster1::> security key-manager key query
 Vserver: cluster1
 Key Manager: onboard
 Node: node1
```

| Key Tag                                                                             | Key Type | Restored |
|-------------------------------------------------------------------------------------|----------|----------|
| -----                                                                               | -----    | -----    |
| node1                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000000000000 |          |          |
| node1                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000000000 |          |          |

```

 Vserver: cluster1
 Key Manager: onboard
 Node: node2
```

| Key Tag                                                                             | Key Type | Restored |
|-------------------------------------------------------------------------------------|----------|----------|
| -----                                                                               | -----    | -----    |
| node1                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000000000000 |          |          |
| node2                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000000000 |          |          |

### Une fois que vous avez terminé

Copiez la phrase secrète dans un emplacement sécurisé à l'extérieur du système de stockage pour une utilisation ultérieure.

Toutes les informations de gestion des clés sont automatiquement sauvegardées dans la base de données répliquée (RDB) pour le cluster. Vous devez également sauvegarder les informations manuellement pour les utiliser en cas d'incident.

### Activez la gestion intégrée des clés dans ONTAP 9.5 et versions antérieures

Vous pouvez utiliser le gestionnaire de clés intégré pour authentifier les nœuds de cluster sur un lecteur FIPS ou SED. Le gestionnaire de clés intégré est un outil intégré qui sert des clés d'authentification aux nœuds du même système de stockage que vos données. Le gestionnaire de clés intégré est conforme à la norme FIPS-140-2 de niveau 1.

Vous pouvez utiliser le gestionnaire de clés intégré pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous devez activer le gestionnaire de clés intégré sur chaque cluster qui accède à un volume chiffré ou à un disque auto-chiffré.

## Description de la tâche

Vous devez exécuter le `security key-manager setup` commande à chaque ajout d'un nœud au cluster.

Si vous disposez d'une configuration MetroCluster, consultez les consignes suivantes :

- Dans ONTAP 9.5, vous devez exécuter `security key-manager setup` sur le cluster local et `security key-manager setup -sync-metrocluster-config yes` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.
- Avant ONTAP 9.5, vous devez exécuter `security key-manager setup` sur le cluster local, attendez environ 20 secondes, puis exécutez `security key-manager setup` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.

Par défaut, vous n'êtes pas tenu de saisir la phrase de passe du gestionnaire de clés lors du redémarrage d'un nœud. À partir de ONTAP 9.4, vous pouvez utiliser le `-enable-cc-mode yes` option pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage.

Pour NVE, si vous définissez `-enable-cc-mode yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées. Pour `volume create`, vous n'avez pas besoin de spécifier `-encrypt true`. Pour `volume move start`, vous n'avez pas besoin de spécifier `-encrypt-destination true`.



Après une tentative de phrase de passe, vous devez redémarrer le nœud.

## Avant de commencer

- Si vous utilisez NSE avec un serveur de gestion externe des clés (KMIP), vous devez avoir supprimé la base de données de gestionnaire de clés externe.

["Transition vers la gestion intégrée des clés à partir d'une gestion externe des clés"](#)

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant que le gestionnaire de clés intégré ne soit configuré.

## Étapes

1. Lancez la configuration du gestionnaire de clés :

```
security key-manager setup -enable-cc-mode yes|no
```



À partir de ONTAP 9.4, vous pouvez utiliser le `-enable-cc-mode yes` option permettant aux utilisateurs de saisir la phrase de passe du gestionnaire de clés après un redémarrage. Pour NVE, si vous définissez `-enable-cc-mode yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées.

L'exemple suivant commence à configurer le gestionnaire de clés sur le cluster 1 sans que la phrase de passe ne soit saisie après chaque redémarrage :

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase: <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase: <32..256 ASCII characters long
text>
```

2. Entrez `yes` à l'invite, configurez la gestion intégrée des clés.
3. À l'invite de phrase de passe, entrez une phrase de passe comprise entre 32 et 256 caractères, ou une phrase de passe entre 64 et 256 caractères pour « mode CC ».



Si la phrase de passe « CC-mode » spécifiée est inférieure à 64 caractères, il y a un délai de cinq secondes avant que l'opération de configuration du gestionnaire de clés n'affiche à nouveau l'invite de phrase de passe.

4. À l'invite de confirmation de la phrase de passe, saisissez à nouveau la phrase de passe.
5. Vérifier que les clés sont configurées pour tous les nœuds :

```
security key-manager key show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID Used By

0000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID Used By

0000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

## Une fois que vous avez terminé

Toutes les informations de gestion des clés sont automatiquement sauvegardées dans la base de données répliquée (RDB) pour le cluster.

Chaque fois que vous configurez la phrase secrète Onboard Key Manager, vous devez également sauvegarder les informations manuellement dans un emplacement sécurisé en dehors du système de stockage afin de les utiliser en cas d'incident. Voir ["Sauvegardez manuellement les informations intégrées de gestion des clés"](#).

### Attribution d'une clé d'authentification des données à un lecteur FIPS ou SED (gestion des clés intégrée)

Vous pouvez utiliser le `storage encryption disk modify` Commande permettant d'attribuer une clé d'authentification de données à un lecteur FIPS ou SED. Les nœuds de cluster utilisent cette clé pour accéder aux données du disque.

### Description de la tâche

Un disque à chiffrement automatique est protégé contre tout accès non autorisé uniquement si son ID de clé d'authentification est défini sur une valeur autre que celle par défaut. L'ID sécurisé du fabricant (MSID), qui possède l'ID de clé 0x0, est la valeur par défaut standard des lecteurs SAS. Pour les disques NVMe, la valeur standard par défaut est une clé nulle, représentée sous forme d'ID de clé vierge. Lorsque vous attribuez l'ID de clé à un disque auto-crypté, le système remplace son ID de clé d'authentification par une valeur autre que celle par défaut.

### Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

### Étapes

1. Attribuez une clé d'authentification de données à un lecteur FIPS ou SED :

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Vous pouvez utiliser le `security key-manager key query -key-type NSE-AK` Commande permettant d'afficher les ID de clés.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
0000000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4
```

```
Info: Starting modify on 14 disks.
View the status of the operation by using the
storage encryption disk show-status command.
```

2. Vérifiez que les clés d'authentification ont été attribuées :

```
storage encryption disk show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> storage encryption disk show
Disk Mode Data Key ID

0.0.0 data
00000000000000000000200000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1 data
00000000000000000000200000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

## Attribuez une clé d'authentification FIPS 140-2 à un disque FIPS

Vous pouvez utiliser le `storage encryption disk modify` commande avec `-fips -key-id` Option permettant d'attribuer une clé d'authentification FIPS 140-2 à un disque FIPS. Les nœuds de cluster utilisent cette clé pour des opérations autres que l'accès aux données, comme empêcher les attaques de déni de service sur le disque.

### Description de la tâche

Votre configuration de sécurité peut nécessiter l'utilisation de clés différentes pour l'authentification des données et l'authentification FIPS 140-2-2. Si ce n'est pas le cas, vous pouvez utiliser la même clé d'authentification pour la conformité FIPS que celle utilisée pour l'accès aux données.

Cette procédure n'est pas perturbatrice.

### Avant de commencer

Le firmware du disque doit prendre en charge la conformité à la norme FIPS 140-2-2. Le "[Matrice d'interopérabilité NetApp](#)" contient des informations sur les versions de micrologiciel de lecteur prises en charge.

### Étapes

1. Vous devez d'abord vous assurer que vous avez attribué une clé d'authentification des données. Pour ce faire, utilisez un [gestionnaire de clés externe](#) ou un [gestionnaire de clés intégré](#). Vérifiez que la clé est affectée à la commande `storage encryption disk show`.
2. Attribution d'une clé d'authentification FIPS 140-2 aux disques SED :

```
storage encryption disk modify -disk disk_id -fips-key-id
fips_authentication_key_id
```

Vous pouvez utiliser le `security key-manager query` Commande permettant d'afficher les ID de clés.

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
```

Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.

### 3. Vérifiez que la clé d'authentification a été attribuée :

```
storage encryption disk show -fips
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> storage encryption disk show -fips
Disk Mode FIPS-Compliance Key ID

2.10.0 full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1 full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

## Activez le mode compatible FIPS au niveau du cluster pour les connexions de serveurs KMIP

Vous pouvez utiliser le `security config modify` commande avec `-is-fips-enabled` Option permettant d'activer le mode conforme à la norme FIPS au niveau du cluster pour les données en transit. Cela force le cluster à utiliser OpenSSL en mode FIPS lors de la connexion à des serveurs KMIP.

### Description de la tâche

Lorsque vous activez le mode cluster compatible FIPS, le cluster n'utilise automatiquement que les suites de chiffrement conformes à la norme TLS1.2 et FIPS. Le mode conforme à la norme FIPS à l'échelle du cluster est désactivé par défaut.

Vous devez redémarrer manuellement les nœuds du cluster après avoir modifié la configuration de sécurité à l'échelle du cluster.

### Avant de commencer

- Le contrôleur de stockage doit être configuré en mode conforme à la norme FIPS.
- Tous les serveurs KMIP doivent prendre en charge TLSv1.2. Le système nécessite TLSv1.2 pour terminer la connexion au serveur KMIP lorsque le mode conforme FIPS à l'échelle du cluster est activé.

### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Vérifiez que TLSv1.2 est pris en charge :

```
security config show -supported-protocols
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> security config show
```

|           | Cluster   |                         | Cluster                             |
|-----------|-----------|-------------------------|-------------------------------------|
| Security  |           |                         |                                     |
| Interface | FIPS Mode | Supported Protocols     | Supported Ciphers Config            |
| Ready     |           |                         |                                     |
| -----     | -----     | -----                   | -----                               |
| -----     |           |                         |                                     |
| SSL       | false     | TLSv1.2, TLSv1.1, TLSv1 | ALL:!LOW:<br>!aNULL:!EXP:<br>!eNULL |
|           |           |                         | yes                                 |

3. Activer le mode compatible FIPS à l'échelle du cluster :

```
security config modify -is-fips-enabled true -interface SSL
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

4. Redémarrez les nœuds du cluster manuellement.
5. Vérifiez que le mode compatible FIPS à l'échelle du cluster est activé :

```
security config show
```

```
cluster1::> security config show
```

|           | Cluster   |                     | Cluster                                  |
|-----------|-----------|---------------------|------------------------------------------|
| Security  |           |                     |                                          |
| Interface | FIPS Mode | Supported Protocols | Supported Ciphers Config                 |
| Ready     |           |                     |                                          |
| -----     | -----     | -----               | -----                                    |
| -----     |           |                     |                                          |
| SSL       | true      | TLSv1.2, TLSv1.1    | ALL:!LOW:<br>!aNULL:!EXP:<br>!eNULL:!RC4 |
|           |           |                     | yes                                      |

## Gestion du cryptage NetApp

### Déchiffrement des données de volume

Vous pouvez utiliser le `volume move start` commande pour déplacer et annuler le



chiffrement des données de volume.

### Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche. Vous pouvez également être un administrateur SVM auquel l'administrateur du cluster a délégué des pouvoirs. Pour plus d'informations, voir ["Autorité déléguée pour exécuter la commande volume Move"](#).

### Étapes

1. Déplacer un volume chiffré existant sans chiffrer les données sur le volume :

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate
aggregate_name -encrypt-destination false
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

La commande suivante déplace un volume existant nommé `vol1` vers l'agrégat de destination `aggr3` et déchiffre les données sur le volume :

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr3 -encrypt-destination false
```

Le système supprime la clé de cryptage du volume. Les données du volume sont non chiffrées.

2. Vérifiez que le volume est désactivé pour le chiffrement :

```
volume show -encryption
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

La commande suivante indique si les volumes sont présents `cluster1` sont chiffrées :

```
cluster1::> volume show -encryption
```

| Vserver | Volume | Aggregate | State  | Encryption State |
|---------|--------|-----------|--------|------------------|
| -----   | -----  | -----     | -----  | -----            |
| vs1     | vol1   | aggr1     | online | none             |

### Déplacement d'un volume chiffré

Vous pouvez utiliser le `volume move start` commande permettant de déplacer un volume chiffré. Le volume déplacé peut résider sur le même agrégat ou sur un autre agrégat.

### Description de la tâche

Le déplacement échoue si le nœud de destination ou le volume de destination ne prend pas en charge le chiffrement de volume.

Le `-encrypt-destination` option pour `volume move start` la valeur par défaut est `true` pour les

volumes chiffrés. La nécessité de spécifier que vous ne souhaitez pas que le volume de destination soit chiffré garantit que vous ne déchiffrez pas par inadvertance les données sur le volume.

### Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche. Vous pouvez également être un administrateur SVM auquel l'administrateur du cluster a délégué des pouvoirs. Pour plus d'informations, voir ["autorité déléguée pour exécuter la commande de déplacement de volume"](#).

### Étapes

1. Déplacez un volume chiffré et laissez les données sur le volume chiffré :

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).

La commande suivante déplace un volume existant nommé `vol1` vers l'agrégat de destination `aggr3` et conserve les données sur le volume chiffrées :

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination -aggregate aggr3
```

2. Vérifiez que le volume est activé pour le chiffrement :

```
volume show -is-encrypted true
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).

La commande suivante affiche les volumes chiffrés sur `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State  | Type | Size  | Available | Used |
|---------|--------|-----------|--------|------|-------|-----------|------|
| -----   | -----  | -----     | -----  | ---- | ----- | -----     | ---- |
| vs1     | vol1   | aggr3     | online | RW   | 200GB | 160.0GB   | 20%  |

### Autorité déléguée pour exécuter la commande volume Move

Vous pouvez utiliser le `volume move` commande pour chiffrer un volume existant, déplacer un volume chiffré ou annuler le chiffrement d'un volume. Les administrateurs du cluster peuvent exécuter `volume move` Ils peuvent se passer eux-mêmes de la commande ou déléguer à l'autorité pour qu'elle exécute la commande aux administrateurs du SVM.

### Description de la tâche

Par défaut, les administrateurs du SVM sont affectés au système `vsadmin` rôle, qui ne comprend pas l'autorité nécessaire pour déplacer les volumes. Vous devez affecter le `vsadmin-volume` Rôle aux administrateurs

SVM afin de leur permettre d'exécuter les `volume move` commande.

## Étape

1. Déléguer l'autorité pour exécuter le `volume move` commande :

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role vsadmin-
volume
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

La commande suivante permet à l'administrateur du SVM d'exécuter le `volume move` commande.

```
cluster1::>security login modify -vserver engData -user-or-group-name
SVM-admin -application ssh -authmethod domain -role vsadmin-volume
```

## Modifiez la clé de chiffrement d'un volume à l'aide de la commande `Volume Encryption rekey start`

Il est recommandé de modifier régulièrement la clé de chiffrement d'un volume. Vous pouvez utiliser ONTAP 9.3 à partir de `volume encryption rekey start` commande pour changer la clé de chiffrement.

### Description de la tâche

Une fois que vous avez démarré une opération de recontact, elle doit être terminée. Il n'y a pas de retour à l'ancienne clé. Si vous rencontrez un problème de performances pendant l'opération, vous pouvez exécuter le `volume encryption rekey pause` commande pour mettre l'opération en pause, et le `volume encryption rekey resume` commande pour reprendre l'opération.

Jusqu'à la fin de l'opération de renouvellement de clé, le volume est composé de deux touches. Les nouvelles écritures et les lectures correspondantes utiliseront la nouvelle clé. Sinon, les lectures utilisent l'ancienne clé.



Vous ne pouvez pas utiliser `volume encryption rekey start` Pour rétablir un volume SnapLock.

## Étapes

1. Modifier une clé de chiffrement :

```
volume encryption rekey start -vserver SVM_name -volume volume_name
```

La commande suivante modifie la clé de chiffrement pour `vol1` Sur `SVMvs1`:

```
cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
```

2. Vérifier l'état de l'opération de renouvellement de clé :

```
volume encryption rekey show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

La commande suivante affiche l'état de l'opération de renouvellement de clés :

```
cluster1::> volume encryption rekey show
```

| Vserver | Volume | Start Time         | Status                       |
|---------|--------|--------------------|------------------------------|
| -----   | -----  | -----              | -----                        |
| vs1     | vol1   | 9/18/2017 17:51:41 | Phase 2 of 2 is in progress. |

3. Une fois l'opération de renouvellement de clés terminée, vérifiez que le volume est activé pour le chiffrement :

```
volume show -is-encrypted true
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

La commande suivante affiche les volumes chiffrés sur cluster1:

```
cluster1::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State  | Type  | Size  | Available | Used  |
|---------|--------|-----------|--------|-------|-------|-----------|-------|
| -----   | -----  | -----     | -----  | ----- | ----- | -----     | ----- |
| vs1     | vol1   | aggr2     | online | RW    | 200GB | 160.0GB   | 20%   |

## Modifiez la clé de chiffrement d'un volume à l'aide de la commande volume Move start

Il est recommandé de modifier régulièrement la clé de chiffrement d'un volume. Vous pouvez utiliser le `volume move start` commande pour changer la clé de chiffrement. Vous devez utiliser `volume move start` Dans ONTAP 9.2 et versions antérieures. Le volume déplacé peut résider sur le même agrégat ou sur un autre agrégat.

### Description de la tâche

Vous ne pouvez pas utiliser `volume move start` Pour reKey un volume SnapLock ou FlexGroup.

### Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche. Vous pouvez également être un administrateur SVM auquel l'administrateur du cluster a délégué des pouvoirs. Pour plus d'informations, voir ["autorité déléguée pour exécuter la commande de déplacement de volume"](#).

### Étapes

1. Déplacer un volume existant et modifier la clé de chiffrement :

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -generate-destination-key true
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

La commande suivante déplace un volume existant nommé **vol1** vers l'agrégat de destination **aggr2** et

modifie la clé de chiffrement :

```
cluster1::> volume move start -vserver vs1 -volume voll1 -destination
-aggregate aggr2 -generate-destination-key true
```

Une nouvelle clé de chiffrement est créée pour le volume. Les données du volume restent chiffrées.

2. Vérifiez que le volume est activé pour le chiffrement :

```
volume show -is-encrypted true
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

La commande suivante affiche les volumes chiffrés sur cluster1:

```
cluster1::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State  | Type  | Size  | Available | Used  |
|---------|--------|-----------|--------|-------|-------|-----------|-------|
| -----   | -----  | -----     | -----  | ----- | ----- | -----     | ----- |
| vs1     | voll1  | aggr2     | online | RW    | 200GB | 160.0GB   | 20%   |

## Rotation des clés d'authentification pour NetApp Storage Encryption

Vous pouvez faire tourner les clés d'authentification lorsque vous utilisez NetApp Storage Encryption (NSE).

### Description de la tâche

La rotation des clés d'authentification dans un environnement NSE est prise en charge si vous utilisez External Key Manager (KMIP).



La rotation des clés d'authentification dans un environnement NSE n'est pas prise en charge pour Onboard Key Manager (OKM).

### Étapes

1. Utilisez le `security key-manager create-key` commande permettant de générer de nouvelles clés d'authentification.

Vous devez générer de nouvelles clés d'authentification avant de pouvoir modifier les clés d'authentification.

2. Utilisez le `storage encryption disk modify -disk * -data-key-id` commande pour modifier les clés d'authentification.

## Supprimez un volume chiffré

Vous pouvez utiliser le `volume delete` commande de suppression d'un volume chiffré.

### Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche. Vous pouvez également être un administrateur SVM auquel l'administrateur du cluster a délégué des pouvoirs. Pour plus d'informations, voir ["autorité déléguée pour exécuter la commande de déplacement de volume"](#).
- Le volume doit être hors ligne.

## Étape

1. Supprimez un volume chiffré :

```
volume delete -vserver SVM_name -volume volume_name
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).

La commande suivante supprime un volume chiffré nommé `vol1`:

```
cluster1::> volume delete -vserver vs1 -volume vol1
```

Entrez `yes` lorsque vous êtes invité à confirmer la suppression.

Le système supprime la clé de cryptage du volume au bout de 24 heures.

Utiliser `volume delete` avec le `-force true` option permettant de supprimer un volume et de détruire immédiatement la clé de chiffrement correspondante. Cette commande nécessite des privilèges avancés. Pour plus d'informations, consultez la page [man](#).

## Une fois que vous avez terminé

Vous pouvez utiliser le `volume recovery-queue` pour restaurer un volume supprimé pendant la période de rétention après l'émission du `volume delete` commande :

```
volume recovery-queue SVM_name -volume volume_name
```

["Comment utiliser la fonction de récupération de volume"](#)

## Supprimez les données de façon sécurisée sur un volume chiffré

Supprimez les données de façon sécurisée dans une vue d'ensemble du volume chiffré

Depuis ONTAP 9.4, vous pouvez utiliser la suppression sécurisée pour nettoyer les données sans interruption sur les volumes NVE. La suppression des données sur un volume chiffré garantit qu'elles ne peuvent pas être récupérées depuis le support physique, par exemple en cas de « pillage », où les traces de données peuvent être laissées derrière lors de l'écrasement des blocs ou pour supprimer en toute sécurité les données d'un locataire vide.

La suppression sécurisée fonctionne uniquement pour les fichiers précédemment supprimés sur les volumes NVE. Vous ne pouvez pas nettoyer un volume non chiffré. Vous devez utiliser des serveurs KMIP pour fournir des clés, et non le gestionnaire de clés intégré.

### **Considérations relatives à l'utilisation de la suppression sécurisée**

- Les volumes créés dans un agrégat pour NetApp Aggregate Encryption (NAE) ne prennent pas en charge la suppression sécurisée.
- La suppression sécurisée fonctionne uniquement pour les fichiers précédemment supprimés sur les volumes NVE.
- Vous ne pouvez pas nettoyer un volume non chiffré.
- Vous devez utiliser des serveurs KMIP pour fournir des clés, et non le gestionnaire de clés intégré.

Les fonctions de purge sécurisée varient en fonction de votre version de ONTAP.

### ONTAP 9.8 et versions ultérieures

- La suppression sécurisée est prise en charge par MetroCluster et FlexGroup.
- Si le volume en cours de purge est à l'origine d'une relation SnapMirror, il n'est pas nécessaire de rompre la relation SnapMirror pour effectuer une purge sécurisée.
- La méthode de rechiffrement est différente pour les volumes qui utilisent la protection des données SnapMirror, contre les volumes qui n'utilisent pas la protection des données SnapMirror (DP) ou ceux qui utilisent la protection étendue des données SnapMirror.
  - Par défaut, les volumes utilisant le mode de protection des données SnapMirror (DP) recryptent les données à l'aide de la méthode de chiffrement du déplacement de volume.
  - Par défaut, les volumes qui n'utilisent pas la protection des données SnapMirror ou les volumes en utilisant le mode XDP (SnapMirror Extended Data protection) utilisent la méthode de rechiffrement sur place.
  - Ces valeurs par défaut peuvent être modifiées à l'aide de l' `secure purge re-encryption-method [volume-move|in-place-rekey]` commande.
- Par défaut toutes les copies Snapshot des volumes FlexVol sont automatiquement supprimées lors de l'opération de suppression sécurisée. Par défaut, les copies Snapshot des volumes FlexGroup et les volumes qui utilisent la protection des données SnapMirror ne sont pas automatiquement supprimées lors de l'opération de suppression sécurisée. Ces valeurs par défaut peuvent être modifiées à l'aide de l' `secure purge delete-all-snapshots [true|false]` commande.

### ONTAP 9.7 et versions antérieures :

- La purge sécurisée ne prend pas en charge les éléments suivants :
  - FlexClone
  - SnapVault
  - FabricPool
- Si le volume en cours de purge est la source d'une relation SnapMirror, vous devez interrompre la relation SnapMirror avant de pouvoir purger le volume.

Si des copies Snapshot sont occupées dans le volume, vous devez libérer les copies Snapshot avant de pouvoir purger le volume. Par exemple, vous devrez peut-être séparer un volume FlexClone de son volume parent.

- L'appel réussi de la fonction de suppression sécurisée déclenche un déplacement de volume qui recrypte les données restantes non supprimées avec une nouvelle clé.

Le volume déplacé reste sur l'agrégat actuel. L'ancienne clé est automatiquement détruite, ce qui permet de s'assurer que les données supprimées ne peuvent pas être récupérées du support de stockage.

### Supprimez en toute sécurité les données d'un volume chiffré sans une relation SnapMirror

Depuis ONTAP 9.4, vous pouvez utiliser la suppression sécurisée vers les données « ``cribs" sans interruption sur les volumes NVE.

### Description de la tâche

La suppression sécurisée peut prendre de plusieurs minutes à plusieurs heures, selon la quantité de données



contenues dans les fichiers supprimés. Vous pouvez utiliser le `volume encryption secure-purge show` commande permettant d'afficher le statut de l'opération. Vous pouvez utiliser le `volume encryption secure-purge abort` commande pour mettre fin à l'opération.



Pour effectuer une purge sécurisée sur un hôte SAN, vous devez supprimer la LUN entière contenant les fichiers à purger, ou vous devez pouvoir perforer les trous dans la LUN pour les blocs appartenant aux fichiers à purger. Si vous ne pouvez pas supprimer la LUN ou si votre système d'exploitation hôte ne prend pas en charge la perforation dans la LUN, vous ne pouvez pas effectuer de purge sécurisée.

#### Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des privilèges avancés sont requis pour cette tâche.

#### Étapes

1. Supprimez les fichiers ou la LUN que vous souhaitez supprimer en toute sécurité.
  - Sur un client NAS, supprimez les fichiers que vous souhaitez purger en toute sécurité.
  - Sur un hôte SAN, supprimez le LUN que vous souhaitez purger ou perforer en toute sécurité les blocs appartenant aux fichiers à supprimer.

2. Sur le système de stockage, passez au niveau de privilège avancé :

```
set -privilege advanced
```

3. Si les fichiers que vous souhaitez purger en toute sécurité sont dans les instantanés, supprimez-les :

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot
```

4. Supprimez les fichiers supprimés de manière sécurisée :

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

La commande suivante supprime de manière sécurisée les fichiers supprimés sur `vol1` Sur `SVMvs1`:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

5. Vérifier l'état de l'opération de purge sécurisée :

```
volume encryption secure-purge show
```

#### Supprimez en toute sécurité les données sur un volume chiffré avec une relation asynchrone SnapMirror

À partir de ONTAP 9.8, vous pouvez appliquer une suppression sécurisée aux données « crub » sans interruption sur les volumes NVE avec une relation asynchrone SnapMirror.

#### Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des privilèges avancés sont requis pour cette tâche.

## Description de la tâche

La suppression sécurisée peut prendre de plusieurs minutes à plusieurs heures, selon la quantité de données contenues dans les fichiers supprimés. Vous pouvez utiliser le `volume encryption secure-purge show` commande permettant d'afficher le statut de l'opération. Vous pouvez utiliser le `volume encryption secure-purge abort` commande pour mettre fin à l'opération.



Pour effectuer une purge sécurisée sur un hôte SAN, vous devez supprimer la LUN entière contenant les fichiers à purger, ou vous devez pouvoir perforer les trous dans la LUN pour les blocs appartenant aux fichiers à purger. Si vous ne pouvez pas supprimer la LUN ou si votre système d'exploitation hôte ne prend pas en charge la perforation dans la LUN, vous ne pouvez pas effectuer de purge sécurisée.

## Étapes

1. Sur le système de stockage, basculer sur le niveau de privilège avancé :

```
set -privilege advanced
```

2. Supprimez les fichiers ou la LUN que vous souhaitez supprimer en toute sécurité.
  - Sur un client NAS, supprimez les fichiers que vous souhaitez purger en toute sécurité.
  - Sur un hôte SAN, supprimez le LUN que vous souhaitez purger ou perforer en toute sécurité les blocs appartenant aux fichiers à supprimer.
3. Préparez le volume de destination dans la relation asynchrone à supprimer de manière sécurisée :

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
-prepare true
```

Répétez cette étape pour chaque volume de votre relation SnapMirror asynchrone.

4. Si les fichiers que vous souhaitez supprimer de manière sécurisée se trouvent dans des copies Snapshot, supprimez les copies Snapshot :

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot
```

5. Si les fichiers que vous souhaitez supprimer de manière sécurisée se trouvent dans les copies Snapshot de base, procédez comme suit :

- a. Créer une copie Snapshot sur le volume de destination dans la relation asynchrone SnapMirror :

```
volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
volume_name
```

- b. Mettre à jour SnapMirror pour transférer la copie Snapshot de base :

```
snapmirror update -source-snapshot snapshot_name -destination-path
destination_path
```

Répétez cette étape pour chaque volume de la relation asynchrone SnapMirror.

- a. Les étapes de répétition (a) et (b) sont égales au nombre de copies Snapshot de base plus une.

Par exemple, si vous avez deux copies Snapshot de base, vous devez répéter les étapes (a) et (b) trois fois.

b. Vérifier la présence de la copie Snapshot de base :

```
snapshot show -vserver SVM_name -volume volume_name
```

c. Supprimer la copie Snapshot de base :

```
snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot
```

6. Supprimez les fichiers supprimés de manière sécurisée :

```
volume encryption secure-purge start -vserver svm_name -volume volume_name
```

Répétez cette étape pour chaque volume de la relation asynchrone SnapMirror.

La commande suivante purge de manière sécurisée les fichiers supprimés sur « 'vol1' » du SVM « vs1 » :

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

7. Vérifier l'état de l'opération de purge sécurisée :

```
volume encryption secure-purge show
```

#### Nettoyer les données sur un volume chiffré avec une relation synchrone SnapMirror

À partir de ONTAP 9.8, vous pouvez utiliser une suppression sécurisée pour « nettoyer » les données de volumes NVE avec une relation synchrone SnapMirror, sans interruption.

#### Description de la tâche

Une purge sécurisée peut prendre plusieurs minutes à plusieurs heures, selon la quantité de données contenues dans les fichiers supprimés. Vous pouvez utiliser le `volume encryption secure-purge show` commande permettant d'afficher le statut de l'opération. Vous pouvez utiliser le `volume encryption secure-purge abort` commande pour mettre fin à l'opération.



Pour effectuer une purge sécurisée sur un hôte SAN, vous devez supprimer la LUN entière contenant les fichiers à purger, ou vous devez pouvoir perforer les trous dans la LUN pour les blocs appartenant aux fichiers à purger. Si vous ne pouvez pas supprimer la LUN ou si votre système d'exploitation hôte ne prend pas en charge la perforation dans la LUN, vous ne pouvez pas effectuer de purge sécurisée.

#### Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des privilèges avancés sont requis pour cette tâche.

#### Étapes

1. Sur le système de stockage, passez au niveau de privilège avancé :

```
set -privilege advanced
```

2. Supprimez les fichiers ou la LUN que vous souhaitez supprimer en toute sécurité.

- Sur un client NAS, supprimez les fichiers que vous souhaitez purger en toute sécurité.
- Sur un hôte SAN, supprimez le LUN que vous souhaitez purger ou perforer en toute sécurité les blocs appartenant aux fichiers à supprimer.

3. Préparez le volume de destination dans la relation asynchrone à supprimer de manière sécurisée :

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
-prepare true
```

Répétez cette étape pour l'autre volume de votre relation synchrone SnapMirror.

4. Si les fichiers que vous souhaitez supprimer de manière sécurisée se trouvent dans des copies Snapshot, supprimez les copies Snapshot :

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
```

5. Si le fichier de suppression sécurisée se trouve dans les copies Snapshot de base ou communes, mettez à jour SnapMirror pour déplacer la copie Snapshot commune :

```
snapmirror update -source-snapshot snapshot_name -destination-path
destination_path
```

Il existe deux copies Snapshot communes. Cette commande doit donc être émise deux fois.

6. Si le fichier de suppression sécurisée se trouve dans la copie Snapshot cohérente au niveau des applications, supprimez la copie Snapshot sur les deux volumes de la relation synchrone SnapMirror :

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
```

Effectuer cette étape sur les deux volumes.

7. Supprimez les fichiers supprimés de manière sécurisée :

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

Répétez cette étape pour chaque volume de la relation synchrone SnapMirror.

La commande suivante supprime en toute sécurité les fichiers supprimés sur « vol1 » sur le SMV « vs1 ».

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

8. Vérifier l'état de l'opération de purge sécurisée :

```
volume encryption secure-purge show
```

## Modifiez la phrase secrète intégrée pour la gestion des clés

Il est recommandé d'appliquer régulièrement une meilleure pratique de sécurité à la modification de la phrase secrète intégrée pour la gestion des clés. Copiez la nouvelle phrase secrète intégrée pour la gestion des clés dans un emplacement sécurisé en

dehors du système de stockage pour une utilisation ultérieure.

**Avant de commencer**

- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Des privilèges avancés sont requis pour cette tâche.

**Étapes**

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Modifiez la phrase secrète intégrée pour la gestion des clés :

| Pour cette version ONTAP...       | Utilisez cette commande...                                  |
|-----------------------------------|-------------------------------------------------------------|
| ONTAP 9.6 et versions ultérieures | <code>security key-manager onboard update-passphrase</code> |
| ONTAP 9.5 et versions antérieures | <code>security key-manager update-passphrase</code>         |

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

La commande suivante de ONTAP 9.6 vous permet de modifier la phrase secrète de gestion intégrée des clés pour `cluster1`:

```
cluster1::> security key-manager onboard update-passphrase
Warning: This command will reconfigure the cluster passphrase for
onboard key management for Vserver "cluster1".
Do you want to continue? {y|n}: y
Enter current passphrase:
Enter new passphrase:
```

3. Entrez `y` à l'invite, vous pouvez modifier la phrase secrète intégrée pour la gestion des clés.
4. Saisissez la phrase de passe actuelle à l'invite de phrase de passe actuelle.
5. À l'invite de la nouvelle phrase de passe, entrez une phrase de passe comprise entre 32 et 256 caractères, ou une phrase de passe entre 64 et 256 caractères pour « mode CC ».

Si la phrase de passe « CC-mode » spécifiée est inférieure à 64 caractères, il y a un délai de cinq secondes avant que l'opération de configuration du gestionnaire de clés n'affiche à nouveau l'invite de phrase de passe.

6. À l'invite de confirmation de la phrase de passe, saisissez à nouveau la phrase de passe.

**Une fois que vous avez terminé**

Dans un environnement MetroCluster, vous devez mettre à jour la phrase secrète sur le cluster partenaire :

- Dans ONTAP 9.5 et les versions antérieures, vous devez exécuter `security key-manager update-passphrase` avec la même phrase secrète sur le cluster partenaire.
- Dans ONTAP 9.6 et versions ultérieures, vous êtes invité à exécuter `security key-manager onboard sync` avec la même phrase secrète sur le cluster partenaire.

Copiez le mot de passe de gestion des clés intégré vers un emplacement sécurisé en dehors du système de stockage pour une utilisation ultérieure.

Vous devez sauvegarder manuellement les informations de gestion des clés chaque fois que vous modifiez la phrase secrète de gestion intégrée des clés.

["Sauvegarde manuelle des informations de gestion intégrée des clés"](#)

## Sauvegardez manuellement les informations intégrées de gestion des clés

Vous devez copier les informations de gestion intégrée des clés dans un emplacement sécurisé en dehors du système de stockage dès que vous configurez la phrase secrète Onboard Key Manager.

### Ce dont vous avez besoin

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des privilèges avancés sont requis pour cette tâche.

### Description de la tâche

Toutes les informations de gestion des clés sont automatiquement sauvegardées dans la base de données répliquée (RDB) pour le cluster. Vous devez également sauvegarder manuellement les informations de gestion des clés pour une utilisation en cas d'incident.

### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Afficher les informations de gestion des clés du cluster :

| Pour cette version ONTAP...       | Utilisez cette commande...                            |
|-----------------------------------|-------------------------------------------------------|
| ONTAP 9.6 et versions ultérieures | <code>security key-manager onboard show-backup</code> |
| ONTAP 9.5 et versions antérieures | <code>security key-manager backup show</code>         |

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

+

La commande 9.6 suivante affiche les informations de sauvegarde de la gestion des clés pour `cluster1`:

+

[illegible]

- ## Restaurez les clés de chiffrement intégrées de gestion des clés

## Avant de commencer

- 2645



Si vous utilisez NSE sur un système doté d'un module Flash cache, vous devez également activer NVE ou NAE. NSE ne chiffre pas les données qui résident sur le module Flash cache.

#### ONTAP 9.6 et versions ultérieures



Si vous exécutez ONTAP 9.8 ou une version ultérieure et que votre volume racine est chiffré, suivez la procédure de [\[ontap-9-8\]](#).

1. Vérifiez que la clé doit être restaurée :  
`security key-manager key query -node node`
2. Restaurer la clé :  
`security key-manager onboard sync`

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

La commande ONTAP 9.6 suivante synchronise les clés dans la hiérarchie de clés intégrée :

```
cluster1::> security key-manager onboard sync
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1":: <32..256 ASCII characters long text>
```

3. À l'invite de phrase secrète, entrez la phrase secrète intégrée pour la gestion des clés du cluster.

#### ONTAP 9.8 ou version ultérieure avec volume racine chiffré

Si vous exécutez ONTAP 9.8 ou une version ultérieure et que votre volume racine est chiffré, vous devez définir une phrase de passe de récupération de la gestion des clés intégrée à l'aide du menu de démarrage. Ce processus est également nécessaire si vous effectuez un remplacement de support de démarrage.

1. Démarrez le nœud sur le menu de démarrage et sélectionnez option (10) Set onboard key management recovery secrets.
2. Entrez y pour utiliser cette option.
3. Entrez à l'invite le phrase secrète de gestion intégrée des clés pour le cluster.
4. À l'invite, entrez les données de la clé de sauvegarde.

Le nœud revient au menu de démarrage.

5. Dans le menu de démarrage, sélectionnez option (1) Normal Boot.

#### ONTAP 9.5 et versions antérieures

1. Vérifiez que la clé doit être restaurée :  
`security key-manager key show`
2. Si vous exécutez ONTAP 9.8 ou version ultérieure et que votre volume racine est chiffré, procédez comme suit :

Si vous exécutez ONTAP 9.6 ou 9.7, ou si vous utilisez ONTAP 9.8 ou une version ultérieure et que votre



volume racine n'est pas chiffré, ignorez cette étape.

3. Restaurer la clé :

```
security key-manager setup -node node
```

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

4. À l'invite de phrase secrète, entrez la phrase secrète intégrée pour la gestion des clés du cluster.

## Restaurer les clés de chiffrement externes pour la gestion des clés

Vous pouvez restaurer manuellement des clés de chiffrement de gestion externe des clés et les transférer vers un autre nœud. Vous pouvez le faire si vous redémarrez un nœud qui était temporairement arrêté lorsque vous avez créé les clés du cluster.

### Description de la tâche

Dans ONTAP 9.6 et versions ultérieures, vous pouvez utiliser le `security key-manager key query -node node_name` commande pour vérifier si votre clé doit être restaurée.

Dans ONTAP 9.5 et les versions antérieures, vous pouvez utiliser le `security key-manager key show` commande pour vérifier si votre clé doit être restaurée.



Si vous utilisez NSE sur un système doté d'un module Flash cache, vous devez également activer NVE ou NAE. NSE ne chiffre pas les données qui résident sur le module Flash cache.

### Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

### Étapes

1. Si vous exécutez ONTAP 9.8 ou version ultérieure et que le volume racine est chiffré, procédez comme suit :

Si vous exécutez ONTAP 9.7 ou une version antérieure, ou si vous exécutez ONTAP 9.8 ou une version ultérieure et que votre volume racine n'est pas chiffré, ignorez cette étape.

- a. Définissez les bootargs :

```
setenv kmip.init.ipaddr <ip-address>
```

```
setenv kmip.init.netmask <netmask>
```

```
setenv kmip.init.gateway <gateway>
```

```
setenv kmip.init.interface e0M
```

```
boot_ontap
```

- b. Démarrez le nœud sur le menu de démarrage et sélectionnez option (11) Configure node for external key management.
- c. Suivez les invites pour saisir le certificat de gestion.

Une fois toutes les informations relatives au certificat de gestion saisies, le système revient au menu

de démarrage.

d. Dans le menu de démarrage, sélectionnez option (1) Normal Boot.

## 2. Restaurer la clé :

| Pour cette version ONTAP...                                    | Utilisez cette commande...                                                                         |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| ONTAP 9.6 et versions ultérieures                              | <code>`security key-manager external restore -vserver SVM -node node -key-server host_name`</code> |
| <code>IP_address:port -key-id key_id -key -tag key_tag`</code> | ONTAP 9.5 et versions antérieures                                                                  |



node tous les nœuds par défaut. Pour connaître la syntaxe complète des commandes, consultez les pages de manuels. Cette commande n'est pas prise en charge lorsque la gestion intégrée des clés est activée.

La commande ONTAP 9.6 suivante restaure les clés d'authentification externes de gestion des clés vers tous les nœuds de `cluster1`:

```
cluster1::> security key-manager external restore
```

## Remplacer les certificats SSL

Tous les certificats SSL ont une date d'expiration. Vous devez mettre à jour vos certificats avant qu'ils n'expirent pour éviter toute perte d'accès aux clés d'authentification.

### Avant de commencer

- Vous devez avoir obtenu le certificat public et la clé privée de remplacement pour le cluster (certificat client KMIP).
- Vous devez avoir obtenu le certificat public de remplacement pour le serveur KMIP (certificat KMIP Server-CA).
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Dans un environnement MetroCluster, vous devez remplacer le certificat SSL KMIP sur les deux clusters.



Vous pouvez installer les certificats client et serveur de remplacement sur le serveur KMIP avant ou après l'installation des certificats sur le cluster.

### Étapes

#### 1. Installez le nouveau certificat KMIP Server-ca :

```
security certificate install -type server-ca -vserver <>
```

#### 2. Installez le nouveau certificat client KMIP :

```
security certificate install -type client -vserver <>
```

3. Mettez à jour la configuration du gestionnaire de clés pour utiliser les certificats nouvellement installés :

```
security key-manager external modify -vserver <> -client-cert <> -server-ca
-certs <>
```

Si vous exécutez ONTAP 9.6 ou version ultérieure dans un environnement MetroCluster et que vous souhaitez modifier la configuration du gestionnaire de clés sur le SVM admin, vous devez exécuter la commande sur les deux clusters de la configuration.



La mise à jour de la configuration du gestionnaire de clés pour utiliser les certificats nouvellement installés renvoie une erreur si les clés publiques/privées du nouveau certificat client sont différentes des clés installées précédemment. Consultez l'article de la base de connaissances ["Le nouveau certificat client les clés publiques ou privées sont différentes du certificat client existant"](#) pour obtenir des instructions sur la manière de neutraliser cette erreur.

### Remplacez un lecteur FIPS ou SED

Vous pouvez remplacer un lecteur FIPS ou SED de la même façon que vous remplacez un disque ordinaire. Veillez à attribuer de nouvelles clés d'authentification des données au disque de remplacement. Pour un lecteur FIPS, vous pouvez également attribuer une nouvelle clé d'authentification FIPS 140-2.



Si une paire haute disponibilité est utilisée ["Cryptage SAS ou disques NVMe \(SED, NSE, FIPS\)"](#), vous devez suivre les instructions de la rubrique ["Retour d'un lecteur FIPS ou SED en mode non protégé"](#) Pour tous les disques de la paire HA avant d'initialiser le système (options de démarrage 4 ou 9). Si vous ne le faites pas, vous risquez de subir des pertes de données si les disques sont requalifiés.

### Avant de commencer

- Vous devez connaître l'ID de clé pour la clé d'authentification utilisée par le lecteur.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.

### Étapes

1. Vérifiez que le disque a été marqué défectueux :

```
storage disk show -broken
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> storage disk show -broken
```

```
Original Owner: cluster1-01
```

```
Checksum Compatibility: block
```

|          |        |         |      |       |      |      |       |       |       |         | Usable |
|----------|--------|---------|------|-------|------|------|-------|-------|-------|---------|--------|
| Physical |        |         |      |       |      |      |       |       |       |         |        |
| Disk     | Outage | Reason  | HA   | Shelf | Bay  | Chan | Pool  | Type  | RPM   | Size    |        |
| Size     |        |         |      |       |      |      |       |       |       |         |        |
| -----    | ----   | -----   | ---- | ----  | ---- | ---- | ----- | ----- | ----- | -----   | -----  |
| 0.0.0    | admin  | failed  | 0b   | 1     | 0    | A    | Pool0 | FCAL  | 10000 | 132.8GB |        |
| 133.9GB  |        |         |      |       |      |      |       |       |       |         |        |
| 0.0.7    | admin  | removed | 0b   | 2     | 6    | A    | Pool1 | FCAL  | 10000 | 132.8GB |        |
| 134.2GB  |        |         |      |       |      |      |       |       |       |         |        |
| [...]    |        |         |      |       |      |      |       |       |       |         |        |

2. Retirez le disque défectueux et remplacez-le par un nouveau lecteur FIPS ou SED, en suivant les instructions du guide matériel de votre modèle de tiroir disque.
3. Attribuez la propriété du disque récemment remplacé :

```
storage disk assign -disk disk_name -owner node
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. Vérifiez que le nouveau disque a été affecté :

```
storage encryption disk show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> storage encryption disk show
Disk Mode Data Key ID

0.0.0 data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1 data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.0 data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1 data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1 open 0x0
[...]
```

5. Attribuez les clés d'authentification des données au lecteur FIPS ou SED.

"Attribution d'une clé d'authentification de données à un lecteur FIPS ou SED (gestion de clés externe)"

6. Si nécessaire, attribuez une clé d'authentification FIPS 140-2 au lecteur FIPS.

"Attribution d'une clé d'authentification FIPS 140-2 à un lecteur FIPS"

## Rendre les données d'un lecteur FIPS ou SED inaccessibles

### Rendre les données sur un lecteur FIPS ou SED inaccessibles

Si vous souhaitez rendre les données stockées sur un lecteur FIPS ou SED définitivement inaccessibles, mais que l'espace inutilisé du lecteur reste disponible pour les nouvelles données, vous pouvez désinfecter le disque. Si vous souhaitez rendre les données définitivement inaccessibles et que vous n'avez pas besoin de réutiliser le lecteur, vous pouvez le détruire.

- Nettoyage de disque

Lorsque vous procédez à la suppression d'un disque à auto-cryptage, le système modifie la clé de cryptage sur disque en une nouvelle valeur aléatoire, réinitialise l'état de verrouillage à la mise sous tension sur FALSE et définit l'ID de clé sur une valeur par défaut, soit l'ID sécurisé du fabricant 0x0 (disques SAS), soit une clé nulle (disques NVMe). Cela rend les données sur le disque inaccessibles et impossible à récupérer. Vous pouvez réutiliser des disques aseptisés comme disques de rechange non remis à zéro.

- Destruction du disque

Lorsque vous détruisez un lecteur FIPS ou SED, le système définit la clé de cryptage sur une valeur aléatoire inconnue et verrouille le disque de façon irréversible. Le disque devient ainsi définitivement inutilisable et les données qu'il y a définitivement inaccessibles.

Vous pouvez supprimer ou détruire des disques auto-cryptés ou tous les disques auto-cryptés d'un nœud.

## Désinfectez un lecteur FIPS ou SED

Si vous voulez rendre les données sur un lecteur FIPS ou SED définitivement inaccessibles et utiliser le lecteur pour les nouvelles données, vous pouvez utiliser le `storage encryption disk sanitize` commande de nettoyage du disque.

### Description de la tâche

Lorsque vous procédez à la suppression d'un disque à auto-cryptage, le système modifie la clé de cryptage sur disque en une nouvelle valeur aléatoire, réinitialise l'état de verrouillage à la mise sous tension sur FALSE et définit l'ID de clé sur une valeur par défaut, soit l'ID sécurisé du fabricant 0x0 (disques SAS), soit une clé nulle (disques NVMe). Cela rend les données sur le disque inaccessibles et impossible à récupérer. Vous pouvez réutiliser des disques aseptisés comme disques de rechange non remis à zéro.

### Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

### Étapes

1. Migrer toutes les données qui doivent être conservées vers un agrégat sur un autre disque.
2. Supprimez l'agrégat du lecteur FIPS ou SED pour les désinfecter :

```
storage aggregate delete -aggregate aggregate_name
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

```
cluster1::> storage aggregate delete -aggregate aggr1
```

3. Identifiez l'ID du disque pour le lecteur FIPS ou SED à désinfecter :

```
storage encryption disk show -fields data-key-id,fips-key-id,owner
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

```
cluster1::> storage encryption disk show
Disk Mode Data Key ID

0.0.0 data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1 data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2 data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. Si un lecteur FIPS est exécuté en mode FIPS-Compliance, définissez l'ID de clé d'authentification FIPS du nœud sur le MSID 0x0 par défaut :

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

Vous pouvez utiliser le `security key-manager query` Commande permettant d'afficher les ID de clés.

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0
```

Info: Starting modify on 1 disk.

View the status of the operation by using the  
storage encryption disk show-status command.

#### 5. Désinfectez le lecteur :

```
storage encryption disk sanitize -disk disk_id
```

Vous pouvez utiliser cette commande pour désinfecter uniquement les disques de rechange à chaud ou endommagés. Pour désinfecter tous les disques, quel que soit leur type, utilisez le `-force-all-state` option. Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.



ONTAP vous invite à saisir une phrase de confirmation avant de continuer. Saisissez la phrase exactement comme indiqué à l'écran.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2
```

Warning: This operation will cryptographically sanitize 1 spare or  
broken self-encrypting disk on 1 node.

To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.

View the status of the operation using the  
storage encryption disk show-status command.

#### 6. Éliminez la panne du disque désinfecté :

```
storage disk unfail -spare true -disk disk_id
```

#### 7. Vérifiez si le disque est propriétaire :

```
storage disk show -disk disk_id
```

Si le disque ne possède pas de propriétaire, attribuez-en un.

```
storage disk assign -owner node -disk disk_id
```

#### 8. Entrez le nodeshell pour le nœud qui possède les disques à désinfecter :

```
system node run -node node_name
```

Exécutez le `disk sanitize release` commande.

#### 9. Quittez le nodeshell. Éliminez à nouveau la panne du disque :

```
storage disk unfail -spare true -disk disk_id
```

10. Vérifier que le disque est désormais une pièce de rechange et prêt à être réutilisé dans un agrégat :

```
storage disk show -disk disk_id
```

### Détruire un lecteur FIPS ou SED

Si vous voulez rendre les données sur un lecteur FIPS ou SED définitivement inaccessibles et que vous n'avez pas besoin de réutiliser le lecteur, vous pouvez utiliser `storage encryption disk destroy` commande de destruction du disque.

### Description de la tâche

Lorsque vous détruisez un lecteur FIPS ou SED, le système définit la clé de cryptage sur une valeur aléatoire inconnue et verrouille le disque de façon irréversible. Le disque devient ainsi pratiquement inutilisable et les données qu'il y a définitivement inaccessibles. Cependant, vous pouvez réinitialiser le disque à ses paramètres configurés en usine à l'aide de l'ID de sécurité physique (PSID) imprimé sur l'étiquette du disque. Pour plus d'informations, voir ["Remise en service d'un lecteur FIPS ou SED en cas de perte de clés d'authentification"](#).



Vous ne devez pas détruire un disque FIPS ou SED sauf si vous disposez du service NRD plus (non-Returnable Disk plus). La destruction d'un disque annule sa garantie.

### Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

### Étapes

1. Migrer toutes les données qui doivent être conservées vers un agrégat sur un autre disque.
2. Supprimez l'agrégat du disque FIPS ou SED à détruire :

```
storage aggregate delete -aggregate aggregate_name
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

```
cluster1::> storage aggregate delete -aggregate aggr1
```

3. Identifiez l'ID de disque pour le lecteur FIPS ou SED à détruire :

```
storage encryption disk show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.



```
cluster1::> storage encryption disk show
Disk Mode Data Key ID

0.0.0 data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1 data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2 data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

#### 4. Détruire le disque :

```
storage encryption disk destroy -disk disk_id
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).



Vous êtes invité à entrer une phrase de confirmation avant de continuer. Saisissez la phrase exactement comme indiqué à l'écran.

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
self-encrypting disks on 1 node.
You cannot reuse destroyed disks unless you revert
them to their original state using the PSID value.
To continue, enter
 destroy disk
:destroy disk

Info: Starting destroy on 1 disk.
View the status of the operation by using the
"storage encryption disk show-status" command.
```

#### Données d'urgence déchirées sur un lecteur FIPS ou SED

En cas d'urgence en matière de sécurité, vous pouvez instantanément empêcher l'accès à un disque FIPS ou SED, même si l'alimentation n'est pas disponible pour le système de stockage ou le serveur KMIP.

#### Avant de commencer

- Si vous utilisez un serveur KMIP qui n'est pas alimenté, vous devez configurer le serveur KMIP avec un élément d'authentification facilement détruit (par exemple, une carte à puce ou un lecteur USB).

- Vous devez être un administrateur de cluster pour effectuer cette tâche.

### Étape

1. Exécutez la suppression d'urgence des données sur un lecteur FIPS ou SED :

|       |          |
|-------|----------|
| Si... | Alors... |
|-------|----------|

|                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| <p>L'alimentation est disponible pour le système de stockage et vous avez le temps de mettre celui-ci hors ligne aisément</p> | <ol style="list-style-type: none"> <li>Si le système de stockage est configuré en tant que paire haute disponibilité, désactivez le basculement.</li> <li>Mettre tous les agrégats hors ligne et les supprimer</li> <li>Définissez le niveau de privilège sur avancé : <pre>set -privilege advanced</pre> </li> <li>Si le lecteur est en mode FIPS-compliance, définissez à nouveau l'ID de clé d'authentification FIPS du nœud sur le MSID par défaut : <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> </li> <li>Arrêter le système de stockage.</li> <li>Démarre en mode de maintenance.</li> <li>Procédez à la suppression ou à la destruction des disques : <ul style="list-style-type: none"> <li>Pour rendre les données sur les disques inaccessibles et continuer à réutiliser les disques, procédez comme suit : <pre>disk encrypt sanitize -all</pre> </li> <li>Si vous souhaitez rendre les données sur les disques inaccessibles et que vous n'avez pas besoin d'enregistrer les disques, détruisez les disques : <pre>disk encrypt destroy disk_id1 disk_id2 ...</pre> </li> </ul> </li> </ol> | <p>Le système de stockage est sous tension et vous devez immédiatement détruire les données</p> |
|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>a. <b>Si vous souhaitez rendre les données sur les disques inaccessibles et que vous pourrez toujours les réutiliser, désinfectez les disques :</b></p> <p>b. Si le système de stockage est configuré en tant que paire haute disponibilité, désactivez le basculement.</p> <p>c. Définissez le niveau de privilège sur avancé :</p> <pre>set -privilege advanced</pre> <p>d. Si le lecteur est en mode FIPS-compliance, définissez à nouveau l'ID de clé d'authentification FIPS du nœud sur le MSID par défaut :</p> <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> <p>e. Procédez à la suppression du disque :</p> <pre>storage encryption disk sanitize -disk * -force-all-states true</pre> | <p>a. <b>Si vous souhaitez rendre les données sur les disques inaccessibles et que vous n'avez pas besoin d'enregistrer les disques, détruisez les disques :</b></p> <p>b. Si le système de stockage est configuré en tant que paire haute disponibilité, désactivez le basculement.</p> <p>c. Définissez le niveau de privilège sur avancé :</p> <pre>set -privilege advanced</pre> <p>d. Détruire les disques :</p> <pre>storage encryption disk destroy -disk * -force-all-states true</pre> | <p>Le système de stockage fonctionne de façon incohérente, laissant le système se trouve dans un état désactivé en permanence et toutes les données sont effacées. Pour réutiliser le système, vous devez le reconfigurer.</p> |
| <p>L'alimentation est disponible pour le serveur KMIP, mais pas pour le système de stockage</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <p>a. Connectez-vous au serveur KMIP.</p> <p>b. Détruire toutes les clés associées aux lecteurs FIPS ou les disques SED qui contiennent les données auxquelles vous souhaitez empêcher l'accès. Cela empêche l'accès aux clés de cryptage du disque par le système de stockage.</p>                                                                                                                                                                                                             | <p>L'alimentation n'est pas disponible pour le serveur KMIP ou le système de stockage</p>                                                                                                                                      |

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

## Renvoyez un lecteur FIPS ou SED au service en cas de perte de clés d'authentification

Le système traite un lecteur FIPS ou SED comme étant rompu si vous perdez

définitivement les clés d'authentification pour lui et que vous ne pouvez pas les récupérer du serveur KMIP. Bien que vous ne puissiez pas accéder ou récupérer les données sur le disque, vous pouvez prendre des mesures pour rendre à nouveau disponible l'espace inutilisé de SED pour les données.

**Avant de commencer**

Vous devez être un administrateur de cluster pour effectuer cette tâche.

**Description de la tâche**

Vous ne devez utiliser ce processus que si vous êtes certain que les clés d'authentification du lecteur FIPS ou SED sont définitivement perdues et que vous ne pouvez pas les récupérer.

Si les disques sont partitionnés, ils doivent d'abord être départitionnés avant que vous ne puissiez démarrer ce processus.



La commande permettant de départitionner un disque est uniquement disponible au niveau diagnostic et ne doit être effectuée qu'avec NetApp support supervision. **Il est fortement recommandé de contacter le support NetApp avant de continuer.** vous pouvez également consulter l'article de la base de connaissances "[Comment départitionner un lecteur de réserve dans ONTAP](#)".

**Étapes**

- 1. Renvoyez un lecteur FIPS ou SED au service :

|                   |                        |
|-------------------|------------------------|
| Si le SEDS est... | Procédez comme suit... |
|-------------------|------------------------|

|                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Pas en mode de conformité FIPS, ni en mode de conformité FIPS et la clé FIPS est disponible</p> | <ul style="list-style-type: none"> <li>a. Définissez le niveau de privilège sur avancé :<br/> <code>set -privilege advanced</code></li> <li>b. Réinitialisez la clé FIPS sur l'ID sécurisé de fabrication par défaut 0x0 :<br/> <code>storage encryption disk modify -fips-key-id 0x0 -disk <i>disk_id</i></code></li> <li>c. Vérifiez que l'opération a réussi :<br/> <code>storage encryption disk show-status</code><br/>           Si l'opération a échoué, utilisez le processus PSID dans cette rubrique.</li> <li>d. Procédez au nettoyage du disque défaillant :<br/> <code>storage encryption disk sanitize -disk <i>disk_id</i></code><br/>           Vérifiez que l'opération a réussi avec la commande <code>storage encryption disk show-status</code> avant de passer à l'étape suivante.</li> <li>e. Éliminez la panne du disque désinfecté :<br/> <code>storage disk unfail -spare true -disk <i>disk_id</i></code></li> <li>f. Vérifiez si le disque est propriétaire :<br/> <code>storage disk show -disk <i>disk_id</i></code><br/><br/>           Si le disque ne possède pas de propriétaire, attribuez-en un.<br/> <code>storage disk assign -owner node -disk <i>disk_id</i></code><br/><br/> <ul style="list-style-type: none"> <li>i. Entrez le nodeshell pour le nœud qui possède les disques à désinfecter :<br/><br/> <code>system node run -node <i>node_name</i></code></li> </ul>           Exécutez le <code>disk sanitize release</code> commande.</li> <li>g. Quittez le nodeshell. Éliminez à nouveau la panne du disque :<br/> <code>storage disk unfail -spare true -disk <i>disk_id</i></code></li> <li>h. Vérifier que le disque est désormais une pièce de rechange et prêt à être réutilisé dans un agrégat :<br/> <code>storage disk show -disk <i>disk_id</i></code></li> </ul> |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>En mode FIPS-compliance, la clé FIPS n'est pas disponible et les disques SED ont un PSID imprimé sur l'étiquette</p> | <ol style="list-style-type: none"> <li>a. Procurez-vous le PSID du disque à partir de l'étiquette du disque.</li> <li>b. Définissez le niveau de privilège sur avancé :<br/> <pre>set -privilege advanced</pre> </li> <li>c. Réinitialise le disque en fonction des paramètres configurés en usine :<br/> <pre>storage encryption disk revert-to-original-state -disk <i>disk_id</i> -psid <i>disk_physical_secure_id</i></pre> Vérifiez que l'opération a réussi avec la commande <code>storage encryption disk show-status</code> avant de passer à l'étape suivante. </li> <li>d. Si vous utilisez ONTAP 9.8P5 ou une version antérieure, passez à l'étape suivante. Si vous exécutez ONTAP 9.8P6 ou une version ultérieure, éliminez la panne du disque désinfecté.<br/> <pre>storage disk unfail -disk <i>disk_id</i></pre> </li> <li>e. Vérifiez si le disque est propriétaire :<br/> <pre>storage disk show -disk <i>disk_id</i></pre> <p>Si le disque ne possède pas de propriétaire, attribuez-en un.<br/> <pre>storage disk assign -owner node -disk <i>disk_id</i></pre> </p> <ol style="list-style-type: none"> <li>i. Entrez le nodeshell pour le nœud qui possède les disques à désinfecter :<br/> <pre>system node run -node <i>node_name</i></pre> </li> </ol> <p>Exécutez le <code>disk sanitize release</code> commande.</p> </li> <li>f. Quittez le nodeshell. Éliminez à nouveau la panne du disque :<br/> <pre>storage disk unfail -spare true -disk <i>disk_id</i></pre> </li> <li>g. Vérifier que le disque est désormais une pièce de rechange et prêt à être réutilisé dans un agrégat :<br/> <pre>storage disk show -disk <i>disk_id</i></pre> </li> </ol> |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Pour connaître la syntaxe complète de la commande, reportez-vous au ["référence de commande"](#).

## Retournez un lecteur FIPS ou SED en mode non protégé

Un lecteur FIPS ou SED est protégé contre les accès non autorisés uniquement si l'ID de clé d'authentification du nœud est défini sur une valeur autre que la valeur par défaut. Vous pouvez rétablir un lecteur FIPS ou SED en mode non protégé à l'aide de la `storage encryption disk modify` Commande pour définir l'ID de clé sur la valeur par défaut.

Si une paire haute disponibilité utilise des disques avec cryptage SAS ou NVMe (SED, NSE, FIPS), vous devez suivre cette procédure pour tous les disques de la paire haute disponibilité avant d'initialiser le système (options de démarrage 4 ou 9). Si vous ne le faites pas, vous risquez de subir des pertes de données si les disques sont requalifiés.

## Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

## Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Si un lecteur FIPS est exécuté en mode FIPS-Compliance, définissez l'ID de clé d'authentification FIPS du nœud sur le MSID 0x0 par défaut :

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

Vous pouvez utiliser le `security key-manager query` Commande permettant d'afficher les ID de clés.

```
cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id 0x0
```

```
Info: Starting modify on 14 disks.
View the status of the operation by using the
storage encryption disk show-status command.
```

Confirmer la réussite de l'opération à l'aide de la commande :

```
storage encryption disk show-status
```

Répétez la commande `show-status` jusqu'à ce que les chiffres de "disques commencés" et de "disques réalisés" soient identiques.

```
cluster1:: storage encryption disk show-status
```

|          | FIPS       | Latest  | Start              |       | Execution  | Disks |   |
|----------|------------|---------|--------------------|-------|------------|-------|---|
| Disks    | Disks      |         |                    |       |            |       |   |
| Node     | Support    | Request | Timestamp          |       | Time (sec) | Begun |   |
| Done     | Successful |         |                    |       |            |       |   |
| -----    | -----      | -----   | -----              | ----- | -----      | ----- |   |
| -----    | -----      |         |                    |       |            |       |   |
| cluster1 | true       | modify  | 1/18/2022 15:29:38 | 3     |            | 14    | 5 |
| 5        |            |         |                    |       |            |       |   |

1 entry was displayed.

3. Définissez à nouveau l'ID de clé d'authentification des données du nœud sur le MSID 0x0 par défaut :

```
storage encryption disk modify -disk disk_id -data-key-id 0x0
```

La valeur de `-data-key-id` Doit être défini sur 0x0 si vous retournez un disque SAS ou NVMe en mode non protégé.

Vous pouvez utiliser le `security key-manager query` Commande permettant d'afficher les ID de clés.



```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id 0x0
```

Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.

Confirmer la réussite de l'opération à l'aide de la commande :

```
storage encryption disk show-status
```

Répétez la commande show-status jusqu'à ce que les chiffres soient identiques. L'opération est terminée lorsque les numéros dans "disques commencés" et "disques terminés" sont les mêmes.

### Mode Maintenance

Depuis ONTAP 9.7, vous pouvez ressaisir un disque FIPS à partir du mode de maintenance. Si vous ne pouvez pas utiliser les instructions de l'interface de ligne de commandes ONTAP décrites dans la section précédente, vous devez utiliser le mode de maintenance.

### Étapes

1. Définissez à nouveau l'ID de clé d'authentification FIPS du nœud sur le MSID 0x0 par défaut :

```
disk encrypt rekey_fips 0x0 disklist
```

2. Définissez à nouveau l'ID de clé d'authentification des données du nœud sur le MSID 0x0 par défaut :

```
disk encrypt rekey 0x0 disklist
```

3. Vérifiez que la clé d'authentification FIPS a bien été reclés :

```
disk encrypt show_fips
```

4. Confirmer que la clé d'authentification des données a bien été reclés avec :

```
disk encrypt show
```

Votre sortie affichera probablement soit l'ID de clé MSID 0x0 par défaut, soit la valeur de 64 caractères détenue par le serveur de clés. Le `Locked?` ce champ fait référence au verrouillage des données.

| Disk    | FIPS Key ID | Locked? |
|---------|-------------|---------|
| 0a.01.0 | 0x0         | Yes     |

### Supprimez une connexion externe au gestionnaire de clés

Si vous n'avez plus besoin du serveur, vous pouvez déconnecter un serveur KMIP d'un nœud. Par exemple, vous pouvez déconnecter un serveur KMIP lorsque vous passez au

chiffrement de volume.

**Description de la tâche**

Lorsque vous déconnectez un serveur KMIP d'un nœud d'une paire haute disponibilité, le système déconnecte automatiquement le serveur de tous les nœuds du cluster.



Si vous prévoyez de continuer à utiliser la gestion externe des clés après la déconnexion d'un serveur KMIP, assurez-vous qu'un autre serveur KMIP est disponible pour assurer le service des clés d'authentification.

**Avant de commencer**

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

**Étape**

- 1. Déconnectez un serveur KMIP du nœud actuel :

| Pour cette version ONTAP...       | Utilisez cette commande...                                                                       |
|-----------------------------------|--------------------------------------------------------------------------------------------------|
| ONTAP 9.6 et versions ultérieures | <code>`security key-manager external remove-servers -vserver SVM -key -servers host_name`</code> |
| IP_address:port,...`              | ONTAP 9.5 et versions antérieures                                                                |

Dans un environnement MetroCluster, il faut répéter ces commandes sur les deux clusters pour le SVM admin.

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

La commande ONTAP 9.6 suivante désactive les connexions à deux serveurs de gestion des clés externes pour `cluster1`, le premier nommé `ks1`, Écoute sur le port par défaut 5696, le second avec l'adresse IP 10.0.0.20, écoute sur le port 24482 :

```
cluster1::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

**Modifiez les propriétés du serveur de gestion externe des clés**

À partir de ONTAP 9.6, vous pouvez utiliser le `security key-manager external modify-server` Commande permettant de modifier le délai d'attente d'E/S et le nom d'utilisateur d'un serveur de gestion de clés externe.

**Avant de commencer**

- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Des privilèges avancés sont requis pour cette tâche.
- Dans un environnement MetroCluster, vous devez répéter ces étapes sur les deux clusters pour la SVM d'administration.

**Étapes**

1. Sur le système de stockage, passez au niveau de privilège avancé :

```
set -privilege advanced
```

2. Modifiez les propriétés externes du serveur du gestionnaire de clés pour le cluster :

```
security key-manager external modify-server -vserver admin_SVM -key-server
host_name|IP_address:port,... -timeout 1...60 -username user_name
```



La valeur de temporisation est exprimée en secondes. Si vous modifiez le nom d'utilisateur, vous êtes invité à entrer un nouveau mot de passe. Si vous exécutez la commande à l'invite de connexion du cluster, *admin\_SVM* Par défaut au SVM admin du cluster actuel. Vous devez être l'administrateur de cluster pour modifier les propriétés du serveur du gestionnaire de clés externe.

La commande suivante remplace la valeur de temporisation par 45 secondes pour le *cluster1* serveur de gestion externe des clés à l'écoute sur le port par défaut 5696 :

```
cluster1::> security key-manager external modify-server -vserver
cluster1 -key-server ks1.local -timeout 45
```

3. Modifier les propriétés du serveur gestionnaire de clés externe pour un SVM (NVE uniquement) :

```
security key-manager external modify-server -vserver SVM -key-server
host_name|IP_address:port,... -timeout 1...60 -username user_name
```



La valeur de temporisation est exprimée en secondes. Si vous modifiez le nom d'utilisateur, vous êtes invité à entrer un nouveau mot de passe. Si vous exécutez la commande à l'invite de connexion du SVM, *SVM* Par défaut au SVM actuel Vous devez être l'administrateur du cluster ou de SVM pour modifier les propriétés du serveur externe Key Manager.

La commande suivante modifie le nom d'utilisateur et le mot de passe de *svm1* serveur de gestion externe des clés à l'écoute sur le port par défaut 5696 :

```
svm1::> security key-manager external modify-server -vserver svm11 -key
-server ks1.local -username svmluser
Enter the password:
Reenter the password:
```

4. Répétez la dernière étape pour tout SVM supplémentaire.

### Transition vers la gestion externe des clés à partir de la gestion intégrée des clés

Pour basculer de la gestion externe des clés à partir de la gestion intégrée des clés, vous devez supprimer la configuration intégrée de la gestion des clés avant de pouvoir activer la gestion externe des clés.

#### Avant de commencer

- Pour le chiffrement matériel, vous devez réinitialiser les clés de données de tous les lecteurs FIPS ou SED à la valeur par défaut.

["Retour d'un lecteur FIPS ou SED en mode non protégé"](#)

- Pour le chiffrement logiciel, vous devez déchiffrer tous les volumes.

["Sans chiffrement des données de volume"](#)

- Vous devez être un administrateur de cluster pour effectuer cette tâche.

## Étape

1. Supprimez la configuration intégrée de gestion des clés d'un cluster :

| Pour cette version ONTAP...       | Utilisez cette commande...                                     |
|-----------------------------------|----------------------------------------------------------------|
| ONTAP 9.6 et versions ultérieures | <code>security key-manager onboard disable -vserver SVM</code> |
| ONTAP 9.5 et versions antérieures | <code>security key-manager delete-key-database</code>          |

Pour obtenir la syntaxe complète de la commande, reportez-vous à la ["Référence de commande ONTAP"](#).

## Transition vers la gestion intégrée des clés à partir d'une gestion externe des clés

Pour basculer vers la gestion intégrée des clés à partir d'une gestion externe des clés, vous devez supprimer la configuration de gestion externe des clés pour pouvoir activer la gestion intégrée des clés.

### Avant de commencer

- Pour le chiffrement matériel, vous devez réinitialiser les clés de données de tous les lecteurs FIPS ou SED à la valeur par défaut.

["Retour d'un lecteur FIPS ou SED en mode non protégé"](#)

- Vous devez avoir supprimé toutes les connexions externes du gestionnaire de clés.

["Suppression d'une connexion externe au gestionnaire de clés"](#)

- Vous devez être un administrateur de cluster pour effectuer cette tâche.

## Procédure

La procédure de transition de la gestion des clés dépend de la version de ONTAP que vous utilisez.

### ONTAP 9.6 et versions ultérieures

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Utiliser la commande :

```
security key-manager external disable -vserver admin_SVM
```



Dans un environnement MetroCluster, il faut répéter la commande sur les deux clusters pour la SVM admin.

### ONTAP 9.5 et versions antérieures

Utiliser la commande :

```
security key-manager delete-kmip-config
```

## Que se passe-t-il lorsque les serveurs de gestion des clés ne sont pas accessibles lors du processus de démarrage

ONTAP prend certaines précautions afin d'éviter tout comportement indésirable dans l'éventualité où un système de stockage configuré pour NSE ne puisse pas atteindre l'un des serveurs de gestion des clés spécifiés lors du processus de démarrage.

Si le système de stockage est configuré pour NSE, les disques SED sont de nouveau et verrouillés, et les disques SED sont sous tension, le système de stockage doit récupérer les clés d'authentification requises à partir des serveurs de gestion des clés pour s'authentifier auprès des disques SED avant qu'ils puissent accéder aux données.

Le système de stockage tente de contacter les serveurs de gestion des clés spécifiés pendant jusqu'à trois heures. Si le système de stockage ne peut pas atteindre l'un d'eux après ce délai, le processus d'amorçage s'arrête et le système de stockage s'arrête.

Si le système de stockage contacte avec succès un serveur de gestion de clés spécifié, il tente alors d'établir une connexion SSL pendant 15 minutes. Si le système de stockage ne parvient pas à établir de connexion SSL avec un serveur de gestion de clés spécifié, le processus d'amorçage s'arrête et le système de stockage s'arrête.

Pendant que le système de stockage tente de contacter et de se connecter aux serveurs de gestion des clés, il affiche des informations détaillées sur les tentatives de contact ayant échoué au niveau de l'interface de ligne de commande. Vous pouvez interrompre les tentatives de contact à tout moment en appuyant sur Ctrl-C.

Par mesure de sécurité, les disques SED ne permettent qu'un nombre limité de tentatives d'accès non autorisées, après quoi ils désactivent l'accès aux données existantes. Si le système de stockage ne peut pas contacter les serveurs de gestion des clés spécifiés pour obtenir les clés d'authentification appropriées, il peut uniquement tenter de s'authentifier auprès de la clé par défaut, ce qui entraîne une tentative d'échec et un incident. Si le système de stockage est configuré pour redémarrer automatiquement en cas de panique, il entre dans une boucle d'amorçage qui entraîne des tentatives d'authentification continues sur les disques SED ayant échoué.

Dans ces scénarios, l'arrêt du système de stockage a été conçu pour éviter que le système de stockage ne pénètre dans une boucle d'amorçage et qu'il puisse y avoir des pertes de données inattendues suite au

verrouillage permanent des disques SED, raison du dépassement de la limite de sécurité d'un certain nombre de tentatives d'authentification consécutives ayant échoué. La limite et le type de protection de verrouillage dépendent des spécifications de fabrication et du type de SED :

| Type SED                                                                     | Nombre de tentatives d'authentification consécutives ayant échoué entraînant un blocage | Type de protection de verrouillage lorsque la limite de sécurité est atteinte                                                 |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| DISQUES DURS                                                                 | 1024                                                                                    | Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible. |
| X440_PHM2800MCTO SSD NSE 800 Go avec révisions du firmware NA00 ou NA01      | 5                                                                                       | Temporaire. Le verrouillage est activé uniquement jusqu'à ce que le disque soit mis hors/sous tension.                        |
| X577_PHM2800MNA00 SSD NSE 800 Go avec révisions de firmware ou NA01          | 5                                                                                       | Temporaire. Le verrouillage est activé uniquement jusqu'à ce que le disque soit mis hors/sous tension.                        |
| X440_PHM2800MCTO SSD NSE 800 Go avec révisions de firmware plus élevées      | 1024                                                                                    | Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible. |
| X577_PHM2800MCTO SSD NSE 800 Go avec révisions de micrologiciel plus élevées | 1024                                                                                    | Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible. |
| Tous les autres modèles de SSD                                               | 1024                                                                                    | Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible. |

Pour tous les types SED, une authentification réussie réinitialise le nombre d'essayer à zéro.

Si vous rencontrez ce scénario lorsque le système de stockage est arrêté en raison d'un échec d'accès aux serveurs de gestion de clés spécifiés, vous devez d'abord identifier et corriger la cause de l'échec de communication avant de poursuivre le démarrage du système de stockage.

### Désactiver le chiffrement par défaut

Depuis ONTAP 9.7, le chiffrement d'agrégat et de volume est activé par défaut si vous disposez d'une licence VE (Volume Encryption) et utilisez un gestionnaire de clés intégré ou externe. Si nécessaire, vous pouvez désactiver le chiffrement par défaut pour l'ensemble du cluster.

### Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche, ou un administrateur de SVM à qui l'administrateur du cluster a délégué des pouvoirs.

### Étape

1. Pour désactiver le chiffrement par défaut pour l'ensemble du cluster dans ONTAP 9.7 ou version ultérieure, exécutez la commande suivante :

```
options -option-name encryption.data_at_rest_encryption.disable_by_default
-option-value on
```

## Activez le modèle « zéro confiance »

### NetApp et le modèle « zéro confiance »

La solution « zéro confiance » s'est traditionnellement orientée réseau pour structurer les microsegments et le périmètre (MCAP) afin de protéger les données, les services, les applications ou les ressources grâce à des contrôles appelés « passerelle de segmentation ». NetApp ONTAP adopte une approche « zéro confiance » centrée sur les données, dans laquelle le système de gestion du stockage devient la passerelle de segmentation pour protéger et surveiller l'accès aux données de nos clients. Le moteur « zéro confiance » FPolicy et l'écosystème de partenaires FPolicy deviennent un centre de contrôle pour obtenir une compréhension détaillée des modèles d'accès aux données normaux et aberrants et identifier les menaces internes.



À partir de juillet 2024, le contenu du rapport technique *TR-4829: NetApp et Zero Trust: Activation d'un modèle Zero Trust axé sur les données*, précédemment publié en format PDF, a été intégré au reste de la documentation produit de ONTAP.

Les données constituent les ressources les plus importantes de votre entreprise. Selon le 2022 , les menaces internes sont la cause de 18 % des violations de données "[Rapport d'enquête sur les violations de données Verizon](#)". Les entreprises peuvent améliorer leur vigilance en déployant des contrôles « zéro confiance » de pointe sur les données à l'aide du logiciel de gestion des données NetApp ONTAP.

### Qu'est-ce que le principe zéro confiance ?

Le modèle Zero Trust a été développé pour la première fois par [John Kindervag^] de Forrester Research. Le service informatique envisage la sécurité du réseau de l'intérieur vers l'extérieur plutôt que de l'extérieur vers l'intérieur. L'approche « zéro confiance » de l'intérieur identifie un micronoyau et un périmètre (MCAP). Le MCAP est une définition intérieure des données, des services, des applications et des ressources à protéger avec un ensemble complet de contrôles. Le concept de périmètre extérieur sécurisé est obsolète. Les entités fiables et autorisées à s'authentifier avec succès via le périmètre peuvent alors rendre l'organisation vulnérable aux attaques. Les initiés, par définition, sont déjà à l'intérieur du périmètre sécurisé. Les employés, prestataires et partenaires sont des initiés, et ils doivent être autorisés à opérer avec des contrôles appropriés pour remplir leurs rôles au sein de l'infrastructure de votre entreprise.

Zéro confiance a été mentionné comme une technologie qui offre une promesse au DoD en septembre 2019 "[FY19-23 Stratégie de modernisation numérique du Département de la Défense des États-Unis](#)". Le modèle « zéro confiance » est défini comme « Une stratégie de cybersécurité qui intègre la sécurité dans l'ensemble de l'architecture dans le but d'enrayer les fuites de données. Ce modèle de sécurité centré sur les données élimine l'idée de réseaux, périphériques, rôles ou processus fiables ou non approuvés, et passe à des niveaux

de confiance basés sur plusieurs attributs qui activent des stratégies d'authentification et d'autorisation dans le concept d'accès le moins privilégié. Pour mettre en œuvre la technologie « zéro confiance », il est nécessaire de repenser la façon dont nous utilisons l'infrastructure existante pour mettre en œuvre la sécurité en simplifiant et en améliorant l'efficacité tout en assurant la continuité des opérations. »

En août 2020, le NIST a publié "[Architecture Zero Trust Pub 800-207 spéciale](#)" (ZTA). ZTA se concentre sur la protection des ressources, et non des segments de réseau, car l'emplacement du réseau n'est plus considéré comme le composant principal de la posture de sécurité de la ressource. Les ressources sont des données et de l'informatique. Les stratégies ZTA sont destinées aux architectes de réseaux d'entreprise. ZTA présente une nouvelle terminologie issue des concepts originaux de Forrester. Les mécanismes de protection appelés le point de décision de la politique (PDP) et le point d'application de la politique (PEP) sont analogues à une passerelle de segmentation Forrester. ZTA présente quatre modèles de déploiement :

- Déploiement basé sur un agent ou une passerelle
- Déploiement basé sur l'enclave (un peu similaire au MCAP de Forrester)
- Déploiement sur portail de ressources
- Sandbox d'application de périphérique

Pour les besoins de cette documentation, nous utilisons les concepts et la terminologie de Forrester Research plutôt que le NIST ZTA.

## Ressources de sécurité

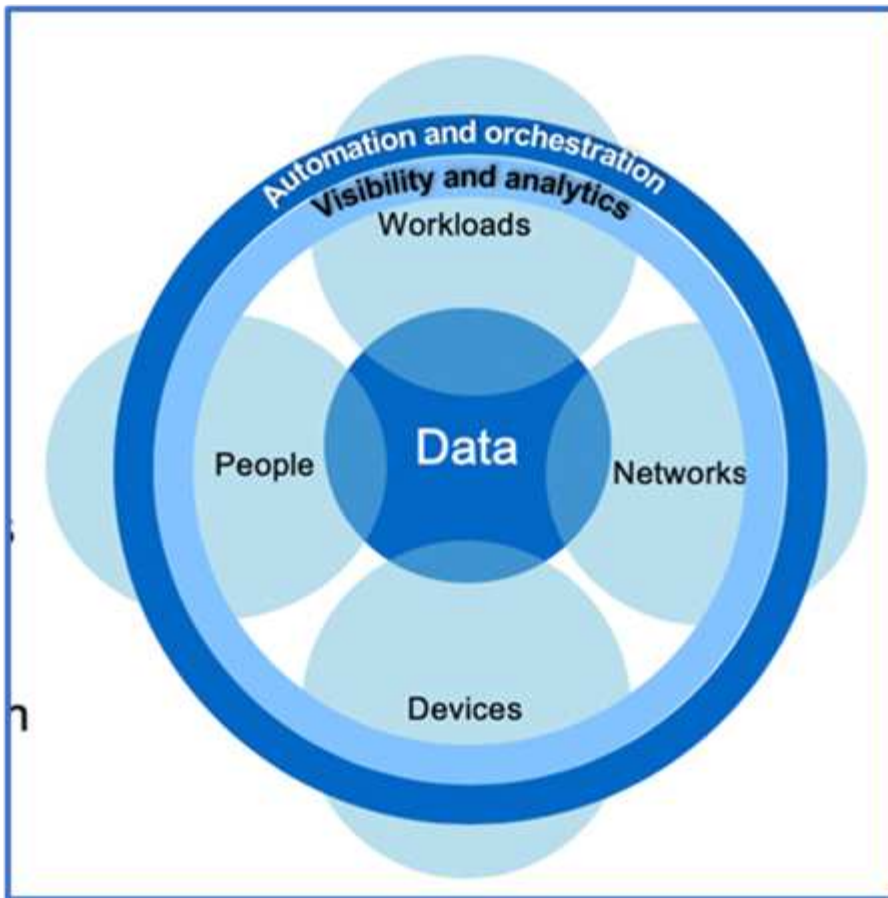
Pour plus d'informations sur le signalement de vulnérabilités et d'incidents, les réponses de sécurité NetApp et la confidentialité des clients, consultez le "[Portail de sécurité NetApp](#)".

## Concevez une approche « zéro confiance » centrée sur les données avec ONTAP

Un réseau « zéro confiance » est défini par une approche centrée sur les données dans laquelle les contrôles de sécurité doivent être aussi proches que possible des données. Les fonctionnalités de ONTAP, associées à l'écosystème de partenaires NetApp FPolicy, peuvent fournir les contrôles nécessaires au modèle « zéro confiance » centré sur les données.

ONTAP est le logiciel de gestion des données riche en fonctions de sécurité de NetApp, et le moteur « zéro confiance » FPolicy est une fonctionnalité ONTAP de pointe qui offre une interface de notification d'événements granulaire et basée sur des fichiers. Les partenaires NetApp FPolicy peuvent utiliser cette interface pour obtenir un niveau d'éclairage plus élevé de l'accès aux données dans ONTAP.





### **Concevez un MCAP « zéro confiance » centré sur les données**

Pour concevoir un MCAP Zero Trust axé sur les données, procédez comme suit :

1. Identifiez l'emplacement de toutes les données de l'entreprise.
2. Classez vos données.
3. Supprimez en toute sécurité les données dont vous n'avez plus besoin.
4. Comprenez quels rôles doivent avoir accès aux classifications de données.
5. Appliquez le principe du privilège minimum pour appliquer les contrôles d'accès.
6. Utilisez l'authentification multifacteur pour l'accès administratif et l'accès aux données.
7. Utilisez le chiffrement pour les données au repos et en transit.
8. Contrôlez et consignez tous les accès.
9. Alerte les accès suspects ou les comportements à adopter.

#### **Identifiez l'emplacement de toutes les données de l'entreprise**

La fonctionnalité FPolicy de ONTAP associée à l'écosystème de partenaires Alliance NetApp de FPolicy vous permet d'identifier l'emplacement des données de votre entreprise et les personnes qui y ont accès. Cette opération est effectuée à l'aide d'une analyse comportementale des utilisateurs qui identifie si les modèles d'accès aux données sont valides. Pour plus d'informations sur l'analyse comportementale des utilisateurs, reportez-vous à la section contrôle et journalisation de tous les accès. Si vous ne comprenez pas où se trouvent vos données et qui y a accès, l'analyse comportementale des utilisateurs peut fournir une base pour établir une classification et une politique à partir d'observations empiriques.

## Classez vos données

Dans la terminologie du modèle zéro confiance, la classification des données implique l'identification des données toxiques. Les données toxiques sont des données sensibles qui ne sont pas destinées à être exposées à l'extérieur d'une organisation. La divulgation de données toxiques peut contrevenir aux règlements et nuire à la réputation d'une entreprise. En termes de conformité réglementaire, les données toxiques incluent les données de titulaire de carte pour l' "[Norme de sécurité de l'industrie des cartes de paiement \(PCI-DSS\)](#)", les données personnelles pour l' UE "[Règlement général sur la protection des données \(RGPD\)](#)" ou les données de santé pour l' "[Loi américaine sur la transférabilité et la responsabilité en matière d'assurance maladie \(HIPAA\)](#)". Utilisez NetApp "[Classification BlueXP](#)" (anciennement Cloud Data Sense), un kit d'outils piloté par l'IA, pour analyser, analyser et catégoriser automatiquement vos données.

## Supprimez les données dont vous n'avez plus besoin en toute sécurité

Une fois les données de votre entreprise classifiées, vous pouvez découvrir que certaines de vos données ne sont plus nécessaires ou pertinentes pour le fonctionnement de votre entreprise. La conservation de données inutiles est une responsabilité et ces données doivent être supprimées. Pour obtenir un mécanisme avancé d'effacement cryptographique des données, consultez la description de la suppression sécurisée dans le chiffrement des données au repos.

## Comprendre quels rôles doivent avoir accès aux classifications de données et appliquer le principe du privilège minimum pour appliquer les contrôles d'accès

Mapper l'accès aux données sensibles et appliquer le principe du privilège minimum implique de donner aux personnes de votre entreprise l'accès aux seules données requises pour accomplir leur travail. Ce processus implique le contrôle d'accès basé sur les rôles ("[RBAC](#)"), qui s'applique à l'accès aux données et à l'accès administratif.

Avec ONTAP, un SVM (Storage Virtual machine) peut être utilisé pour segmenter l'accès aux données de l'entreprise par les locataires au sein d'un cluster ONTAP. Le RBAC peut être appliqué à l'accès aux données ainsi qu'à l'accès administratif à la SVM. Le RBAC peut également être appliqué au niveau administratif du cluster.

En plus de RBAC, vous pouvez utiliser ONTAP "[vérification multiadministrateur](#)" (MAV) pour demander à un ou plusieurs administrateurs d'approuver des commandes telles que `volume delete` ou `volume snapshot delete`. Une fois MAV activé, la modification ou la désactivation de MAV nécessite l'approbation de l'administrateur MAV.

ONTAP est une autre façon de protéger les copies Snapshot "[Verrouillage des copies Snapshot](#)". Le verrouillage des copies Snapshot est une fonctionnalité SnapLock qui permet de rendre les copies Snapshot indélébiles, manuellement ou automatiquement, avec une période de conservation définie sur la règle de copie Snapshot du volume. Le verrouillage des copies Snapshot est également appelé verrouillage inviolable des copies Snapshot. L'objectif du verrouillage des copies Snapshot est d'empêcher les administrateurs peu scrupuleux ou non approuvés de supprimer les copies Snapshot sur les systèmes ONTAP primaires et secondaires. Il est possible d'effectuer une restauration rapide des copies Snapshot verrouillées sur des systèmes primaires afin de restaurer les volumes corrompus par des ransomwares.

## Utilisez l'authentification multifacteur pour l'accès administratif et l'accès aux données

Outre le RBAC d'administration de cluster, "[Authentification multifacteur \(MFA\)](#)" peut être déployé pour l'accès administratif web ONTAP et l'accès à la ligne de commande SSH (Secure Shell). L'authentification multifacteur en matière d'accès administratif est obligatoire pour les organisations du secteur public américain ou celles qui doivent suivre la norme PCI-DSS. L'authentification multifacteur empêche un attaquant de compromettre un compte en utilisant uniquement un nom d'utilisateur et un mot de passe. L'authentification MFA nécessite au moins deux facteurs indépendants. Un exemple d'authentification à deux facteurs est quelque chose qu'un

utilisateur possède, comme une clé privée, et quelque chose qu'un utilisateur sait, comme un mot de passe. L'accès administratif Web à ONTAP System Manager ou à ActiveIQ Unified Manager est activé par le langage SAML (Security assertion Markup Language) 2.0. L'accès en ligne de commande SSH utilise une authentification à deux facteurs chaînée avec une clé publique et un mot de passe.

Vous pouvez contrôler l'accès des utilisateurs et des machines via des API dotées des fonctionnalités de gestion des identités et des accès de ONTAP :

- Utilisateur :
  - **Authentification et autorisation.** Grâce aux fonctionnalités de protocole NAS pour SMB et NFS.
  - **Vérification.** Syslog d'accès et d'événements. Une journalisation d'audit détaillée du protocole CIFS pour tester les règles d'authentification et d'autorisation. Audit précis et granulaire de l'accès NAS détaillé dans FPolicy au niveau des fichiers.
- Périphérique :
  - **Authentification.** Authentification basée sur certificat pour l'accès à l'API.
  - **Autorisation.** Contrôle d'accès basé sur des rôles (RBAC) par défaut ou personnalisé.
  - **Vérification.** Syslog de toutes les actions entreprises.

Utilisez le chiffrement pour les données au repos et en transit

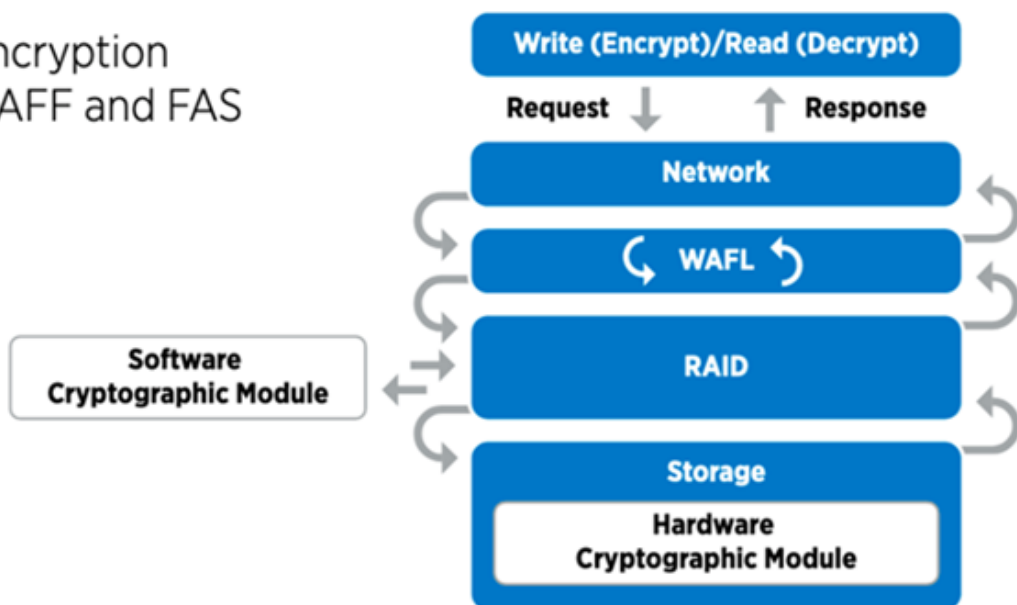
### Chiffrement des données au repos

Chaque jour, lorsqu'une entreprise réutilise des disques, renvoie des disques défectueux ou effectue des mises à niveau vers des disques de plus grande capacité, elle doit satisfaire de nouvelles exigences afin de réduire les risques liés aux systèmes de stockage et les écarts d'infrastructure. En tant qu'administrateurs et opérateurs de ressources de données, les ingénieurs du stockage doivent gérer et maintenir les données en toute sécurité tout au long de leur cycle de vie. "[Chiffrement de stockage NetApp \(NSE\) ;#44 ; NetApp Volume Encryption \(NVE\) ;#44 ; et chiffrement d'agrégat NetApp](#)" vous aider à chiffrer toutes vos données au repos en permanence, qu'elles soient toxiques ou non, et sans affecter les opérations quotidiennes. "[NSE](#)" Est une solution matérielle ONTAP "[données au repos](#)" qui utilise des disques auto-cryptés conformes à la norme FIPS 140-2 de niveau 2. "[NVE et NAE](#)" Sont une solution logicielle ONTAP "[données au repos](#)" qui utilise le "[Module cryptographique NetApp conforme à la norme FIPS 140-2 de niveau 1](#)". Avec NVE et NAE, vous pouvez utiliser des disques durs ou des disques SSD pour le chiffrement des données au repos. De plus, les disques NSE peuvent être utilisés pour fournir une solution de chiffrement à plusieurs couches native qui assure la redondance du chiffrement et une sécurité supplémentaire. Si l'une des couches est rompue, la seconde couche sécurise toujours les données. Ces fonctionnalités font de ONTAP une solution bien positionnée pour "[chiffrement prêt pour le quantum](#)".

NVE propose également une fonctionnalité appelée "[suppression sécurisée](#)" qui supprime de manière cryptographique les données toxiques des fuites de données lorsque les fichiers sensibles sont écrits sur un volume non classifié.

Soit le "[Gestionnaire de clés intégré Onboard Key Manager \(OKM\)](#)", qui est le gestionnaire de clés intégré dans ONTAP, soit un "[approuvée](#)" tiers "[gestionnaires de clés externes](#)" peut être utilisé avec NSE et NVE pour stocker des clés en toute sécurité.

## Two-layer encryption solution for AFF and FAS



Comme le montre la figure ci-dessus, le chiffrement matériel et logiciel peut être combiné. Cette fonctionnalité a permis à l' ["Validation de ONTAP dans les solutions commerciales de la NSA pour le programme classifié"](#) de stocker des données les plus secrètes.

### Chiffrement des données à la volée

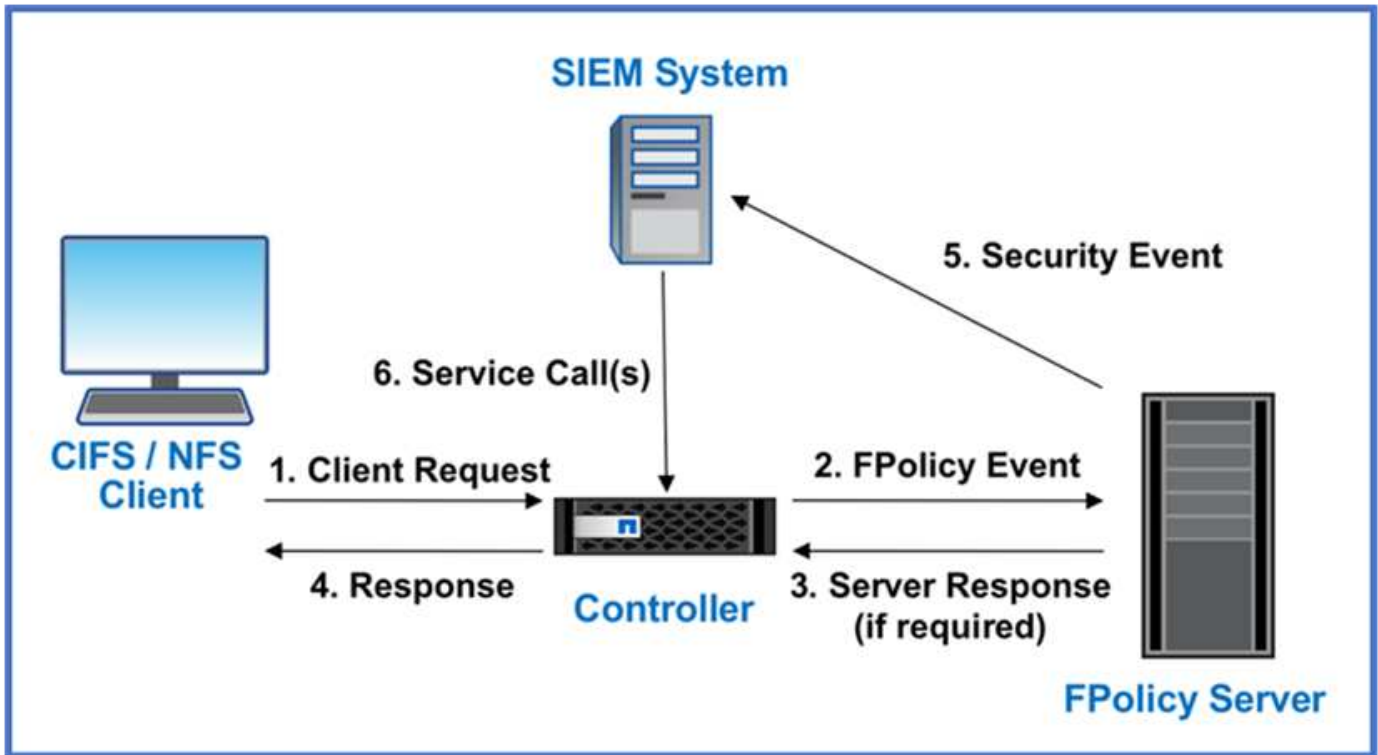
Le chiffrement des données à la volée ONTAP protège l'accès aux données utilisateur et l'accès au plan de contrôle. L'accès aux données utilisateur peut être chiffré par chiffrement SMB 3.0 pour l'accès aux partages Microsoft CIFS ou par krb5P pour NFS Kerberos 5. L'accès aux données utilisateur peut également être chiffré avec ["IPSec"](#) pour CIFS, NFS et iSCSI. L'accès au plan de contrôle est chiffré avec TLS (transport Layer Security). ONTAP fournit ["FIPS"](#) le mode de conformité pour l'accès au plan de contrôle, qui active les algorithmes approuvés FIPS et désactive les algorithmes non approuvés FIPS. La réplication des données est chiffrée avec ["chiffrement des pairs de cluster"](#). Cela assure le cryptage pour les technologies ONTAP SnapVault et SnapMirror.

### Contrôlez et consignez tous les accès

Une fois les règles RBAC en place, vous devez déployer des fonctionnalités actives de surveillance, d'audit et d'alerte. Le moteur « zéro confiance » FPolicy de NetApp ONTAP, couplé au ["Écosystème de partenaires NetApp FPolicy"](#), fournit les contrôles nécessaires au modèle « zéro confiance » centré sur les données. NetApp ONTAP est un logiciel de gestion des données riche en fonctions de sécurité. Il ["FPolicy"](#) s'agit d'une fonctionnalité ONTAP de pointe qui offre une interface de notification d'événements granulaire basée sur des fichiers. Les partenaires NetApp FPolicy peuvent utiliser cette interface pour obtenir un niveau d'éclairage plus élevé de l'accès aux données dans ONTAP. La fonctionnalité FPolicy de ONTAP, associée à l'écosystème de partenaires Alliance NetApp de FPolicy, vous permet d'identifier l'emplacement et l'accès aux données de votre entreprise. Cette opération est effectuée à l'aide d'une analyse comportementale des utilisateurs qui identifie si les modèles d'accès aux données sont valides. L'analyse comportementale des utilisateurs peut être utilisée pour alerter l'utilisateur en cas d'accès aux données suspect ou aberrant qui ne correspond pas au modèle normal et, si nécessaire, prendre des mesures pour refuser l'accès.

Les partenaires FPolicy vont au-delà de l'analyse comportementale des utilisateurs et s'orientent vers le machine learning (ML) et l'intelligence artificielle (IA) pour assurer la fidélité des événements et réduire le nombre de faux positifs, voire de faux positifs. Tous les événements doivent être consignés sur un serveur

syslog ou sur un système de gestion des informations et des événements de sécurité (SIEM) pouvant également utiliser le ML et l'IA.



La solution Storage Workload Security de NetApp (anciennement appelée "Cloud Secure") utilise l'interface FPolicy et l'analytique comportementale des utilisateurs sur les systèmes de stockage ONTAP dans le cloud et sur site pour vous fournir des alertes en temps réel sur les comportements malveillants des utilisateurs. Storage Workload Security protège les données de l'entreprise contre les activités abusives ou les usurpations d'identité à l'aide de fonctionnalités avancées de machine learning et de détection des anomalies. Storage Workload Security : identifie les attaques par ransomware ou d'autres comportements malveillants, invoque les copies Snapshot et met en quarantaine les utilisateurs malveillants. Storage Workload Security dispose également d'une fonctionnalité d'analyse permettant de visualiser en détail les activités des utilisateurs et des entités. La sécurité des workloads de stockage fait partie de NetApp Cloud Insights.

Outre la sécurité des workloads de stockage, ONTAP dispose d'une fonctionnalité intégrée de détection des ransomwares appelée "Protection autonome contre les ransomwares" ARP. ARP utilise le machine learning pour déterminer si une activité anormale sur les fichiers indique qu'une attaque par ransomware est en cours, puis appelle une copie Snapshot et une alerte aux administrateurs. Storage Workload Security s'intègre à ONTAP pour recevoir des événements ARP et fournit une couche supplémentaire d'analytique et de réponses automatiques.

## Contrôles d'orchestration et d'automatisation de la sécurité NetApp externes à ONTAP

L'automatisation vous permet d'effectuer un processus ou une procédure avec une assistance humaine minimale. L'automatisation permet aux entreprises d'étendre les déploiements « zéro confiance » bien au-delà des procédures manuelles pour se défendre contre les activités imcretes également automatisées.

Ansible est un outil open source de provisionnement logiciel, de gestion de la configuration et de déploiement des applications. Il fonctionne sur de nombreux systèmes Unix et peut configurer à la fois les systèmes Unix et Microsoft Windows. Il comprend son propre langage déclaratif pour décrire la configuration du système.

Ansible a été écrit par Michael DeHaan et acquis par Red Hat en 2015. Ansible se connecte temporairement à distance sans agent via SSH ou Windows Remote Management (permettant l'exécution à distance de PowerShell). NetApp a développé plus de "[150 modules Ansible pour le logiciel ONTAP](#)", permettant une intégration supplémentaire avec la structure d'automatisation Ansible. Les modules Ansible pour NetApp fournissent un ensemble d'instructions sur la manière de définir l'état souhaité et de le relayer vers l'environnement NetApp cible. Les modules sont conçus pour prendre en charge des tâches telles que la configuration de licences, la création d'agrégats et de machines virtuelles de stockage, la création de volumes et la restauration de snapshots, pour n'en nommer que quelques-uns. Un rôle Ansible a été "[Publié sur GitHub](#)" spécifique au guide de déploiement des fonctionnalités unifiées du Ministère de la Défense NetApp.

Avec la bibliothèque de modules disponibles, les utilisateurs peuvent facilement développer des playbooks Ansible et les personnaliser en fonction de leurs propres applications et des besoins de l'entreprise pour automatiser des tâches courantes. Une fois qu'un PlayBook est écrit, vous pouvez l'exécuter pour exécuter la tâche spécifiée, ce qui permet de gagner du temps et d'améliorer la productivité. NetApp a créé et partagé des exemples de playbooks pouvant être utilisés directement ou personnalisés en fonction de vos besoins.

Cloud Insights est un outil de surveillance de l'infrastructure qui permet de bénéficier d'une grande visibilité sur l'ensemble de l'infrastructure. Avec Cloud Insights, vous pouvez surveiller et optimiser toutes les ressources et résoudre les problèmes, y compris dans les instances de cloud public et dans vos data centers privés. Cloud Insights réduit le délai moyen de résolution de 90 % et empêche 80 % des problèmes cloud d'affecter les utilisateurs finaux. Il permet également de réduire de 33 % en moyenne les coûts de l'infrastructure cloud et de réduire l'exposition aux menaces internes en protégeant les données à l'aide d'informations exploitables. La fonctionnalité de sécurité des workloads de stockage d'Cloud Insights permet d'analyser le comportement des utilisateurs avec l'IA et LE ML afin d'alerter les utilisateurs en cas de comportements anormaux liés à une menace interne. Pour ONTAP, Storage Workload Security utilise le moteur FPolicy « zéro confiance ».

## **Zero Trust et déploiements de cloud hybride**

NetApp est la référence en matière de gestion des données dans le cloud hybride. NetApp propose diverses options d'extension des systèmes de gestion des données sur site au cloud hybride avec Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) et les principaux fournisseurs. Les solutions de cloud hybride NetApp prennent en charge les mêmes contrôles de sécurité « zéro confiance » que ceux disponibles avec les systèmes ONTAP sur site et le stockage Software-defined ONTAP Select.

Vous pouvez facilement étendre la capacité des clouds publics sans contraintes classiques de dépenses d'investissement en utilisant NetApp Cloud Volumes Service, le premier service de fichiers cloud haute performance pour AWS et GCP, et Azure NetApp Files pour Microsoft Azure. Idéales pour les charges de travail qui exploitent les données de manière intensive, telles que l'analytique et le DevOps, ces services cloud associent un stockage à la demande flexible de NetApp à la gestion des données ONTAP dans une offre entièrement gérée.

Pour ceux qui recherchent des services de données avancés pour les services de stockage bloc dans le cloud ou objet, tels que AWS EBS et S3 ou le stockage Azure, Cloud Volumes ONTAP assure la gestion des données entre votre environnement sur site et le cloud public avec une seule vue commune. Exécuté dans AWS ou Azure en tant qu'instance à la demande, Cloud Volumes ONTAP fournit l'efficacité du stockage, la disponibilité et l'évolutivité du logiciel ONTAP. ONTAP permet de déplacer les données entre vos systèmes ONTAP sur site et votre environnement de stockage AWS ou Azure grâce au logiciel de réplication des données NetApp SnapMirror.



# Protection des données et reprise d'activité

## Cluster et SVM peering

### Présentation du cluster et de SVM peering

Il est possible de créer des relations entre les clusters source et de destination et entre les machines virtuelles de stockage source et de destination. Vous devez créer des relations de pairs entre ces entités avant de répliquer des copies Snapshot à l'aide de SnapMirror.

ONTAP 9.3 apporte des améliorations qui simplifient la configuration des relations entre les clusters et les SVM. Les procédures de peering de clusters et de SVM sont disponibles pour toutes les versions de ONTAP 9. Utilisez la procédure appropriée pour votre version de ONTAP.

Vous effectuez les procédures à l'aide de l'interface de ligne de commandes, et non de System Manager ou d'un outil de script automatisé.

### Préparation du cluster et de la SVM peering

#### Bases du peering

Vous devez créer des relations *peer* entre les clusters source et de destination, et entre les SVM source et destination avant de pouvoir répliquer les copies Snapshot à l'aide de SnapMirror. Une relation de type peer-to-peer définit les connexions réseau qui permettent aux clusters et aux SVM d'échanger les données de manière sécurisée.

Les clusters et les SVM dans des relations entre pairs communiquent sur le réseau intercluster à l'aide de *interfaces logiques (LIF) intercluster*. une LIF intercluster est une LIF qui prend en charge le service d'interface réseau « intercluster-core » et qui est généralement créée en utilisant la politique de service d'interface réseau « default-intercluster ». On doit créer des LIF intercluster sur chaque nœud des clusters en cours de peering.

Les LIFs intercluster utilisent des routes qui appartiennent au SVM système auquel elles sont assignées. ONTAP crée automatiquement un SVM système pour les communications au niveau du cluster au sein d'un IPspace.

Les topologies en mode « Fan-Out » et en cascade sont toutes deux prises en charge. Dans une topologie en cascade, il suffit de créer des réseaux intercluster entre les clusters principal et secondaire, et entre les clusters secondaire et tertiaire. Il n'est pas nécessaire de créer un réseau intercluster entre le cluster principal et le cluster tertiaire.



Il est possible (mais pas conseillé) à un administrateur de supprimer le service intercluster de la politique de service default-intercluster. Dans ce cas, les LIFs créées à l'aide de « Default-intercluster » ne seront en fait pas des LIFs intercluster. Pour vérifier que la politique de service par défaut-intercluster contient le service intercluster-core, utiliser la commande suivante :

```
network interface service-policy show -policy default-intercluster
```

## Conditions préalables au peering de clusters

Avant de configurer le peering de cluster, vous devez vérifier que la connectivité, le port, l'adresse IP, le sous-réseau, le pare-feu, et les exigences de nommage des clusters sont respectées.



À partir de ONTAP 9.6, Cluster peering fournit par défaut la prise en charge du chiffrement TLS 1.2 AES-256 GCM pour la réplication des données. Les chiffrements de sécurité par défaut (« PSK-AES256-GCM-SHA384 ») sont requis pour que le chiffrement de cluster fonctionne même si le chiffrement est désactivé.

À partir de ONTAP 9.11.1, les chiffrements de sécurité DHE-PSK sont disponibles par défaut.

À partir de ONTAP 9.15.1, Cluster peering assure par défaut la prise en charge du chiffrement TLS 1.3 pour la réplication des données.

### Les besoins en connectivité

Chaque LIF intercluster du cluster local doit pouvoir communiquer avec chaque LIF intercluster sur le cluster distant.

Bien qu'il ne soit pas nécessaire, il est généralement plus simple de configurer les adresses IP utilisées pour les LIF intercluster dans le même sous-réseau. Les adresses IP peuvent résider dans le même sous-réseau que les LIF de données ou dans un autre sous-réseau. Le sous-réseau utilisé dans chaque cluster doit respecter les exigences suivantes :

- Le sous-réseau doit appartenir au broadcast domain qui contient les ports utilisés pour la communication intercluster.
- Le sous-réseau doit disposer de suffisamment d'adresses IP disponibles pour allouer à une LIF intercluster par nœud.

Par exemple, dans un cluster à quatre nœuds, le sous-réseau utilisé pour la communication intercluster doit disposer de quatre adresses IP disponibles.

Chaque nœud doit disposer d'un LIF intercluster avec une adresse IP sur le réseau intercluster.

Les LIF intercluster peuvent disposer d'une adresse IPv4 ou IPv6.



ONTAP vous permet de migrer vos réseaux de peering depuis IPv4 vers IPv6 en autorisant éventuellement la présence des deux protocoles simultanément sur les LIF intercluster. Dans les versions précédentes, toutes les relations intercluster pour un cluster entier étaient au format IPv4 ou IPv6. Cela signifiait que le changement de protocole était potentiellement source de perturbation.

### Configuration requise pour les ports

Vous pouvez utiliser des ports dédiés pour la communication intercluster ou partager les ports utilisés par le réseau de données. Les ports doivent répondre aux exigences suivantes :

- Tous les ports utilisés pour communiquer avec un cluster distant donné doivent se trouver dans le même IPspace.

Vous pouvez utiliser plusieurs IPspaces pour gérer plusieurs clusters dans un même cluster. Une



connectivité à maillage complet par paire est requise uniquement au sein d'un IPspace.

- Le broadcast domain utilisé pour la communication intercluster doit inclure au moins deux ports par nœud afin que la communication intercluster puisse basculer d'un port vers un autre.

Les ports ajoutés à un domaine de diffusion peuvent être des ports réseau physiques, des VLAN ou des groupes d'interfaces (ifgrps).

- Tous les ports doivent être câblés.
- Tous les ports doivent être en état de santé.
- Les paramètres MTU des ports doivent être cohérents.

#### Exigences relatives au pare-feu



Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "[Configuration des politiques de pare-feu pour les LIF](#)".

Les pare-feu et la politique de pare-feu intercluster doivent autoriser les protocoles suivants :

- Trafic ICMP bidirectionnel
- Le trafic TCP initié bidirectionnel vers les adresses IP de toutes les LIFs intercluster sur les ports 11104 et 11105
- HTTPS bidirectionnel entre les LIFs intercluster

Bien que HTTPS n'est pas requis lors de la configuration du peering de clusters à l'aide de l'interface de ligne de commande, HTTPS est requis plus tard si vous utilisez System Manager pour configurer la protection des données.

La valeur par défaut `intercluster` La politique de pare-feu permet l'accès via le protocole HTTPS et à partir de toutes les adresses IP (0.0.0.0/0). Vous pouvez modifier ou remplacer la stratégie si nécessaire.

#### Regroupement des clusters

Les clusters doivent répondre aux exigences suivantes :

- Un cluster ne peut pas se trouver dans une relation entre pairs et plus de 255 clusters.

#### Utiliser des ports partagés ou dédiés

Vous pouvez utiliser des ports dédiés pour la communication intercluster ou partager les ports utilisés par le réseau de données. Lors de la décision de partager des ports, vous devez tenir compte de la bande passante du réseau, de l'intervalle de réplication et de la disponibilité des ports.



Vous pouvez partager les ports sur un cluster en utilisant des ports dédiés sur l'autre.

#### La bande passante du réseau

Si vous disposez d'un réseau haut débit (par exemple 10 GbE), vous disposez peut-être d'une bande passante LAN locale suffisante pour effectuer la réplication à l'aide des mêmes ports 10 GbE utilisés pour l'accès aux

données.

Vous devriez même comparer votre bande passante WAN disponible à celle de votre réseau local. Si la bande passante WAN disponible est bien inférieure à 10 GbE, vous devrez peut-être utiliser des ports dédiés.



À l'exception de cette règle, on peut trouver lorsque tous les nœuds du cluster répliquent des données, auquel cas l'utilisation de la bande passante est généralement répartie entre ces nœuds.

Si vous n'utilisez pas de ports dédiés, la taille de l'unité de transmission maximale (MTU) du réseau de réplication doit généralement être identique à la taille de MTU du réseau de données.

### Intervalle de réplication

Si la réplication se déroule en dehors des heures de pointe, vous devriez pouvoir utiliser des ports de données pour la réplication, même sans connexion LAN 10 GbE.

Si la réplication a lieu pendant les heures de bureau, vous devez tenir compte de la quantité de données à répliquer et de la quantité de bande passante nécessaire pour créer des conflits avec les protocoles de données. Si l'utilisation du réseau par les protocoles de données (SMB, NFS, iSCSI) est supérieure à 50 %, il est recommandé d'utiliser des ports dédiés pour la communication intercluster afin de permettre des performances non dégradées en cas de basculement du nœud.

### Disponibilité du port

Si vous déterminez que le trafic de réplication interfère sur le trafic de données, vous pouvez migrer des LIFs intercluster vers n'importe quel autre port partagé intercluster sur le même nœud.

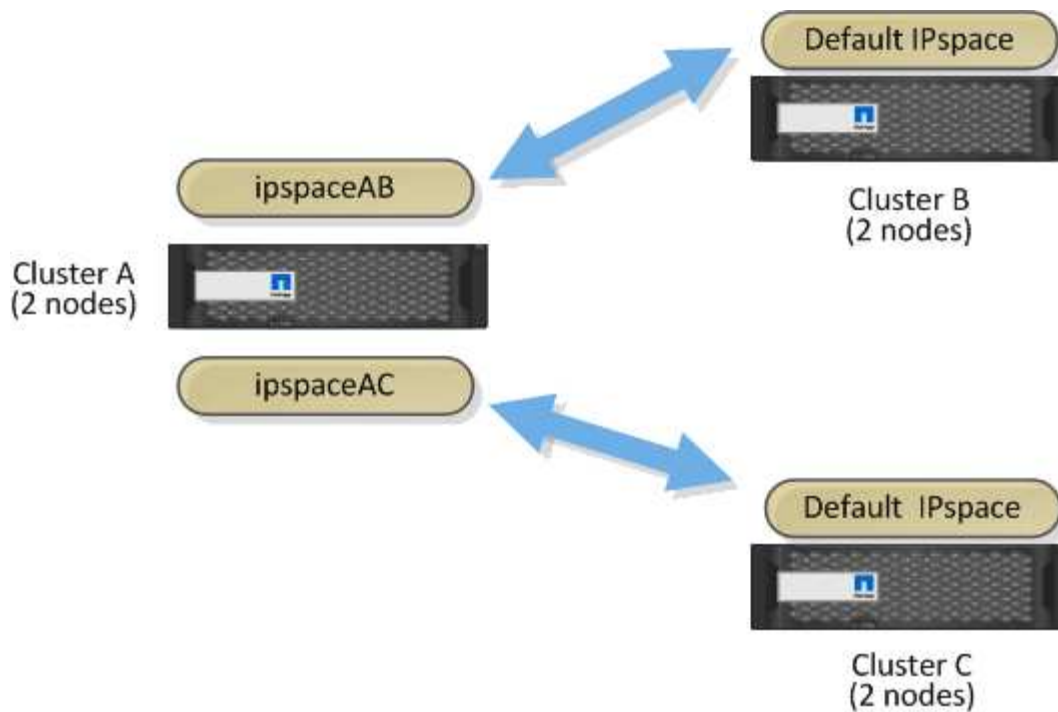
Vous pouvez également dédier des ports VLAN à la réplication. La bande passante du port est partagée entre tous les VLAN et le port de base.

### Utilisez les IPspaces personnalisés pour isoler le trafic de réplication

Vous pouvez utiliser des IPspaces personnalisés pour séparer les interactions d'un cluster avec ses pairs. Appelée *connectivité intercluster désignée*, cette configuration permet aux fournisseurs de services d'isoler le trafic de réplication dans des environnements mutualisés.

Supposons, par exemple, que vous souhaitez que le trafic de réplication entre le Cluster A et le Cluster B soit séparé du trafic de réplication entre le Cluster A et le Cluster C. Pour ce faire, vous pouvez créer deux IPspaces sur le Cluster A.

Un IPspace contient les LIF intercluster que vous utilisez pour communiquer avec le Cluster B. L'autre contient les LIFs intercluster que vous utilisez pour communiquer avec le Cluster C, comme indiqué sur l'illustration suivante.



Pour une configuration IPspace personnalisée, consultez le *Network Management Guide*.

## Configurer les LIFs intercluster

### Configurer les LIFs intercluster sur des ports data partagés

Vous pouvez configurer les LIFs intercluster sur des ports partagés avec le réseau de données. Cela réduit le nombre de ports nécessaires pour la mise en réseau intercluster.

#### Étapes

1. Lister les ports dans le cluster :

```
network port show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant montre les ports réseau dans `cluster01`:

```
cluster01::> network port show
```

|              |       |         |                  |       |       | Speed      |
|--------------|-------|---------|------------------|-------|-------|------------|
| (Mbps)       |       |         |                  |       |       |            |
| Node         | Port  | IPspace | Broadcast Domain | Link  | MTU   | Admin/Oper |
| -----        | ----- | -----   | -----            | ----- | ----- |            |
| cluster01-01 |       |         |                  |       |       |            |
|              | e0a   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0b   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0c   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0d   | Default | Default          | up    | 1500  | auto/1000  |
| cluster01-02 |       |         |                  |       |       |            |
|              | e0a   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0b   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0c   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0d   | Default | Default          | up    | 1500  | auto/1000  |

2. Créer des LIF intercluster sur un SVM admin (IPspace par défaut) ou un SVM système (IPspace personnalisé) :

| Option                                         | Description                                                                                                                                                                                                                |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Dans ONTAP 9.6 et plus tard:</b>            | <code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -service -policy default-intercluster -home -node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></code> |
| <b>Dans ONTAP 9.5 et versions antérieures:</b> | <code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -role intercluster -home-node <i>node</i> -home -port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></code>                    |

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création de LIFs intercluster `cluster01_icl01` et `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

### 3. Vérifier que les LIFs intercluster ont été créés :

| Option                                         | Description                                                              |
|------------------------------------------------|--------------------------------------------------------------------------|
| <b>Dans ONTAP 9.6 et plus tard:</b>            | <code>network interface show -service-policy default-intercluster</code> |
| <b>Dans ONTAP 9.5 et versions antérieures:</b> | <code>network interface show -role intercluster</code>                   |

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).

```
cluster01::> network interface show -service-policy default-intercluster
```

|            | Logical         | Status     | Network          | Current          |
|------------|-----------------|------------|------------------|------------------|
| Current Is |                 |            |                  |                  |
| Vserver    | Interface       | Admin/Oper | Address/Mask     | Node             |
| Home       |                 |            |                  | Port             |
| cluster01  | cluster01_icl01 | up/up      | 192.168.1.201/24 | cluster01-01 e0c |
| true       | cluster01_icl02 | up/up      | 192.168.1.202/24 | cluster01-02 e0c |
| true       |                 |            |                  |                  |

### 4. Vérifier que les LIFs intercluster sont redondants :

| Option                                  | Description                                                           |
|-----------------------------------------|-----------------------------------------------------------------------|
| Dans ONTAP 9.6 et plus tard:            | network interface show -service-policy default-intercluster -failover |
| Dans ONTAP 9.5 et versions antérieures: | network interface show -role intercluster -failover                   |

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant indique que les LIFs intercluster `cluster01_icl01` et `cluster01_icl02` sur le `e0c` le port basculera vers le `e0d` port.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

| Vserver          | Logical<br>Interface | Home<br>Node:Port | Failover<br>Policy                                      | Failover<br>Group |
|------------------|----------------------|-------------------|---------------------------------------------------------|-------------------|
| cluster01        | cluster01_icl01      | cluster01-01:e0c  | local-only                                              |                   |
| 192.168.1.201/24 |                      |                   | Failover Targets: cluster01-01:e0c,<br>cluster01-01:e0d |                   |
|                  | cluster01_icl02      | cluster01-02:e0c  | local-only                                              |                   |
| 192.168.1.201/24 |                      |                   | Failover Targets: cluster01-02:e0c,<br>cluster01-02:e0d |                   |

## Configurer les LIFs intercluster sur les ports dédiés

Vous pouvez configurer les LIFs intercluster sur des ports dédiés. Cela augmente généralement la bande passante disponible pour le trafic de réplication.

### Étapes

1. Lister les ports dans le cluster :

```
network port show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant montre les ports réseau dans `cluster01`:

```
cluster01::> network port show
```

| (Mbps)       |      | Speed   |                  |      |      |            |
|--------------|------|---------|------------------|------|------|------------|
| Node         | Port | IPspace | Broadcast Domain | Link | MTU  | Admin/Oper |
| -----        |      |         |                  |      |      |            |
| -----        |      |         |                  |      |      |            |
| cluster01-01 |      |         |                  |      |      |            |
|              | e0a  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0b  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0c  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0d  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0e  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0f  | Default | Default          | up   | 1500 | auto/1000  |
| cluster01-02 |      |         |                  |      |      |            |
|              | e0a  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0b  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0c  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0d  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0e  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0f  | Default | Default          | up   | 1500 | auto/1000  |

## 2. Déterminer les ports disponibles pour dédier aux communications intercluster :

```
network interface show -fields home-port,curr-port
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant indique ces ports e0e et e0f Ne se sont pas affectés de LIFs :

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif home-port curr-port

Cluster cluster01-01_clus1 e0a e0a
Cluster cluster01-01_clus2 e0b e0b
Cluster cluster01-02_clus1 e0a e0a
Cluster cluster01-02_clus2 e0b e0b
cluster01
 cluster_mgmt e0c e0c
cluster01
 cluster01-01_mgmt1 e0c e0c
cluster01
 cluster01-02_mgmt1 e0c e0c
```

## 3. Créer un failover group pour les ports dédiés :

```
network interface failover-groups create -vserver system_SVM -failover-group failover_group -targets physical_or_logical_ports
```

L'exemple suivant attribue des ports e0e et e0f vers le groupe de basculement intercluster01 Sur le SVM système cluster01:

```
cluster01::> network interface failover-groups create -vserver cluster01 -failover-group intercluster01 -targets cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Vérifier que le groupe de basculement a été créé :

```
network interface failover-groups show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface failover-groups show
Vserver Group Failover

Targets

Cluster
Cluster
cluster01 cluster01-01:e0a, cluster01-01:e0b,
 cluster01-02:e0a, cluster01-02:e0b
 Default
 cluster01-01:e0c, cluster01-01:e0d,
 cluster01-02:e0c, cluster01-02:e0d,
 cluster01-01:e0e, cluster01-01:e0f
 cluster01-02:e0e, cluster01-02:e0f
 intercluster01
 cluster01-01:e0e, cluster01-01:e0f
 cluster01-02:e0e, cluster01-02:e0f
```

5. Créer les LIF intercluster sur le SVM système et les assigner au failover group.

| Option                       | Description                                                                                                                                                                                          |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dans ONTAP 9.6 et plus tard: | network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home- port port -address port_IP -netmask netmask -failover -group failover_group |



| Option                                         | Description                                                                                                                                                                                                                                  |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Dans ONTAP 9.5 et versions antérieures:</b> | <code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -role intercluster -home-node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i> -failover-group <i>failover_group</i></code> |

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

L'exemple suivant illustre la création de LIFs intercluster `cluster01_icl01` et `cluster01_icl02` dans le groupe de basculement `intercluster01`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

#### 6. Vérifier que les LIFs intercluster ont été créés :

| Option                                         | Description                                                              |
|------------------------------------------------|--------------------------------------------------------------------------|
| <b>Dans ONTAP 9.6 et plus tard:</b>            | <code>network interface show -service-policy default-intercluster</code> |
| <b>Dans ONTAP 9.5 et versions antérieures:</b> | <code>network interface show -role intercluster</code>                   |

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

```

cluster01::> network interface show -service-policy default-intercluster
 Logical Status Network Current
Current Is
Vserver Interface Admin/Oper Address/Mask Node Port
Home

cluster01
 cluster01_icl01
 up/up 192.168.1.201/24 cluster01-01 e0e
true
 cluster01_icl02
 up/up 192.168.1.202/24 cluster01-02 e0f
true

```

#### 7. Vérifier que les LIFs intercluster sont redondants :

| Option                                         | Description                                                                        |
|------------------------------------------------|------------------------------------------------------------------------------------|
| <b>Dans ONTAP 9.6 et plus tard:</b>            | <code>network interface show -service-policy default-intercluster -failover</code> |
| <b>Dans ONTAP 9.5 et versions antérieures:</b> | <code>network interface show -role intercluster -failover</code>                   |

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

L'exemple suivant indique que les LIFs intercluster `cluster01_icl01` et `cluster01_icl02` Sur le SVM `e0e` le port basculera vers le `e0f` port.

```

cluster01::> network interface show -service-policy default-intercluster
-failover
 Logical Home Failover Failover
Vserver Interface Node:Port Policy Group

cluster01
 cluster01_icl01 cluster01-01:e0e local-only
intercluster01
 Failover Targets: cluster01-01:e0e,
 cluster01-01:e0f
 cluster01_icl02 cluster01-02:e0e local-only
intercluster01
 Failover Targets: cluster01-02:e0e,
 cluster01-02:e0f

```

## Configurez les LIF intercluster dans des IPspaces personnalisés

Vous pouvez configurer les LIF intercluster dans des IPspaces personnalisés. Il est ainsi possible d'isoler le trafic de réplication dans des environnements mutualisés.

Lorsque vous créez un IPspace personnalisé, le système crée une machine virtuelle de stockage système (SVM) afin de servir de conteneur pour les objets système dans cet IPspace. Vous pouvez utiliser le nouveau SVM en tant que conteneur pour toutes les LIF intercluster dans le nouvel IPspace. Le nouveau SVM porte le même nom que l'IPspace personnalisé.

### Étapes

1. Lister les ports dans le cluster :

```
network port show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).

L'exemple suivant montre les ports réseau dans `cluster01`:

```
cluster01::> network port show
```

|              |       |         |                  |       |       | Speed      |
|--------------|-------|---------|------------------|-------|-------|------------|
| (Mbps)       |       |         |                  |       |       |            |
| Node         | Port  | IPspace | Broadcast Domain | Link  | MTU   | Admin/Oper |
| -----        | ----- | -----   | -----            | ----- | ----- | -----      |
| cluster01-01 |       |         |                  |       |       |            |
|              | e0a   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0b   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0c   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0d   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0e   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0f   | Default | Default          | up    | 1500  | auto/1000  |
| cluster01-02 |       |         |                  |       |       |            |
|              | e0a   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0b   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0c   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0d   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0e   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0f   | Default | Default          | up    | 1500  | auto/1000  |

2. Créez des IPspaces personnalisés sur le cluster :

```
network ipspace create -ipspace ipspace
```

L'exemple suivant crée l'IPspace personnalisé `ipspace-IC1`:

```
cluster01::> network ipspace create -ipspace ipspace-IC1
```

### 3. Déterminer les ports disponibles pour dédier aux communications intercluster :

```
network interface show -fields home-port,curr-port
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant indique ces ports e0e et e0f Ne se sont pas affectés de LIFs :

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif home-port curr-port

Cluster cluster01_clus1 e0a e0a
Cluster cluster01_clus2 e0b e0b
Cluster cluster02_clus1 e0a e0a
Cluster cluster02_clus2 e0b e0b
cluster01
 cluster_mgmt e0c e0c
cluster01
 cluster01-01_mgmt1 e0c e0c
cluster01
 cluster01-02_mgmt1 e0c e0c
```

### 4. Supprimer les ports disponibles du broadcast domain par défaut :

```
network port broadcast-domain remove-ports -broadcast-domain Default -ports
ports
```

Un port ne peut pas se trouver dans plusieurs domaines de diffusion à la fois. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant supprime les ports e0e et e0f depuis le broadcast domain par défaut :

```
cluster01::> network port broadcast-domain remove-ports -broadcast
-domain Default -ports
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

### 5. Vérifiez que les ports ont été supprimés du broadcast domain par défaut :

```
network port show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant indique ces ports e0e et e0f ont été supprimés du broadcast domain par défaut :

```
cluster01::> network port show
```

|              |       |         |                  |       |       | Speed (Mbps) |
|--------------|-------|---------|------------------|-------|-------|--------------|
| Node         | Port  | IPspace | Broadcast Domain | Link  | MTU   | Admin/Oper   |
| -----        | ----- | -----   | -----            | ----- | ----- | -----        |
| cluster01-01 |       |         |                  |       |       |              |
|              | e0a   | Cluster | Cluster          | up    | 9000  | auto/1000    |
|              | e0b   | Cluster | Cluster          | up    | 9000  | auto/1000    |
|              | e0c   | Default | Default          | up    | 1500  | auto/1000    |
|              | e0d   | Default | Default          | up    | 1500  | auto/1000    |
|              | e0e   | Default | -                | up    | 1500  | auto/1000    |
|              | e0f   | Default | -                | up    | 1500  | auto/1000    |
|              | e0g   | Default | Default          | up    | 1500  | auto/1000    |
| cluster01-02 |       |         |                  |       |       |              |
|              | e0a   | Cluster | Cluster          | up    | 9000  | auto/1000    |
|              | e0b   | Cluster | Cluster          | up    | 9000  | auto/1000    |
|              | e0c   | Default | Default          | up    | 1500  | auto/1000    |
|              | e0d   | Default | Default          | up    | 1500  | auto/1000    |
|              | e0e   | Default | -                | up    | 1500  | auto/1000    |
|              | e0f   | Default | -                | up    | 1500  | auto/1000    |
|              | e0g   | Default | Default          | up    | 1500  | auto/1000    |

#### 6. Créer un domaine de diffusion dans l'IPspace personnalisé :

```
network port broadcast-domain create -ipspace ipspace -broadcast-domain
broadcast_domain -mtu MTU -ports ports
```

L'exemple suivant crée le domaine de diffusion `ipspace-IC1-bd` Dans l'IPspace `ipspace-IC1`:

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1
-broadcast-domain
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

#### 7. Vérifiez que le domaine de diffusion a été créé :

```
network port broadcast-domain show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

```

cluster01::> network port broadcast-domain show
IPspace Broadcast
Name Domain Name MTU Port List

Cluster Cluster 9000
 cluster01-01:e0a complete
 cluster01-01:e0b complete
 cluster01-02:e0a complete
 cluster01-02:e0b complete
Default Default 1500
 cluster01-01:e0c complete
 cluster01-01:e0d complete
 cluster01-01:e0f complete
 cluster01-01:e0g complete
 cluster01-02:e0c complete
 cluster01-02:e0d complete
 cluster01-02:e0f complete
 cluster01-02:e0g complete
ipspace-IC1
 ipspace-IC1-bd
 1500
 cluster01-01:e0e complete
 cluster01-01:e0f complete
 cluster01-02:e0e complete
 cluster01-02:e0f complete

```

#### 8. Créer les LIFs intercluster sur le SVM système et les assigner au broadcast domain :

| Option                                         | Description                                                                                                                                                                      |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Dans ONTAP 9.6 et plus tard:</b>            | <pre> network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home-port port -address port_IP -netmask netmask </pre> |
| <b>Dans ONTAP 9.5 et versions antérieures:</b> | <pre> network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask </pre>                    |

Le LIF est créé dans le broadcast domain auquel le home port est attribué. Le broadcast domain a un failover group par défaut avec le même nom que le broadcast domain. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création de LIFs intercluster `cluster01_icl01` et `cluster01_icl02` dans le domaine de broadcast `ipspace-IC1-bd`:

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. Vérifier que les LIFs intercluster ont été créés :

| Option                                  | Description                                                 |
|-----------------------------------------|-------------------------------------------------------------|
| Dans ONTAP 9.6 et plus tard:            | network interface show -service-policy default-intercluster |
| Dans ONTAP 9.5 et versions antérieures: | network interface show -role intercluster                   |

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface show -service-policy default-intercluster
Logical Status Network Current
Current Is
Vserver Interface Admin/Oper Address/Mask Node Port
Home

ipspace-IC1
 cluster01_icl01
 up/up 192.168.1.201/24 cluster01-01 e0e
true
 cluster01_icl02
 up/up 192.168.1.202/24 cluster01-02 e0f
true
```

10. Vérifier que les LIFs intercluster sont redondants :

| Option                                  | Description                                                           |
|-----------------------------------------|-----------------------------------------------------------------------|
| Dans ONTAP 9.6 et plus tard:            | network interface show -service-policy default-intercluster -failover |
| Dans ONTAP 9.5 et versions antérieures: | network interface show -role intercluster -failover                   |

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant indique que les LIFs intercluster `cluster01_icl01` et `cluster01_icl02` Sur le SVM `e0e` le port passe au port « `e0f` » :

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

| Vserver        | Logical<br>Interface | Home<br>Node:Port | Failover<br>Policy | Failover<br>Group |
|----------------|----------------------|-------------------|--------------------|-------------------|
| -----          | -----                | -----             | -----              | -----             |
| ipspace-IC1    |                      |                   |                    |                   |
|                | cluster01_icl01      | cluster01-01:e0e  | local-only         |                   |
| intercluster01 |                      |                   |                    |                   |
|                |                      | Failover Targets: | cluster01-01:e0e,  |                   |
|                |                      |                   | cluster01-01:e0f   |                   |
|                | cluster01_icl02      | cluster01-02:e0e  | local-only         |                   |
| intercluster01 |                      |                   |                    |                   |
|                |                      | Failover Targets: | cluster01-02:e0e,  |                   |
|                |                      |                   | cluster01-02:e0f   |                   |

## Configurer les relations de pairs

### Créer une relation entre clusters

Avant de protéger vos données en les répliquant sur un cluster distant à des fins de sauvegarde des données et de reprise sur incident, vous devez créer une relation entre les pairs de cluster entre le cluster local et distant.

Plusieurs stratégies de protection par défaut sont disponibles. Vous devez avoir créé vos stratégies de protection si vous souhaitez utiliser des stratégies personnalisées.

### Avant de commencer

- Si vous utilisez l'interface de ligne de commandes ONTAP, vous devez avoir créé des LIFs intercluster sur chaque nœud des clusters peering en utilisant l'une des méthodes suivantes :
  - ["Configurer les LIFs intercluster sur des ports data partagés"](#)
  - ["Configurer les LIFs intercluster sur des ports data dédiés"](#)
  - ["Configurez les LIF intercluster dans des IPspaces personnalisés"](#)



- Les clusters doivent exécuter ONTAP 9.3 ou version ultérieure. (Si les clusters exécutent ONTAP 9.2 ou une version antérieure, reportez-vous aux procédures de la ["ce document archivé"](#).)



### Étapes

Effectuez cette tâche à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes de ONTAP.

## System Manager

1. Dans le cluster local, cliquez sur **Cluster > Paramètres**.
2. Dans la section **intercluster Settings**, cliquez sur **Add Network interfaces** et entrez l'adresse IP et le masque de sous-réseau pour ajouter les interfaces réseau intercluster du cluster.

Répétez cette étape sur le cluster distant.

3. Dans le cluster distant, cliquez sur **Cluster > Paramètres**.
4. Cliquez sur  dans la section **homologues du cluster** et sélectionnez **générer une phrase de passe**.
5. Sélectionnez la version du cluster ONTAP distant.
6. Copiez la phrase de passe générée.
7. Dans le cluster local, sous **clusters homologues**, cliquez sur  et sélectionnez **Peer Cluster**.
8. Dans la fenêtre **Peer Cluster**, collez la phrase de passe et cliquez sur **Initiate cluster peering**.

## CLI

1. Sur le cluster destination, créez une relation entre pairs et le cluster source :

```
cluster peer create -generate-passphrase -offer-expiration
<MM/DD/YYYY HH:MM:SS|1...7days|1...168hours> -peer-addr
<peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name|*> -ip
<ipspace>
```

Si vous spécifiez les deux `-generate-passphrase` et `-peer-addr`, Uniquement le cluster dont les LIFs intercluster sont spécifiés dans `-peer-addr` peut utiliser le mot de passe généré.

Vous pouvez ignorer `-ip` Option si vous n'utilisez pas un IPspace personnalisé. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Si vous créez la relation de peering dans ONTAP 9.6 ou version ultérieure et que vous ne souhaitez pas que les communications de peering de clusters soient cryptées, vous devez utiliser le `-encryption-protocol-proposed none` option pour désactiver le cryptage.

L'exemple suivant crée une relation de cluster peer-to-peer avec un cluster distant non spécifié, et autorise pré-les relations de pairs avec les SVM `vs1` et `vs2` sur le cluster local :

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: vs1,vs2
Intercluster LIF IP: 192.140.112.101
Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

L'exemple suivant crée une relation de cluster peer-to-peer avec le cluster distant aux adresses IP LIF intercluster 192.140.112.103 et 192.140.112.104, et autorise pré-une relation de peer-to-peer avec n'importe quel SVM sur le cluster local :

```
cluster02::> cluster peer create -generate-passphrase -peer-addr
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: vs1,vs2
Intercluster LIF IP: 192.140.112.101,192.140.112.102
Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

L'exemple suivant crée une relation de cluster peer-to-peer avec un cluster distant non spécifié, et autorise pré-les relations de pairs avec les SVM<sub>vs1</sub> et <sub>vs2</sub> sur le cluster local :

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: vs1,vs2
Intercluster LIF IP: 192.140.112.101
Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. Sur le cluster source, authentifier le cluster source sur le cluster destination :

```
cluster peer create -peer-addr <peer_LIF_IPs> -ipspace <ipspace>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant authentifier le cluster local sur le cluster distant aux adresses IP 192.140.112.101 et 192.140.112.102 de LIF intercluster :

```
cluster01::> cluster peer create -peer-addr
192.140.112.101,192.140.112.102
```

Notice: Use a generated passphrase or choose a passphrase of 8 or more characters.

To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:

Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.

Entrez la phrase de passe de la relation homologue lorsque vous y êtes invité.

3. Vérifiez que la relation entre clusters a été créée :

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance
```

```
Peer Cluster Name: cluster02
Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
Availability of the Remote Cluster: Available
Remote Cluster Name: cluster2
Active IP Addresses: 192.140.112.101,
192.140.112.102
Cluster Serial Number: 1-80-123456
Address Family of Relationship: ipv4
Authentication Status Administrative: no-authentication
Authentication Status Operational: absent
Last Update Time: 02/05 21:05:41
IPspace for the Relationship: Default
```

#### 4. Vérifier la connectivité et l'état des nœuds de la relation peer-to-peer :

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node cluster-Name Node-Name
 Ping-Status RDB-Health Cluster-Health
Avail...

cluster01-01
 cluster02 cluster02-01
 Data: interface_reachable
 ICMP: interface_reachable true true
true
 cluster02-02
 Data: interface_reachable
 ICMP: interface_reachable true true
true
cluster01-02
 cluster02 cluster02-01
 Data: interface_reachable
 ICMP: interface_reachable true true
true
 cluster02-02
 Data: interface_reachable
 ICMP: interface_reachable true true
true
```

#### D'autres façons de le faire dans ONTAP

| Pour effectuer ces tâches avec...                                          | Voir ce contenu...                                                                    |
|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures) | <a href="#">"Présentation de la préparation de la reprise sur incident de volume"</a> |

#### Créer une relation SVM peer-to-peer

Vous pouvez utiliser le `vserver peer create` Commande pour créer une relation entre les SVM sur des clusters locaux et distants.

#### Avant de commencer

- Les clusters source et destination doivent être associés.
- Les clusters doivent exécuter ONTAP 9.3. (Si les clusters exécutent ONTAP 9.2 ou une version antérieure,

reportez-vous aux procédures de la ["ce document archivé"](#).)

- Vous devez avoir des relations de pairs « pré-autorisées » pour les SVM sur le cluster distant.

Pour plus d'informations, voir ["Création d'une relation entre clusters"](#).

### Description de la tâche

Dans ONTAP 9.2 et versions antérieures, vous pouvez autoriser une relation de pairs pour un seul SVM à la fois. Cela signifie que vous devez exécuter `vserver peer accept` Chaque fois que vous autorisez une relation de SVM peer en attente.

Depuis ONTAP 9.3, vous pouvez « pré-autoriser » des relations entre pairs pour plusieurs SVM en répertoriant les SVM dans le `-initial-allowed-vserver` option lors de la création d'une relation de type cluster. Pour plus d'informations, voir ["Création d'une relation entre clusters"](#).

### Étapes

1. Sur le cluster destination de protection des données, afficher les SVM qui sont pré-autorisés pour le peering :

```
vserver peer permission show
```

```
cluster02::> vserver peer permission show
Peer Cluster Vserver Applications

cluster02 vs1,vs2 snapmirror
```

2. Sur le cluster source de protection des données, créez une relation entre pairs et un SVM pré-autorisé sur le cluster cible de protection des données :

```
vserver peer create -vserver local_SVM -peer-vserver remote_SVM
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

L'exemple suivant crée une relation de pairs entre le SVM local `pvs1` Et le SVM distant pré-autorisé `vs1`:

```
cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
```

3. Vérifier la relation entre SVM et :

```
vserver peer show
```

```
cluster01::> vserver peer show
```

|         | Peer    | Peer   |              | Peering      |
|---------|---------|--------|--------------|--------------|
| Remote  |         |        |              |              |
| Vserver | Vserver | State  | Peer Cluster | Applications |
| Vserver |         |        |              |              |
| -----   | -----   | -----  | -----        | -----        |
| -----   |         |        |              |              |
| pvs1    | vs1     | peered | cluster02    | snapmirror   |
| vs1     |         |        |              |              |

## Ajouter une relation SVM peer-to-peer intercluster

Si vous créez un SVM après avoir configuré une relation de cluster peer-to-peer, vous devez ajouter manuellement une relation de peer-to-peer pour la SVM. Vous pouvez utiliser le `vserver peer create` Commande pour créer une relation entre SVM. Une fois la relation homologue créée, vous pouvez exécuter `vserver peer accept` sur le cluster distant, afin d'autoriser la relation peer-to-peer.

### Avant de commencer

Les clusters source et destination doivent être associés.

### Description de la tâche

Vous pouvez créer des relations peer-to-peer entre les SVM et dans le même cluster pour la sauvegarde des données locales. Pour plus d'informations, reportez-vous à la section `vserver peer create` page de manuel.

Les administrateurs utilisent parfois le `vserver peer reject` Commande permettant de refuser une relation SVM peer-to-peer proposée. Si la relation entre les SVM se trouve dans le `rejected` état, vous devez supprimer la relation pour en créer une nouvelle. Pour plus d'informations, reportez-vous à la section `vserver peer delete` page de manuel.

### Étapes

1. Sur le cluster source de protection des données, créez une relation entre pairs et un SVM sur le cluster cible de protection des données :

```
vserver peer create -vserver local_SVM -peer-vserver remote_SVM -applications snapmirror|file-copy|lun-copy -peer-cluster remote_cluster
```

L'exemple suivant crée une relation de pairs entre le SVM local `pvs1` Et le SVM distant `vs1`

```
cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
-applications snapmirror -peer-cluster cluster02
```

Si les SVM locaux et distants ont les mêmes noms, vous devez utiliser un *local name* pour créer la relation SVM peer :

```
cluster01::> vserver peer create -vserver vs1 -peer-vserver
vs1 -applications snapmirror -peer-cluster cluster01
-local-name cluster1vs1LocallyUniqueName
```

2. Sur le cluster source de protection des données, vérifiez que la relation de pairs a été initiée :

```
vserver peer show-all
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant montre que la relation de pairs entre SVM<sub>pvs1</sub> Et SVM<sub>vs1</sub> a été lancé :

```
cluster01::> vserver peer show-all
```

| Vserver | Peer<br>Vserver | Peer<br>State | Peer Cluster | Peering<br>Applications |
|---------|-----------------|---------------|--------------|-------------------------|
| -----   | -----           | -----         | -----        | -----                   |
| pvs1    | vs1             | initiated     | Cluster02    | snapmirror              |

3. Sur le cluster destination de protection des données, afficher la relation SVM peer-to-peer en attente :

```
vserver peer show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant répertorie les relations homologues en attente pour cluster02:

```
cluster02::> vserver peer show
```

| Vserver | Peer<br>Vserver | Peer<br>State |
|---------|-----------------|---------------|
| -----   | -----           | -----         |
| vs1     | pvs1            | pending       |

4. Sur le cluster cible de protection des données, autoriser la relation peer-to-peer en attente :

```
vserver peer accept -vserver local_SVM -peer-vserver remote_SVM
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant autorise la relation de pairs entre la SVM locale vs1 Et le SVM distant pvs1:

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. Vérifier la relation entre SVM et :



```
vserver peer show
```

```
cluster01::> vserver peer show
```

| Remote Vserver | Peer Vserver | Peer State | Peer Cluster | Peering Applications |
|----------------|--------------|------------|--------------|----------------------|
| -----          | -----        | -----      | -----        | -----                |
| pvs1<br>vs1    | vs1          | peered     | cluster02    | snapmirror           |

## Activer le chiffrement de peering de cluster sur une relation de pairs existante

Depuis ONTAP 9.6, le chiffrement de peering de cluster est activé par défaut sur toutes les relations de peering de cluster que nous avons récemment créées. Le chiffrement de peering de cluster utilise une clé pré-partagée (PSK) et la couche de sécurité du transport (TLS) pour sécuriser les communications de peering entre clusters. Cela ajoute une couche de sécurité supplémentaire entre les clusters avec points.

### Description de la tâche

Si vous mettez à niveau des clusters de peering vers ONTAP 9.6 ou version ultérieure et que la relation de peering a été créée dans ONTAP 9.5 ou version antérieure, le chiffrement de peering de cluster doit être activé manuellement après la mise à niveau. Les deux clusters de la relation de peering doivent exécuter ONTAP 9.6 ou version ultérieure afin de permettre le cryptage du cluster peering.

### Étapes

1. Sur le cluster de destination, activez le chiffrement pour les communications avec le cluster source :

```
cluster peer modify source_cluster -auth-status-admin use-authentication
-encryption-protocol-proposed tls-psk
```

2. Entrez une phrase de passe lorsque vous y êtes invité.
3. Sur le cluster source de protection des données, activez le chiffrement pour la communication avec le cluster cible de protection des données :

```
cluster peer modify data_protection_destination_cluster -auth-status-admin
use-authentication -encryption-protocol-proposed tls-psk
```

4. Indiquez la même phrase secrète entrée sur le cluster de destination.

## Retirer le cryptage de peering de cluster d'une relation de pairs existante

Par défaut, le cryptage de peering de cluster est activé sur toutes les relations entre pairs créées dans ONTAP 9.6 ou version ultérieure. Si vous ne souhaitez pas utiliser le cryptage pour les communications de peering intercluster, vous pouvez le désactiver.

## Étapes

1. Sur le cluster de destination, modifiez les communications avec le cluster source pour interrompre l'utilisation du chiffrement de peering de cluster :

- Pour supprimer le cryptage mais maintenir l'authentification, entrez :

```
cluster peer modify <source_cluster> -auth-status-admin use-
authentication -encryption-protocol-proposed none
```

- Pour supprimer le cryptage et l'authentification :

- i. Modifiez la stratégie de peering de cluster pour autoriser l'accès non authentifié :

```
cluster peer policy modify -is-unauthenticated-access-permitted
true
```

- ii. Modifier le cryptage et l'accès d'authentification :

```
cluster peer modify <source_cluster> -auth-status no-
authentication
```

2. Lorsque vous y êtes invité, saisissez la phrase de passe.
3. Confirmez la phrase de passe en la saisissant à nouveau.
4. Sur le cluster source, désactiver le cryptage pour la communication avec le cluster destination :

- Pour supprimer le cryptage mais maintenir l'authentification, entrez :

```
cluster peer modify <destination_cluster> -auth-status-admin use-
authentication -encryption-protocol-proposed none
```

- Pour supprimer le cryptage et l'authentification :

- i. Modifiez la stratégie de peering de cluster pour autoriser l'accès non authentifié :

```
cluster peer policy modify -is-unauthenticated-access-permitted
true
```

- ii. Modifier le cryptage et l'accès d'authentification :

```
cluster peer modify <destination_cluster> -auth-status no-
authentication
```

5. Lorsque vous y êtes invité, entrez et saisissez à nouveau la phrase de passe que vous avez utilisée sur le cluster de destination.

# Gérez les copies Snapshot locales

## Gérer les copies Snapshot locales

Une *copie snapshot* est une image ponctuelle en lecture seule d'un volume. L'image consomme un espace de stockage minimal et entraîne une surcharge minime des performances, car elle enregistre uniquement les modifications apportées aux fichiers depuis la dernière copie Snapshot.

Vous pouvez utiliser une copie Snapshot pour restaurer l'intégralité du contenu d'un volume, ou restaurer des fichiers ou des LUN individuels. Les copies Snapshot sont stockées dans le répertoire `.snapshot` sur le volume.

Dans ONTAP 9.3 et versions antérieures, un volume peut contenir jusqu'à 255 copies Snapshot. Dans ONTAP 9.4 et versions ultérieures, un volume FlexVol peut contenir jusqu'à 1023 copies Snapshot.



Depuis ONTAP 9.8, les volumes FlexGroup peuvent contenir 1023 copies Snapshot. Pour plus d'informations, voir ["Protection des volumes FlexGroup à l'aide de copies Snapshot"](#).

## Configuration de règles Snapshot personnalisées

### Présentation de la configuration de règles Snapshot personnalisées

Une règle *Snapshot* définit la façon dont le système crée des copies Snapshot. La règle indique quand créer des copies Snapshot, le nombre de copies à conserver et comment les nommer. Par exemple, un système peut créer une copie Snapshot tous les jours à 12 h 10, conserver les deux copies les plus récentes et nommer les copies « *otidienne.timestamp* ».

La règle par défaut d'un volume crée automatiquement des copies Snapshot selon le calendrier suivant, avec les plus anciennes copies Snapshot supprimées pour laisser de l'espace disponible pour les copies les plus récentes :

- Six copies Snapshot toutes les heures ont été effectuées au maximum cinq minutes au-delà de l'heure.
- Deux copies Snapshot quotidiennes maximum sont effectuées du lundi au samedi 10 minutes après minuit.
- Deux copies Snapshot hebdomadaires maximum sont réalisées tous les dimanches à 15 minutes après minuit.

Sauf si vous spécifiez une règle Snapshot lorsque vous créez un volume, le volume hérite des règles de Snapshot associées à sa machine virtuelle de stockage (SVM).

### A quel moment configurer une règle Snapshot personnalisée

Si la politique Snapshot par défaut n'est pas adaptée à un volume, vous pouvez configurer une règle personnalisée modifiant la fréquence, la conservation et le nom des copies Snapshot. Le planning sera dicté principalement par le taux de changement du système de fichiers actif.

Vous pouvez sauvegarder toutes les heures un système de fichiers très utilisé, comme une base de données, et sauvegarder les fichiers rarement utilisés une fois par jour. Même pour une base de données, vous exécutez généralement une sauvegarde complète une ou deux fois par jour, tout en sauvegardant les journaux de transactions toutes les heures.

Les autres facteurs sont l'importance des fichiers pour votre entreprise, votre contrat de niveau de service (SLA), votre objectif de point de récupération (RPO) et votre objectif de délai de restauration (RTO). De manière générale, vous devez conserver autant de copies Snapshot que nécessaire.

### **Créer un planning de travail instantané**

Une règle Snapshot requiert une planification d'au moins une tâche de copie Snapshot. Vous pouvez utiliser System Manager ou `job schedule cron create` commande permettant de créer un programme de travail.

#### **Description de la tâche**

Par défaut, ONTAP forme les noms des copies Snapshot en ajoutant un horodatage au nom du calendrier des travaux.

Si vous spécifiez des valeurs pour le jour du mois et le jour de la semaine, elles sont considérées indépendamment. Par exemple, une planification cron avec la spécification de jour `Friday` et le jour du mois `13` S'étend tous les vendredis et le 13ème jour de chaque mois, pas seulement tous les vendredis du 13ème.

## Exemple 22. Étapes

### System Manager

1. Accédez à **protection > vue d'ensemble** et développez **Paramètres de stratégie locale**.
2. Dans le volet **programmes**, cliquez sur ➔.
3. Dans la fenêtre **Schedules**, cliquez sur + Add.
4. Dans la fenêtre **Ajouter un planning**, entrez le nom du planning et choisissez le contexte et le type de planning.
5. Cliquez sur **Enregistrer**.

### CLI

1. Création d'un programme de travail :

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

Pour `-month`, `-dayofweek`, et `-hour`, vous pouvez spécifier `all` pour exécuter le travail chaque mois, jour de la semaine et heure, respectivement.

Depuis ONTAP 9.10.1, vous pouvez inclure le vServer dans votre calendrier des tâches :

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

L'exemple suivant crée un programme de travail nommé `myweekly` Le samedi à 3:00 :

```
cluster1::> job schedule cron create -name myweekly -dayofweek
"Saturday" -hour 3 -minute 0
```

L'exemple suivant crée un programme nommé `myweeklymulti` ce délai est spécifié pour plusieurs jours, heures et minutes :

```
job schedule cron create -name myweeklymulti -dayofweek
"Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
```

## Créer une règle Snapshot

Une règle Snapshot spécifie quand créer des copies Snapshot, le nombre de copies à conserver et comment les nommer. Par exemple, un système peut créer une copie Snapshot tous les jours à 12 h 10, conserver les deux copies les plus récentes et les

nommer « `diotidienne.`timestamp`` » Une règle Snapshot peut contenir jusqu'à cinq planifications de tâches.

### Description de la tâche

Par défaut, ONTAP forme les noms des copies Snapshot en ajoutant un horodatage au nom de la planification des travaux :

|                                      |                                      |
|--------------------------------------|--------------------------------------|
| <code>daily.2017-05-14_0013/</code>  | <code>hourly.2017-05-15_1106/</code> |
| <code>daily.2017-05-15_0012/</code>  | <code>hourly.2017-05-15_1206/</code> |
| <code>hourly.2017-05-15_1006/</code> | <code>hourly.2017-05-15_1306/</code> |

Si vous préférez, vous pouvez remplacer un préfixe par le nom du programme de travail.

Le `snapmirror-label` L'option concerne la réplication SnapMirror. Pour plus d'informations, voir ["Définition d'une règle pour une règle"](#).

### Étapes

Vous pouvez créer une règle de copie Snapshot à l'aide de System Manager ou de l'interface de ligne de commandes de ONTAP. La procédure crée une règle de copie Snapshot sur le cluster local uniquement.

## System Manager

1. Accédez à **protection > vue d'ensemble** et développez **Paramètres de stratégie locale**.
2. Dans le volet **stratégies d'instantanés**, cliquez sur ➔.
3. Dans l'onglet **stratégies d'instantanés**, cliquez sur + Add.
4. Dans la fenêtre **Add Snapshot policy**, entrez le nom de la stratégie et choisissez la portée.
5. Cliquez sur + Add.
6. Pour sélectionner un planning, cliquez sur le nom du planning actuellement affiché, cliquez sur ▼, puis choisissez un autre planning.
7. Indiquez le nombre maximal de copies Snapshot à conserver, et, le cas échéant, saisissez l'étiquette SnapMirror et la période de conservation SnapLock.
8. Cliquez sur **Enregistrer**.

## CLI

1. Création d'une règle Snapshot :

```
volume snapshot policy create -vserver <SVM> -policy <policy_name>
-enabled true|false -schedule1 <schedule1_name> -count1
<copies_to_retain> -prefix1 <snapshot_prefix> -snapmirror-label1
<snapshot_label> ... -schedule5 <schedule5_name> -count5
<copies_to_retain> -prefix5 <snapshot_prefix> -snapmirror-label5
<snapshot_label>
```

L'exemple suivant illustre la création de la règle Snapshot nommée `snap_policy_daily` cela fonctionne sur un `daily` planification. La règle possède un maximum de cinq copies Snapshot, chacune portant le nom `daily.timestamp` Et étiquette SnapMirror `daily`:

```
cluster1::> volume snapshot policy create -vserver vs0 -policy
snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1
daily
```

## Gestion manuelle des copies Snapshot

### Créez et supprimez des copies Snapshot manuellement

Vous pouvez créer des copies Snapshot manuellement si vous ne pouvez pas attendre la création d'une copie Snapshot planifiée et supprimer les copies Snapshot lorsqu'elles ne sont plus nécessaires.

### Créez une copie Snapshot manuellement

Vous pouvez créer manuellement une copie Snapshot à l'aide de System Manager ou de l'interface de ligne de commandes de ONTAP.

## System Manager

### Étapes

1. Accédez à **stockage > volumes** et sélectionnez l'onglet **copies Snapshot**.
2. Cliquez sur **+ Add**.
3. Dans la fenêtre **Ajouter une copie Snapshot**, acceptez le nom de la copie Snapshot par défaut ou modifiez-le si vous le souhaitez.
4. **Facultatif** : ajoutez une étiquette SnapMirror.
5. Cliquez sur **Ajouter**.

### CLI

1. Créer une copie Snapshot :

```
volume snapshot create -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

## Supprimez manuellement une copie Snapshot

Vous pouvez supprimer manuellement une copie Snapshot à l'aide de System Manager ou de l'interface de ligne de commandes de ONTAP.

## System Manager

### Étapes

1. Accédez à **stockage > volumes** et sélectionnez l'onglet **copies Snapshot**.
2. Localisez la copie Snapshot que vous souhaitez supprimer, cliquez sur **:** et sélectionnez **Supprimer**.
3. Dans la fenêtre **Supprimer la copie Snapshot**, sélectionnez **Supprimer la copie Snapshot**.
4. Cliquez sur **Supprimer**.

### CLI

1. Supprimer une copie Snapshot :

```
volume snapshot delete -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

## Calculer l'espace récupérable avant de supprimer les copies Snapshot

Depuis la version ONTAP 9.10.1, vous pouvez utiliser System Manager pour sélectionner les copies Snapshot à supprimer et calculer l'espace récupérable avant de les supprimer.

### Étapes

1. Cliquez sur **Storage > volumes**.



2. Sélectionnez le volume depuis lequel vous souhaitez supprimer les copies Snapshot.
3. Cliquez sur **copies snapshot**.
4. Sélectionnez une ou plusieurs copies Snapshot.
5. Cliquez sur **calculer l'espace de récupération**.

## Gérez la réserve de copies Snapshot

### Gérer la présentation de la réserve de copies Snapshot

Le paramètre *Snapshot copy Reserve* permet de réserver un pourcentage d'espace disque pour les copies Snapshot, cinq pour cent par défaut. Lorsque les copies Snapshot utilisent de l'espace dans le système de fichiers actif lorsque la réserve de copies Snapshot est épuisée, il peut donc être nécessaire d'augmenter la réserve de copies Snapshot si nécessaire. Vous pouvez également supprimer automatiquement les copies Snapshot lorsque la réserve est saturée.

### Quand augmenter la réserve de copies Snapshot

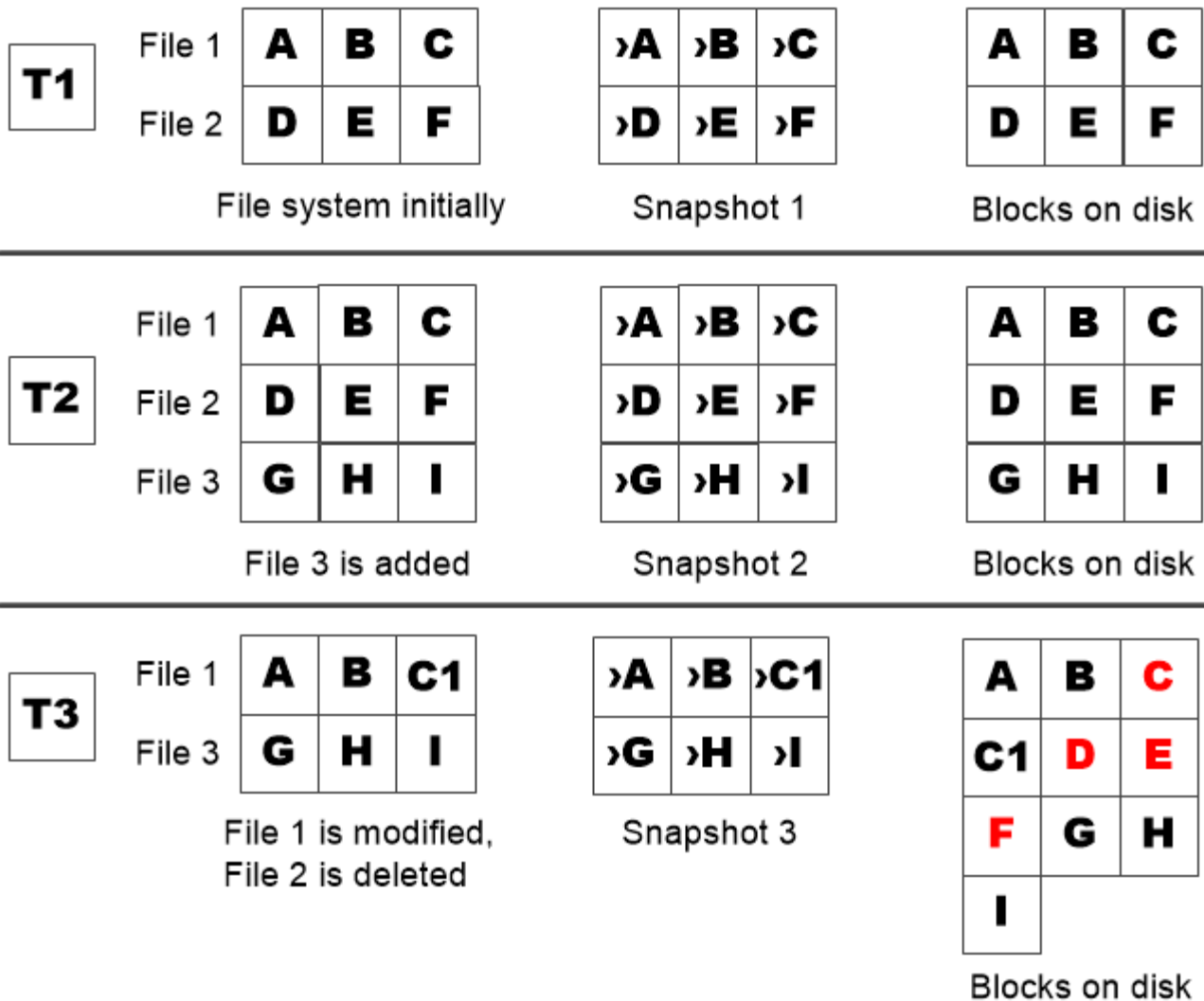
Lors du choix d'augmenter la réserve Snapshot, il est important de rappeler qu'une copie Snapshot n'enregistre que les modifications apportées aux fichiers depuis la dernière copie Snapshot. Elle consomme de l'espace disque uniquement lorsque des blocs du système de fichiers actif sont modifiés ou supprimés.

Cela signifie que le taux de changement du système de fichiers est le principal facteur déterminant la quantité d'espace disque utilisée par les copies Snapshot. Quel que soit le nombre de copies Snapshot que vous créez, elles ne consomment pas d'espace disque si le système de fichiers actif n'a pas changé.

Un volume FlexVol contenant les journaux de transactions de base de données, par exemple, peut disposer d'une réserve de copies Snapshot pouvant atteindre 20 % pour prendre en compte son taux de modification supérieur. Vous souhaitez non seulement créer davantage de copies Snapshot pour capturer les mises à jour plus fréquentes de la base de données, mais également disposer d'une plus grande réserve de copies Snapshot pour gérer l'espace disque supplémentaire consommé par les copies Snapshot.



Une copie Snapshot se compose de pointeurs vers des blocs au lieu de copies de blocs. Vous pouvez considérer un pointeur comme une « réclamation » sur un bloc : la ONTAP « maintient » le bloc jusqu'à ce que la copie Snapshot soit supprimée.



*A Snapshot copy consumes disk space only when blocks in the active file system are modified or deleted.*

La manière dont la suppression des fichiers protégés peut entraîner une diminution de l'espace fichier par rapport aux attentes

Une copie Snapshot pointe vers un bloc, même après la suppression du fichier utilisé par ce bloc. Cela explique pourquoi une réserve de copies Snapshot épuisée peut entraîner un résultat contre-intuitif, dans lequel la suppression d'un système de fichiers entier réduit l'espace disponible par rapport au système de fichiers occupé.

Prenons l'exemple suivant. Avant de supprimer des fichiers, le `df` la sortie de la commande est la suivante :

```

Filesystem kbytes used avail capacity
/vol/vol10/ 3000000 3000000 0 100%
/vol/vol10/.snapshot 1000000 500000 500000 50%
```

Après avoir supprimé l'intégralité du système de fichiers et créé une copie Snapshot du volume, le `df` la

commande génère la sortie suivante :

```
Filesystem kbytes used avail capacity
/vol/vol0/ 3000000 2500000 500000 83%
/vol/vol0/.snapshot 1000000 3500000 0 350%
```

Comme le montre le résultat, l'intégralité des 3 Go utilisés auparavant par le système de fichiers actif est désormais utilisée par les copies Snapshot, en plus des 0.5 Go utilisés avant la suppression.

L'espace disque utilisé par les copies Snapshot dépasse maintenant la réserve de copies Snapshot, le débordement de 2.5 Go de « spillss » dans l'espace réservé aux fichiers actifs, vous laissant avec 0.5 Go d'espace libre pour les fichiers où vous aviez raisonnablement prévu des 3 Go.

### Surveillez la consommation des copies Snapshot

Vous pouvez surveiller l'utilisation des copies Snapshot disque à l'aide du `df` commande. La commande affiche la quantité d'espace libre dans le système de fichiers actif et la réserve de copie Snapshot.

#### Étape

1. Afficher la consommation des copies Snapshot : `df`

L'exemple suivant montre la consommation de disque de copie Snapshot :

```
cluster1::> df
Filesystem kbytes used avail capacity
/vol/vol0/ 3000000 3000000 0 100%
/vol/vol0/.snapshot 1000000 500000 500000 50%
```

### Vérifiez la réserve de copies Snapshot disponible sur un volume

Vous pouvez vérifier la quantité de réserve Snapshot disponible sur un volume en utilisant le `snapshot-reserve-available` paramètre avec le `volume show` commande.

#### Étape

1. Vérifier la réserve Snapshot disponible sur un volume :

```
vol show -vserver SVM -volume volume -fields snapshot-reserve-available
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

L'exemple suivant montre la réserve de copie Snapshot disponible pour `vol11`:

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-reserve-
available

vserver volume snapshot-reserve-available

vs0 vol1 4.84GB
```

## Modifiez la réserve de copies Snapshot

Vous pouvez vouloir configurer une plus grande réserve de copies Snapshot pour empêcher les copies Snapshot d'utiliser l'espace réservé pour le système de fichiers actif. La réserve Snapshot est réduite lorsque l'espace nécessaire aux copies Snapshot est réduit.

### Étape

1. Modifiez la réserve Snapshot :

```
volume modify -vserver SVM -volume volume -percent-snapshot-space snap_reserve
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant définit la réserve de copie Snapshot pour `vol1` à 10 % :

```
cluster1::> volume modify -vserver vs0 -volume vol1 -percent-snapshot
-space 10
```

## Supprimer automatiquement les copies Snapshot

Vous pouvez utiliser le `volume snapshot autodelete modify` Commande permettant de déclencher la suppression automatique des copies Snapshot lorsque la réserve Snapshot est dépassée. Par défaut, les copies Snapshot les plus anciennes sont supprimées en premier.

### Description de la tâche

Les clones de LUN et de fichiers sont supprimés lorsqu'il n'y a plus de copie Snapshot à supprimer.

### Étape

1. Suppression automatique des copies Snapshot :

```
volume snapshot autodelete modify -vserver SVM -volume volume -enabled
true|false -trigger volume|snap_reserve
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la suppression automatique des copies Snapshot de `vol1` Lorsque la réserve de copie Snapshot est épuisée :

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume voll
-enabled true -trigger snap_reserve
```

## Restaurez les fichiers à partir de copies Snapshot

### Restaurez un fichier à partir d'une copie Snapshot sur un client NFS ou SMB

Un utilisateur d'un client NFS ou SMB peut restaurer un fichier directement à partir d'une copie Snapshot sans l'intervention d'un administrateur de système de stockage.

Chaque répertoire du système de fichiers contient un sous-répertoire nommé `.snapshot` Accessible aux utilisateurs NFS et SMB. Le `.snapshot` Le sous-répertoire contient des sous-répertoires correspondant aux copies Snapshot du volume :

```
$ ls .snapshot
daily.2017-05-14_0013/ hourly.2017-05-15_1106/
daily.2017-05-15_0012/ hourly.2017-05-15_1206/
hourly.2017-05-15_1006/ hourly.2017-05-15_1306/
```

Chaque sous-répertoire contient les fichiers référencés par la copie Snapshot. Si les utilisateurs suppriment ou remplacent accidentellement un fichier, ils peuvent restaurer ce dernier dans le répertoire de lecture-écriture parent en copiant le fichier du sous-répertoire Snapshot vers le répertoire de lecture-écriture :

```
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2017-05-14_0013/ hourly.2017-05-15_1106/
daily.2017-05-15_0012/ hourly.2017-05-15_1206/
hourly.2017-05-15_1006/ hourly.2017-05-15_1306/
$ ls .snapshot/hourly.2017-05-15_1306/my.txt
my.txt
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .
$ ls my.txt
my.txt
```

### Activez et désactivez l'accès des clients NFS et SMB au répertoire de copie Snapshot

Vous pouvez activer et désactiver l'accès au répertoire des copies Snapshot à l'aide de l'option d'interface de ligne de commandes ONTAP `-snapdir-access` de la `volume modify` commande. Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour activer ou désactiver l'accès des systèmes clients au répertoire des copies Snapshot d'un volume. L'activation de l'accès rend le répertoire des copies Snapshot visible aux clients et permet aux clients Windows de mapper un disque au répertoire des copies

Snapshot pour afficher et accéder à son contenu. Les clients NFS et SMB peuvent ensuite restaurer un fichier ou une LUN à partir d'un snapshot.


Vous pouvez activer ou désactiver l'accès au répertoire de copie Snapshot d'un volume en modifiant les paramètres du volume ou en modifiant les paramètres de partage du volume.

**Activez ou désactivez l'accès client au répertoire de copie Snapshot en modifiant un volume**

### **Étapes**

Vous pouvez activer et désactiver l'accès au répertoire des copies Snapshot du client à l'aide de ONTAP System Manager ou de l'interface de ligne de commande ONTAP. Par défaut, le répertoire de copies Snapshot d'un volume est accessible aux clients.

## System Manager

1. Cliquez sur **Storage > volumes**.
2. Sélectionnez le volume contenant le répertoire des copies Snapshot que vous souhaitez afficher ou masquer.
3. Cliquez sur  et sélectionnez **Modifier**.
4. Dans la section Paramètres\* **copies snapshot (local)**, sélectionnez ou désélectionnez **\*Afficher le répertoire copies Snapshot sur les clients**.
5. Cliquez sur **Enregistrer**.

## CLI

1. Vérifier l'état d'accès au répertoire Snapshot :

```
volume show -vserver <SVM_name> -volume <vol_name> -fields snapdir-
access
```

Exemple :

```
clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-
access
vserver volume snapdir-access

vs0 vol1 false
```

2. Activer ou désactiver l'accès au répertoire de copies Snapshot :

```
volume modify -vserver <SVM_name> -volume <vol_name> -snapdir-access
<true|false>
```

L'exemple suivant active l'accès au répertoire de copie Snapshot sur vol1 :


```
clus1::> volume modify -vserver vs0 -volume vol1 -snapdir-access
true
Volume modify successful on volume vol1 of Vserver vs0.
```

## Activez ou désactivez l'accès client au répertoire de copie Snapshot en modifiant un partage

Par défaut, le répertoire de copies Snapshot d'un volume est accessible aux clients.

### Étapes

1. Cliquez sur **stockage > partages**.

2. Sélectionnez le volume contenant le répertoire des copies Snapshot que vous souhaitez afficher ou masquer.
3. Cliquez sur  et sélectionnez **Modifier**.
4. Dans la section **Share Properties**, sélectionnez ou désélectionnez **Allow clients to Access Snapshot copies Directory**.
5. Cliquez sur **Enregistrer**.

## Restaurez un seul fichier à partir d'une copie Snapshot

Vous pouvez utiliser le `volume snapshot restore-file` Commande permettant de restaurer un fichier ou une LUN à partir d'une copie Snapshot. Vous pouvez restaurer le fichier à un autre emplacement dans le volume en lecture-écriture parent si vous ne souhaitez pas remplacer un fichier existant.

### Description de la tâche

Si vous restaurez une LUN existante, un clone de LUN est créé et sauvegardé sous le format d'une copie Snapshot. Pendant l'opération de restauration, vous pouvez lire et écrire sur la LUN.

Par défaut, les fichiers contenant des flux sont restaurés.

### Étapes

1. Lister les copies Snapshot dans un volume :

```
volume snapshot show -vserver SVM -volume volume
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant montre les copies Snapshot dans `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

| Vserver | Volume | Snapshot               | State | Size  | Total% | Used% |
|---------|--------|------------------------|-------|-------|--------|-------|
| -----   | -----  | -----                  | ----- | ----- | -----  | ----- |
| vs1     | vol1   | hourly.2013-01-25_0005 | valid | 224KB | 0%     | 0%    |
|         |        | daily.2013-01-25_0010  | valid | 92KB  | 0%     | 0%    |
|         |        | hourly.2013-01-25_0105 | valid | 228KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0205 | valid | 236KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0305 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0405 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0505 | valid | 244KB | 0%     | 0%    |

7 entries were displayed.

2. Restaurer un fichier à partir d'une copie Snapshot :

```
volume snapshot restore-file -vserver SVM -volume volume -snapshot snapshot
-path file_path -restore-path destination_path
```



Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant restaure le fichier `myfile.txt`:

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

### Restaurez une partie d'un fichier à partir d'une copie Snapshot

Vous pouvez utiliser le `volume snapshot partial-restore-file` Commande permettant de restaurer une plage de données à partir d'une copie Snapshot vers une LUN ou vers un fichier de conteneur NFS ou SMB, en supposant que vous connaissez le décalage d'octet de départ des données et le nombre d'octets. Vous pouvez utiliser cette commande pour restaurer l'une des bases de données d'un hôte qui stocke plusieurs bases de données dans la même LUN.

À partir de ONTAP 9.12.1, une restauration partielle est disponible pour les volumes utilisant [Synchronisation active SnapMirror](#).

#### Étapes

1. Lister les copies Snapshot dans un volume :

```
volume snapshot show -vserver SVM -volume volume
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant montre les copies Snapshot dans `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

| Vserver | Volume | Snapshot               | State | Size  | Total% | Used% |
|---------|--------|------------------------|-------|-------|--------|-------|
| -----   | -----  | -----                  | ----- | ----- | -----  | ----- |
| vs1     | vol1   | hourly.2013-01-25_0005 | valid | 224KB | 0%     | 0%    |
|         |        | daily.2013-01-25_0010  | valid | 92KB  | 0%     | 0%    |
|         |        | hourly.2013-01-25_0105 | valid | 228KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0205 | valid | 236KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0305 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0405 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0505 | valid | 244KB | 0%     | 0%    |

7 entries were displayed.

2. Restaurer une partie d'un fichier à partir d'une copie Snapshot :

```
volume snapshot partial-restore-file -vserver SVM -volume volume -snapshot
snapshot -path file_path -start-byte starting_byte -byte-count byte_count
```

Le décalage d'octet de départ et le nombre d'octets doivent être des multiples de 4,096.

L'exemple suivant restaure les 4,096 premiers octets du fichier `myfile.txt`:

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume
vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt -start-byte 0
-byte-count 4096
```

### Restaurer le contenu d'un volume à partir d'une copie Snapshot

Vous pouvez restaurer un volume à un point antérieur, grâce à la restauration à partir d'une copie Snapshot. Vous pouvez utiliser System Manager ou `volume snapshot restore` la commande pour restaurer le contenu d'un volume à partir d'une copie Snapshot.


#### Description de la tâche

Si le volume possède des relations SnapMirror, répliquez manuellement toutes les copies miroir du volume immédiatement après la restauration à partir d'une copie Snapshot. Cette opération risque d'entraîner des copies miroir inutilisables qui doivent d'être supprimées et recrées.

#### Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour effectuer une restauration à partir d'une copie Snapshot antérieure.

## System Manager

1. Cliquez sur **Storage** et sélectionnez un volume.
2. Sous **copies Snapshot**, cliquez sur  en regard de la copie Snapshot que vous souhaitez restaurer, puis sélectionnez **Restaurer**.

## CLI

1. Lister les copies Snapshot dans un volume :

```
volume snapshot show -vserver <SVM> -volume <volume>
```

L'exemple suivant montre les copies Snapshot dans vol1:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

| Vserver | Volume | Snapshot               | State | Size  | Total% | Used% |
|---------|--------|------------------------|-------|-------|--------|-------|
| -----   | -----  | -----                  | ----- | ----- | -----  | ----- |
| vs1     | vol1   | hourly.2013-01-25_0005 | valid | 224KB | 0%     | 0%    |
|         |        | daily.2013-01-25_0010  | valid | 92KB  | 0%     | 0%    |
|         |        | hourly.2013-01-25_0105 | valid | 228KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0205 | valid | 236KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0305 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0405 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0505 | valid | 244KB | 0%     | 0%    |

7 entries were displayed.

2. Restaurer le contenu d'un volume à partir d'une copie Snapshot :

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

L'exemple suivant restaure le contenu de vol1:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

## Réplication de volume SnapMirror

## Notions de base sur la reprise après incident asynchrone SnapMirror

*SnapMirror* est une technologie de reprise après incident conçue pour le basculement du stockage primaire vers le stockage secondaire sur un site distant. Comme son nom l'indique, SnapMirror crée une réplique ou *mirror* de vos données de travail dans un stockage secondaire à partir duquel vous pouvez continuer à transmettre des données en cas de catastrophe sur le site primaire.

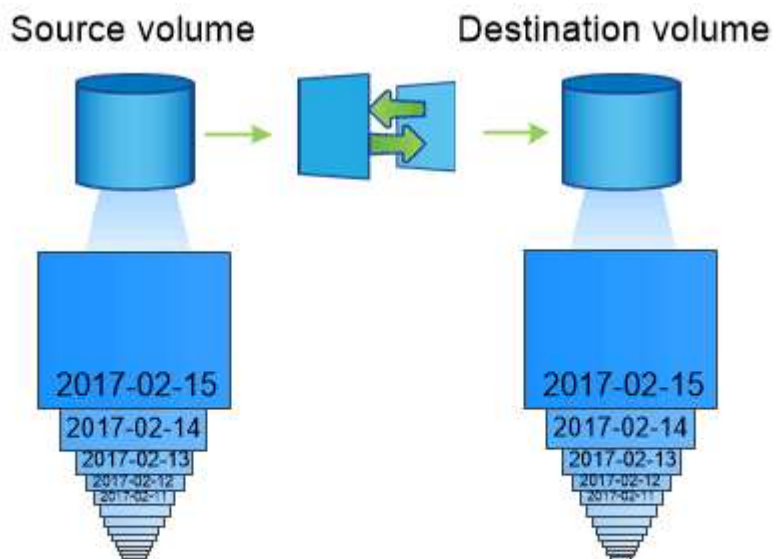
Si le site primaire assure toujours le service des données, il vous suffit de transférer les données requises vers celui-ci et ne transmet plus le tout aux clients depuis le miroir. Comme l'indique le cas de basculement, les contrôleurs du système secondaire doivent être équivalents ou presque équivalents aux contrôleurs du système primaire pour assurer un service efficace des données à partir du stockage en miroir.

### Relations de protection des données

Les données sont mises en miroir au niveau du volume. La relation entre le volume source du stockage primaire et le volume de destination du stockage secondaire est appelée « relation *protection des données* ». les clusters dans lesquels résident les volumes et les SVM qui fournissent des données à partir de ces volumes doivent être *peered*. Une relation de pairs permet l'échange de clusters et de SVM sécurité des données.

#### "Cluster et SVM peering"

La figure ci-dessous illustre les relations de protection des données SnapMirror.



*A SnapMirror data protection relationship typically mirrors the Snapshot copies available on the source volume.*

### Portée des relations de protection des données

Vous pouvez créer une relation de protection des données directement entre des volumes ou entre les SVM qui possèdent des volumes. Dans une relation de protection des données de SVM, tout ou partie de la configuration du SVM, depuis les exportations NFS et les partages SMB jusqu'au RBAC, est répliqué, ainsi que les données des volumes que la SVM possède.

Vous pouvez également utiliser SnapMirror pour des applications spéciales de protection des données :

- Une *partage de charge mirror* du volume root du SVM permet de garantir que les données restent accessibles en cas de panne ou de basculement du nœud.
- Une relation de protection des données entre *SnapLock volumes* vous permet de répliquer des fichiers WORM sur un stockage secondaire.

#### "Archivage et conformité grâce à la technologie SnapLock"

- À partir de ONTAP 9.13.1, vous pouvez utiliser SnapMirror asynchrone pour protéger [groupes de cohérence](#). Depuis la version ONTAP 9.14.1, vous pouvez utiliser la réplication asynchrone SnapMirror pour la réplication de copies Snapshot granulaires par volume vers le cluster de destination à l'aide de la relation de groupe de cohérence. Pour plus d'informations, voir [Configurer la protection asynchrone SnapMirror](#).

### Comment les relations de protection des données SnapMirror sont initialisées

La première fois que vous appelez SnapMirror, il effectue un *transfert de base* du volume source vers le volume de destination. La *SnapMirror policy* pour la relation définit le contenu de la base et toutes les mises à jour.

Transfert de base avec la règle SnapMirror par défaut `MirrorAllSnapshots` implique les étapes suivantes :

- Créer une copie Snapshot du volume source.
- Transférez la copie Snapshot et tous les blocs de données qu'elle référence vers le volume de destination.
- Transférez les copies Snapshot restantes et moins récentes sur le volume source vers le volume de destination pour toute utilisation en cas de corruption du miroir « actif ».

### Mise à jour des relations de protection des données SnapMirror

Les mises à jour sont asynchrones, en fonction du planning que vous configurez. La conservation met en miroir la règle Snapshot sur la source.

À chaque mise à jour sous `MirrorAllSnapshots` SnapMirror crée une copie Snapshot du volume source, et transfère cette copie Snapshot ainsi que toutes les copies Snapshot qui ont été effectuées depuis la dernière mise à jour. Dans la sortie suivante du `snapmirror policy show` commande pour le `MirrorAllSnapshots` notez la règle suivante :

- `Create Snapshot` est « vrai », ce qui indique cela `MirrorAllSnapshots` Crée une copie Snapshot lorsque SnapMirror met à jour la relation.
- `MirrorAllSnapshots` Possède des règles « `m_created` » et « `All_source_snapshots` », ce qui indique que la copie Snapshot créée par SnapMirror et toutes les copies Snapshot effectuées depuis la dernière mise à jour sont transférées lorsque SnapMirror met à jour la relation.

```

cluster_dst:> snapmirror policy show -policy MirrorAllSnapshots -instance

 Vserver: vs0
SnapMirror Policy Name: MirrorAllSnapshots
SnapMirror Policy Type: async-mirror
 Policy Owner: cluster-admin
 Tries Limit: 8
 Transfer Priority: normal
Ignore accesstime Enabled: false
 Transfer Restartability: always
Network Compression Enabled: false
 Create Snapshot: true
 Comment: SnapMirror asynchronous policy for mirroring
all snapshots
 and the latest active file system.
 Total Number of Rules: 2
 Total Keep: 2
 Rules: SnapMirror Label Keep Preserve Warn
Schedule Prefix

sm_created 1 false 0 -
all_source_snapshots 1 false 0 -

```

## Politique MirrorLatest

Le préconfiguré MirrorLatest la politique fonctionne exactement de la même manière que MirrorAllSnapshots, Sauf que seule la copie Snapshot créée par SnapMirror est transférée à l'initialisation et à la mise à jour.

```

 Rules: SnapMirror Label Keep Preserve Warn
Schedule Prefix

sm_created 1 false 0 -

```

## Principes de base de la reprise d'activité synchrone SnapMirror

À partir de ONTAP 9.5, la technologie SnapMirror synchrone (SM-S) est prise en charge sur toutes les plateformes FAS et AFF disposant d'au moins 16 Go de mémoire et sur toutes les plateformes ONTAP Select. La technologie synchrone SnapMirror est une

fonction sous licence par nœud qui permet la réplication synchrone des données au niveau des volumes.

Cette fonctionnalité répond aux exigences réglementaires et nationales en matière de réplication synchrone dans les secteurs financiers, de la santé et autres secteurs réglementés où aucune perte de données n'est requise.

### Opérations synchrones SnapMirror autorisées

La limite du nombre d'opérations de réplication synchrone SnapMirror par paire HA dépend du modèle de contrôleur.

Le tableau ci-dessous répertorie le nombre d'opérations SnapMirror synchrones autorisées par paire haute disponibilité selon le type de plateforme et la version de ONTAP.

| Plateforme   | Versions antérieures à ONTAP 9.9.1 | ONTAP 9.9.1 | ONTAP 9.10.1 | ONTAP 9.11.1 à ONTAP 9.14.1 |
|--------------|------------------------------------|-------------|--------------|-----------------------------|
| AFF          | 80                                 | 160         | 200          | 400                         |
| ASA          | 80                                 | 160         | 200          | 400                         |
| FAS          | 40                                 | 80          | 80           | 80                          |
| ONTAP Select | 20                                 | 40          | 40           | 40                          |

### Fonctionnalités prises en charge

Le tableau suivant indique les fonctionnalités prises en charge par SnapMirror synchrone et les versions ONTAP dans lesquelles la prise en charge est disponible.

| Fonction                                                             | Version d'abord prise en charge | Informations supplémentaires |
|----------------------------------------------------------------------|---------------------------------|------------------------------|
| Antivirus sur le volume primaire de la relation synchrone SnapMirror | ONTAP 9.6                       |                              |

|                                                                                                                                                     |              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Réplication de copie Snapshot créée par les applications                                                                                            | ONTAP 9.7    | Si une copie Snapshot est étiquetée avec le libellé approprié au moment de <code>snapshot create</code> l'opération, via l'interface de ligne de commande ou l'API ONTAP, SnapMirror réplique synchrone les copies Snapshot, créées par l'utilisateur ou créées avec des scripts externes, après avoir mis les applications en veille. Les copies Snapshot planifiées créées à l'aide d'une règle Snapshot ne sont pas répliquées. Pour plus d'informations sur la réplication de copies Snapshot créées par les applications, reportez-vous à l'article suivant <a href="#">"Comment répliquer les snapshots créés par les applications avec SnapMirror synchrone"</a> de la base de connaissances : . |
| Suppression automatique des clones                                                                                                                  | ONTAP 9.6    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Les agrégats FabricPool avec règles de Tiering aucune, Snapshot ou Auto sont pris en charge avec la source et la destination synchrones SnapMirror. | ONTAP 9.5    | Le volume de destination d'un agrégat FabricPool ne peut pas être défini sur l'ensemble des règles de Tiering.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| FC                                                                                                                                                  | ONTAP 9.5    | Sur tous les réseaux pour lesquels la latence ne dépasse pas 10 ms.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| NVMe-FC                                                                                                                                             | ONTAP 9.7    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Clones de fichiers                                                                                                                                  | ONTAP 9.7    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| FPolicy sur le volume principal de la relation synchrone SnapMirror                                                                                 | ONTAP 9.6    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Quotas matériels et conditionnels sur le volume primaire de la relation synchrone SnapMirror                                                        | ONTAP 9.6    | Les règles de quota ne sont pas répliquées vers la destination. Par conséquent, la base de données de quota n'est pas répliquée vers la destination.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Relations synchrones intra-cluster                                                                                                                  | ONTAP 9.14.1 | Les volumes source et de destination sont placés sur différentes paires haute disponibilité. En cas de panne de l'intégralité du cluster, l'accès aux volumes ne sera pas possible tant que le cluster n'aura pas été restauré. Les relations synchrones SnapMirror intra-cluster contribueront à la limite globale de simultanément <a href="#">Relations par paire haute disponibilité</a> .                                                                                                                                                                                                                                                                                                          |
| ISCSI                                                                                                                                               | ONTAP 9.5    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Clones de LUN et clones d'espace de noms NVMe                                                                                                       | ONTAP 9.7    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Clones LUN sauvegardés par des copies Snapshot créées par les applications                                                                          | ONTAP 9.7    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Accès à des protocoles mixtes (NFS v3 et SMB)                                                                                                       | ONTAP 9.6    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



|                                                                                                                         |              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restauration NDMP/NDMP                                                                                                  | ONTAP 9.13.1 | Le cluster source et le cluster destination doivent exécuter ONTAP 9.13.1 ou une version ultérieure pour pouvoir utiliser NDMP avec SnapMirror synchrone. Pour plus d'informations, voir <a href="#">Transfert de données à l'aide d'une copie ndmp</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| CONTINUITÉ de l'ACTIVITÉ (SnapMirror Synchronous Operations) sans interruption sur les plateformes AFF/ASA, uniquement. | ONTAP 9.12.1 | La prise en charge de la continuité de l'activité vous permet d'effectuer de nombreuses tâches de maintenance courantes sans planifier de temps d'indisponibilité. Les opérations prises en charge incluent le basculement et le retour, ainsi que le déplacement de volumes, à condition qu'un seul nœud survive au sein de chacun des deux clusters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| NFS v4.2                                                                                                                | ONTAP 9.10.1 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| NFS v4.3                                                                                                                | ONTAP 9.5    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| NFS v4.0                                                                                                                | ONTAP 9.6    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| NFS v4.1                                                                                                                | ONTAP 9.6    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| NVMe/TCP                                                                                                                | 9.10.1       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Suppression de la limitation de fréquence d'opération de métadonnées élevée                                             | ONTAP 9.6    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Sécurité des données sensibles en transit avec le chiffrement TLS 1.2                                                   | ONTAP 9.6    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Restauration de fichiers uniques et partiels                                                                            | ONTAP 9.13.1 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SMB 2.0 ou version ultérieure                                                                                           | ONTAP 9.6    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Cascade miroir-miroir synchrone SnapMirror                                                                              | ONTAP 9.6    | La relation provenant du volume de destination de la relation synchrone SnapMirror doit être une relation asynchrone SnapMirror.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Reprise d'activité de SVM                                                                                               | ONTAP 9.6    | * Une source synchrone de SnapMirror peut également être une source de reprise d'activité de SVM, par exemple une configuration « Fan-Out » avec SnapMirror synchrone comme une seule étape et SVM de reprise d'activité comme l'autre. * Une source synchrone SnapMirror ne peut pas être une destination de reprise d'activité SVM, car SnapMirror synchrone ne prend pas en charge le cascading d'une source de protection des données. Vous devez relâcher la relation synchrone avant d'effectuer une resynchronisation de reprise d'activité SVM dans le cluster destination. * Une destination synchrone SnapMirror ne peut pas être une source de reprise d'activité SVM, car la reprise d'activité SVM ne prend pas en charge la réplication des volumes DP. Une resynchronisation de la source synchrone entraînerait la reprise d'activité du SVM excluant le volume DP dans le cluster de destination. |

|                                                                          |              |                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restauration sur bande vers le volume source                             | ONTAP 9.13.1 |                                                                                                                                                                                                                                                     |
| Parité temporelle entre les volumes source et de destination pour le NAS | ONTAP 9.6    | Si vous avez effectué une mise à niveau de ONTAP 9.5 vers ONTAP 9.6, l'horodatage est uniquement répliqué pour les fichiers nouveaux et modifiés du volume source. L'horodatage des fichiers existants dans le volume source n'est pas synchronisé. |

## Fonctions non prises en charge

Les fonctionnalités suivantes ne sont pas prises en charge avec les relations SnapMirror synchrones :

- Groupes de cohérence
- Systèmes DP\_optimisés (DPO)
- Volumes FlexGroup
- Volumes FlexCache
- Limitation globale
- Dans une configuration « Fan-Out », une seule relation peut être une relation synchrone SnapMirror ; toutes les autres relations du volume source doivent être des relations SnapMirror asynchrones.
- Déplacement de LUN
- Configurations MetroCluster
- Accès mixte SAN/NVMe  
Les LUN et les namespaces NVMe ne sont pas pris en charge sur le même volume ou SVM.
- SnapCenter
- Volumes SnapLock
- Copies Snapshot inviolables
- Sauvegarde sur bande ou restauration à l'aide de dump et SMTape sur le volume de destination
- Débit au sol (QoS min) pour les volumes source
- SnapRestore du volume
- VVol

## Modes de fonctionnement

SnapMirror synchrone dispose de deux modes de fonctionnement basés sur le type de la règle SnapMirror utilisée :

- **Mode de synchronisation** en mode de synchronisation, les opérations d'E/S d'application sont envoyées en parallèle aux systèmes de stockage primaire et secondaire. Si l'écriture dans le stockage secondaire n'est pas terminée, pour une raison quelconque, l'application peut continuer à écrire sur le stockage primaire. Une fois l'erreur corrigée, la technologie synchrone SnapMirror se resynchronise automatiquement avec le stockage secondaire et reprend la réplication du stockage primaire vers le stockage secondaire en mode synchrone. En mode synchrone, RPO=0 et RTO sont très faibles jusqu'à ce qu'une défaillance de réplication secondaire se produise. Ainsi, les objectifs RPO et RTO deviennent indéterminés, mais équivalent au temps de résolution du problème à l'origine de la défaillance de la réplication secondaire et de la resynchronisation à réaliser.

- **StrictSync mode** SnapMirror synchrone peut fonctionner en mode StrictSync. Si l'écriture sur le stockage secondaire n'est pas terminée, pour une raison quelconque, les E/S de l'application échouent, ce qui permet de s'assurer que les stockages primaire et secondaire sont identiques. Les E/S de l'application vers le primaire ne reprennent que lorsque la relation SnapMirror revient au InSync statut. En cas de panne du stockage primaire, les E/S des applications peuvent reprendre sur le système de stockage secondaire, après le basculement, sans perte de données. En mode StrictSync, le RPO est toujours nul et le RTO très faible.

## État des relations

L'état d'une relation synchrone SnapMirror est toujours en InSync cours de fonctionnement normal. Si le transfert SnapMirror échoue pour une raison quelconque, la destination n'est pas synchronisée avec la source et peut passer à l' `OutOfSync` état.

Pour les relations synchrones SnapMirror, le système vérifie automatiquement l'état de InSync la relation ou OutofSync) à un intervalle fixe. Si l'état de la relation est OutofSync, ONTAP déclenche automatiquement le processus de resynchronisation automatique pour ramener la relation à l' InSync`état. La resynchronisation automatique n'est déclenchée que si le transfert échoue en raison de certaines opérations, telles que le basculement non planifié du stockage à la source ou à la destination, ou en cas de panne réseau. Les opérations initiées par l'utilisateur telles que `snapmirror quiesce et snapmirror break ne déclenchent pas de resynchronisation automatique.

Si la relation devient OutofSync pour une relation synchrone SnapMirror en mode StrictSync, toutes les opérations d'E/S vers le volume primaire sont arrêtées. L' `OutOfSync` état de la relation synchrone SnapMirror en mode synchrone ne perturbe pas les opérations principales et les opérations d'E/S sont autorisées sur le volume principal.

## Informations associées

["Rapport technique NetApp 4733 : configuration synchrone et bonnes pratiques SnapMirror"](#)

## À propos des workloads pris en charge par les règles de synchronisation et de synchronisation StrictSync

Les règles StrictSync et Sync prennent en charge toutes les applications basées sur les LUN avec les protocoles FC, iSCSI et FC-NVMe, ainsi que les protocoles NFSv3 et NFSv4 pour les applications d'entreprise telles que les bases de données, VMware, les quotas, SMB, etc. À partir de la version ONTAP 9.6, SnapMirror synchrone peut être utilisé pour les services de fichiers d'entreprise tels que l'automatisation de la conception électronique (EDA), les répertoires locaux et les workloads de conception logicielle.

Dans ONTAP 9.5, pour une règle de synchronisation, vous devez tenir compte de quelques aspects importants lors de la sélection des workloads NFSv3 ou NFSv4. Le nombre d'opérations de lecture ou d'écriture de données par workload n'est pas pris en compte, car la règle de synchronisation peut gérer des workloads d'E/S haute capacité de lecture ou d'écriture. Dans ONTAP 9.5, les charges de travail dont la création de fichiers, la création de répertoires, les modifications d'autorisations liées aux fichiers ou les modifications d'autorisations de répertoire sont excessives peuvent ne pas convenir (on parle alors de charges de travail hautement métadonnées). Un workload de métadonnées élevé est un exemple de workload DevOps dans lequel vous créez plusieurs fichiers de test, exécutez une automatisation et supprimez les fichiers. Il est également possible, par exemple, de créer une charge de travail parallèle qui génère plusieurs fichiers temporaires lors de la compilation. L'impact d'un taux élevé d'activité de métadonnées d'écriture est qu'il peut entraîner une rupture temporaire entre les miroirs, ce qui bloque les E/S de lecture et d'écriture du client.

Depuis la version ONTAP 9.6, ces limitations sont supprimées et SnapMirror synchrone peut être utilisé pour les workloads de services de fichiers d'entreprise qui incluent des environnements multi-utilisateurs, tels que les répertoires locaux et les workloads de développement logiciel.

#### Informations associées

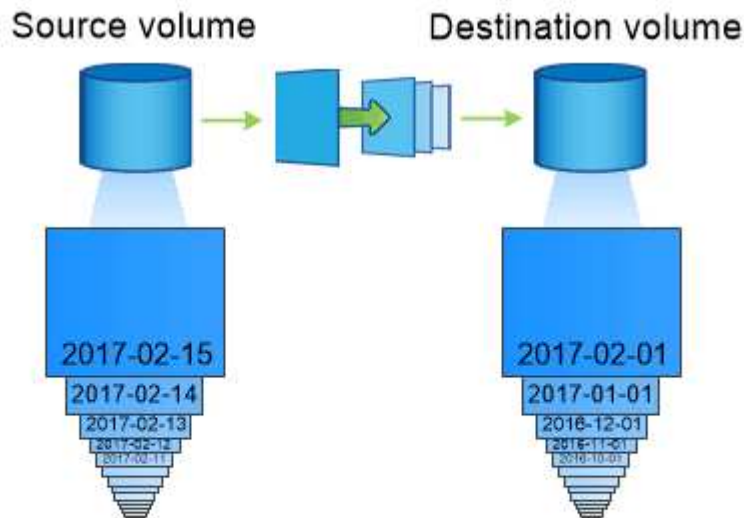
["Configuration synchrone de SnapMirror et bonnes pratiques"](#)

## Archivage à distance grâce à la technologie SnapMirror

Les règles d'archivage sécurisé SnapMirror remplacent la technologie SnapVault dans ONTAP 9.3 et versions ultérieures. Vous utilisez une règle de copie SnapMirror pour la réplication de copie Snapshot disque à disque à des fins de conformité aux normes et autres pour la gouvernance. Contrairement à une relation SnapMirror, dans laquelle la destination contient généralement uniquement les copies Snapshot actuellement dans le volume source, la destination d'une copie à distance conserve en général les copies Snapshot instantanées créées sur une période bien plus longue.

Vous pouvez conserver tous les mois des copies Snapshot de vos données sur une période de 20 ans, par exemple, pour vous conformer aux réglementations gouvernementales relatives à la comptabilité de votre entreprise. Etant donné qu'il n'est pas nécessaire de transmettre des données à partir du stockage Vault, vous pouvez utiliser des disques plus lents et moins coûteux sur le système de destination.

La figure ci-dessous illustre les relations de protection des données du coffre-fort SnapMirror.



*A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.*

#### Comment les relations de protection des données du coffre-fort sont initialisées

La règle SnapMirror pour la relation définit le contenu de la base et toutes les mises à jour.

Transfert de base sous la stratégie de coffre-fort par défaut XDPDefault Crée une copie Snapshot du volume source, puis transfère cette copie et les blocs de données qu'il renvoie vers le volume de destination.

Contrairement aux relations SnapMirror, une sauvegarde forte n'inclut pas d'anciennes copies Snapshot dans

la configuration de base.

Mise à jour des relations de protection des données Vault

Les mises à jour sont asynchrones, en fonction du planning que vous configurez. Les règles que vous définissez dans la règle pour la relation identifient les nouvelles copies Snapshot à inclure dans les mises à jour et le nombre de copies à conserver. Les libellés définis dans la politique (« mensuel », par exemple) doivent correspondre à un ou plusieurs libellés définis dans la politique Snapshot de la source. Dans le cas contraire, la réplication échoue.

À chaque mise à jour sous XDPDefault Cette règle transfère les copies Snapshot qui ont été effectuées depuis la dernière mise à jour, à condition que leurs étiquettes correspondent aux étiquettes définies dans les règles de règle. Dans la sortie suivante du snapmirror policy show commande pour le XDPDefault notez la règle suivante :

- Create Snapshot est « faux », ce qui indique cela XDPDefault Ne crée pas de copie Snapshot lorsque SnapMirror met à jour la relation.
- XDPDefault Dispose de règles « diotidienne » et « hebdomadaire », ce qui indique que toutes les copies Snapshot avec des étiquettes correspondantes sur la source sont transférées lorsque SnapMirror met à jour la relation.

```
cluster_dst::> snapmirror policy show -policy XDPDefault -instance

 Vserver: vs0
 SnapMirror Policy Name: XDPDefault
 SnapMirror Policy Type: vault
 Policy Owner: cluster-admin
 Tries Limit: 8
 Transfer Priority: normal
 Ignore accesstime Enabled: false
 Transfer Restartability: always
 Network Compression Enabled: false
 Create Snapshot: false
 Comment: Default policy for XDP relationships with
daily and weekly
 rules.
 Total Number of Rules: 2
 Total Keep: 59
 Rules: SnapMirror Label Keep Preserve Warn
Schedule Prefix

 daily 7 false 0 -
-
 weekly 52 false 0 -
-
```

## Notions de base sur la réplication unifiée SnapMirror

SnapMirror *réplication unifiée* permet de configurer la reprise après incident et l'archivage sur le même volume de destination. Lorsque la réplication unifiée est appropriée, elle offre des avantages en réduisant la quantité de stockage secondaire nécessaire, en limitant le nombre de transferts de base et en diminuant le trafic réseau.

### Mode d'initialisation des relations de protection unifiée des données

Comme pour SnapMirror, la protection unifiée des données effectue un transfert de base dès le premier appel que vous l'appellez. La règle SnapMirror pour la relation définit le contenu de la base et toutes les mises à jour.

Transfert de base avec la règle de protection des données unifiée par défaut `MirrorAndVault` Crée une copie Snapshot du volume source, puis transfère cette copie et les blocs de données qu'il renvoie vers le volume de destination. Tout comme l'archivage sécurisé, la protection unifiée des données n'inclut pas d'anciennes copies Snapshot de la ligne de base.

### Mise à jour des relations de protection unifiée des données

À chaque mise à jour sous `MirrorAndVault` Règle : SnapMirror crée une copie Snapshot du volume source et transfère la copie Snapshot ainsi que toutes les copies Snapshot créées depuis la dernière mise à jour, à condition que leurs étiquettes correspondent aux règles de règles Snapshot. Dans la sortie suivante du `snapmirror policy show` commande pour le `MirrorAndVault` notez la règle suivante :

- `Create Snapshot` est « vrai », ce qui indique cela `MirrorAndVault` Crée une copie Snapshot lorsque SnapMirror met à jour la relation.
- `MirrorAndVault` A règles « ``sm_created`` », « `quotidienne` » et « `hebdomadaire` », ce qui indique que la copie Snapshot créée par SnapMirror et les copies Snapshot portant des étiquettes correspondantes sur la source sont transférées lorsque SnapMirror met à jour la relation.

```
cluster_dst:> snapmirror policy show -policy MirrorAndVault -instance
```

```

 Vserver: vs0
 SnapMirror Policy Name: MirrorAndVault
 SnapMirror Policy Type: mirror-vault
 Policy Owner: cluster-admin
 Tries Limit: 8
 Transfer Priority: normal
 Ignore accesstime Enabled: false
 Transfer Restartability: always
 Network Compression Enabled: false
 Create Snapshot: true
 Comment: A unified SnapMirror synchronous and
SnapVault policy for
 mirroring the latest file system and daily
and weekly snapshots.
 Total Number of Rules: 3
 Total Keep: 59
 Rules: SnapMirror Label Keep Preserve Warn
Schedule Prefix

sm_created 1 false 0 -
-
daily 7 false 0 -
-
weekly 52 false 0 -
-
```

### Politique unifiée sur 7ans

Le préconfiguré Unified7year la politique fonctionne exactement de la même manière que MirrorAndVault, Sauf qu'une quatrième règle transfère les copies Snapshot mensuelles et les conserve pendant sept ans.

| Schedule Prefix | Rules: SnapMirror Label | Keep | Preserve | Warn |
|-----------------|-------------------------|------|----------|------|
| -----           | -----                   | ---- | -----    | ---- |
| -               | sm_created              | 1    | false    | 0 -  |
| -               | daily                   | 7    | false    | 0 -  |
| -               | weekly                  | 52   | false    | 0 -  |
| -               | monthly                 | 84   | false    | 0 -  |
| -               |                         |      |          |      |

## Protégez-vous contre les risques de corruption

La réplication unifiée limite le contenu du transfert de base vers la copie Snapshot créée par SnapMirror à l'initialisation. À chaque mise à jour, SnapMirror crée une autre copie Snapshot de la source et transfère cette copie Snapshot ainsi que toutes les nouvelles copies Snapshot dont les étiquettes correspondent aux règles définies dans les règles de règle Snapshot.

Vous pouvez vous protéger contre la possibilité de corruption d'une copie Snapshot mise à jour en créant une copie de la dernière copie Snapshot transférée sur le volume de destination. Cette « copie locale » est conservée indépendamment des règles de conservation à la source, de sorte que même si la copie Snapshot transférée à l'origine par SnapMirror n'est plus disponible sur la source, une copie de celle-ci sera disponible sur la destination.

## À quel moment utiliser la réplication unifiée des données

Vous devez évaluer les avantages de la maintenance d'un miroir complet par rapport aux avantages offerts par la réplication unifiée : réduction de la quantité de stockage secondaire, limitation du nombre de transferts de base et diminution du trafic réseau.

Le facteur clé pour déterminer la pertinence de la réplication unifiée est le taux de changement du système de fichiers actif. Un miroir traditionnel peut mieux convenir à un volume qui contient des copies Snapshot horaires de journaux de transactions de base de données, par exemple.

## XDP remplace DP par défaut SnapMirror

Depuis ONTAP 9.3, le mode SnapMirror Extended Data protection (XDP) remplace le mode SnapMirror Data protection (DP) par défaut.

Avant de mettre à niveau votre système vers ONTAP 9.12.1, vous devez convertir les relations de type DP en relation XDP avant de pouvoir procéder à une mise à niveau vers ONTAP 9.12.1 et versions ultérieures. Pour plus d'informations, voir ["Convertir une relation de type DP existante en XDP"](#).

Jusqu'à ONTAP 9.3, SnapMirror invoqué en mode DP et SnapMirror invoqué en mode XDP utilisait différents moteurs de réplication, avec différentes approches de la dépendance vis-à-vis de la version :

- SnapMirror appelé en mode DP utilisait un moteur de réplication *version-dépendante* dans lequel la version de ONTAP était requise pour le stockage primaire et secondaire :



```
cluster_dst:> snapmirror create -type DP -source-path ... -destination
-path ...
```

- SnapMirror appelé en mode XDP utilisait un moteur de réplication *version-flexible* qui prenait en charge différentes versions ONTAP sur le stockage primaire et secondaire :

```
cluster_dst:> snapmirror create -type XDP -source-path ...
-destination-path ...
```

Grâce aux améliorations des performances, les avantages significatifs de SnapMirror flexible à la version compensent légèrement l'avantage en termes de débit de réplication obtenu avec le mode dépendant de la version. C'est pour cette raison, depuis ONTAP 9.3, le mode XDP est devenu le nouveau paramètre par défaut et toutes les invocations du mode DP sur la ligne de commande ou dans les scripts nouveaux ou existants sont automatiquement converties en mode XDP.

Les relations existantes ne sont pas affectées. Si une relation est déjà de type DP, elle continuera d'être de type DP. Depuis ONTAP 9.5, MirrorAndVault est la nouvelle règle par défaut lorsqu'aucun mode de protection des données n'est spécifié ou lorsque le mode XDP est spécifié comme type de relation. Le tableau ci-dessous montre le comportement auquel vous pouvez vous attendre.

| Si vous spécifiez... | Le type est... | La stratégie par défaut (si vous ne spécifiez pas de règle) est... |
|----------------------|----------------|--------------------------------------------------------------------|
| DP                   | XDP            | MirrorAllsnapshots (reprise après incident SnapMirror)             |
| Rien                 | XDP            | MirrorAndVault (réplication unifiée)                               |
| XDP                  | XDP            | MirrorAndVault (réplication unifiée)                               |

Comme le tableau le montre, les règles par défaut attribuées à XDP dans différentes circonstances garantissent que la conversion conserve l'équivalence fonctionnelle des anciens types. Vous pouvez bien sûr utiliser différentes règles si nécessaire, y compris des règles pour la réplication unifiée :

| Si vous spécifiez...            | Et la politique est... | Résultat :                      |
|---------------------------------|------------------------|---------------------------------|
| DP                              | MirrorAllsnapshots     | Reprise sur incident SnapMirror |
| XDPDefault                      | SnapVault              | MirrorAndVault                  |
| Réplication unifiée             | XDP                    | MirrorAllsnapshots              |
| Reprise sur incident SnapMirror | XDPDefault             | SnapVault                       |

Les seules exceptions à la conversion sont les suivantes :

- Les relations de protection des données de SVM continuent à être par défaut en mode DP dans ONTAP 9.3 et versions antérieures.

Depuis ONTAP 9.4, les relations de protection des données du SVM sont définies par défaut en mode XDP

- Les relations de protection des données de partage de la charge du volume racine continuent à être par défaut en mode DP.
- Les relations de protection des données SnapLock continuent à être par défaut en mode DP dans ONTAP 9.4 et versions antérieures.

Depuis ONTAP 9.5, les relations de protection des données SnapLock se servent par défaut du mode XDP.

- Les invocations explicites de DP continuent à être activées par défaut avec le mode DP si vous définissez l'option d'ensemble du cluster suivante :

```
options replication.create_data_protection_rels.enable on
```

Cette option est ignorée si vous n'appellez pas explicitement DP.

## Lorsqu'un volume de destination augmente automatiquement

Lors d'un transfert de miroir de protection des données, la taille du volume de destination augmente automatiquement si le volume source a augmenté, à condition que l'espace disponible soit présent dans l'agrégat qui contient le volume.

Ce comportement se produit quel que soit le paramètre de croissance automatique sur la destination. Vous ne pouvez ni limiter la croissance du volume ni empêcher ONTAP de l'augmenter.

Par défaut, les volumes de protection des données sont définis sur le `grow_shrink` le mode `autosize`, qui permet au volume d'augmenter ou de diminuer en réponse à la quantité d'espace utilisé. La taille automatique max. Des volumes de protection des données est égale à la taille maximale des FlexVol et dépend de la plateforme. Par exemple :

- FAS6220, DP volume DP max-autosize par défaut = 70 To
- FAS8200, volume DP par défaut max. Par auto = 100 To

Pour plus d'informations, voir ["NetApp Hardware Universe"](#).

## Déploiements de la protection des données en cascade et « Fan-Out »

Vous pouvez utiliser un déploiement *Fan-Out* pour étendre la protection des données à plusieurs systèmes secondaires. Vous pouvez utiliser un déploiement *cascade* pour étendre la protection des données aux systèmes tertiaires.

Les déploiements « Fan-Out » et « Cascade » prennent en charge toutes les combinaisons de SnapMirror DR, SnapVault ou de réplication unifiée. Cependant, les relations SnapMirror synchrones (prises en charge depuis ONTAP 9.5) prennent uniquement en charge les déploiements « Fan-Out » avec une ou plusieurs relations SnapMirror asynchrones et ne prennent pas en charge les déploiements en cascade. Une seule relation de la configuration « Fan-Out » peut être une relation synchrone SnapMirror ; toutes les autres relations du volume

source doivent être des relations SnapMirror asynchrones. [Synchronisation active SnapMirror](#) (Pris en charge à partir de ONTAP 9.3.1) prend également en charge les configurations « Fan-Out ».



Vous pouvez utiliser un déploiement *Fan-In* pour créer des relations de protection des données entre plusieurs systèmes primaires et un seul système secondaire. Chaque relation doit utiliser un volume différent sur le système secondaire.

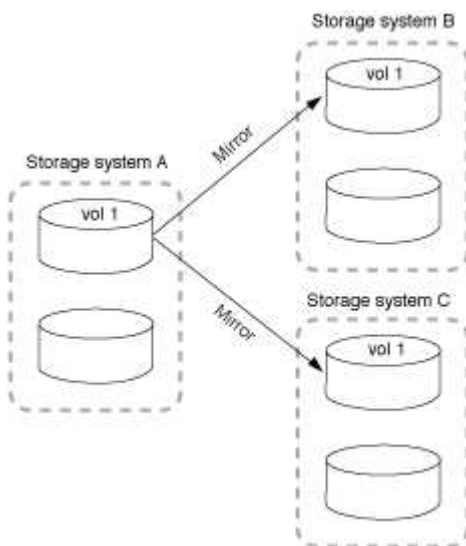


Sachez que les volumes faisant partie d'une configuration en cascade ou en « Fan-Out » peuvent prendre plus de temps resynchroniser. Il n'est pas rare d'avoir accès aux rapports de relation SnapMirror l'état « préparation » pour une période prolongée.

## Fonctionnement des déploiements « Fan-Out »

SnapMirror prend en charge les déploiements *plusieurs-miroirs* et *mirror-vault* Fan-Out.

Un déploiement à plusieurs miroirs multiples sur « Fan-Out » comprend un volume source possédant une relation de mise en miroir sur plusieurs volumes secondaires.



Le déploiement de « fan-out » en miroir-coffre-fort consiste en un volume source avec une relation de miroir vers un volume secondaire et une relation SnapVault vers un autre volume secondaire.



À partir de ONTAP 9.5, vous pouvez avoir des déploiements « Fan-Out » avec des relations SnapMirror synchrones. Cependant, une seule relation de la configuration « Fan-Out » peut être une relation SnapMirror synchrone, toutes les autres relations du volume source doivent être des relations SnapMirror asynchrones.



### Fonctionnement des déploiements en cascade

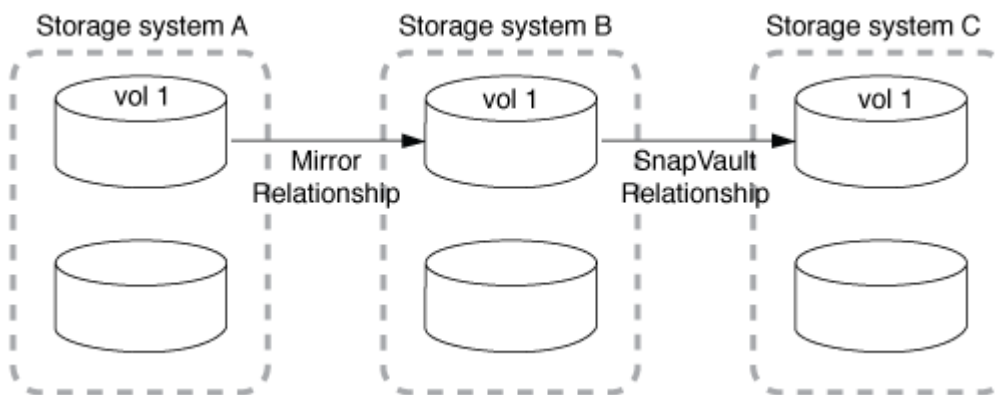
SnapMirror prend en charge les déploiements *mirror-mirror*, *mirror-vault*, *vault-mirror* et *vault-vault* cascade.

Le déploiement en cascade de mise en miroir consiste en une chaîne de relations dans laquelle un volume source est mis en miroir sur un volume secondaire, et le volume secondaire est mis en miroir sur un volume tertiaire. Si le volume secondaire n'est plus disponible, vous pouvez synchroniser la relation entre les volumes primaire et tertiaire sans effectuer de nouveau transfert de base.

Depuis ONTAP 9.6, les relations SnapMirror synchrones sont prises en charge dans un déploiement en cascade miroir-miroir. Seuls les volumes principaux et secondaires peuvent se trouver dans une relation synchrone SnapMirror. La relation entre les volumes secondaires et les volumes tertiaires doit être asynchrone.



Le déploiement de la mise en miroir à distance en cascade consiste en une chaîne de relations dans laquelle le volume source est mis en miroir sur un volume secondaire, et le volume secondaire est copié sur un volume tertiaire.



Les déploiements vault-mirror et, depuis ONTAP 9.2, vault-vault-vault en cascade sont également pris en charge :

- Le déploiement de la mise en miroir en cascade de l'espace de stockage comprend une chaîne de relations dans laquelle le volume source est copié sur un volume secondaire et le volume secondaire est mis en miroir sur un volume tertiaire.
- (Depuis ONTAP 9.2), Le déploiement de coffre-fort en cascade consiste en une chaîne de relations dans laquelle un volume source est copié sur un volume secondaire, et le volume secondaire est copié sur un volume tertiaire.

#### Plus de lecture

- [Reprenez la protection dans une configuration « Fan-Out » avec la synchronisation active SnapMirror](#)

## Licences SnapMirror

### Présentation des licences SnapMirror

Depuis ONTAP 9.3, la licence a été simplifiée pour la réplique entre les instances ONTAP. Dans les versions de ONTAP 9, la licence SnapMirror prend en charge les relations d'archivage sécurisé et en miroir. Vous pouvez utiliser une licence SnapMirror pour prendre en charge la réplique ONTAP, aussi bien pour la sauvegarde que pour la reprise après incident.

Avant la version ONTAP 9.3, une licence SnapVault distincte était nécessaire pour configurer les relations *vault* entre les instances ONTAP. L'instance DP pouvait conserver un nombre plus élevé de copies Snapshot pour prendre en charge les cas d'utilisation de sauvegarde avec des durées de conservation plus longues. Une licence SnapMirror était nécessaire pour configurer les relations *mirror* entre les instances ONTAP, où chaque instance ONTAP devait conserver le même nombre de copies Snapshot (c'est-à-dire, une image *mirror*) pour prendre en charge les cas d'utilisation de reprise sur incident afin de permettre le basculement du cluster. Les licences SnapMirror et SnapVault sont toujours utilisées et prises en charge pour les versions ONTAP 8.x et 9.x.

Les licences SnapVault continuent de fonctionner et sont prises en charge aussi bien pour les versions ONTAP 8.x que 9.x, mais la licence SnapMirror peut être utilisée à la place d'une licence SnapVault et peut être utilisée pour les configurations en miroir et en coffre-fort.

Pour la réplication asynchrone ONTAP, à partir de ONTAP 9.3, un moteur de réplication unifié unique est utilisé pour configurer les règles de mode de protection étendue des données (XDP), où la licence SnapMirror peut être configurée pour une règle de miroir, une règle de copie à distance ou une règle de copie miroir-coffre. Une licence SnapMirror est requise sur les clusters source et de destination. Une licence SnapVault n'est pas requise si une licence SnapMirror est déjà installée. La licence perpétuelle asynchrone SnapMirror est incluse dans la suite logicielle ONTAP One installée sur les nouveaux systèmes AFF et FAS.

Les limites de configuration de la protection des données sont déterminées à l'aide de plusieurs facteurs, notamment la version de ONTAP, la plateforme matérielle et les licences installées. Pour plus d'informations, voir "[Hardware Universe](#)".

#### **Licence synchrone SnapMirror**

Depuis ONTAP 9.5, les relations SnapMirror synchrones sont prises en charge. Pour créer une relation synchrone SnapMirror, vous avez besoin des licences suivantes :

- La licence synchrone SnapMirror est requise à la fois sur le cluster source et sur le cluster destination.

La licence synchrone SnapMirror fait partie du "[Suite de licences ONTAP One](#)".

Si votre système a été acheté avant juin 2019 avec un bundle Premium ou Flash, vous pouvez télécharger une clé principale NetApp pour obtenir la licence synchrone SnapMirror requise sur le site de support NetApp : "[Clés de licence maîtresse](#)".

- La licence SnapMirror est requise sur le cluster source et le cluster cible.

#### **Licence cloud SnapMirror**

Depuis la version ONTAP 9.8, la licence cloud SnapMirror assure la réplication asynchrone des copies Snapshot entre des instances ONTAP et des terminaux de stockage objet. Les cibles de réplication peuvent être configurées à la fois via des magasins d'objets sur site et des services de stockage objet dans le cloud public compatibles S3 et S3. Les relations cloud SnapMirror sont prises en charge par les systèmes ONTAP vers les cibles de stockage objet préqualifiées.

SnapMirror Cloud n'est pas disponible en tant que licence autonome. Une seule licence est requise par cluster ONTAP. Outre une licence cloud SnapMirror, la licence asynchrone SnapMirror est également requise.

Pour créer une relation cloud avec SnapMirror, vous avez besoin des licences suivantes :

- Licence SnapMirror et licence cloud SnapMirror pour la réplication directe sur le terminal du magasin d'objets.
- Lors de la configuration d'un workflow de réplication à règles multiples (par exemple, disque à disque à

cloud), une licence SnapMirror est requise sur toutes les instances ONTAP, tandis que la licence cloud SnapMirror est uniquement requise pour le cluster source qui réplique directement sur le terminal de stockage objet.

A partir de ONTAP 9.9.1, vous pouvez ["Utilisez System Manager pour la réplication cloud SnapMirror"](#).

La liste des applications tierces cloud SnapMirror autorisées est publiée sur le site Web de NetApp.

### **Licence optimisée pour Data protection**

Les licences DPO (Data protection Optimized) ne sont plus vendues et DPO n'est pas pris en charge sur les plates-formes actuelles. Cependant, si vous disposez d'une licence DPO installée sur une plate-forme prise en charge, NetApp continue à fournir le support jusqu'à la fin de la disponibilité de cette plate-forme.

DPO n'est pas inclus avec le pack de licences ONTAP One et vous ne pouvez pas mettre à niveau vers le pack de licences ONTAP One si la licence DPO est installée sur un système.

Pour plus d'informations sur les plates-formes prises en charge, voir ["Hardware Universe"](#).

### **Installez les licences cloud SnapMirror**

Les relations cloud de SnapMirror peuvent être orchestrées à l'aide d'applications de sauvegarde tierces préqualifiées. Depuis la version ONTAP 9.9.1, vous pouvez également utiliser System Manager pour orchestrer la réplication cloud SnapMirror. Des licences de capacité cloud SnapMirror et SnapMirror sont requises pour orchestrer les sauvegardes de stockage objet avec ONTAP sur site à l'aide de System Manager. Vous devez également demander et installer la licence d'API cloud SnapMirror.

### **Description de la tâche**

Les licences SnapMirror cloud et SnapMirror S3 sont des licences de cluster, pas des licences de nœud. Elles sont donc *non* fournies avec le bundle de licences ONTAP One. Ces licences sont incluses dans le pack de compatibilité ONTAP One distinct. Pour activer le cloud SnapMirror, vous devez demander ce pack.

En outre, l'orchestration par System Manager des sauvegardes cloud SnapMirror vers le stockage objet nécessite une clé d'API cloud SnapMirror. Cette licence d'API est une licence à instance unique au niveau du cluster, ce qui signifie qu'il n'est pas nécessaire de l'installer sur chaque nœud du cluster.

### **Étapes**

Vous devez demander et télécharger le pack de compatibilité ONTAP One et la licence d'API cloud SnapMirror, puis les installer à l'aide de System Manager.

1. Recherchez et enregistrez l'UUID de cluster pour le cluster que vous souhaitez obtenir une licence.

L'UUID de cluster est requis lorsque vous envoyez votre demande de commande du bundle ONTAP One Compatibility pour votre cluster.

2. Contactez votre équipe commerciale NetApp et demandez le pack compatibilité ONTAP One.
3. Demandez la licence d'API cloud SnapMirror en suivant les instructions fournies sur le site du support NetApp.

["Demandez la clé de licence de l'API cloud SnapMirror"](#)

4. Une fois que vous avez reçu et téléchargé les fichiers de licence, utilisez System Manager pour

télécharger le fichier NLF de compatibilité cloud ONTAP et le fichier NLF de l'API cloud SnapMirror sur le cluster :

- a. Cliquez sur **Cluster > Paramètres**.
- b. Dans la fenêtre **Paramètres**, cliquez sur **licences**.
- c. Dans la fenêtre **licences**, cliquez sur **+ Add**.
- d. Dans la boîte de dialogue **Ajouter une licence**, cliquez sur **Parcourir** pour sélectionner le fichier NLF que vous avez téléchargé, puis cliquez sur **Ajouter** pour télécharger le fichier sur le cluster.

#### Informations associées

["Sauvegardez les données dans le cloud avec SnapMirror"](#)

["Recherche de licences logicielles NetApp"](#)

## Améliorations des fonctionnalités des systèmes DPO

Depuis ONTAP 9.6, le nombre maximal de volumes FlexVol pris en charge augmente lorsque la licence DP\_Optimized (DPO) est installée. Depuis ONTAP 9.4, les systèmes dotés d'une licence DPO prennent en charge la fonctionnalité SnapMirror Backoff, la déduplication en arrière-plan entre les volumes, l'utilisation des blocs Snapshot comme donneurs et la compaction.

Depuis ONTAP 9.6, le nombre maximal de volumes FlexVol pris en charge sur les systèmes de protection des données ou secondaires a augmenté pour vous permettre de monter jusqu'à 2,500 volumes FlexVol par nœud ou jusqu'à 5,000 en mode de basculement. L'augmentation des volumes FlexVol est activée avec ["Licence DP\\_Optimized \(DPO\)"](#). A ["Licence SnapMirror"](#) reste requis sur les nœuds source et de destination.

À partir de ONTAP 9.4, les fonctions suivantes sont améliorées pour les systèmes DPO :

- Retour arrière SnapMirror : dans les systèmes DPO, le trafic de réplication se voit attribuer la même priorité que les charges de travail client.

La désactivation de la sauvegarde SnapMirror est désactivée par défaut sur les systèmes DPO.

- La déduplication en arrière-plan des volumes et la déduplication en arrière-plan entre les volumes : la déduplication en arrière-plan des volumes et la déduplication en arrière-plan entre les volumes sont activées dans les systèmes DPO.

Vous pouvez exécuter le `storage aggregate efficiency cross-volume-dedupe start -aggregate aggregate_name -scan-old-data true` commande de déduplication des données existantes. Il est recommandé d'exécuter la commande pendant les heures creuses afin de réduire l'impact sur les performances.

- Économies accrues grâce à l'utilisation des blocs Snapshot en tant que donneurs : les blocs de données non disponibles dans le système de fichiers actif, mais bloqués dans des copies Snapshot, sont utilisés comme donneurs pour la déduplication du volume.

Les nouvelles données peuvent être dédupliquées avec les données piégées dans les copies Snapshot, ce qui est également le partage efficace des blocs Snapshot. L'augmentation de l'espace de donneurs permet de réaliser plus d'économies, notamment lorsque le volume possède un grand nombre de copies Snapshot.



- Compaction : la compaction des données est activée par défaut sur les volumes DPO.

## Gérer la réplication de volume SnapMirror

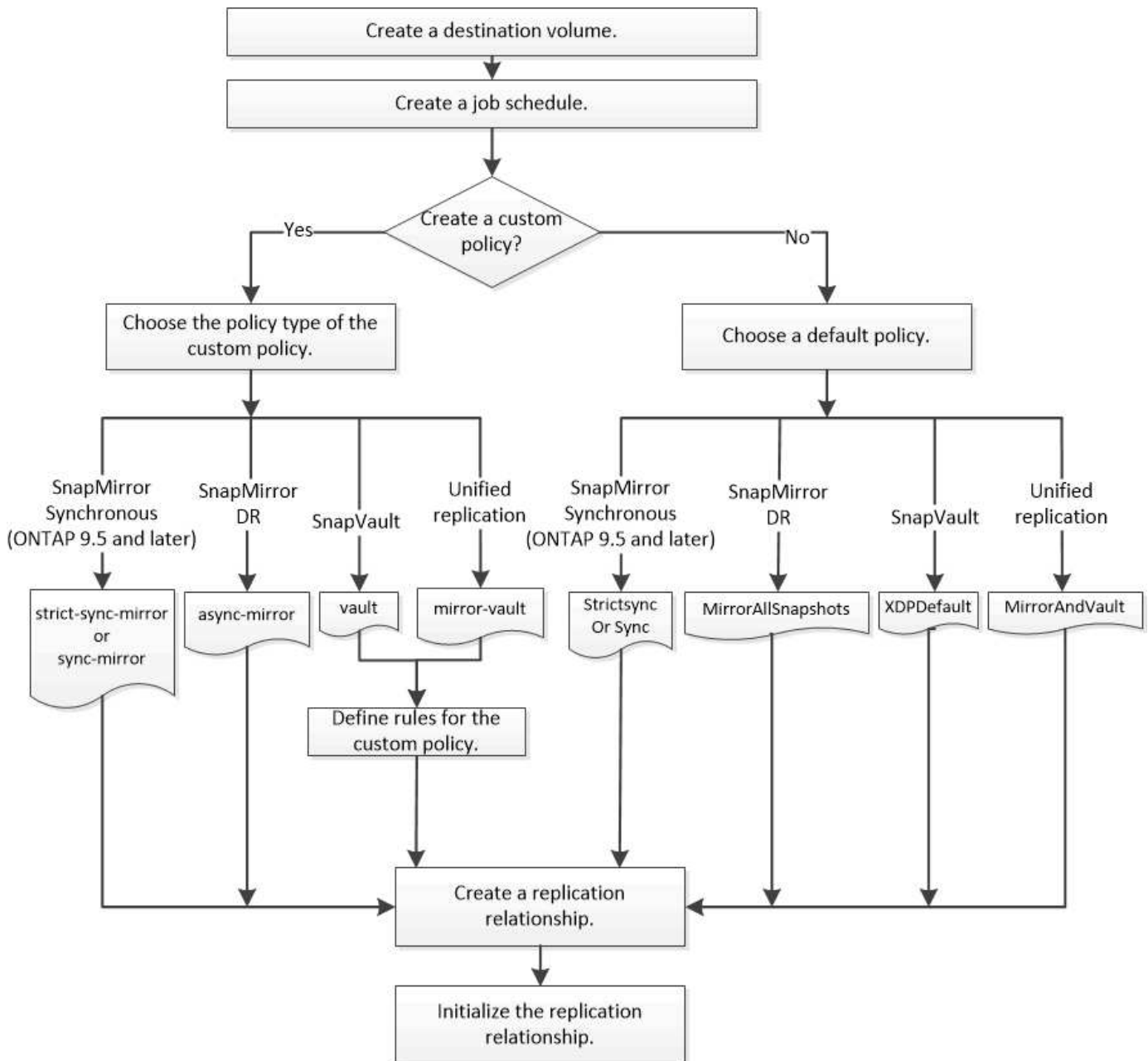
### Workflow de réplication SnapMirror

SnapMirror propose trois types de relation de protection des données : la reprise après incident SnapMirror, l'archivage (anciennement SnapVault) et la réplication unifiée. Vous pouvez suivre le même workflow de base pour configurer chaque type de relation.

À compter de la disponibilité générale dans ONTAP 9.9.1, "[Synchronisation active SnapMirror](#)" Assure un délai de restauration nul (RTO nul) ou un basculement transparent des applications (TAF) pour permettre le basculement automatique des applications stratégiques dans les environnements SAN.

Pour chaque type de relation SnapMirror de protection des données, le workflow est identique : créer un volume de destination, créer un job schedule, spécifier une règle, créer et initialiser la relation.

Vous pouvez utiliser ONTAP 9.3 à partir de `snapmirror protect` commande permettant de configurer une relation de protection des données en une seule étape. Même si vous utilisez `snapmirror protect`, vous devez comprendre chaque étape du workflow.



## Configurer une relation de réplication en une seule étape

Vous pouvez utiliser ONTAP 9.3 à partir de `snapmirror protect` commande permettant de configurer une relation de protection des données en une seule étape. Vous spécifiez une liste de volumes à répliquer, un SVM sur le cluster de destination, une planification de tâches et une policy SnapMirror. `snapmirror protect` se charge du reste.

### Ce dont vous avez besoin

- Les clusters source et de destination et les SVM doivent être associés.

["Cluster et SVM peering"](#)

- La langue du volume de destination doit être identique à celle du volume source.

## Description de la tâche

Le `snapmirror protect` La commande choisit un agrégat associé au SVM spécifié. Si aucun agrégat n'est associé à la SVM, il choisit tous les agrégats du cluster. Le choix de l'agrégat dépend de la quantité d'espace libre et du nombre de volumes sur l'agrégat.

Le `snapmirror protect` puis effectue les opérations suivantes :

- Crée un volume de destination avec un type et une quantité appropriés d'espace réservé pour chaque volume de la liste des volumes à répliquer.
- Configure une relation de réplication appropriée à la règle que vous spécifiez.
- Initialise la relation.

Le nom du volume de destination est du formulaire `source_volume_name_dst`. En cas de conflit avec le nom existant, la commande ajoute un nombre au nom du volume. Vous pouvez indiquer un préfixe et/ou un suffixe dans les options de la commande. Ce suffixe remplace le système fourni `dst` suffixe.

Dans ONTAP 9.3 et version antérieure, un volume de destination peut contenir jusqu'à 251 copies Snapshot. Dans ONTAP 9.4 et versions ultérieures, un volume de destination peut contenir jusqu'à 1019 copies Snapshot.



L'initialisation peut prendre beaucoup de temps. `snapmirror protect` n'attend pas la fin de l'initialisation avant la fin du travail. Pour cette raison, vous devez utiliser le `snapmirror show` plutôt que le `job show` commande pour déterminer une fois l'initialisation terminée.

Depuis ONTAP 9.5, vous pouvez créer des relations SnapMirror synchrones à l'aide de la `snapmirror protect` commande.

## Étape

1. Créer et initialiser une relation de réplication en une étape :

Vous devez remplacer les variables entre parenthèses angulaires par les valeurs requises avant d'exécuter cette commande.

```
snapmirror protect -path-list <SVM:volume> -destination-vserver
<destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
<true|false> -destination-volume-prefix <prefix> -destination-volume
-suffix <suffix>
```



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination. Le `-auto-initialize` l'option est définie par défaut sur « vrai ».

L'exemple suivant crée et initialise une relation SnapMirror DR à l'aide de la valeur par défaut `MirrorAllSnapshots` règle :

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
replication_daily
```



Vous pouvez utiliser une police personnalisée si vous préférez. Pour plus d'informations, voir "[Création d'une règle de réplication personnalisée](#)".

L'exemple suivant crée et initialise une relation SnapVault à l'aide de la valeur par défaut XDPDefault règle :

```
cluster_dst:> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

L'exemple suivant crée et initialise une relation de réplication unifiée à l'aide de la valeur par défaut MirrorAndVault règle :

```
cluster_dst:> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

L'exemple suivant crée et initialise une relation synchrone SnapMirror à l'aide de la Sync règle par défaut :

```
cluster_dst:> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```



Pour les règles de réplication SnapVault et unifiée, il est utile de définir une planification de la création d'une copie de la dernière copie Snapshot transférée sur la destination. Pour plus d'informations, voir "[Définition d'un programme de création d'une copie locale sur la destination](#)".

### Une fois que vous avez terminé

Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

## Configurer une relation de réplication une étape à la fois

### Créer un volume de destination

Vous pouvez utiliser le `volume create` commande située sur le volume de destination pour créer un volume de destination Le volume de destination doit avoir une taille égale ou supérieure à celle du volume source.

#### Étape

1. Créer un volume de destination :

```
volume create -vserver SVM -volume volume -aggregate aggregate -type DP -size
size
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant crée un volume de destination de 2 Go nommé `volA_dst`:

```
cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
-aggregate node01_aggr -type DP -size 2GB
```

## Créer une planification de tâche de réplication

La planification des tâches détermine lorsque SnapMirror met automatiquement à jour la relation de protection des données à laquelle la planification est attribuée. Vous pouvez utiliser System Manager ou `job schedule cron create` commande pour créer une planification de tâche de réplication.

### Description de la tâche

Vous affectez un planning de travail lorsque vous créez une relation de protection des données. Si vous n'attribuez pas de programme de travail, vous devez mettre à jour la relation manuellement.

### Étapes

Vous pouvez créer une planification de tâches de réplication à l'aide de System Manager ou de l'interface de ligne de commandes de ONTAP.

## System Manager

1. Accédez à **protection > vue d'ensemble** et développez **Paramètres de stratégie locale**.
2. Dans le volet **programmes**, cliquez sur ➔.
3. Dans la fenêtre **Schedules**, cliquez sur **+ Add**.
4. Dans la fenêtre **Ajouter un planning**, entrez le nom du planning et choisissez le contexte et le type de planning.
5. Cliquez sur **Enregistrer**.

## CLI

1. Création d'un programme de travail :

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

Pour `-month`, `-dayofweek`, et `-hour`, vous pouvez spécifier `all` pour exécuter le travail chaque mois, jour de la semaine et heure, respectivement.

Depuis ONTAP 9.10.1, vous pouvez inclure le vServer dans votre calendrier des tâches :

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```



La planification (RPO) minimale prise en charge pour les volumes FlexVol dans une relation SnapMirror volume est de 5 minutes. La planification (RPO) minimale prise en charge pour les volumes FlexGroup dans une relation SnapMirror volume est de 30 minutes.

L'exemple suivant crée un programme de travail nommé `my_weekly` Le samedi à 3:00 :

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

## Personnaliser une règle de réplication

### Création d'une règle de réplication personnalisée

Vous pouvez créer une stratégie de réplication personnalisée si la stratégie par défaut d'une relation n'est pas appropriée. Vous pouvez compresser les données d'un transfert réseau, par exemple, ou modifier le nombre de tentatives de transfert de copies Snapshot par SnapMirror.

Vous pouvez utiliser une règle par défaut ou personnalisée lorsque vous créez une relation de réplication. Pour une archive personnalisée (anciennement SnapVault) ou une règle de réplication unifiée, vous devez définir une ou plusieurs *règles* qui déterminent quelles copies Snapshot sont transférées au cours de l'initialisation et de la mise à jour. Vous pouvez également planifier la création de copies Snapshot locales sur la destination.

Le *policy type* de la règle de réplication détermine le type de relation qu'elle prend en charge. Le tableau ci-dessous présente les types de stratégies disponibles.

| Type de règle             | Type de relation                                                               |
|---------------------------|--------------------------------------------------------------------------------|
| mise en miroir asynchrone | Reprise sur incident SnapMirror                                                |
| coffre-fort               | SnapVault                                                                      |
| coffre-fort               | Réplication unifiée                                                            |
| miroir-synchro-strict     | SnapMirror synchrone en mode StrictSync (pris en charge à partir de ONTAP 9.5) |
| miroir synchrone          | SnapMirror synchrone en mode synchrone (pris en charge à partir de ONTAP 9.5)  |



Lorsque vous créez une stratégie de réplication personnalisée, il est conseillé de modéliser la stratégie après une stratégie par défaut.

Étapes

Vous pouvez créer des règles de protection des données personnalisées avec System Manager ou l'interface de ligne de commandes de ONTAP. Depuis ONTAP 9.11.1, vous pouvez utiliser System Manager pour créer des règles de miroir et de coffre-fort personnalisées, ainsi que pour afficher et sélectionner des règles héritées. Cette fonctionnalité est également disponible dans ONTAP 9.8P12 et versions ultérieures de ONTAP 9.8.

Créez des règles de protection personnalisées sur le cluster source et destination.

## System Manager

1. Cliquez sur **protection > Présentation > Paramètres de stratégie locale**.
2. Sous **politiques de protection**, cliquez sur ➔.
3. Dans le volet **stratégies de protection**, cliquez sur **+ Add**.
4. Entrez le nouveau nom de la stratégie et sélectionnez sa portée.
5. Choisissez un type de stratégie. Pour ajouter une stratégie de coffre-fort ou de miroir uniquement, choisissez **Asynchronous**, puis cliquez sur **utiliser un type de stratégie hérité**.
6. Renseignez les champs obligatoires.
7. Cliquez sur **Enregistrer**.
8. Répétez ces étapes sur l'autre cluster.

## CLI

1. Création d'une règle de réplication personnalisée :

```
snapmirror policy create -vserver <SVM> -policy _policy_ -type
<async-mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror>
-comment <comment> -tries <transfer_tries> -transfer-priority
<low|normal> -is-network-compression-enabled <true|false>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Depuis la version ONTAP 9.5, vous pouvez spécifier la planification de la création d'une planification commune des copies Snapshot pour les relations SnapMirror synchrones à l'aide du `-common -snapshot-schedule` paramètre. Par défaut, la planification commune des copies Snapshot pour les relations SnapMirror synchrones est d'une heure. Vous pouvez définir une valeur comprise entre 30 minutes et deux heures pour la planification des copies Snapshot des relations SnapMirror synchrones.

L'exemple suivant crée une règle de réplication personnalisée pour SnapMirror DR qui permet la compression réseau pour les transferts de données :

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_compressed -type async-mirror -comment "DR with network
compression enabled" -is-network-compression-enabled true
```

L'exemple suivant illustre la création d'une règle de réplication personnalisée pour SnapVault :

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_snapvault -type vault
```

L'exemple suivant crée une règle de réplication personnalisée pour la réplication unifiée :



```
cluster_dst:> snapmirror policy create -vserver svml -policy
my_unified -type mirror-vault
```

L'exemple suivant crée une règle de réplication personnalisée pour la relation synchrone SnapMirror en mode StrictSync :

```
cluster_dst:> snapmirror policy create -vserver svml -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

### Une fois que vous avez terminé

Pour les types de règles « vault » et « miroir-coffre-fort », vous devez définir des règles qui déterminent les copies Snapshot qui sont transférées lors de l'initialisation et de la mise à jour.

Utilisez le `snapmirror policy show` Commande pour vérifier que la règle SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

### Définir une règle pour une règle

Pour les règles personnalisées avec le type de règle « vault » ou « miroir-coffre-fort », vous devez définir au moins une règle qui détermine les copies Snapshot qui sont transférées lors de l'initialisation et de la mise à jour. Vous pouvez également définir des règles pour les stratégies par défaut avec le type de stratégie « coffre-fort » ou « miroir-coffre-fort ».

### Description de la tâche

Chaque règle avec le type de règle « vault » ou « miroir-coffre-fort » doit disposer d'une règle qui spécifie les copies Snapshot à répliquer. La règle « bimensuelle », par exemple, indique que seules les copies Snapshot affectées au label SnapMirror « bimensuel » doivent être répliquées. Vous spécifiez l'étiquette SnapMirror lors de la configuration de la règle Snapshot sur la source.

Chaque type de stratégie est associé à une ou plusieurs règles définies par le système. Ces règles sont automatiquement attribuées à une règle lorsque vous spécifiez son type de stratégie. Le tableau ci-dessous présente les règles définies par le système.

| Règle définie par le système | Utilisé dans les types de stratégie          | Résultat                                                                                                   |
|------------------------------|----------------------------------------------|------------------------------------------------------------------------------------------------------------|
| sm_créé                      | Async-mirror, mirror-vault, Sync, StrictSync | Une copie Snapshot créée par SnapMirror est transférée lors de l'initialisation et de la mise à jour.      |
| all_source_snapshots         | mise en miroir asynchrone                    | Les nouvelles copies Snapshot de la source sont transférées lors de l'initialisation et de la mise à jour. |

|                |                                |                                                                                                                                                                               |
|----------------|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tous les jours | coffre-fort,miroir-coffre-fort | Les nouvelles copies Snapshot de la source portant le label SnapMirror « `diotidienne` » sont transférées lors de l'initialisation et de la mise à jour.                      |
| hebdomadaire   | coffre-fort,miroir-coffre-fort | Les nouvelles copies Snapshot de la source portant l'étiquette SnapMirror « hebdomadaire » sont transférées lors de l'initialisation et de la mise à jour.                    |
| tous les mois  | coffre-fort                    | Les nouvelles copies Snapshot de la source avec le libellé SnapMirror « `mensuel` » sont transférées lors de l'initialisation et de la mise à jour.                           |
| cohérent_app   | Sync., StrictSync              | Les copies snapshot portant le label SnapMirror « APP_cohérent » sur la source sont répliquées de manière synchrone sur la destination. Pris en charge à partir de ONTAP 9.7. |

À l'exception du type de politique « async-mirror », vous pouvez spécifier des règles supplémentaires selon vos besoins, pour les stratégies par défaut ou personnalisées. Par exemple :

- Pour la valeur par défaut `MirrorAndVault` Politique, vous pouvez créer une règle appelée « deux mois » pour faire correspondre les copies Snapshot de la source avec l'étiquette SnapMirror « deux mois ».
- Dans le cas d'une règle personnalisée avec le type de règle « miroir-coffre-fort », vous pouvez créer une règle appelée « deux semaines » pour faire correspondre les copies Snapshot de la source avec l'étiquette SnapMirror « deux semaines ».

## Étape

1. Définir une règle pour une règle :

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
-label snapmirror-label -keep retention_count
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).

L'exemple suivant ajoute une règle avec l'étiquette SnapMirror `bi-monthly` par défaut `MirrorAndVault` règle :

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

L'exemple suivant ajoute une règle avec l'étiquette SnapMirror `bi-weekly` au personnalisé

my\_snapvault règle :

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

L'exemple suivant ajoute une règle avec l'étiquette SnapMirror app\_consistent au personnalisé Sync règle :

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

Vous pouvez ensuite répliquer les copies Snapshot à partir du cluster source correspondant à l'étiquette SnapMirror :

```
cluster_src::> snapshot create -vserver vs1 -volume voll -snapshot
snapshot1 -snapmirror-label app_consistent
```

#### Définissez un programme de création d'une copie locale sur la destination

Pour les relations SnapVault et de réplication unifiée, vous pouvez vous protéger contre la possibilité de corruption d'une copie Snapshot mise à jour en créant une copie de la dernière copie Snapshot transférée sur la destination. Cette « copie locale » est conservée indépendamment des règles de conservation à la source, de sorte que même si la copie Snapshot transférée à l'origine par SnapMirror n'est plus disponible sur la source, une copie de celle-ci sera disponible sur la destination.

#### Description de la tâche

Vous spécifiez le planning de création d'une copie locale dans `-schedule` de la `snapmirror policy add-rule` commande.

#### Étape

1. Définissez un planning de création d'une copie locale sur la destination :

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
-label snapmirror-label -schedule schedule
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man. Pour obtenir un exemple de création d'un programme de travail, reportez-vous à la section ["Création d'une planification de tâche de réplication"](#).

L'exemple suivant ajoute un calendrier de création d'une copie locale par défaut MirrorAndVault règle :

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
```

L'exemple suivant ajoute un calendrier de création d'une copie locale à la personnalisée `my_unified` règle :

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy
my_unified -snapmirror-label my_monthly -schedule my_monthly
```

## Créer une relation de réplication

La relation entre le volume source dans le stockage primaire et le volume de destination dans le stockage secondaire est appelée « relation de protection des données ». Vous pouvez utiliser le `snapmirror create` Créez des relations de protection des données avec SnapMirror de reprise après incident, SnapVault ou réplication unifiée.

Depuis ONTAP 9.11.1, System Manager permet de sélectionner des règles de copie en miroir et de copie à distance prédéfinies et personnalisées, d'afficher et de sélectionner des règles existantes, et de remplacer les planifications de transfert définies dans une règle de protection lorsque les volumes et les machines virtuelles de stockage sont protégés. Cette fonctionnalité est également disponible dans ONTAP 9.8P12 et versions ultérieures de ONTAP 9.8.



Si vous utilisez ONTAP 9.8P12 ou une version ultérieure de correctif ONTAP 9.8 et si vous avez configuré SnapMirror à l'aide de System Manager, vous devez utiliser ONTAP 9.9.1P13 ou version ultérieure et ONTAP 9.10.1P10 ou version ultérieure pour une mise à niveau vers ONTAP 9.9.1 ou ONTAP 9.10.1.

### Avant de commencer

- Les clusters source et de destination et les SVM doivent être associés.

["Cluster et SVM peering"](#)

- La langue du volume de destination doit être identique à celle du volume source.

### Description de la tâche

Jusqu'à ONTAP 9.3, SnapMirror invoqué en mode DP et SnapMirror invoqué en mode XDP utilisait différents moteurs de réplication, avec différentes approches de la dépendance vis-à-vis de la version :

- SnapMirror appelé en mode DP utilisait un moteur de réplication *version-dépendante* dans lequel la version de ONTAP était requise pour le stockage primaire et secondaire :

```
cluster_dst::> snapmirror create -type DP -source-path ... -destination
-path ...
```

- SnapMirror appelé en mode XDP utilisait un moteur de réplication *version-flexible* qui prenait en charge différentes versions ONTAP sur le stockage primaire et secondaire :

```
cluster_dst::> snapmirror create -type XDP -source-path ...
-destination-path ...
```

Grâce aux améliorations des performances, les avantages significatifs de SnapMirror flexible à la version compensent légèrement l'avantage en termes de débit de réplication obtenu avec le mode dépendant de la version. C'est pour cette raison, depuis ONTAP 9.3, le mode XDP est devenu le nouveau paramètre par défaut et toutes les invocations du mode DP sur la ligne de commande ou dans les scripts nouveaux ou existants sont automatiquement converties en mode XDP.

Les relations existantes ne sont pas affectées. Si une relation est déjà de type DP, elle continuera d'être de type DP. Le tableau ci-dessous montre le comportement auquel vous pouvez vous attendre.

| Si vous spécifiez... | Le type est... | La stratégie par défaut (si vous ne spécifiez pas de règle) est... |
|----------------------|----------------|--------------------------------------------------------------------|
| DP                   | XDP            | MirrorAllsnapshots (reprise après incident SnapMirror)             |
| Rien                 | XDP            | MirrorAllsnapshots (reprise après incident SnapMirror)             |
| XDP                  | XDP            | XDPDefault (SnapVault)                                             |

Voir également les exemples de la procédure ci-dessous.

Les seules exceptions à la conversion sont les suivantes :

- Les relations de protection des données des SVM continuent à être par défaut en mode DP.  
Spécifiez explicitement XDP pour obtenir le mode XDP par défaut MirrorAllSnapshots politique.
- Les relations de protection des données de partage de charge continuent à être par défaut en mode DP.
- Les relations de protection des données SnapLock continuent à être par défaut en mode DP.
- Les invocations explicites de DP continuent à être activées par défaut avec le mode DP si vous définissez l'option d'ensemble du cluster suivante :

```
options replication.create_data_protection_rels.enable on
```

Cette option est ignorée si vous n'appellez pas explicitement DP.

Dans ONTAP 9.3 et version antérieure, un volume de destination peut contenir jusqu'à 251 copies Snapshot. Dans ONTAP 9.4 et versions ultérieures, un volume de destination peut contenir jusqu'à 1019 copies Snapshot

Depuis ONTAP 9.5, les relations SnapMirror synchrones sont prises en charge.


À partir de ONTAP 9.14.1, l' `-backoff-level` option est ajoutée aux `snapmirror create` commandes , `snapmirror modify` et `snapmirror restore` pour vous permettre de spécifier le niveau de retour arrière par relation. L'option n'est prise en charge qu'avec les relations FlexVol SnapMirror. La commande facultative spécifie le niveau de backoff SnapMirror dû aux opérations du client. Les valeurs de retour arrière peuvent être élevées, moyennes ou aucune. La valeur par défaut est élevée.

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour créer une relation

de réplication.

## System Manager

1. Sélectionnez le volume ou le LUN à protéger : cliquez sur **Storage > volumes** ou **Storage > LUN**, puis cliquez sur le nom de volume ou de LUN souhaité.
2. Cliquez sur  **Protect**.
3. Sélectionnez le cluster de destination et la VM de stockage.
4. La règle asynchrone est sélectionnée par défaut. Pour sélectionner une stratégie synchrone, cliquez sur **plus d'options**.
5. Cliquez sur **protéger**.
6. Cliquez sur l'onglet **SnapMirror (local ou Remote)** du volume ou du LUN sélectionné pour vérifier que la protection est correctement configurée.

## CLI

1. Depuis le cluster destination, créer une relation de réplication :

Vous devez remplacer les variables entre parenthèses angulaires par les valeurs requises avant d'exécuter cette commande.

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Le schedule paramètre n'est pas applicable lors de la création de relations SnapMirror synchrones.

L'exemple suivant illustre la création d'une relation SnapMirror DR à l'aide de la valeur par défaut MirrorLatest règle :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
MirrorLatest
```

L'exemple suivant illustre la création d'une relation SnapVault à l'aide de la valeur par défaut XDPDefault règle :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
XDPDefault
```

L'exemple suivant illustre la création d'une relation de réplication unifiée à l'aide de la valeur par défaut MirrorAndVault règle :

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
MirrorAndVault
```

L'exemple suivant illustre la création d'une relation de réplication unifiée à l'aide de la commande personnalisée `my_unified` règle :

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
my_unified
```

L'exemple suivant illustre la création d'une relation synchrone SnapMirror à l'aide de la `Sync` règle par défaut :

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy Sync
```

L'exemple suivant illustre la création d'une relation synchrone SnapMirror à l'aide de la `StrictSync` règle par défaut :

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

L'exemple suivant illustre la création d'une relation SnapMirror DR. Lorsque le type DP est automatiquement converti en XDP et sans policy spécifiée, la règle passe par défaut sur le `MirrorAllSnapshots` règle :

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

L'exemple suivant illustre la création d'une relation SnapMirror DR. Sans type ni règle définie, la règle de gestion par défaut est définie sur le `MirrorAllSnapshots` règle :

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

L'exemple suivant illustre la création d'une relation SnapMirror DR. Sans règle spécifiée, la règle est définie par défaut sur le `XDPDefault` règle :



```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

L'exemple suivant crée une relation synchrone SnapMirror avec la règle prédéfinie SnapCenterSync :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```



La règle prédéfinie SnapCenterSync est de type Sync. Cette règle réplique toute copie Snapshot créée avec le snapmirror-label de « cohérent\_app ».

### Une fois que vous avez terminé

Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

### Informations associées

- ["Créez et supprimez des volumes de test de basculement SnapMirror"](#).

### D'autres façons de le faire dans ONTAP

| Pour effectuer ces tâches avec...                                          | Voir ce contenu...                                                       |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------|
| System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures) | <a href="#">"Présentation de la sauvegarde de volume avec SnapVault"</a> |

### Initialiser une relation de réplication

Pour tous les types de relations, l'initialisation effectue un *transfert de base* : il effectue une copie Snapshot du volume source, puis transfère cette copie et tous les blocs de données qu'elle référence au volume de destination. Dans le cas contraire, le contenu du transfert dépend de la police.

### Ce dont vous avez besoin

Les clusters source et de destination et les SVM doivent être associés.

["Cluster et SVM peering"](#)

### Description de la tâche

L'initialisation peut prendre beaucoup de temps. Vous pouvez exécuter le transfert de base en dehors des heures creuses.

Depuis ONTAP 9.5, les relations SnapMirror synchrones sont prises en charge.

### Étape

1. Initialiser une relation de réplication :

```
snapmirror initialize -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ...
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

L'exemple suivant initialise la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

### Exemple : configurer une cascade de coffre-fort

Un exemple montre en termes concrets comment vous pouvez configurer des relations de réplication une étape à la fois. Vous pouvez utiliser le déploiement Vault-vault en cascade configuré dans cet exemple pour conserver plus de 251 copies Snapshot étiquetées « my-hebdomadaire ».

#### Ce dont vous avez besoin

- Les clusters source et de destination et les SVM doivent être associés.
- Vous devez exécuter ONTAP 9.2 ou version ultérieure. Les cascades de coffre-fort ne sont pas prises en charge dans les versions précédentes de ONTAP.

#### Description de la tâche

L'exemple suppose ce qui suit :

- Vous avez configuré des copies Snapshot sur le cluster source avec les libellés SnapMirror « my-Daily », « my-hebdomadaire » et « my-monmensuel ».
- Des volumes de destination nommés « Vola » ont été configurés sur les clusters de destination secondaire et tertiaire.
- Vous avez configuré des planifications de tâches de réplication nommées « my\_snapvault » sur les clusters de destination secondaire et tertiaire.

L'exemple montre comment créer des relations de réplication basées sur deux règles personnalisées :

- La politique « napvault\_Secondary » conserve 3 7 copies Snapshot par jour, 5 52 hebdomadaires et 3 180 mois dans le cluster de destination secondaire.
- La « politique napvault\_tertiaire » conserve 250 copies Snapshot hebdomadaires sur le cluster de destination tertiaire.

#### Étapes

1. Sur le cluster de destination secondaire, créez la stratégie « napvault\_Secondary » :

```
cluster_secondary::> snapmirror policy create -policy snapvault_secondary
-type vault -comment "Policy on secondary for vault to vault cascade" -vserver
svm_secondary
```

2. Sur le cluster de destination secondaire, définissez la règle "my-Daily" pour la politique :

```
cluster_secondary:> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-daily -keep 7 -vserver svm_secondary
```

3. Sur le cluster de destination secondaire, définissez la règle "my-hebdomadaire" pour la politique :

```
cluster_secondary:> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-weekly -keep 52 -vserver svm_secondary
```

4. Sur le cluster de destination secondaire, définissez la règle "mois-mois" pour la politique :

```
cluster_secondary:> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-monthly -keep 180 -vserver svm_secondary
```

5. Sur le cluster de destination secondaire, vérifiez la policy :

```
cluster_secondary:> snapmirror policy show snapvault_secondary -instance
```

```

 Vserver: svm_secondary
SnapMirror Policy Name: snapvault_secondary
SnapMirror Policy Type: vault
 Policy Owner: cluster-admin
 Tries Limit: 8
 Transfer Priority: normal
Ignore accesstime Enabled: false
 Transfer Restartability: always
Network Compression Enabled: false
 Create Snapshot: false
 Comment: Policy on secondary for vault to vault
cascade
 Total Number of Rules: 3
 Total Keep: 239
 Rules: SnapMirror Label Keep Preserve Warn
Schedule Prefix

my-daily 7 false 0 -
-
my-weekly 52 false 0 -
-
my-monthly 180 false 0 -
-
```

6. Sur le cluster de destination secondaire, créez la relation avec le cluster source :

```
cluster_secondary:> snapmirror create -source-path svm_primary:volA
-destination-path svm_secondary:volA -type XDP -schedule my_snapvault -policy
```

```
snapvault_secondary
```

7. Sur le cluster destination secondaire, initialiser la relation avec le cluster source :

```
cluster_secondary::> snapmirror initialize -source-path svm_primary:volA
-destination-path svm_secondary:volA
```

8. Sur le cluster de destination tertiaire, créez la stratégie "napvault\_tertiaire" :

```
cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type
vault -comment "Policy on tertiary for vault to vault cascade" -vserver
svm_tertiary
```

9. Sur le cluster de destination tertiaire, définissez la règle "semaine-moyenne" pour la politique :

```
cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary
-snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
```

10. Sur le cluster de destination tertiaire, vérifiez la règle :

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```

 Vserver: svm_tertiary
SnapMirror Policy Name: snapvault_tertiary
SnapMirror Policy Type: vault
 Policy Owner: cluster-admin
 Tries Limit: 8
 Transfer Priority: normal
Ignore accesstime Enabled: false
 Transfer Restartability: always
Network Compression Enabled: false
 Create Snapshot: false
 Comment: Policy on tertiary for vault to vault
cascade
 Total Number of Rules: 1
 Total Keep: 250
 Rules: SnapMirror Label Keep Preserve Warn
Schedule Prefix

 my-weekly 250 false 0 -
-
```

11. Sur le cluster de destination tertiaire, créez la relation avec le cluster secondaire :

```
cluster_tertiary::> snapmirror create -source-path svm_secondary:volA
-destination-path svm_tertiary:volA -type XDP -schedule my_snapvault -policy
snapvault_tertiary
```

12. Sur le cluster destination tertiaire, initialisez la relation avec le cluster secondaire :

```
cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA
-destination-path svm_tertiary:volA
```

## Convertir une relation de type DP existante en XDP

Si vous procédez à une mise à niveau vers ONTAP 9.12.1 ou version ultérieure, vous devez convertir les relations de type DP en relation XDP avant la mise à niveau. ONTAP 9.12.1 et versions ultérieures ne prennent pas en charge les relations de type DP. Vous pouvez facilement convertir une relation de type DP existante en XDP pour tirer parti de SnapMirror flexible à la version.

### Description de la tâche

- SnapMirror ne convertit pas automatiquement les relations de type DP existantes en relation XDP. Pour convertir la relation, vous devez rompre et supprimer la relation existante, créer une nouvelle relation XDP et resynchroniser la relation. Pour plus d'informations, reportez-vous à la section "[XDP remplace DP par défaut SnapMirror](#)".
- Lors de la planification de votre conversion, notez que la préparation en arrière-plan et la phase d'entreposage des données d'une relation SnapMirror XDP peuvent prendre un certain temps. Il n'est pas rare de voir la relation SnapMirror indiquant l'état « préparation » pour une période prolongée.



Après avoir converti un type de relation SnapMirror de DP en XDP, les paramètres d'espace, tels que la taille automatique et la garantie d'espace ne sont plus répliqués vers la destination.

### Étapes

1. Depuis le cluster de destination, s'assurer que la relation SnapMirror est de type DP, que l'état du miroir est SnapMirror, que l'état de la relation est inactif et que la relation fonctionne correctement :

```
snapmirror show -destination-path <SVM:volume>
```

L'exemple suivant montre la sortie du `snapmirror show` commande :

```
cluster_dst:>snapmirror show -destination-path svm_backup:volA_dst
```

```
Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```



Vous pouvez le trouver utile de conserver une copie du `snapmirror show` sortie de la commande pour garder le suivi existant des paramètres de relation.

2. Depuis les volumes source et de destination, assurez-vous que les deux volumes disposent d'une copie Snapshot commune :

```
volume snapshot show -vserver <SVM> -volume <volume>
```

L'exemple suivant montre le `volume snapshot show` sortie pour les volumes source et de destination :

```
cluster_src:> volume snapshot show -vserver svm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%

svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.
```

```
cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%

svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. Pour vous assurer que les mises à jour planifiées ne s'exécutent pas pendant la conversion, mettez au repos la relation de type DP existante :

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["page de manuel"](#).



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

L'exemple suivant arrête la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

#### 4. Casser la relation de type DP existante :

```
snapmirror break -destination-path <SVM:volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous au ["page de manuel"](#).



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

L'exemple suivant rompt la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

#### 5. Si la suppression automatique des copies Snapshot est activée sur le volume de destination, désactivez-la :

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

L'exemple suivant désactive la suppression automatique de la copie Snapshot sur le volume de destination `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

#### 6. Supprimez la relation DP-type existante :

```
snapmirror delete -destination-path <SVM:volume>
```



Pour connaître la syntaxe complète de la commande, reportez-vous au ["page de manuel"](#).



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

L'exemple suivant supprime la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

#### 7. Relâcher la relation de reprise d'activité SVM d'origine sur la source :

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

L'exemple suivant permet de libérer la relation de SVM Disaster Recovery :

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

#### 8. Vous pouvez utiliser la sortie que vous avez conservée de l' `snapmirror show` Commande pour créer la nouvelle relation de type XDP :

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type XDP -schedule <schedule> -policy <policy>
```

La nouvelle relation doit utiliser le même volume source et destination. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

L'exemple suivant illustre la création d'une relation de reprise d'activité SnapMirror entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup` utilisation de la valeur par défaut `MirrorAllSnapshots` règle :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

#### 9. Resynchronisation des volumes source et de destination :

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Pour améliorer le temps de resynchronisation, vous pouvez utiliser le `-quick-resync` mais vous devez savoir que vous pouvez perdre des économies en matière d'efficacité du stockage. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man : "[Commande SnapMirror resync](#)".



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination. Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.

L'exemple suivant resynchronise la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

10. Si vous avez désactivé la suppression automatique de copies Snapshot, réactivez-la :

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

### Une fois que vous avez terminé

1. Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée.
2. Une fois que le volume de destination SnapMirror XDP commence à mettre à jour les copies Snapshot, comme défini par la règle SnapMirror, utilisez les valeurs de sortie de `snapmirror list-destinations` Commande depuis le cluster source pour afficher la nouvelle relation SnapMirror XDP

## Convertir le type de relation SnapMirror

À partir de ONTAP 9.5, SnapMirror synchrone est pris en charge. Vous pouvez convertir une relation asynchrone SnapMirror en relation synchrone SnapMirror, et inversement, sans effectuer de transfert de base.

### Description de la tâche

Vous ne pouvez pas convertir une relation asynchrone SnapMirror en relation synchrone SnapMirror, ni inversement, en modifiant la règle SnapMirror

### Étapes

- **Conversion d'une relation asynchrone SnapMirror en relation synchrone SnapMirror**

- a. Depuis le cluster destination, supprimer la relation asynchrone SnapMirror :

```
snapmirror delete -destination-path <SVM:volume>
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

- b. Depuis le cluster source, libérer la relation SnapMirror sans supprimer les copies Snapshot courantes :

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM>:<destination_volume>
```

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

- c. Depuis le cluster destination, créer une relation synchrone SnapMirror :

```
snapmirror create -source-path src_SVM:src_volume -destination-path
<destination_SVM>:<destination_volume> -policy sync-mirror
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

- d. Resynchroniser la relation synchrone SnapMirror :

```
snapmirror resync -destination-path <destination_SVM:destination_volume>
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

#### • Conversion d'une relation synchrone SnapMirror en relation asynchrone SnapMirror

- a. Depuis le cluster de destination, arrêter la relation synchrone SnapMirror existante :

```
snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

- b. Depuis le cluster destination, supprimer la relation asynchrone SnapMirror :

```
snapmirror delete -destination-path <SVM:volume>
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

- c. Depuis le cluster source, libérer la relation SnapMirror sans supprimer les copies Snapshot courantes :

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM:destination_volume>
```

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

d. Depuis le cluster destination, créer une relation asynchrone SnapMirror :

```
snapmirror create -source-path src_SVM:src_volume -destination-path
<destination_SVM:destination_volume> -policy MirrorAllSnapshots
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

e. Resynchroniser la relation synchrone SnapMirror :

```
snapmirror resync -destination-path <destination_SVM:destination_volume>
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

## Convertir le mode d'une relation synchrone SnapMirror

Depuis ONTAP 9.5, les relations SnapMirror synchrones sont prises en charge. Vous pouvez convertir le mode d'une relation synchrone SnapMirror de StrictSync en Sync ou vice versa.

### Description de la tâche

Vous ne pouvez pas modifier la règle d'une relation synchrone SnapMirror pour convertir son mode.

### Étapes

1. Depuis le cluster de destination, arrêter la relation synchrone SnapMirror existante :

```
snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

2. Depuis le cluster de destination, supprimer la relation synchrone SnapMirror existante :

```
snapmirror delete -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror delete -destination-path vs1_dr:vol1
```

3. Depuis le cluster source, libérer la relation SnapMirror sans supprimer les copies Snapshot courantes :

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM>:<destination_volume>
```

```
cluster1::> snapmirror release -relationship-info-only true -destination
-path vs1_dr:vol1
```

4. Depuis le cluster de destination, créer une relation synchrone SnapMirror en spécifiant le mode de conversion de la relation synchrone SnapMirror :

```
snapmirror create -source-path vs1:vol1 -destination-path
<destination_SVM>:<destination_volume> -policy Sync|StrictSync
```

```
cluster2::> snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy Sync
```

5. Depuis le cluster de destination, resynchroniser la relation SnapMirror :

```
snapmirror resync -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror resync -destination-path vs1_dr:vol1
```

## Créez et supprimez des volumes de test de basculement SnapMirror

Depuis la version ONTAP 9.14.1, vous pouvez utiliser System Manager pour créer un clone de volume afin de tester le basculement SnapMirror et la reprise d'activité sans interrompre la relation SnapMirror active. Une fois le test terminé, vous pouvez nettoyer les données associées et supprimer le volume test.

### Créez un volume de test de basculement SnapMirror


#### Description de la tâche


- Vous pouvez effectuer des tests de basculement sur des relations synchrones et asynchrones SnapMirror.
- Un clone de volume est créé pour effectuer le test de reprise d'activité.
- Le volume clone est créé sur la même machine virtuelle de stockage que la destination SnapMirror.
- Vous pouvez utiliser les relations FlexVol et FlexGroup SnapMirror.
- Si un clone test existe déjà pour la relation sélectionnée, vous ne pouvez pas créer un autre clone pour cette relation.
- Les relations de coffre-fort SnapLock ne sont pas prises en charge.

#### Avant de commencer

- Vous devez être un administrateur de cluster.
- La licence SnapMirror doit être installée sur le cluster source et le cluster destination.

#### Étapes


1. Sur le cluster de destination, sélectionnez **protection > relations**.
2. Sélectionnez  en regard de la source de la relation et choisissez **Test Failover**.

3. Dans la fenêtre **Test Failover**, sélectionnez **Test Failover**.
4. Sélectionnez **stockage > volumes** et vérifiez que le volume de basculement test est répertorié.
5. Sélectionnez **stockage > partager**.
6. Cliquez sur  et choisissez **partager**.
7. Dans la fenêtre **Ajouter un partage**, saisissez un nom pour le partage dans le champ **Nom du partage**.
8. Dans le champ **Folder**, sélectionnez **Browse**, sélectionnez le volume clone test et **Save**.
9. Au bas de la fenêtre **Ajouter un partage**, choisissez **Enregistrer**.
10. Ouvrez le partage sur le client et vérifiez que le volume test dispose de capacités de lecture et d'écriture.

### Nettoyez les données de basculement et supprimez le volume test

Une fois le test de basculement terminé, vous pouvez nettoyer toutes les données associées au volume test et les supprimer.

#### Étapes

1. Sur le cluster de destination, sélectionnez **protection > relations**.
2. Sélectionnez  en regard de la source de la relation et choisissez **nettoyer le basculement du test**.
3. Dans la fenêtre **nettoyage du basculement de test**, sélectionnez **nettoyage**.
4. Sélectionnez **stockage > volumes** et vérifiez que le volume test a été supprimé.

### Activation des données à partir d'un volume de destination de reprise après incident SnapMirror

#### Rendre le volume de destination inscriptible

Vous devez rendre le volume de destination inscriptible avant de pouvoir transmettre les données du volume à des clients. Pour transmettre des données à partir d'une destination de miroir lorsqu'une source devient indisponible, arrêter les transferts programmés vers la destination, puis interrompre la relation SnapMirror pour rendre la destination inscriptible.


#### Description de la tâche

Cette tâche doit être effectuée depuis le SVM de destination ou le cluster de destination.

#### Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour rendre un volume de destination inscriptible.

## System Manager

1. Sélectionnez la relation de protection : cliquez sur **protection > relations**, puis cliquez sur le nom du volume souhaité.
2. Cliquez sur .
3. Arrêter les transferts programmés : cliquez sur **Pause**.
4. Rendre la destination inscriptible : cliquez sur **Pause**.
5. Accédez à la page principale **relations** pour vérifier que l'état de la relation s'affiche comme « rompu ».

## Étapes suivantes

Une fois le volume de destination inscriptible, vous devez ["refaites la resynchronisation inverse de la relation de réplication"](#) le faire.

Lorsque le volume source désactivé est de nouveau disponible, vous devez inverser à nouveau la resynchronisation de la relation pour copier les données actuelles sur le volume source d'origine.

## CLI

1. Arrêter les transferts programmés vers la destination :

```
snapmirror quiesce -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant arrête les transferts programmés entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror quiesce -source-path svm1:volA
-destination-path svm_backup:volA_dst
```

2. Arrêter les transferts en cours vers la destination :

```
snapmirror abort -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Cette étape n'est pas requise pour les relations synchrones SnapMirror (prises en charge à partir de ONTAP 9.5).

L'exemple suivant arrête les transferts en cours entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

### 3. Interrompre la relation SnapMirror DR :

```
snapmirror break -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant rompt la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

#### Étapes suivantes

Une fois le volume de destination inscriptible, vous devez ["resynchroniser la relation de réplication"](#) le faire.

#### D'autres façons de le faire dans ONTAP

| Pour effectuer ces tâches avec...                                          | Voir ce contenu...                                                    |
|----------------------------------------------------------------------------|-----------------------------------------------------------------------|
| System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures) | <a href="#">"Présentation de la reprise après incident de volume"</a> |

#### Configurer le volume de destination pour l'accès aux données

Une fois le volume de destination inscriptible, vous devez configurer le volume pour l'accès aux données. Les clients NAS, le sous-système NVMe et les hôtes SAN peuvent accéder aux données à partir du volume de destination jusqu'à ce que le volume source soit réactivé.

Environnement NAS :

1. Monter le volume NAS sur l'espace de noms en utilisant la même Junction path que le volume source a été monté sur dans le SVM source.
2. Appliquez les ACL appropriées aux partages SMB du volume de destination.
3. Attribuez les export-polices NFS au volume de destination.
4. Appliquer les règles de quota au volume de destination
5. Redirection des clients vers le volume de destination.
6. Remontez les partages NFS et SMB sur les clients.



## Environnement SAN :

1. Mappez les LUN du volume sur le groupe initiateur approprié.
2. Pour iSCSI, créez des sessions iSCSI des initiateurs hôtes SAN vers les LIF SAN.
3. Sur le client SAN, effectuez une nouvelle analyse de stockage pour détecter les LUN connectés.

Pour plus d'informations sur l'environnement NVMe, reportez-vous à la section ["Administration SAN"](#).

## Réactiver le volume source d'origine

Vous pouvez rétablir la relation initiale de protection des données entre les volumes source et destination lorsque vous n'avez plus besoin de transmettre des données depuis la destination.

### Description de la tâche

- La procédure ci-dessous suppose que la ligne de base du volume source d'origine est intacte. Si la base n'est pas intacte, vous devez créer et initialiser la relation entre le volume dont vous accédez aux données et le volume source d'origine avant d'effectuer la procédure.
- La préparation en arrière-plan et la phase d'entreposage des données d'une relation SnapMirror XDP peuvent prendre un certain temps. Il n'est pas rare de voir la relation SnapMirror indiquant l'état « préparation » pour une période prolongée.

### Étapes

1. Inverser la relation de protection des données d'origine :

```
snapmirror resync -source-path SVM:volume -destination-path SVM:volume
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Vous devez exécuter cette commande à partir du SVM source d'origine ou du cluster source d'origine. Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe. Échec de la commande si une copie Snapshot commune n'existe pas sur la source et la destination. Utiliser `snapmirror initialize` pour réinitialiser la relation.

L'exemple suivant inverse la relation entre le volume source d'origine, `volA` marche `svm1` et le volume que vous servant de données, ``volA_dst` marche `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

2. Lorsque vous êtes prêt à rétablir l'accès aux données à la source d'origine, l'accès au volume de destination d'origine est interrompu. L'une des façons de faire est d'arrêter le SVM de destination d'origine :

```
vserver stop -vserver SVM
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Vous devez exécuter cette commande à partir du SVM destination d'origine ou du cluster destination d'origine. Cette commande arrête l'accès de l'utilisateur à l'ensemble du SVM de destination d'origine. Vous pouvez arrêter l'accès au volume de destination d'origine à l'aide d'autres méthodes.

L'exemple suivant arrête le SVM destination original :

```
cluster_dst::> vserver stop svm_backup
```

### 3. Mettre à jour la relation inversée :

```
snapmirror update -source-path SVM:volume -destination-path SVM:volume
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Vous devez exécuter cette commande à partir du SVM source d'origine ou du cluster source d'origine.

L'exemple suivant met à jour la relation entre le volume que vous servant des données, volA\_dst marche svm\_backup, et le volume source d'origine, volA marche svm1:

```
cluster_src::> snapmirror update -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

### 4. Depuis le SVM source d'origine ou le cluster source d'origine, arrêter les transferts programmés pour la relation inversée :

```
snapmirror quiesce -source-path SVM:volume -destination-path SVM:volume
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Vous devez exécuter cette commande à partir du SVM source d'origine ou du cluster source d'origine.

L'exemple suivant illustre la fin des transferts programmés entre le volume de destination d'origine. volA\_dst marche svm\_backup, et le volume source d'origine, volA marche svm1:

```
cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

### 5. Lorsque la mise à jour finale est terminée et que la relation indique « suspendu » pour l'état de la relation, exécutez la commande suivante à partir du SVM source d'origine ou du cluster source d'origine pour interrompre la relation inversée :

```
snapmirror break -source-path SVM:volume -destination-path SVM:volume
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Vous devez exécuter cette commande à partir du SVM source d'origine ou du cluster source.

L'exemple suivant rompt la relation entre le volume de destination d'origine, `volA_dst` marche `svm_backup`, et le volume source d'origine, `volA` marche `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

6. Depuis le SVM source d'origine ou le cluster source d'origine, supprimer la relation de protection des données inversée :

```
snapmirror delete -source-path SVM:volume -destination-path SVM:volume
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.



Vous devez exécuter cette commande à partir du SVM source d'origine ou du cluster source d'origine.

L'exemple suivant supprime la relation inversée entre le volume source d'origine, `volA` marche `svm1` et le volume que vous servant de données, `volA_dst` marche `svm_backup`:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

7. Libérer la relation inverse de la SVM destination d'origine ou du cluster destination d'origine.

```
snapmirror release -source-path SVM:volume -destination-path SVM:volume
```



Vous devez exécuter cette commande à partir du SVM destination d'origine ou du cluster destination d'origine.

L'exemple suivant libère la relation inversée entre le volume de destination d'origine, `volA_dst` marche `svm_backup`, et le volume source d'origine, `volA` marche `svm1`:

```
cluster_dst::> snapmirror release -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

8. Rétablir la relation de protection des données d'origine à partir de la destination d'origine :

```
snapmirror resync -source-path SVM:volume -destination-path SVM:volume
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

L'exemple suivant rétablit la relation entre le volume source d'origine, `volA` marche `svm1`, et le volume de destination d'origine, `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

9. Si besoin démarrer le SVM de destination d'origine :

```
vserver start -vserver SVM
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant démarre le SVM de destination d'origine :

```
cluster_dst::> vserver start svm_backup
```

### Une fois que vous avez terminé

Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

## Restaurer les fichiers à partir d'un volume de destination SnapMirror

### Restaurez un seul fichier, LUN ou namespace NVMe à partir d'une destination SnapMirror

Vous pouvez restaurer un seul fichier, une LUN, un ensemble de fichiers ou de LUN à partir d'une copie Snapshot ou un namespace NVMe à partir d'un volume de destination SnapMirror. Depuis la version ONTAP 9.7, vous pouvez également restaurer des espaces de noms NVMe à partir d'une destination synchrone SnapMirror. Vous pouvez restaurer des fichiers vers le volume source d'origine ou vers un volume différent.

### Ce dont vous avez besoin

Pour restaurer un fichier ou une LUN à partir d'une destination synchrone SnapMirror (prise en charge à partir de ONTAP 9.5), vous devez d'abord supprimer et libérer la relation.

### Description de la tâche

Le volume vers lequel vous restaurez des fichiers ou des LUN (le volume de destination) doit être un volume en lecture-écriture :

- SnapMirror effectue une *restauration incrémentielle* si les volumes source et de destination ont une copie Snapshot commune (comme c'est généralement le cas lors de la restauration vers le volume source d'origine).
- Sinon, SnapMirror exécute une *restauration de base*, dans laquelle la copie Snapshot spécifiée et tous les blocs de données qui lui sont transférés vers le volume de destination.

### Étapes

1. Lister les copies Snapshot dans le volume de destination :

```
volume snapshot show -vserver <SVM> -volume volume
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant montre les copies Snapshot sur le `vserverB:secondary1` destination :

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1
```

| Vserver<br>Used% | Volume     | Snapshot               | State | Size  | Total% |
|------------------|------------|------------------------|-------|-------|--------|
| -----<br>-----   | -----      | -----                  | ----- | ----- | -----  |
| vserverB<br>0%   | secondary1 | hourly.2013-01-25_0005 | valid | 224KB | 0%     |
| 0%               |            | daily.2013-01-25_0010  | valid | 92KB  | 0%     |
| 0%               |            | hourly.2013-01-25_0105 | valid | 228KB | 0%     |
| 0%               |            | hourly.2013-01-25_0205 | valid | 236KB | 0%     |
| 0%               |            | hourly.2013-01-25_0305 | valid | 244KB | 0%     |
| 0%               |            | hourly.2013-01-25_0405 | valid | 244KB | 0%     |
| 0%               |            | hourly.2013-01-25_0505 | valid | 244KB | 0%     |

7 entries were displayed.

2. Restaurer un seul fichier ou une LUN, ou un ensemble de fichiers ou de LUN à partir d'une copie Snapshot dans un volume de destination SnapMirror :

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -source-snapshot
snapshot -file-list <source_file_path,@destination_file_path>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

La commande suivante restaure les fichiers `file1` et `file2` A partir de la copie Snapshot `daily.2013-01-25_0010` dans le volume de destination d'origine `secondary1`, au même emplacement dans le système de fichiers actif du volume source d'origine `primary1`:

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

La commande suivante restaure les fichiers `file1` et `file2` A partir de la copie Snapshot `daily.2013-01-25_0010` dans le volume de destination d'origine `secondary1`, à un autre emplacement dans le système de fichiers actif du volume source d'origine `primary1`.

Le chemin du fichier de destination commence par le symbole `@` suivi du chemin du fichier à partir de la racine du volume source d'origine. Dans cet exemple, `file1` est restauré sur `/dir1/file1.new` et le fichier 2 est restauré dans `/dir2.new/file2` marche `primary1`:

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

La commande suivante restaure les fichiers `file1` et `file3` A partir de la copie Snapshot `daily.2013-01-25_0010` dans le volume de destination d'origine `secondary1`, à différents emplacements dans le système de fichiers actif du volume source d'origine `primary1`, et restaure `file2` de `snap1` au même emplacement dans le système de fichiers actif de `primary1`.

Dans cet exemple, le fichier `file1` est restauré sur `/dir1/file1.new` et `file3` est restauré sur `/dir3.new/file3`:

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

## Restaurer le contenu d'un volume à partir d'une destination SnapMirror

Vous pouvez restaurer le contenu d'un volume entier à partir d'une copie Snapshot dans un volume de destination SnapMirror. Vous pouvez restaurer le contenu du volume vers le volume source d'origine ou vers un volume différent.

## Description de la tâche

Le volume de destination de l'opération de restauration doit être l'un des suivants :

- Un volume de lecture/écriture, dans lequel cas SnapMirror exécute une *restauration incrémentielle*, à condition que les volumes source et de destination aient une copie Snapshot commune (comme c'est généralement le cas lors de la restauration vers le volume source d'origine).



La commande échoue si une copie Snapshot commune n'est pas disponible. Vous ne pouvez pas restaurer le contenu d'un volume sur un volume en lecture-écriture vide.

- Un volume de protection des données vide, dans lequel cas SnapMirror exécute une *restauration de base*, dans lequel la copie Snapshot spécifiée et tous les blocs de données qui lui font référence sont transférés vers le volume source.

La restauration du contenu d'un volume constitue une opération perturbateur. Lors de l'exécution d'une opération de restauration, le trafic SMB ne doit pas être exécuté sur le volume primaire SnapVault.

Si la compression est activée sur le volume de destination pour l'opération de restauration et que la compression n'est pas activée sur le volume source, désactivez la compression sur le volume de destination. Vous devez réactiver la compression une fois l'opération de restauration terminée.

Toute règle de quotas définie pour le volume de destination est désactivée avant la restauration effectuée. Vous pouvez utiliser le `volume quota modify` commande permettant de réactiver les règles de quota une fois l'opération de restauration terminée.

Lorsque les données d'un volume sont perdues ou corrompues, vous pouvez restaurer les données à partir d'une copie Snapshot antérieure.

Cette procédure remplace les données actuelles sur le volume source par des données issues d'une version antérieure de la copie Snapshot. Vous devez effectuer cette tâche sur le cluster de destination.

## Étapes

Vous pouvez restaurer le contenu d'un volume à l'aide de System Manager ou de l'interface de ligne de commandes de ONTAP.

## System Manager

1. Cliquez sur **protection > relations**, puis sur le nom du volume source.
2. Cliquez sur, puis sélectionnez **Restaurer**.
3. Sous **Source**, le volume source est sélectionné par défaut. Cliquez sur **Other Volume** si vous souhaitez choisir un volume autre que la source.
4. Sous **destination**, choisissez la copie Snapshot à restaurer.
5. Si votre source et votre destination sont situées sur différents clusters, sur le cluster distant, cliquez sur **protection > relations** pour contrôler la progression de la restauration.

## CLI

1. Lister les copies Snapshot dans le volume de destination :

```
volume snapshot show -vserver <SVM> -volume <volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant montre les copies Snapshot sur le `vserverB:secondary1` destination :

```
cluster_dst::> volume snapshot show -vserver vserverB -volume
secondary1
```

| Vserver  | Volume     | Snapshot               | State | Size  | Total% | Used% |
|----------|------------|------------------------|-------|-------|--------|-------|
| -----    | -----      | -----                  | ----- | ----- | -----  | ----- |
| vserverB | secondary1 | hourly.2013-01-25_0005 | valid | 224KB | 0%     | 0%    |
|          |            | daily.2013-01-25_0010  | valid | 92KB  | 0%     | 0%    |
|          |            | hourly.2013-01-25_0105 | valid | 228KB | 0%     | 0%    |
|          |            | hourly.2013-01-25_0205 | valid | 236KB | 0%     | 0%    |
|          |            | hourly.2013-01-25_0305 | valid | 244KB | 0%     | 0%    |
|          |            | hourly.2013-01-25_0405 | valid | 244KB | 0%     | 0%    |
|          |            | hourly.2013-01-25_0505 | valid | 244KB | 0%     | 0%    |

7 entries were displayed.

2. Restaurer le contenu d'un volume à partir d'une copie Snapshot dans un volume de destination SnapMirror :



```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot
<snapshot>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Vous devez exécuter cette commande à partir du SVM source d'origine ou du cluster source d'origine.

La commande suivante restaure le contenu du volume source d'origine `primary1` A partir de la copie Snapshot `daily.2013-01-25_0010` dans le volume de destination d'origine `secondary1`:

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010
```

```
Warning: All data newer than Snapshot copy daily.2013-01-25_0010 on
volume vserverA:primary1 will be deleted.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 34] Job is queued: snapmirror restore from source
vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
```

3. Remontez le volume restauré et redémarrez toutes les applications qui utilisent le volume.

#### D'autres façons de le faire dans ONTAP

| Pour effectuer ces tâches avec...                                          | Voir ce contenu...                                                                |
|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures) | <a href="#">"Présentation de la restauration de volume à l'aide de SnapVault"</a> |

## Mettre à jour une relation de réplication manuellement

Vous devrez peut-être mettre à jour une relation de réplication manuellement si une mise à jour échoue, car le volume source a été déplacé.

### Description de la tâche

SnapMirror interrompt tous les transferts depuis un volume source déplacé jusqu'à ce que vous mette à jour la relation de réplication manuellement.

Depuis ONTAP 9.5, les relations SnapMirror synchrones sont prises en charge. Bien que les volumes source et de destination soient synchronisés à tout moment dans ces relations, la vue du cluster secondaire est synchronisée avec la vue principale uniquement toutes les heures. Si vous souhaitez afficher les données à un point dans le temps à la destination, vous devez effectuer une mise à jour manuelle en exécutant `snapmirror update` la commande.

## Étape

### 1. Mettre à jour une relation de réplication manuellement :

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ...
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination. Échec de la commande si une copie Snapshot commune n'existe pas sur la source et la destination. Utiliser `snapmirror initialize` pour réinitialiser la relation.

L'exemple suivant met à jour la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_src::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

## Resynchroniser une relation de réplication

Vous devez resynchroniser une relation de réplication après avoir créé un volume de destination inscriptible, après une mise à jour échoue, car une copie Snapshot commune n'existe pas sur les volumes source et de destination, ou si vous souhaitez modifier la règle de réplication pour la relation.

Depuis ONTAP 9.8, System Manager permet d'effectuer une opération de resynchronisation inverse en vue de supprimer une relation de protection existante et d'inverser les fonctions des volumes source et de destination. Ensuite, vous utilisez le volume de destination pour transmettre des données pendant que vous réparez ou remplacez la source, mettez à jour la source, et rétablissez la configuration d'origine des systèmes.

### Description de la tâche

- Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.
- La resynchronisation des volumes qui font partie d'une configuration « fan-out » ou en cascade peut prendre plus de temps. Il n'est pas rare de voir la relation SnapMirror indiquant l'état « préparation » pour une période prolongée.




System Manager ne prend pas en charge la resynchronisation inverse avec des relations intracluster. Vous pouvez utiliser l'interface de ligne de commandes de ONTAP pour effectuer des opérations de resynchronisation inverse avec des relations intracluster.

## Étapes

Vous pouvez effectuer cette tâche à l'aide de System Manager ou de l'interface de ligne de commandes de ONTAP. Si vous utilisez l'interface de ligne de commandes de ONTAP, la procédure est identique, que vous enregistrez sur un volume de destination ou que vous mettez à jour la relation de réplication.

## Resynchronisation inverse de System Manager



Après "[rompre une relation](#)" avoir effectué une destination inscriptible, resynchronisez la relation de manière inverse :

1. Sur le cluster de destination, cliquez sur **protection > relations**.
2. Placez le pointeur de la souris sur la relation interrompue que vous souhaitez inverser, cliquez sur  et sélectionnez **Inverser la resynchronisation**.
3. Dans la fenêtre **Reverse resync Relationship**, cliquez sur **Reverse resync**.
4. Sous **Relationship**, surveillez la progression de la resynchronisation inverse en visualisant **Transfer Status** pour la relation.

### Étapes suivantes

Lorsque la source d'origine est de nouveau disponible, vous pouvez rétablir la relation d'origine en rompant la relation inversée et en exécutant une autre opération de resynchronisation inverse. Le processus de resynchronisation inverse copie toutes les modifications du site qui diffuse des données vers la source d'origine et réécrit la source d'origine.

## Resynchronisation de System Manager

1. Cliquez sur **protection > relations**.
2. Placez le pointeur de la souris sur la relation que vous souhaitez resynchroniser, puis cliquez sur  et sélectionnez **rompre**.
3. Lorsque l'état de la relation affiche "Broken off", cliquez sur  et sélectionnez **Resync**.
4. Sous **relations**, surveiller la progression de la resynchronisation en vérifiant l'état de la relation. L'état est modifié en « mis en miroir » une fois la resynchronisation terminée.

## CLI

1. Resynchronisation des volumes source et de destination :

```
snapmirror resync -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume> -type DP|XDP
-policy <policy>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

L'exemple suivant resynchronise la relation entre le volume source `volA` sur et le volume de destination sur `svml volA_dst svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svml:volA -destination
-path svm_backup:volA_dst
```

## Supprime une relation de réplication de volume

Vous pouvez utiliser le `snapmirror delete` et `snapmirror release` commandes permettant de supprimer une relation de réplication de volume. Vous pouvez ensuite supprimer manuellement les volumes de destination inutiles.

### Description de la tâche

Le `snapmirror release` Commande permet de supprimer toutes les copies Snapshot créées par SnapMirror de la source. Vous pouvez utiliser le `-relationship-info-only` Option pour conserver les copies Snapshot.

### Étapes

1. Arrêter la relation de réplication :

```
snapmirror quiesce -destination-path <SVM:volume>|<cluster://SVM/volume>
```

```
cluster_dst:> snapmirror quiesce -destination-path svm_backup:volA_dst
```

2. (Facultatif) si vous souhaitez que le volume de destination soit un volume de lecture/écriture, rompez la relation de réplication. Vous pouvez ignorer cette étape si vous prévoyez de supprimer le volume de destination ou si vous n'avez pas besoin d'un volume en lecture/écriture :

```
snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ...
```

```
cluster_dst:> snapmirror break -source-path svm1:volA -destination-path
svm_backup:volA_dst
```

3. Supprimez la relation de réplication :

```
snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ...
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).



On doit exécuter cette commande depuis le cluster de destination ou le SVM de destination.

L'exemple suivant supprime la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst:> snapmirror delete -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

4. Libérer les informations de relation de réplication depuis le SVM source :

```
snapmirror release -source-path <SVM:volume>|<cluster://SVM/volume>, ...
```

-destination-path <SVM:volume>|<cluster://SVM/volume>, ...

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Vous devez exécuter cette commande à partir du cluster source ou du SVM source.

L'exemple suivant publie des informations pour la relation de réplication spécifiée à partir du SVM source svm1:

```
cluster_src::> snapmirror release -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

## Gérer l'efficacité du stockage

SnapMirror préserve l'efficacité du stockage sur les volumes source et de destination, sauf lorsque la compression post-traitement est activée sur le volume de destination. Dans ce cas, toute l'efficacité du stockage est perdue sur le volume de destination. Pour résoudre ce problème, vous devez désactiver la compression post-traitement sur le volume de destination, mettre à jour la relation manuellement et réactiver l'efficacité du stockage.

### Description de la tâche

Vous pouvez utiliser le `volume efficiency show` commande pour déterminer si l'efficacité est activée sur un volume. Pour plus d'informations, consultez les pages de manuel.

Vous pouvez vérifier si SnapMirror préserve l'efficacité du stockage en consultant les journaux d'audit SnapMirror et en localiser la description du transfert. Si la description du transfert affiche `transfer_desc=Logical Transfer with Storage Efficiency`, SnapMirror maintient l'efficacité du stockage. Si la description du transfert affiche `transfer_desc=Logical Transfer`, SnapMirror ne maintient pas l'efficacité du stockage. Par exemple :

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

### Avant de commencer

- Les clusters source et de destination et les SVM doivent être associés.

#### "Cluster et SVM peering"

- Vous devez désactiver la compression post-traitement sur le volume de destination.
- Transfert logique avec stockage : à partir de ONTAP 9.3, il n'est plus nécessaire de procéder à une mise à jour manuelle pour réactiver l'efficacité du stockage. Si SnapMirror détecte que la compression post-

traitement a été désactivée, l'efficacité du stockage est réactivée automatiquement lors de la prochaine mise à jour planifiée. La source et la destination doivent exécuter ONTAP 9.3.

- Depuis ONTAP 9.3, les systèmes AFF gèrent les paramètres d'efficacité du stockage différemment des systèmes FAS après la création d'un volume de destination inscriptible :
  - Après avoir créé un volume de destination inscriptible à l'aide du `snapmirror break` commande, la politique de mise en cache du volume est automatiquement définie sur « auto » (par défaut).



Ce comportement est applicable aux volumes FlexVol, uniquement et ne s'applique pas aux volumes FlexGroup.

- Lors de la resynchronisation, la règle de mise en cache est automatiquement définie sur « aucune » et la déduplication et la compression à la volée sont automatiquement désactivées, quels que soient vos paramètres d'origine. Vous devez modifier les paramètres manuellement si nécessaire.



Les mises à jour manuelles optimisant l'efficacité du stockage peuvent s'avérer chronophages. Vous pouvez exécuter l'opération en dehors des heures de pointe.

## Étapes

1. Mettre à jour une relation de réplication et réactiver l'efficacité du stockage :

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -enable
-storage-efficiency true
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



On doit exécuter cette commande depuis le SVM de destination ou le cluster destination. Si aucune copie Snapshot commune n'existe sur la source et la destination, la commande échoue. Utilisez `snapmirror initialize` pour réinitialiser la relation.

L'exemple suivant met à jour la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`, et réactive l'efficacité du stockage :

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst -enable-storage-efficiency true
```

## Utilisez l'accélération globale de SnapMirror

La limitation du réseau globale est disponible pour tous les transferts SnapMirror et SnapVault au niveau de chaque nœud.

### Description de la tâche

La limitation globale de SnapMirror restreint la bande passante utilisée par les transferts SnapMirror et SnapVault entrants et/ou sortants. La restriction est appliquée à l'échelle du cluster sur tous les nœuds du cluster.

Par exemple, si l'accélérateur sortant est réglé sur 100 Mbit/s, la bande passante sortante est définie sur 100 Mbit/s. Si l'accélération globale est désactivée, celle-ci est désactivée sur tous les nœuds.

Bien que les taux de transfert de données soient souvent exprimés en bits par seconde (bit/s), les valeurs de l'accélérateur doivent être saisies en kilo-octets par seconde (Kbit/s).



Dans ONTAP 9.9.1 et versions antérieures, le papillon n'a aucun effet sur `volume move` transferts ou transferts entre miroirs de partage de charge. À partir de ONTAP 9.10.0, vous pouvez spécifier une option pour accélérer les opérations de déplacement de volume. Pour plus de détails, voir ["Comment accélérer le déplacement du volume dans ONTAP 9.10 et versions ultérieures."](#)

La régulation globale fonctionne à l'aide de la fonction de régulation de la relation pour les transferts SnapMirror et SnapVault. Le papillon par relation est appliqué jusqu'à ce que la bande passante combinée des transferts par relation dépasse la valeur de l'accélérateur global, après quoi l'accélérateur global est appliqué. Une valeur d'accélérateur 0 implique que la régulation globale est désactivée.



La restriction globale SnapMirror n'a aucun effet sur les relations synchrones SnapMirror lorsqu'elles sont synchronisées. Cependant, l'accélérateur affecte les relations synchrones SnapMirror lorsqu'ils effectuent une phase de transfert asynchrone telle qu'une opération d'initialisation ou après un événement de désynchronisation. C'est pourquoi il n'est pas recommandé d'activer l'accélération globale avec les relations SnapMirror synchrones.

## Étapes

### 1. Activation de l'accélération globale :

```
options -option-name replication.throttle.enable on|off
```

L'exemple suivant montre comment activer la régulation globale de SnapMirror `cluster_dst`:

```
cluster_dst::> options -option-name replication.throttle.enable on
```

### 2. Spécifiez la bande passante totale maximale utilisée par les transferts entrants sur le cluster de destination :

```
options -option-name replication.throttle.incoming.max_kbs KBps
```

La bande passante minimale recommandée de l'accélérateur est de 4 kbit/s et la largeur maximale est de 2 Tbit/s. La valeur par défaut de cette option est `unlimited`, ce qui signifie qu'il n'y a pas de limite sur la bande passante totale utilisée.

L'exemple suivant montre comment définir la bande passante totale maximale utilisée par les transferts entrants sur 100 Mbit/s :

```
cluster_dst::> options -option-name
replication.throttle.incoming.max_kbs 12500
```



100 Mbit/s = 12500 Kbit/s

3. Spécifiez la bande passante totale maximale utilisée par les transferts sortants sur le cluster source :

```
options -option-name replication.throttle.outgoing.max_kbs KBps
```

La bande passante minimale recommandée de l'accélérateur est de 4 kbit/s et la largeur maximale est de 2 Tbit/s. La valeur par défaut de cette option est `unlimited`, ce qui signifie qu'il n'y a pas de limite sur la bande passante totale utilisée. Les valeurs des paramètres sont en Kbit/s.

L'exemple suivant montre comment définir la bande passante totale maximale utilisée par les transferts sortants sur 100 Mbit/s :

```
cluster_src::> options -option-name
replication.throttle.outgoing.max_kbs 12500
```

## Gérer la réplication de SVM SnapMirror

### À propos de la réplication SnapMirror SVM

Vous pouvez utiliser SnapMirror pour créer une relation de protection des données entre les SVM. Dans ce type de relation de protection des données, tout ou partie de la configuration du SVM, depuis les exportations NFS et les partages SMB jusqu'au RBAC, est répliquée, ainsi que les données des volumes que le SVM possède.

#### Types de relations pris en charge

Seuls les SVM servant les données peuvent être répliqués. Les types de relations de protection des données suivants sont pris en charge :

- *Reprise sur incident SnapMirror*, dans laquelle la destination contient généralement uniquement les copies Snapshot actuellement sur la source.

À partir de ONTAP 9.9.1, ce comportement change lorsque vous utilisez la stratégie de coffre-fort miroir. Depuis la version ONTAP 9.9.1, vous pouvez créer différentes règles Snapshot sur la source et la destination, et les copies Snapshot de la destination ne sont pas écrasées par les copies Snapshot de la source :

- Elles ne sont pas remplacées de la source vers la destination pendant les opérations, les mises à jour et les synchronisations standard
- Ils ne sont pas supprimés pendant les opérations de pause.
- Elles ne sont pas supprimées lors des opérations de bascule et resynchronisation.  
Lorsque vous configurez une relation de SVM Disaster à l'aide de la règle `mirror-vault` à l'aide de ONTAP 9.9.1 et versions ultérieures, la règle se comporte comme suit :
- Les règles de copie Snapshot définies par l'utilisateur au niveau de la source ne sont pas copiées vers la destination.
- Les règles de copie Snapshot définies par le système ne sont pas copiées vers la destination.
- L'association de volumes aux règles Snapshot définies par l'utilisateur et par le système ne sont pas copiées vers la destination.



SVM.

- Depuis ONTAP 9.2, la réplication unifiée *SnapMirror*, dans laquelle la destination est configurée pour la reprise après incident et la conservation à long terme.

Pour plus d'informations sur la réplication unifiée *SnapMirror*, reportez-vous à la section "[Notions de base sur la réplication unifiée \*SnapMirror\*](#)".

Le *policy type* de la règle de réplication détermine le type de relation qu'elle prend en charge. Le tableau suivant présente les types de politiques disponibles.

| Type de règle             | Type de relation                       |
|---------------------------|----------------------------------------|
| mise en miroir asynchrone | Reprise sur incident <i>SnapMirror</i> |
| coffre-fort               | Réplication unifiée                    |

### XDP remplace DP en tant que valeur par défaut de réplication SVM dans ONTAP 9.4

Depuis ONTAP 9.4, les relations de protection des données du SVM sont définies par défaut en mode XDP. Les relations de protection des données de SVM continuent à être par défaut en mode DP dans ONTAP 9.3 et versions antérieures.

Les relations existantes ne sont pas affectées par la nouvelle valeur par défaut. Si une relation est déjà de type DP, elle continuera d'être de type DP. Le tableau suivant montre le comportement auquel vous pouvez vous attendre.

| Si vous spécifiez... | Le type est... | La stratégie par défaut (si vous ne spécifiez pas de règle) est... |
|----------------------|----------------|--------------------------------------------------------------------|
| DP                   | XDP            | MirrorAllsnapshots (reprise après incident <i>SnapMirror</i> )     |
| Rien                 | XDP            | MirrorAllsnapshots (reprise après incident <i>SnapMirror</i> )     |
| XDP                  | XDP            | MirrorAndVault (réplication unifiée)                               |

Vous trouverez ici des informations sur les modifications apportées par défaut : "[XDP remplace DP par défaut \*SnapMirror\*](#)".



L'indépendance de version n'est pas prise en charge pour la réplication des SVM. En configuration de reprise d'activité d'un SVM, le SVM de destination doit se trouver sur un cluster exécutant la même version ONTAP que le cluster SVM source pour prendre en charge les opérations de basculement et de retour arrière.

["Compatibilité des versions ONTAP pour les relations \*SnapMirror\*"](#)

### Réplication des configurations SVM

Le contenu d'une relation de réplication SVM est déterminé par l'interaction des champs suivants :

- Le `-identity-preserve true` de la `snapmirror create` La commande réplique l'ensemble de la configuration du SVM.

Le `-identity-preserve false` Option réplique uniquement les volumes et les configurations d'authentification et d'autorisation du SVM, ainsi que les paramètres de protocole et de service de nom répertoriés dans "[Configurations répliquées dans des relations SVM DR](#)".

- Le `-discard-configs network` de la `snapmirror policy create` La commande n'exclut pas les LIFs et les paramètres réseau associés de la réplication SVM, pour les cas où les SVM source et de destination se trouvent dans différents sous-réseaux.
- Le `-vserver-dr-protection unprotected` de la `volume modify` La commande exclut le volume spécifié de la réplication SVM.

Sinon, la réplication SVM est quasiment identique à la réplication de volume. Vous pouvez utiliser quasiment le même workflow pour la réplication SVM que celui utilisé pour la réplication de volume.

## Détails du support

Le tableau suivant présente les détails de prise en charge de la réplication de SVM SnapMirror.

| Ressource ou fonctionnalité                         | Détails du support                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Types de déploiement                                | <ul style="list-style-type: none"> <li>• D'une source unique vers une destination unique</li> <li>• Depuis la version ONTAP 9.4, « Fan-Out ». Vous ne pouvez effectuer un « fan-out » que vers deux destinations.</li> </ul> <p>Par défaut, une seule relation <code>-Identity-preserve true</code> est autorisée par SVM source.</p> |
| Types de relations                                  | <ul style="list-style-type: none"> <li>• Reprise sur incident SnapMirror</li> <li>• La réplication unifiée SnapMirror est à partir de ONTAP 9.2</li> </ul>                                                                                                                                                                            |
| Étendue de la réplication                           | Intercluster uniquement. Vous ne pouvez pas répliquer de SVM au sein du même cluster.                                                                                                                                                                                                                                                 |
| Protection autonome contre les ransomwares          | <ul style="list-style-type: none"> <li>• Pris en charge à partir de ONTAP 9.12.1. Pour plus d'informations, voir "<a href="#">Protection autonome contre les ransomwares</a>".</li> </ul>                                                                                                                                             |
| Prise en charge asynchrone des groupes de cohérence | Depuis la version ONTAP 9.14.1, un maximum de 32 relations de reprise d'activité SVM sont prises en charge lorsque des groupes de cohérence existent. Voir " <a href="#">Protéger un groupe de cohérence</a> " et " <a href="#">Limites des groupes de cohérence</a> " pour en savoir plus.                                           |
| FabricPool                                          | Depuis ONTAP 9.6, la réplication des SVM SnapMirror est prise en charge par FabricPool.                                                                                                                                                                                                                                               |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MetroCluster        | <p>Depuis la version ONTAP 9.11.1, les deux côtés d'une relation de reprise d'activité de SVM dans une configuration MetroCluster peuvent servir de source pour des configurations supplémentaires de reprise d'activité de SVM.</p> <p>Depuis ONTAP 9.5, la réplication de SnapMirror SVM est prise en charge dans les configurations MetroCluster.</p> <ul style="list-style-type: none"> <li>• Dans les versions antérieures à ONTAP 9.10.X, une configuration MetroCluster ne peut pas être la destination d'une relation de SVM DR.</li> <li>• Dans ONTAP 9.10.1 et versions ultérieures, une configuration MetroCluster peut faire l'objet d'une relation de reprise d'activité de SVM à des fins de migration uniquement et elle doit répondre à toutes les exigences nécessaires décrites dans <a href="#">"Tr-4966 : migration d'une SVM vers une solution MetroCluster"</a>.</li> <li>• Seul un SVM actif au sein d'une configuration MetroCluster peut être à l'origine d'une relation de reprise d'activité de SVM.</li> </ul> <p>Une source peut être un SVM source synchrone avant le basculement ou un SVM de destination synchrone après le basculement.</p> <ul style="list-style-type: none"> <li>• Lorsqu'une configuration MetroCluster est dans un état stable, le SVM MetroCluster destination ne peut pas être à l'origine d'une relation de reprise d'activité SVM, car les volumes ne sont pas en ligne.</li> <li>• Lorsque le SVM source est la source d'une relation de SVM DR, les informations de la relation de SVM DR source sont répliquées vers le partenaire MetroCluster.</li> <li>• Lors des processus de basculement et de rétablissement, la réplication vers la destination de reprise d'activité du SVM peut échouer.</li> </ul> <p>Cependant, une fois le processus de basculement ou de rétablissement terminé, les mises à jour planifiées de reprise d'activité du SVM suivant réussiront.</p> |
| Groupe de cohérence | <p>Pris en charge à partir de ONTAP 9.14.1. Pour plus d'informations, voir <a href="#">Protéger un groupe de cohérence</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ONTAP S3            | <p>Non pris en charge avec la reprise d'activité SVM.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SnapMirror synchrone      | Non pris en charge avec la reprise d'activité SVM.                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Indépendance des versions | Non pris en charge.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Chiffrement de volume     | <ul style="list-style-type: none"> <li>• Les volumes chiffrés de la source sont chiffrés sur la destination.</li> <li>• Les serveurs KMIP ou Key Manager intégrés doivent être configurés sur le système de destination.</li> <li>• De nouvelles clés de chiffrement sont générées au niveau de la destination.</li> <li>• Si la destination ne contient pas de noeud qui prend en charge le cryptage de volume, la réplication réussit, mais les volumes de destination ne sont pas chiffrés.</li> </ul> |

### Configurations répliquées dans des relations SVM DR

Le tableau suivant montre l'interaction du `snapmirror create -identity-preserve` et le `snapmirror policy create -discard-configs network` option :

| Réplication de la configuration  |             | <b>-identity-preserve true</b>                                   |                                                                  | <b>-identity-preserve false</b> |
|----------------------------------|-------------|------------------------------------------------------------------|------------------------------------------------------------------|---------------------------------|
|                                  |             | <b>Police sans<br/>-discard<br/>-configs<br/>network réglage</b> | <b>Police avec<br/>-discard<br/>-configs<br/>network réglage</b> |                                 |
| Le réseau                        | LIF NAS     | Oui.                                                             | Non                                                              | Non                             |
| Configuration Kerberos de la LIF | Oui.        | Non                                                              | Non                                                              | LIF SAN                         |
| Non                              | Non         | Non                                                              | Politiques de pare-feu                                           | Oui.                            |
| Oui.                             | Non         | Stratégies de service                                            | Oui.                                                             | Oui.                            |
| Non                              | Itinéraires | Oui.                                                             | Non                                                              | Non                             |
| Broadcast-Domain                 | Non         | Non                                                              | Non                                                              | Sous-réseau                     |
| Non                              | Non         | Non                                                              | IPspace                                                          | Non                             |
| Non                              | Non         | PME                                                              | Serveur SMB                                                      | Oui.                            |

|                         |                                |                                     |                               |                                                                                     |
|-------------------------|--------------------------------|-------------------------------------|-------------------------------|-------------------------------------------------------------------------------------|
| Oui.                    | Non                            | Groupes locaux et utilisateur local | Oui.                          | Oui.                                                                                |
| Oui.                    | Privilège                      | Oui.                                | Oui.                          | Oui.                                                                                |
| Copie en double         | Oui.                           | Oui.                                | Oui.                          | BranchCache                                                                         |
| Oui.                    | Oui.                           | Oui.                                | Options du serveur            | Oui.                                                                                |
| Oui.                    | Oui.                           | Sécurité des serveurs               | Oui.                          | Oui.                                                                                |
| Non                     | Répertoire personnel, partager | Oui.                                | Oui.                          | Oui.                                                                                |
| Symlink                 | Oui.                           | Oui.                                | Oui.                          | Politique de FPolicy, politique de FSecurity et NTFS de FSecurity                   |
| Oui.                    | Oui.                           | Oui.                                | Mapping de noms et de groupes | Oui.                                                                                |
| Oui.                    | Oui.                           | Informations d'audit                | Oui.                          | Oui.                                                                                |
| Oui.                    | NFS                            | Export-polices                      | Oui.                          | Oui.                                                                                |
| Non                     | Règles des export-policy       | Oui.                                | Oui.                          | Non                                                                                 |
| Serveur NFS             | Oui.                           | Oui.                                | Non                           | RBAC                                                                                |
| Certificats de sécurité | Oui.                           | Oui.                                | Non                           | Configuration de l'utilisateur de connexion, de la clé publique, du rôle et du rôle |
| Oui.                    | Oui.                           | Oui.                                | SSL                           | Oui.                                                                                |
| Oui.                    | Non                            | Nommer les services                 | Hôtes DNS et DNS              | Oui.                                                                                |
| Oui.                    | Non                            | Utilisateur UNIX et groupe UNIX     | Oui.                          | Oui.                                                                                |

|                     |                                            |                     |                                                                                                              |                                                   |
|---------------------|--------------------------------------------|---------------------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| Oui.                | Domaine Kerberos et blocs de clés Kerberos | Oui.                | Oui.                                                                                                         | Non                                               |
| Client LDAP et LDAP | Oui.                                       | Oui.                | Non                                                                                                          | Groupe réseau                                     |
| Oui.                | Oui.                                       | Non                 | NIS                                                                                                          | Oui.                                              |
| Oui.                | Non                                        | Accès Web et Web    | Oui.                                                                                                         | Oui.                                              |
| Non                 | Volumétrie                                 | Objet               | Oui.                                                                                                         | Oui.                                              |
| Oui.                | Copies Snapshot et règles Snapshot         | Oui.                | Oui.                                                                                                         | Oui.                                              |
| Règle d'efficacité  | Oui.                                       | Oui.                | Oui.                                                                                                         | Règle des quotas et règle de politique des quotas |
| Oui.                | Oui.                                       | Oui.                | File d'attente de récupération                                                                               | Oui.                                              |
| Oui.                | Oui.                                       | Volume racine       | Espace de noms                                                                                               | Oui.                                              |
| Oui.                | Oui.                                       | Données utilisateur | Non                                                                                                          | Non                                               |
| Non                 | Qtrees                                     | Non                 | Non                                                                                                          | Non                                               |
| Quotas              | Non                                        | Non                 | Non                                                                                                          | QoS au niveau des fichiers                        |
| Non                 | Non                                        | Non                 | Attributs : état du volume racine, garantie d'espace, taille, taille automatique et nombre total de fichiers | Non                                               |
| Non                 | Non                                        | QoS du stockage     | Groupe de règles de QoS                                                                                      | Oui.                                              |
| Oui.                | Oui.                                       | Fibre Channel (FC)  | Non                                                                                                          | Non                                               |
| Non                 | ISCSI                                      | Non                 | Non                                                                                                          | Non                                               |

|         |       |      |                  |                    |
|---------|-------|------|------------------|--------------------|
| LUN     | Objet | Oui. | Oui.             | Oui.               |
| igroups | Non   | Non  | Non              | ensembles de ports |
| Non     | Non   | Non  | Numéros de série | Non                |
| Non     | Non   | SNMP | v3 utilisateurs  | Oui.               |

### Limites du stockage de reprise d'activité SVM

Le tableau ci-dessous présente le nombre maximal recommandé de volumes et de relations de reprise d'activité SVM pris en charge par objet de stockage. Notez que les limites dépendent souvent de la plateforme. Reportez-vous à la ["Hardware Universe"](#) pour connaître les limites de votre configuration spécifique.

| Objet de stockage | Limite                  |
|-------------------|-------------------------|
| SVM               | 300 volumes flexibles   |
| Paire HA          | 1,000 volumes flexibles |
| Cluster           | 128 relations SVM DR    |

## Répliquer les configurations de SVM

### Flux de production de réplication de SVM SnapMirror

La réplication SVM SnapMirror implique la création du SVM de destination, la création d'une planification des tâches de réplication et la création et l'initialisation d'une relation SnapMirror.

Vous devez déterminer le workflow de réplication le mieux adapté à vos besoins :

- ["Réplication de l'ensemble d'une configuration de SVM"](#)
- ["Exclure les LIF et les paramètres réseau associés de la réplication du SVM"](#)
- ["Exclure network, name service et autres paramètres de la configuration des SVM"](#)

### Critères de placement des volumes sur des SVM de destination

Lors de la réplication de volumes du SVM source vers le SVM de destination, il est important de connaître les critères de sélection des agrégats.

Les agrégats sont sélectionnés selon les critères suivants :

- Les volumes sont toujours placés sur des agrégats non racines.
- Les agrégats non racines sont sélectionnés en fonction de l'espace disponible et du nombre de volumes déjà hébergés sur l'agrégat.

Les agrégats disposant d'un espace libre supérieur et avec moins de volumes sont prioritaires. L'agrégat avec la priorité la plus élevée est sélectionné.

- Les volumes source des agrégats FabricPool sont situés sur des agrégats FabricPool de destination avec la même règle de Tiering.
- Si un volume du SVM source se trouve sur un agrégat Flash Pool, celui-ci est placé sur un agrégat Flash Pool sur le SVM de destination, si un tel agrégat existe et dispose de suffisamment d'espace libre.
- Si le `-space-guarantee` l'option du volume répliqué est définie sur `volume`, seuls les agrégats avec un espace libre supérieur à la taille du volume sont pris en compte.
- La taille du volume augmente automatiquement sur le SVM de destination pendant la réplication, en fonction de la taille du volume source.

Si vous souhaitez pré-réserver la taille sur le SVM de destination, vous devez redimensionner le volume. La taille du volume n'est pas réduite automatiquement sur le SVM de destination, en fonction du SVM source.

Si vous souhaitez déplacer un volume d'un agrégat à un autre, vous pouvez utiliser le `volume move` Commande sur le SVM de destination.

## Réplication de l'ensemble d'une configuration de SVM

Vous pouvez créer une relation de SVM Disaster Recovery (SVM DR) pour répliquer une configuration de SVM vers une autre. En cas d'incident sur le site primaire, vous pouvez activer rapidement la SVM de destination.

### Avant de commencer

Les clusters source et de destination et les SVM doivent être associés.

Pour plus d'informations, voir ["Créer une relation entre clusters"](#) et ["Créer une relation SVM intercluster"](#).

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

### Description de la tâche

Ce flux de travail suppose que vous utilisez déjà une règle par défaut ou une règle de réplication personnalisée.

Depuis ONTAP 9.9.1, lorsque vous utilisez la règle de copie en miroir, vous pouvez créer différentes règles Snapshot sur le SVM source et de destination, et les copies Snapshot de la destination ne sont pas écrasées par les copies Snapshot de la source. Pour plus d'informations, voir ["Présentation de la réplication des SVM SnapMirror"](#).

Effectuez cette procédure à partir de la destination. Si vous devez créer une nouvelle stratégie de protection, par exemple, lorsque votre machine virtuelle de stockage source a configuré SMB, vous devez créer la stratégie et utiliser l'option **Identity Preserve**. Pour plus de détails, voir ["Création de règles personnalisées de protection des données"](#).

### Étapes

Vous pouvez effectuer cette tâche depuis System Manager ou l'interface de ligne de commandes de ONTAP.



## System Manager

1. Sur le cluster de destination, cliquez sur **protection > relations**.
2. Sous **Relationships**, cliquez sur **Protect** et choisissez **Storage VMS (DR)**.
3. Sélectionnez une stratégie de protection. Si vous avez créé une règle de protection personnalisée, sélectionnez-la, puis choisissez le cluster source et la VM de stockage que vous souhaitez répliquer. Vous pouvez également créer une nouvelle machine virtuelle de stockage cible en entrant un nouveau nom de machine virtuelle de stockage.
4. Si vous le souhaitez, modifiez les paramètres de destination pour remplacer la conservation des identités et inclure ou exclure des interfaces et des protocoles réseau.
5. Cliquez sur **Enregistrer**.

## CLI

1. Création d'un SVM de destination :

```
vserver create -vserver <SVM_name> -subtype dp-destination
```

Le nom de SVM doit être unique sur les clusters source et destination.

L'exemple suivant crée un SVM de destination nommé `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. Depuis le cluster destination, créez une relation de type SVM peer-to-peer à l'aide de `vserver peer create` commande.

Pour plus d'informations, voir ["Créer une relation SVM intercluster"](#).

3. Créer une planification de travaux de réplication :

```
job schedule cron create -name <job_name> -month <month> -dayofweek <day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

Pour `-month`, `-dayofweek`, et `-hour`, vous pouvez spécifier `all` pour exécuter le travail chaque mois, jour de la semaine et heure, respectivement.



La planification (RPO) minimale prise en charge pour les volumes FlexVol dans une relation de SVM SnapMirror est de 15 minutes. La planification (RPO) minimale prise en charge pour les volumes FlexGroup dans une relation de SVM SnapMirror est de 30 minutes.

L'exemple suivant crée un programme de travail nommé `my_weekly` Le samedi à 3:00 :

```
cluster_dst:> job schedule cron create -name my_weekly -dayofweek
saturday -hour 3 -minute 0
```

4. Depuis le SVM destination ou le cluster destination, créer une relation de réplication :

```
snapmirror create -source-path <SVM_name>: -destination-path
<SVM_name>: -type <DP|XDP> -schedule <schedule> -policy <policy>
-identity-preserve true
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options.

L'exemple suivant illustre la création d'une relation SnapMirror DR à l'aide de la valeur par défaut `MirrorAllSnapshots` règle :

```
cluster_dst:> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy
MirrorAllSnapshots -identity-preserve true
```

L'exemple suivant illustre la création d'une relation de réplication unifiée à l'aide de la valeur par défaut `MirrorAndVault` règle :

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

En supposant que vous avez créé une police personnalisée avec le type de police `async-mirror`, l'exemple suivant illustre la création d'une relation SnapMirror DR :

```
cluster_dst:> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_mirrored
-identity-preserve true
```

En supposant que vous avez créé une police personnalisée avec le type de police `mirror-vault`, l'exemple suivant crée une relation de réplication unifiée :

```
cluster_dst:> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_unified
-identity-preserve true
```

5. Arrêter le SVM de destination :

```
vserver stop -vserver <SVM_name>
```

L'exemple suivant arrête un SVM de destination nommé svm\_Backup :

```
cluster_dst::> vserver stop -vserver svm_backup
```

6. Depuis le SVM destination ou le cluster destination, initialiser la relation SVM de réplication :

```
snapmirror initialize -source-path <SVM_name>: -destination-path
<SVM_name>:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options.

L'exemple suivant initialise la relation entre le SVM source, svm1, Et le SVM de destination, svm\_backup:

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

## Exclure les LIF et les paramètres réseau associés de la réplication du SVM

Si les SVM source et destination se trouvent dans des sous-réseaux différents, vous pouvez utiliser le `-discard-configs network` de la `snapmirror policy create` Commande permettant d'exclure les LIFs et les paramètres réseau associés de la réplication du SVM.

### Ce dont vous avez besoin

Les clusters source et de destination et les SVM doivent être associés.

Pour plus d'informations, voir ["Créer une relation entre clusters"](#) et ["Créer une relation SVM intercluster"](#).

### Description de la tâche

Le `-identity-preserve` de la `snapmirror create` la commande doit être définie sur `true` Lorsque vous créez la relation de réplication SVM.

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

### Étapes

1. Création d'un SVM de destination :

```
vserver create -vserver SVM -subtype dp-destination
```

Le nom de SVM doit être unique sur les clusters source et destination.

L'exemple suivant crée un SVM de destination nommé `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. Depuis le cluster destination, créez une relation de type SVM peer-to-peer à l'aide de `vserver peer create` commande.

Pour plus d'informations, voir ["Créer une relation SVM intercluster"](#).

3. Création d'un programme de travail :

```
job schedule cron create -name job_name -month month -dayofweek day_of_week
-day day_of_month -hour hour -minute minute
```

Pour `-month`, `-dayofweek`, et `-hour`, vous pouvez spécifier `all` pour exécuter le travail chaque mois, jour de la semaine et heure, respectivement.



La planification (RPO) minimale prise en charge pour les volumes FlexVol dans une relation de SVM SnapMirror est de 15 minutes. La planification (RPO) minimale prise en charge pour les volumes FlexGroup dans une relation de SVM SnapMirror est de 30 minutes.

L'exemple suivant crée un programme de travail nommé `my_weekly` Le samedi à 3:00 :

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. Création d'une règle de réplication personnalisée :

```
snapmirror policy create -vserver SVM -policy policy -type async-
mirror|vault|mirror-vault -comment comment -tries transfer_tries -transfer
-priority low|normal -is-network-compression-enabled true|false -discard
-configs network
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

L'exemple suivant illustre la création d'une règle de réplication personnalisée pour la reprise sur incident de SnapMirror, à l'exception des LIFs :

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_exclude_LIFs -type async-mirror -discard-configs network
```

L'exemple suivant crée une règle de réplication personnalisée pour la réplication unifiée, qui exclut les LIFs :

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```



Envisagez de créer la même règle SnapMirror personnalisée sur le cluster source pour les scénarios futurs de basculement et de rétablissement.

5. Depuis le SVM destination ou le cluster destination, lancer la commande suivante pour créer une relation de réplication :

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP
-schedule schedule -policy policy -identity-preserve true|false -discard
-configs true|false
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir les exemples ci-dessous.

L'exemple suivant crée une relation SnapMirror DR qui exclut les LIF :

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_weekly -policy DR_exclude_LIFs
-identity-preserve true
```

L'exemple suivant crée une relation de réplication unifiée SnapMirror qui exclut les LIF :

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_weekly -policy unified_exclude_LIFs
-identity-preserve true -discard-configs true
```

6. Arrêter le SVM de destination :

```
vserver stop
```

*SVM name*

L'exemple suivant arrête le SVM de destination nommé `svm_Backup` :

```
cluster_dst::> vserver stop -vserver svm_backup
```

7. Depuis le SVM destination ou le cluster destination, initialiser une relation de réplication :

```
snapmirror initialize -source-path SVM: -destination-path SVM:
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

L'exemple suivant initialise la relation entre la source, `svm1` et la destination, `svm_backup`:

```
cluster_dst:> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

### Une fois que vous avez terminé

Vous devez configurer le réseau et les protocoles sur le SVM de destination pour l'accès aux données en cas d'incident.

### Exclure le réseau, le nom service et d'autres paramètres de la réplication SVM

Vous pouvez utiliser le `-identity-preserve false` de la `snapmirror create` Commande permettant de répliquer uniquement les volumes et les configurations de sécurité d'un SVM. Certains paramètres de protocole et de service de nom sont également conservés.

### Description de la tâche

Pour obtenir la liste des paramètres de protocole et de service de noms conservés, reportez-vous à la section ["Configurations répliquées dans les relations de reprise après incident des SVM"](#).

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

### Avant de commencer

Les clusters source et de destination et les SVM doivent être associés.

Pour plus d'informations, voir ["Créer une relation entre clusters"](#) et ["Créer une relation SVM intercluster"](#).

### Étapes

1. Création d'un SVM de destination :

```
vserver create -vserver SVM -subtype dp-destination
```

Le nom de SVM doit être unique sur les clusters source et destination.

L'exemple suivant crée un SVM de destination nommé `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. Depuis le cluster destination, créez une relation de type SVM peer-to-peer à l'aide de `vserver peer create` commande.

Pour plus d'informations, voir ["Créer une relation SVM intercluster"](#).

3. Créer une planification de travaux de réplication :

```
job schedule cron create -name job_name -month month -dayofweek day_of_week
-day day_of_month -hour hour -minute minute
```

Pour `-month`, `-dayofweek`, et `-hour`, vous pouvez spécifier `all` pour exécuter le travail chaque mois, jour de la semaine et heure, respectivement.



La planification (RPO) minimale prise en charge pour les volumes FlexVol dans une relation de SVM SnapMirror est de 15 minutes. La planification (RPO) minimale prise en charge pour les volumes FlexGroup dans une relation de SVM SnapMirror est de 30 minutes.

L'exemple suivant crée un programme de travail nommé `my_weekly` Le samedi à 3:00 :

```
cluster_dst:> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. Créez une relation de réplication qui exclut le réseau, le service de noms et d'autres paramètres de configuration :

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP
-schedule schedule -policy policy -identity-preserve false
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir les exemples ci-dessous. On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

L'exemple suivant illustre la création d'une relation SnapMirror DR à l'aide de la valeur par défaut `MirrorAllSnapshots` politique. La relation exclut le réseau, le nom service et d'autres paramètres de configuration de la réplication SVM :

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve false
```

L'exemple suivant illustre la création d'une relation de réplication unifiée à l'aide de la valeur par défaut `MirrorAndVault` politique. La relation exclut le réseau, le service de nom et d'autres paramètres de configuration :

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
false
```

En supposant que vous avez créé une police personnalisée avec le type de police `async-mirror`, l'exemple suivant illustre la création d'une relation SnapMirror DR. La relation exclut le réseau, le nom service et d'autres paramètres de configuration de la réplication SVM :

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

En supposant que vous avez créé une police personnalisée avec le type de police `mirror-vault`,

l'exemple suivant crée une relation de réplication unifiée. La relation exclut le réseau, le nom service et d'autres paramètres de configuration de la réplication SVM :

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

#### 5. Arrêter le SVM de destination :

```
vserver stop
```

*SVM name*

L'exemple suivant arrête un SVM de destination nommé dvs1 :

```
destination_cluster::> vserver stop -vserver dvs1
```

#### 6. Si vous utilisez SMB, vous devez également configurer un serveur SMB.

Voir ["SMB uniquement : création d'un serveur SMB"](#).

#### 7. Depuis le SVM destination ou le cluster destination, initialiser la relation SVM de réplication :

```
snapmirror initialize -source-path SVM_name: -destination-path SVM_name:
```

### Une fois que vous avez terminé

Vous devez configurer le réseau et les protocoles sur le SVM de destination pour l'accès aux données en cas d'incident.

### Spécifiez les agrégats à utiliser pour les relations SVM DR

Une fois un SVM de reprise d'activité créé, vous pouvez utiliser le `aggr-list` option avec `vserver modify` Commande pour limiter les agrégats utilisés pour héberger les volumes de destination du SVM DR

#### Étape

##### 1. Création d'un SVM de destination :

```
vserver create -vserver SVM -subtype dp-destination
```

##### 2. Modifiez la liste d'agrégats du SVM de reprise d'activité pour limiter les agrégats utilisés pour héberger le volume du SVM de reprise d'activité :

```
cluster_dest::> vserver modify -vserver SVM -aggr-list <comma-separated-list>
```

### SMB uniquement : créez un serveur SMB

Si le SVM source dispose d'une configuration SMB et que vous avez décidé de le définir



identity-preserve à false, Vous devez créer un serveur SMB pour le SVM de destination. Le serveur SMB est requis pour certaines configurations SMB, par exemple les partages lors de l'initialisation de la relation SnapMirror.

## Étapes

1. Démarrer le SVM de destination à l'aide de l' `vserver start` commande.

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

2. Vérifier que le SVM de destination est bien dans le running état et sous-type dp-destination à l'aide du `vserver show` commande.

```
destination_cluster::> vserver show
```

| Vserver   | Type | Subtype        | Admin State | Operational State | Root Volume |
|-----------|------|----------------|-------------|-------------------|-------------|
| Aggregate |      |                |             |                   |             |
| -----     |      |                |             |                   |             |
| dvs1      | data | dp-destination | running     | running           | -           |

3. Créer une LIF en utilisant le `network interface create` commande.

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101 -address 192.0.2.128 -netmask 255.255.255.128
```

4. Créez une route à l'aide de `network route create` commande.

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

## "Gestion du réseau"

5. Configurez DNS à l'aide de `vserver services dns create` commande.

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

6. Ajoutez le contrôleur de domaine préféré à l'aide du `vserver cifs domain preferred-dc add` commande.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-pREFERRED-DC
192.0.2.128 -domain mydomain.example.com
```

7. Créez le serveur SMB à l'aide de `vserver cifs create` commande.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

8. Arrêtez le SVM de destination à l'aide de `vserver stop` commande.

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

## Exclure des volumes de la réplication SVM

Par défaut tous les volumes de données RW du SVM source sont répliqués. Si vous ne souhaitez pas protéger tous les volumes du SVM source, vous pouvez utiliser le `-vserver-dr-protection unprotected` de la `volume modify` Commande pour exclure des volumes de la réplication SVM.

### Étapes

1. Exclure un volume de la réplication SVM :

```
volume modify -vserver SVM -volume volume -vserver-dr-protection unprotected
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

L'exemple suivant exclut le volume `volA_src` De la réplication SVM :

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection unprotected
```

Si vous souhaitez inclure par la suite un volume dans la réplication SVM que vous avez initialement exclue, exécutez la commande suivante :

```
volume modify -vserver SVM -volume volume -vserver-dr-protection protected
```

L'exemple suivant inclut le volume `volA_src` Dans la SVM de réplication :

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection protected
```

2. Créer et initialiser la relation de réplication SVM comme décrit à la ["Réplication de l'ensemble d'une configuration de SVM"](#).

## **Service des données à partir d'une destination de reprise après incident des SVM**

### **Flux de travail de reprise d'activité des SVM**

Pour restaurer des données après un incident et transmettre leur données depuis le SVM de destination, vous devez activer le SVM de destination. L'activation de la SVM de destination implique l'arrêt de transferts SnapMirror planifiés, l'abandon de transferts SnapMirror en cours, le démantèlement de la relation de réplication, l'arrêt de la SVM source et le démarrage de la SVM de destination.



### Rendre les volumes de destination du SVM inscriptibles

Vous devez rendre les volumes SVM de destination inscriptibles avant de pouvoir transmettre des données aux clients.

La procédure est en grande partie identique à la procédure de réplication de volume, à exception près. Si vous avez défini `-identity-preserve true` lors de la création de la relation de réplication du SVM, vous devez arrêter le SVM source avant d'activer le SVM de destination.

### Description de la tâche

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.





En cas de reprise d'activité, vous ne pouvez pas effectuer de mise à jour SnapMirror depuis le SVM source vers le SVM de destination de reprise après incident car votre SVM source et ses données sont inaccessibles. Les mises à jour depuis la dernière resynchronisation peuvent être en mauvais état ou corrompues.

Depuis ONTAP 9.8, il est possible d'utiliser System Manager pour activer une machine virtuelle de stockage de destination après un incident. L'activation de la VM de stockage de destination rend les volumes de destination du SVM inscriptibles et vous permet de transmettre des données aux clients.

### **Étapes**

Vous pouvez effectuer cette tâche depuis System Manager ou l'interface de ligne de commandes de ONTAP.

## System Manager

1. Si le cluster source est accessible, vérifiez que le SVM est arrêté : accédez à **stockage > VM de stockage** et vérifiez la colonne **State** de la SVM.
2. Si l'état du SVM source est « running », arrêtez-le : sélectionnez  et choisissez **Stop**.
3. Sur le cluster de destination, recherchez la relation de protection souhaitée : accédez à **protection > relations**.
4. Passez le curseur sur le nom de la machine virtuelle de stockage source souhaitée, cliquez sur , puis choisissez **Activer la machine virtuelle de stockage de destination**.
5. Dans la fenêtre **Activer la VM de stockage de destination**, sélectionnez **Activer la VM de stockage de destination et rompre la relation**.
6. Cliquez sur **Activer**.

## CLI

1. Depuis le SVM de destination ou le cluster de destination, arrêter les transferts programmés vers la destination :

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant arrête les transferts planifiés entre la SVM source `svm1` Et le SVM de destination `svm_backup`:

```
cluster_dst::> snapmirror quiesce -source-path svm1: -destination
-path svm_backup:
```

2. Depuis le SVM destination ou le cluster destination, arrêter les transferts en cours vers la destination :

```
snapmirror abort -source-path <SVM>: -destination-path <SVM>:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant arrête les transferts en cours entre la SVM source `svm1` Et le SVM de destination `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path svm1: -destination-path
svm_backup:
```

3. Depuis le SVM destination ou le cluster destination, faire un break de la relation de réplication :

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant rompt la relation entre la SVM source `svm1` Et le SVM de destination `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

4. Si vous avez défini `-identity-preserve true` Lorsque vous avez créé la relation de réplication de SVM, arrêter le SVM source :

```
vserver stop -vserver <SVM>
```

L'exemple suivant arrête le SVM source `svm1`:

```
cluster_src::> vserver stop svm1
```

5. Démarrer le SVM de destination :

```
vserver start -vserver <SVM>
```

L'exemple suivant démarre le SVM de destination `svm_backup`:

```
cluster_dst::> vserver start svm_backup
```

### Une fois que vous avez terminé

Configuration des volumes de destination des SVM pour l'accès aux données, comme décrit à la section ["Configuration du volume de destination pour l'accès aux données"](#).

## Réactiver la SVM source

### Flux de travail de réactivation des SVM source

Si la SVM source existe après un incident, vous pouvez la réactiver et la protéger en recréant la relation de reprise d'activité de la SVM.



### Réactiver la SVM source d'origine

Cette relation permet de rétablir la relation initiale de protection des données entre les SVM source et destination lorsque vous n'avez plus besoin de transmettre des données depuis la destination. La procédure est en grande partie identique à la procédure de réplication de volume, à exception près. On doit arrêter le SVM de destination avant de réactiver la SVM source.

#### Avant de commencer

Si vous avez augmenté la taille du volume de destination tout en y servant des données, avant de réactiver le volume source, vous devez augmenter manuellement la taille automatique maximale sur le volume source d'origine afin de garantir une croissance suffisante.

["Lorsqu'un volume de destination augmente automatiquement"](#)

#### Description de la tâche

Depuis la version ONTAP 9.11.1, vous pouvez réduire le temps de resynchronisation pendant une répétition de reprise d'activité à l'aide ``-quick-resync true`` de l'option de l'interface de ligne de ``snapmirror resync`` commande de la commande tout en effectuant une resynchronisation inverse d'une relation de SVM DR. Une resynchronisation rapide permet de réduire le temps nécessaire au retour à la production en contournant les opérations de reconstruction et de restauration des entrepôts de données.



La resynchronisation rapide ne permet pas de préserver l'efficacité du stockage des volumes de destination. L'activation des synchronisations rapides peut augmenter l'espace volume utilisé par les volumes de destination.



Cette procédure suppose que la ligne de base du volume source d'origine est intacte. Si la base n'est pas intacte, vous devez créer et initialiser la relation entre le volume dont vous accédez aux données et le volume source d'origine avant d'effectuer la procédure.

Depuis ONTAP 9.8, vous pouvez utiliser System Manager pour réactiver une machine virtuelle de stockage source après un incident. La réactivation de la machine virtuelle de stockage source arrête la machine virtuelle de stockage de destination et permet de réactiver la réplication de la source vers la destination.


Lorsque vous utilisez System Manager pour réactiver la VM de stockage source, System Manager effectue les opérations suivantes en arrière-plan :

- Crée une relation SVM DR inverse de la destination initiale à la source d'origine à l'aide de la resynchronisation SnapMirror
- Arrête le SVM de destination
- Met à jour la relation SnapMirror
- Interrompt la relation SnapMirror
- Redémarre le SVM d'origine
- Renvoie une resynchronisation SnapMirror de la source d'origine vers la destination d'origine
- Nettoie les relations SnapMirror

### **Étapes**

Vous pouvez effectuer cette tâche depuis System Manager ou l'interface de ligne de commandes de ONTAP.

## System Manager

1. Dans le cluster de destination, cliquez sur **protection > relations**, puis localisez la relation de protection souhaitée.
2. Passez le curseur sur le nom de la relation source, cliquez sur , puis sélectionnez **réactiver la VM de stockage source**.
3. Dans la fenêtre **réactiver la VM de stockage source**, cliquez sur **réactiver**.
4. Sous **Relationship**, surveillez la progression de la réactivation de la source en visualisant **Transfer Status** pour la relation de protection. Une fois la réactivation terminée, l'état de la relation doit revenir à « miroir ».

## CLI

1. Depuis le SVM source d'origine ou le cluster source d'origine, créez une relation SVM DR inverse en utilisant les mêmes paramètres de configuration, de politique et de préservation de l'identité que la relation SVM DR d'origine :

```
snapmirror create -source-path <SVM>: -destination-path <SVM>:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant crée une relation entre le SVM à partir duquel vous transmet des données, `svm_backup`, Et le SVM source d'origine, `svm1`:

```
cluster_src::> snapmirror create -source-path svm_backup:
-destination-path svm1:
```

2. Depuis le SVM source d'origine ou le cluster source d'origine, exécutez la commande suivante pour inverser la relation de protection des données :

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.



Échec de la commande si une copie Snapshot commune n'existe pas sur la source et la destination. Utiliser `snapmirror initialize` pour réinitialiser la relation.

L'exemple suivant inverse la relation entre la SVM source d'origine, `svm1`, Et le SVM depuis lequel vous servant des données, `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1:
```

Exemple avec l'option -rapide-resynchronisation :

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1: -quick-resync true
```

3. Lorsque vous êtes prêt à rétablir l'accès aux données au SVM source d'origine, arrêter le SVM de destination d'origine pour déconnecter les clients actuellement connectés au SVM de destination d'origine.

```
vserver stop -vserver <SVM>
```

L'exemple suivant arrête le SVM destination d'origine qui transmet actuellement des données :

```
cluster_dst::> vserver stop svm_backup
```

4. Vérifier que le SVM destination d'origine est bien à l'état stopped en utilisant le `vserver show` commande.

```
cluster_dst::> vserver show
```

| Vserver    | Type  | Subtype | Admin State | Operational State | Root Volume |
|------------|-------|---------|-------------|-------------------|-------------|
| Aggregate  |       |         |             |                   |             |
| -----      | ----- | -----   | -----       | -----             | -----       |
| -----      |       |         |             |                   |             |
| svm_backup | data  | default | stopped     | stopped           | rv          |
| aggr1      |       |         |             |                   |             |

5. Depuis le SVM source d'origine ou le cluster source d'origine, lancer la commande suivante pour effectuer la mise à jour finale de la relation inversée afin de transférer toutes les modifications du SVM de destination d'origine vers le SVM source d'origine :

```
snapmirror update -source-path <SVM>: -destination-path <SVM>:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant met à jour la relation entre le SVM de destination d'origine à partir duquel vous accédez aux données, `svm_backup`, Et le SVM source d'origine, `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup:
-destination-path svm1:
```

6. Depuis le SVM source d'origine ou le cluster source d'origine, lancer la commande suivante pour arrêter les transferts programmés pour la relation inverse :

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant arrête les transferts programmés entre le SVM où vous transmet des données, `svm_backup`, Et le SVM d'origine, `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup:
-destination-path svm1:
```

7. Lorsque la mise à jour finale est terminée et que la relation indique « suspendu » pour l'état de la relation, exécutez la commande suivante à partir du SVM source d'origine ou du cluster source d'origine pour interrompre la relation inversée :

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant rupture de la relation entre le SVM de destination d'origine duquel vous servant des données, `svm_backup`, Et le SVM source d'origine, `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup:
-destination-path svm1:
```

8. Si le SVM source d'origine était auparavant arrêté, depuis le cluster source d'origine, démarrer le SVM source d'origine :

```
vserver start -vserver <SVM>
```

L'exemple suivant démarre le SVM source d'origine :

```
cluster_src::> vserver start svm1
```

9. Depuis le SVM destination d'origine ou le cluster destination d'origine, rétablir la relation de protection des données d'origine :

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant rétablit la relation entre le SVM source d'origine, `svm1`, Et le SVM de destination d'origine, `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination
-path svm_backup:
```

10. Depuis le SVM source d'origine ou le cluster source d'origine, lancer la commande suivante pour supprimer la relation de protection des données inversée :

```
snapmirror delete -source-path <SVM>: -destination-path <SVM>:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant supprime la relation inversée entre le SVM de destination d'origine, `svm_backup`, Et le SVM source d'origine, `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup:
-destination-path svm1:
```

11. Depuis le SVM de destination d'origine ou le cluster de destination d'origine, relâcher la relation de protection des données inversée :

```
snapmirror release -source-path <SVM>: -destination-path <SVM>:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant libère la relation inversée entre le SVM de destination d'origine, `svm_backup` et le SVM source d'origine, `svm1`

```
cluster_dst::> snapmirror release -source-path svm_backup:
-destination-path svm1:
```

### Une fois que vous avez terminé

Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

### Réactiver le SVM source d'origine (volumes FlexGroup uniquement)

Cette relation permet de rétablir la relation initiale de protection des données entre les SVM source et destination lorsque vous n'avez plus besoin de transmettre des données depuis la destination. Pour réactiver la SVM source d'origine lorsque vous utilisez des volumes FlexGroup, vous devez effectuer quelques étapes supplémentaires, notamment la suppression de la relation SVM DR d'origine et la libération de la relation d'origine avant d'inverser la relation. Vous devez également libérer la relation inversée et recréer la relation d'origine avant d'arrêter les transferts programmés.

#### Étapes

1. Depuis le SVM destination d'origine ou le cluster destination d'origine, supprimer la relation SVM DR d'origine :

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant supprime la relation d'origine entre le SVM source d'origine, `svm1` et le SVM de destination d'origine, `svm_backup`:

```
cluster_dst::> snapmirror delete -source-path svm1: -destination-path
svm_backup:
```

2. Depuis le SVM source d'origine ou le cluster source d'origine, libérer la relation d'origine tout en conservant les copies Snapshot intactes :

```
snapmirror release -source-path SVM: -destination-path SVM: -relationship-info
-only true
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant libère la relation initiale entre la SVM source d'origine, `svm1` et la SVM de destination d'origine, `svm_backup`.

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup: -relationship-info-only true
```

3. Depuis le SVM source d'origine ou le cluster source d'origine, créez une relation SVM DR inverse en utilisant les mêmes paramètres de configuration, de politique et de préservation de l'identité que la relation

SVM DR d'origine :

```
snapmirror create -source-path SVM: -destination-path SVM:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant crée une relation entre le SVM à partir duquel vous transmet des données, `svm_backup`, Et le SVM source d'origine, `svm1`:

```
cluster_src::> snapmirror create -source-path svm_backup: -destination
-path svm1:
```

4. Depuis le SVM source d'origine ou le cluster source d'origine, exécutez la commande suivante pour inverser la relation de protection des données :

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.



Échec de la commande si une copie Snapshot commune n'existe pas sur la source et la destination. Utiliser `snapmirror initialize` pour réinitialiser la relation.

L'exemple suivant inverse la relation entre la SVM source d'origine, `svm1`, Et le SVM depuis lequel vous servant des données, `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1:
```

5. Lorsque vous êtes prêt à rétablir l'accès aux données au SVM source d'origine, arrêter le SVM de destination d'origine pour déconnecter les clients actuellement connectés au SVM de destination d'origine.

```
vserver stop -vserver SVM
```

L'exemple suivant arrête le SVM destination d'origine qui transmet actuellement des données :

```
cluster_dst::> vserver stop svm_backup
```

6. Vérifier que le SVM destination d'origine est bien à l'état stopped en utilisant le `vserver show` commande.

```
cluster_dst:> vserver show
```

| Vserver    | Type  | Subtype | Admin State | Operational State | Root Volume |
|------------|-------|---------|-------------|-------------------|-------------|
| Aggregate  |       |         |             |                   |             |
| -----      | ----- | -----   | -----       | -----             | -----       |
| svm_backup | data  | default | stopped     | stopped           | rv          |
| aggr1      |       |         |             |                   |             |

7. Depuis le SVM source d'origine ou le cluster source d'origine, lancer la commande suivante pour effectuer la mise à jour finale de la relation inversée afin de transférer toutes les modifications du SVM de destination d'origine vers le SVM source d'origine :

```
snapmirror update -source-path SVM: -destination-path SVM:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant met à jour la relation entre le SVM de destination d'origine à partir duquel vous accédez aux données, `svm_backup`, Et le SVM source d'origine, `svm1`:

```
cluster_src:> snapmirror update -source-path svm_backup: -destination
-path svm1:
```

8. Depuis le SVM source d'origine ou le cluster source d'origine, lancer la commande suivante pour arrêter les transferts programmés pour la relation inverse :

```
snapmirror quiesce -source-path SVM: -destination-path SVM:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant arrête les transferts programmés entre le SVM où vous transmet des données, `svm_backup`, Et le SVM d'origine, `svm1`:

```
cluster_src:> snapmirror quiesce -source-path svm_backup: -destination
-path svm1:
```

9. Lorsque la mise à jour finale est terminée et que la relation indique « suspendu » pour l'état de la relation, exécutez la commande suivante à partir du SVM source d'origine ou du cluster source d'origine pour interrompre la relation inversée :

```
snapmirror break -source-path SVM: -destination-path SVM:
```





Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant rupture de la relation entre le SVM de destination d'origine duquel vous servant des données, `svm_backup`, Et le SVM source d'origine, `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup: -destination
-path svm1:
```

10. Si le SVM source d'origine était auparavant arrêté, depuis le cluster source d'origine, démarrer le SVM source d'origine :

```
vserver start -vserver SVM
```

L'exemple suivant démarre le SVM source d'origine :

```
cluster_src::> vserver start svm1
```

11. Depuis le SVM source d'origine ou le cluster source d'origine, supprimer la relation SVM DR inversée :

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant supprime la relation inversée entre le SVM de destination d'origine, `svm_backup` et le SVM source d'origine, `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

12. Depuis le SVM de destination d'origine ou le cluster de destination d'origine, relâcher la relation inversée tout en préservant l'intégrité des copies Snapshot :

```
snapmirror release -source-path SVM: -destination-path SVM: -relationship-info
-only true
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant libère la relation inversée entre la SVM de destination d'origine, `svm_backup` et la SVM source d'origine, `svm1` :

```
cluster_dst:> snapmirror release -source-path svm_backup: -destination
-path svm1: -relationship-info-only true
```

13. Depuis le SVM destination d'origine ou le cluster destination d'origine, recréer la relation d'origine. Utilisez le même paramètre de configuration, de politique et de préservation de l'identité que la relation SVM DR d'origine :

```
snapmirror create -source-path SVM: -destination-path SVM:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant crée une relation entre le SVM source d'origine, `svm1`, Et le SVM de destination d'origine, `svm_backup`:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup:
```

14. Depuis le SVM destination d'origine ou le cluster destination d'origine, rétablir la relation de protection des données d'origine :

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant rétablit la relation entre le SVM source d'origine, `svm1`, Et le SVM de destination d'origine, `svm_backup`:

```
cluster_dst:> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

## Resynchroniser une machine virtuelle de stockage de destination

Depuis ONTAP 9.8, vous pouvez utiliser System Manager pour resynchroniser les données et les détails de configuration depuis la machine virtuelle de stockage source vers la machine virtuelle de stockage de destination dans une relation de protection défaillante et rétablir la relation.

ONTAP 9.11.1 offre la possibilité de contourner la reconstruction complète d'un entrepôt de données lorsque vous effectuez une répétition de reprise après incident, pour que vous puissiez revenir plus rapidement à la production.


Vous effectuez l'opération de resynchronisation uniquement à partir de la destination de la relation d'origine. La resynchronisation supprime toutes les données de la machine virtuelle de stockage de destination qui sont

plus récentes que celles contenues dans la machine virtuelle de stockage source.

## Étapes

Vous pouvez effectuer cette tâche à l'aide de System Manager ou de l'interface de ligne de commandes de ONTAP.

### System Manager

1. Dans la destination, sélectionnez la relation de protection souhaitée : cliquez sur **protection > relations**.
2. Vous pouvez également sélectionner **effectuer une resynchronisation rapide** pour contourner la reconstruction complète d'un entrepôt de données lors d'une répétition de reprise après sinistre.
3. Cliquez sur  et cliquez sur **Resync**.
4. Sous **Relationship**, surveillez la progression de la resynchronisation en affichant **Transfer Status** pour la relation.

### CLI

1. Depuis le cluster destination, resynchroniser la relation :

```
snapmirror resync -source-path <svm>: -destination-path <svm>:
-quick-resync true|false
```

## Conversion des relations de réplication de volume en relation de réplication SVM

Vous pouvez convertir des relations de réplication entre les volumes en une relation de réplication entre les SVM (Storage Virtual machines) qui sont propriétaires des volumes, à condition que chaque volume de la source (à l'exception du volume root) soit répliqué, et chaque volume de la source (y compris le volume root) porte le même nom que le volume de destination.

### Description de la tâche

Utilisez le `volume rename` Commande lorsque la relation SnapMirror est inactive pour renommer des volumes de destination, si nécessaire.

## Étapes

1. Depuis le SVM de destination ou le cluster de destination, exécutez la commande suivante pour resynchroniser les volumes source et destination :

```
snapmirror resync -source-path <SVM:volume> -destination-path <SVM:volume>
-type DP|XDP -policy <policy>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.



Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.

L'exemple suivant resynchronise la relation entre le volume source `volA` marche `svm1` et le volume de

destination volA marche svm\_backup:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA
```

2. Créer une relation de réplication SVM entre les SVM source et destination, comme décrit à la ["Réplication des configurations de SVM"](#).

Vous devez utiliser le `-identity-preserve true` de la `snapmirror create` commande lorsque vous créez votre relation de réplication.

3. Arrêter le SVM de destination :

```
vserver stop -vserver SVM
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant arrête le SVM de destination svm\_backup:

```
cluster_dst::> vserver stop svm_backup
```

4. Depuis le SVM de destination ou le cluster de destination, exécutez la commande suivante pour resynchroniser les SVM source et destination :

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>: -type DP|XDP
-policy <policy>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.

L'exemple suivant resynchronise la relation entre le SVM source svm1 Et le SVM de destination svm\_backup:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

## Supprime une relation de réplication SVM

Vous pouvez utiliser le `snapmirror delete` et `snapmirror release` Commandes permettant de supprimer une relation de réplication SVM. Vous pouvez ensuite supprimer manuellement les volumes de destination inutiles.

## Description de la tâche

Le `snapmirror release` Commande permet de supprimer toutes les copies Snapshot créées par SnapMirror de la source. Vous pouvez utiliser le `-relationship-info-only` Option pour conserver les copies Snapshot.

Pour connaître la syntaxe complète des commandes, reportez-vous à la page [man](#).

## Étapes

1. Lancer la commande suivante depuis le SVM de destination ou le cluster de destination pour faire un break de la relation de réplication :

```
snapmirror break -source-path SVM: -destination-path SVM:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant rompt la relation entre la SVM source `svm1` Et le SVM de destination `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

2. Lancer la commande suivante depuis le SVM de destination ou le cluster de destination pour supprimer la relation de réplication :

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant supprime la relation entre la SVM source `svm1` Et le SVM de destination `svm_backup`:

```
cluster_dst::> snapmirror delete -source-path svm1: -destination-path
svm_backup:
```

3. Lancer la commande suivante depuis le cluster source ou le SVM source pour libérer les informations relatives aux relations de réplication du SVM source :

```
snapmirror release -source-path SVM: -destination-path SVM:
```



Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant publie des informations pour la relation de réplication spécifiée à partir du SVM source `svm1`:

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup:
```

## Gérer la réplication de volume root SnapMirror

### Gérer la présentation de la réplication du volume racine SnapMirror

Chaque SVM d'un environnement NAS possède un espace de noms unique. Le SVM *root volume*, contenant le système d'exploitation et les informations associées, est le point d'entrée de la hiérarchie de l'espace de noms. Pour garantir que les données restent accessibles aux clients en cas de panne ou de basculement d'un nœud, vous devez créer une copie miroir de partage de la charge du volume racine du SVM.

L'objectif principal des miroirs de partage de charge pour les volumes root des SVM n'est plus de permettre le partage de charge ; ils ont plutôt pour objectif la reprise sur incident.

- Si le volume racine est temporairement indisponible, le miroir de partage de charge permet un accès en lecture seule aux données du volume racine.
- Si le volume racine n'est définitivement pas disponible, vous pouvez promouvoir l'un des volumes de partage de charge pour fournir un accès en écriture aux données du volume racine.

### Créer et initialiser des relations de miroir de partage de charge

Il est recommandé de créer un miroir de partage de charge (LSM) pour chaque volume root du SVM qui transmet les données NAS au sein du cluster. Pour les clusters composés d'au moins deux paires HA, il est conseillé de tenir compte des miroirs de partage de charge des volumes root du SVM afin de s'assurer que le namespace reste accessible aux clients dans le cas contraire.

Les deux nœuds d'une paire haute disponibilité sont défaillants. Les miroirs de partage de charge ne sont pas adaptés aux clusters constitués d'une seule paire haute disponibilité.

#### Description de la tâche

Si vous créez un LSM sur le même nœud et que le nœud n'est pas disponible, vous disposez d'un point d'échec unique et vous ne disposez pas d'une seconde copie pour vous assurer que les données restent accessibles aux clients. Cependant, si vous créez le LSM sur un nœud autre que celui contenant le volume root ou sur une autre paire HA, vos données sont toujours accessibles en cas de panne.

Par exemple, dans un cluster à quatre nœuds avec un volume racine sur trois nœuds :

- Pour le volume racine sur HA 1 nœud 1, créez le LSM sur HA 2 nœud 1 ou HA 2 nœud 2.
- Pour le volume racine sur HA 1 nœud 2, créez le LSM sur HA 2 nœud 1 ou HA 2 nœud 2.
- Pour le volume racine sur HA 2 nœud 1, créez le LSM sur HA 1 nœud 1 ou HA 1 nœud 2.

#### Étapes

1. Créer un volume de destination pour le LSM :

```
volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
-type DP -size <size>
```

La taille du volume de destination doit être identique ou supérieure à celle du volume racine.

Il est recommandé de nommer le volume racine et le volume de destination avec des suffixes, par exemple `_root` et `_m1`.

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création d'un volume miroir de partage de charge pour le volume racine `svm1_root` dans `cluster_src`:

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. "Créez un planning de travaux de réplication".
3. Créer une relation de miroir de partage de charge entre le volume root du SVM et le volume de destination pour le LSM :

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type LS -schedule <schedule>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant crée une relation de miroir de partage de charge entre le volume racine `svm1_root` et le volume du miroir de partage de charge `svm1_m1`:

```
cluster_src::> snapmirror create -source-path svm1:svm1_root
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

L'attribut type du miroir de partage de charge passe de DP à LS.

4. Initialiser le miroir de partage de charge :

```
snapmirror initialize-ls-set -source-path <SVM:volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant initialise le miroir de partage de charge pour le volume racine `svm1_root`:

```
cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
```

## Mettre à jour une relation de miroir de partage de charge

Les relations LSM (Load-sharing mirror) sont mises à jour automatiquement pour les volumes root du SVM après le montage ou le montage d'un volume du SVM et pendant volume create opérations qui incluent l'option `junction-path`. Vous pouvez mettre à jour manuellement une relation LSM si vous souhaitez la mettre à jour avant la prochaine mise à jour planifiée.

Les relations miroir de partage de charge sont mises à jour automatiquement dans les cas suivants :

- Il est temps d'effectuer une mise à jour planifiée
- Une opération de montage ou de démontage est effectuée sur un volume dans le volume root du SVM
- A volume create la commande a été émise qui inclut le junction-path option

### Étape

1. Mettre à jour manuellement une relation de miroir de partage de charge :

Vous devez remplacer les variables entre parenthèses angulaires par les valeurs requises avant d'exécuter cette commande.

```
snapmirror update-ls-set -source-path <SVM:volume>
```

L'exemple suivant met à jour la relation entre miroir de partage de charge pour le volume racine svm1\_root:

```
cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
```

## Promotion d'un miroir de partage de charge

Si un volume racine est définitivement indisponible, vous pouvez promouvoir le volume LSM (Load-sharing mirror) pour fournir un accès en écriture aux données du volume racine.

### Ce dont vous avez besoin

Vous devez utiliser des commandes de niveau de privilège avancé pour cette tâche.

### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Promouvoir un volume LSM :

Vous devez remplacer les variables entre parenthèses angulaires par les valeurs requises avant d'exécuter cette commande.



```
snapmirror promote -destination-path <SVM:volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant promeut le volume `svm1_m2` En tant que nouveau volume root SVM :

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
cluster_src://svm1/svm1_root and replace it with
cluster_src://svm1/svm1_m2. Because the volume is offline,
it is not possible to determine whether this promote will
affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

Entrez `y`. ONTAP fait du volume LSM un volume en lecture/écriture et supprime le volume racine d'origine s'il est accessible.



Le volume racine promu peut ne pas avoir toutes les données contenues dans le volume racine d'origine si la dernière mise à jour n'a pas eu lieu récemment.

### 3. Retour au niveau de privilège admin :

```
set -privilege admin
```

### 4. Renommez le volume promu en respectant la convention de nommage utilisée pour le volume racine :

Vous devez remplacer les variables entre parenthèses angulaires par les valeurs requises avant d'exécuter cette commande.

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

L'exemple suivant renomme le volume promu `svm1_m2` avec le nom `svm1_root`:

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

### 5. Protégez le volume racine renommé, comme décrit aux étapes 3 à 4 de la section "[Création et initialisation de relations de miroir de partage de charge](#)".

# Sauvegarder dans le cloud

## Sauvegardez les données dans le cloud avec SnapMirror

Depuis ONTAP 9.9.1, vous pouvez sauvegarder vos données dans le cloud et les restaurer à partir du stockage cloud vers un autre volume à l'aide de System Manager. Vous pouvez utiliser StorageGRID ou ONTAP S3 en tant que magasin d'objets cloud.

Avant d'utiliser la fonctionnalité cloud SnapMirror, vous devez demander une clé de licence d'API cloud SnapMirror sur le site de support NetApp : "[Demandez la clé de licence de l'API cloud SnapMirror](#)". En suivant les instructions, vous devez fournir une description simple de votre opportunité commerciale et demander la clé API en envoyant un e-mail à l'adresse e-mail fournie. Vous devriez recevoir une réponse par e-mail dans les 24 heures avec des instructions supplémentaires sur l'acquisition de la clé API.

### Ajouter un magasin d'objets cloud

Avant de configurer les sauvegardes cloud SnapMirror, vous devez ajouter un magasin d'objets cloud StorageGRID ou ONTAP S3.

#### Étapes

1. Cliquez sur **protection > Présentation > magasins d'objets cloud**.
2. Cliquez sur **+ Add**.

### Sauvegardez à l'aide de la règle par défaut

Vous pouvez rapidement configurer une sauvegarde cloud SnapMirror pour un volume existant à l'aide de la règle de protection cloud par défaut, DailyBackup.

#### Étapes

1. Cliquez sur **protection > Présentation** et sélectionnez **Sauvegarder les volumes dans le cloud**.
2. Si vous effectuez la première sauvegarde vers le cloud, saisissez votre clé de licence d'API cloud SnapMirror dans le champ de licence, comme indiqué.
3. Cliquez sur **authentifier et continuer**.
4. Sélectionnez un volume source.
5. Sélectionnez un magasin d'objets cloud.
6. Cliquez sur **Enregistrer**.

### Création d'une politique de sauvegarde cloud personnalisée

Si vous ne souhaitez pas utiliser la stratégie cloud DailyBackup par défaut pour vos sauvegardes cloud SnapMirror, vous pouvez créer votre propre stratégie.

#### Étapes

1. Cliquez sur **protection > Présentation > Paramètres de stratégie locale** et sélectionnez **stratégies de protection**.
2. Cliquez sur **Ajouter** et entrez les détails de la nouvelle stratégie.
3. Dans la section **Policy Type**, sélectionnez **Sauvegarder dans le cloud** pour indiquer que vous créez une stratégie de cloud.

4. Cliquez sur **Enregistrer**.

## Créez une sauvegarde à partir de la page volumes

Vous pouvez utiliser la page System Manager **volumes** pour sélectionner et créer des sauvegardes de cloud pour plusieurs volumes à la fois ou lorsque vous souhaitez utiliser une règle de protection personnalisée.

### Étapes

1. Cliquez sur **Storage > volumes**.
2. Sélectionnez les volumes que vous souhaitez sauvegarder dans le nuage, puis cliquez sur **Protect**.
3. Dans la fenêtre **Protect Volume**, cliquez sur **plus d'options**.
4. Sélectionnez une stratégie.


Vous pouvez sélectionner la stratégie par défaut, DailyBackup ou une stratégie cloud personnalisée que vous avez créée.

5. Sélectionnez un magasin d'objets cloud.
6. Cliquez sur **Enregistrer**.

## Restaurez vos données à partir du cloud

System Manager permet de restaurer les données sauvegardées depuis le stockage cloud vers un autre volume du cluster source.


### Étapes

1. Dans le cluster source d'une relation SnapMirror-to-Cloud, cliquez sur **stockage > volumes**.
2. Sélectionnez le volume à restaurer.
3. Sélectionnez l'onglet **Sauvegarder dans le Cloud**.
4. Cliquez sur  en regard du volume source que vous souhaitez restaurer pour afficher le menu, puis sélectionnez **Restaurer**.
5. Sous **Source**, sélectionnez une VM de stockage, puis entrez le nom du volume sur lequel vous souhaitez restaurer les données.
6. Sous **destination**, sélectionnez la copie Snapshot à restaurer.
7. Cliquez sur **Enregistrer**.

## Supprimez une relation cloud SnapMirror

Vous pouvez utiliser System Manager pour supprimer une relation cloud.


### Étapes

1. Cliquez sur **Storage > volumes** et sélectionnez le volume à supprimer.
2. Cliquez sur  en regard du volume source et sélectionnez **Supprimer**.
3. Sélectionnez **Supprimer le noeud final du magasin d'objets Cloud (facultatif)** si vous souhaitez supprimer le noeud final du magasin d'objets Cloud.
4. Cliquez sur **Supprimer**.

## Supprime un magasin d'objets cloud

Vous pouvez utiliser System Manager pour supprimer un magasin d'objets cloud s'il ne fait pas partie d'une relation de sauvegarde dans le cloud. Lorsqu'un magasin d'objets cloud fait partie d'une relation de sauvegarde dans le cloud, il ne peut pas être supprimé.

### Étapes

1. Cliquez sur **protection > Présentation > magasins d'objets cloud**.
2. Sélectionnez le magasin d'objets à supprimer, cliquez sur  et sélectionnez **Supprimer**.

## Sauvegardez les données à l'aide de Cloud Backup

Depuis ONTAP 9.9.1, vous pouvez utiliser System Manager pour sauvegarder les données dans le cloud à l'aide de Cloud Backup.



Cloud Backup prend en charge les volumes FlexVol de lecture-écriture et de protection des données (DP). Les volumes FlexGroup et SnapLock ne sont pas pris en charge.

### Avant de commencer

Pour créer un compte dans BlueXP, vous devez effectuer les procédures suivantes. Pour le compte de service, vous devez créer le rôle « Administrateur de compte ». (Les autres rôles de compte de service ne disposent pas des privilèges requis pour établir une connexion à partir de System Manager.)

1. "[Créez un compte dans BlueXP](#)".
2. "[Créez un connecteur dans BlueXP](#)" avec l'un des nombreux fournisseurs de cloud suivants :
  - Microsoft Azure
  - Services Web Amazon (AWS)
  - Google Cloud Platform (GCP)
  - StorageGRID (ONTAP 9.10.1)



Depuis ONTAP 9.10.1, vous pouvez sélectionner StorageGRID comme fournisseur de sauvegarde cloud, mais uniquement si BlueXP est déployé sur site. Le connecteur BlueXP doit être installé sur site et disponible via l'application BlueXP Software-as-a-service (SaaS).

3. "[Abonnez-vous à Cloud Backup Service dans BlueXP](#)" (nécessite la licence appropriée).
4. "[Générez une clé d'accès et une clé secrète à l'aide de BlueXP](#)".

## Enregistrez le cluster avec BlueXP

Vous pouvez enregistrer le cluster avec BlueXP en utilisant BlueXP ou System Manager.

### Étapes

1. Dans System Manager, accédez à **Présentation de la protection**.
2. Sous **Cloud Backup Service**, fournissez les détails suivants :
  - ID client
  - Clé secrète du client

3. Sélectionnez **Enregistrer et continuer**.

## Activation de Cloud Backup

Une fois le cluster enregistré auprès de BlueXP, vous devez activer Cloud Backup et lancer la première sauvegarde dans le cloud.

### Étapes

1. Dans System Manager, cliquez sur **protection > Présentation**, puis faites défiler jusqu'à la section **Cloud Backup Service**.
2. Saisissez **ID client** et **secret client**.



Depuis ONTAP 9.10.1, vous pouvez en savoir plus sur le coût d'utilisation du cloud en cliquant sur **en savoir plus sur le coût d'utilisation du cloud**.

3. Cliquez sur **connexion et activez Cloud Backup Service**.
4. Sur la page **Activer Cloud Backup Service**, indiquez les détails suivants, en fonction du fournisseur que vous avez sélectionné.

| Pour ce fournisseur de cloud...                                                                          | Entrez les données suivantes...                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Azure                                                                                                    | <ul style="list-style-type: none"><li>• ID d'abonnement Azure</li><li>• Région</li><li>• Nom du groupe de ressources (existant ou nouveau)</li></ul>               |
| AWS                                                                                                      | <ul style="list-style-type: none"><li>• ID de compte AWS</li><li>• Touche d'accès</li><li>• Clé secrète</li><li>• Région</li></ul>                                 |
| Projet Google Cloud (GCP)                                                                                | <ul style="list-style-type: none"><li>• Nom du projet Google Cloud</li><li>• Clé Google Cloud Access</li><li>• Clé secrète Google Cloud</li><li>• Région</li></ul> |
| StorageGRID<br>(ONTAP 9.10.1 et versions ultérieures, pour le déploiement sur site de BlueXP uniquement) | <ul style="list-style-type: none"><li>• Serveur</li><li>• Clé d'accès SG</li><li>• Clé secrète SG</li></ul>                                                        |

5. Sélectionnez une **stratégie de protection** :
  - **Politique existante** : choisir une politique existante.
  - **Nouvelle stratégie** : spécifiez un nom et définissez un calendrier de transfert.



Depuis ONTAP 9.10.1, vous pouvez indiquer si vous souhaitez activer l'archivage avec Azure ou AWS.



Si vous activez l'archivage pour un volume avec Azure ou AWS, vous ne pouvez pas désactiver l'archivage.

Si vous activez l'archivage pour Azure ou AWS, spécifiez les éléments suivants :

- Nombre de jours après lequel le volume est archivé.
- Nombre de sauvegardes à conserver dans l'archive. Spécifiez "0" (zéro) pour archiver jusqu'à la dernière sauvegarde.
- Pour AWS, sélectionnez la classe de stockage d'archivage.

6. Sélectionnez les volumes à sauvegarder.

7. Sélectionnez **Enregistrer**.

## Modifiez la règle de protection utilisée pour Cloud Backup

Vous pouvez modifier la règle de protection utilisée avec Cloud Backup.

### Étapes

1. Dans System Manager, cliquez sur **protection > Présentation**, puis faites défiler jusqu'à la section **Cloud Backup Service**.
2. Cliquez sur , puis sur **Modifier**.
3. Sélectionnez une **stratégie de protection** :
  - **Politique existante** : choisir une politique existante.
  - **Nouvelle stratégie** : spécifiez un nom et définissez un calendrier de transfert.



Depuis ONTAP 9.10.1, vous pouvez indiquer si vous souhaitez activer l'archivage avec Azure ou AWS.



Si vous activez l'archivage pour un volume avec Azure ou AWS, vous ne pouvez pas désactiver l'archivage.

Si vous activez l'archivage pour Azure ou AWS, spécifiez les éléments suivants :

- Nombre de jours après lequel le volume est archivé.
- Nombre de sauvegardes à conserver dans l'archive. Spécifiez "0" (zéro) pour archiver jusqu'à la dernière sauvegarde.
- Pour AWS, sélectionnez la classe de stockage d'archivage.

4. Sélectionnez **Enregistrer**.

## Protection de nouveaux volumes ou LUN sur le cloud

Lorsque vous créez un nouveau volume ou une LUN, vous pouvez établir une relation de protection SnapMirror qui permet de sauvegarder les données dans le cloud pour le volume ou la LUN.

### Avant de commencer

- Vous devez disposer d'une licence SnapMirror.
- Les LIFs intercluster doivent être configurées.
- NTP doit être configuré.
- Le cluster doit exécuter ONTAP 9.9.1.

### Description de la tâche

Vous ne pouvez pas protéger de nouveaux volumes ou de nouvelles LUN dans le cloud pour les configurations de cluster suivantes :

- Le cluster ne peut pas se trouver dans un environnement MetroCluster.
- SVM-DR n'est pas pris en charge.
- Impossible de sauvegarder FlexGroups à l'aide de Cloud Backup.

### Étapes

1. Lors du provisionnement d'un volume ou d'une LUN, sur la page **protection** dans System Manager, cochez la case **Activer SnapMirror (local ou distant)**.
2. Sélectionnez le type de stratégie Cloud Backup.
3. Si la sauvegarde dans le cloud n'est pas activée, sélectionnez **Activer Cloud Backup Service**.

### Protection des volumes ou des LUN existants sur le cloud

Vous pouvez établir une relation de protection SnapMirror pour les volumes et les LUN existants.

### Étapes

1. Sélectionnez un volume ou une LUN existant, puis cliquez sur **Protect**.
2. Sur la page **Protect volumes**, spécifiez **Backup utilisant Cloud Backup Service** pour la stratégie de protection.
3. Cliquez sur **protéger**.
4. Sur la page **protection**, cochez la case **Activer SnapMirror (local ou distant)**.
5. Sélectionnez **Activer Cloud Backup Service**.

### Restaurez les données à partir des fichiers de sauvegarde

Vous pouvez effectuer des opérations de gestion de sauvegarde, telles que la restauration de données, la mise à jour de relations et la suppression de relations, uniquement lorsque vous utilisez l'interface BlueXP. Reportez-vous à la section ["Restauration des données à partir des fichiers de sauvegarde"](#) pour en savoir plus.

## Détails techniques de SnapMirror

### Utiliser la correspondance de motif de nom de chemin d'accès

Vous pouvez utiliser la correspondance de motif pour spécifier les chemins source et de destination dans `snapmirror` commandes.

`snapmirror` les commandes utilisent des noms de chemin complets au format suivant : `vserver:volume`. Vous pouvez abréger le nom du chemin en n'entrant pas le nom de la SVM. Si vous le faites, le `snapmirror` Commande suppose le contexte SVM local de l'utilisateur.

En supposant que la SVM est appelée « vserver1 » et que le volume est appelé « vol1 », le chemin d'accès complet est `vserver1:vol1`.

Vous pouvez utiliser l'astérisque (\*) dans les chemins comme caractère générique pour sélectionner des noms de chemin complets et correspondants. Le tableau suivant fournit des exemples d'utilisation du caractère générique pour sélectionner une plage de volumes.

|                    |                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------|
| <code>*</code>     | Correspond à tous les chemins.                                                                  |
| <code>vs*</code>   | Correspondance de tous les SVM et volumes avec des noms de SVM commençant par <code>vs</code> . |
| <code>:*src</code> | Correspond à tous les SVM avec des noms de volume contenant le <code>src</code> texte.          |
| <code>:vol</code>  | Correspond à tous les SVM avec des noms de volume commençant par <code>vol</code> .             |

```
vs1::> snapmirror show -destination-path *:*dest*
```

Progress

| Source  | Destination | Mirror | Relationship | Total  |          |
|---------|-------------|--------|--------------|--------|----------|
| Last    |             |        |              |        |          |
| Path    | Type        | Path   | State        | Status | Progress |
| Healthy | Updated     |        |              |        |          |

vs1:sm\_src2

DP vs2:sm\_dest1

Snapmirrored Idle

true -

## Utilisez des requêtes étendues pour agir sur de nombreuses relations SnapMirror

Vous pouvez utiliser *requêtes étendues* pour effectuer des opérations SnapMirror simultanément sur de nombreuses relations SnapMirror. Par exemple, vous pouvez avoir plusieurs relations SnapMirror non initialisées que vous souhaitez initialiser à l'aide d'une commande.



## Description de la tâche

Vous pouvez appliquer des requêtes étendues aux opérations SnapMirror suivantes :

- Initialisation des relations non initialisées
- Reprise des relations suspendues
- Resynchronisation des relations interrompues
- Mise à jour des relations inactives
- Abandon des transferts de données de relation

## Étape

1. Effectuer une opération SnapMirror sur de nombreuses relations :

```
snapmirror command {-state state } *
```

La commande suivante initialise les relations SnapMirror qui se trouvent dans un Uninitialized état :

```
vs1::> snapmirror initialize {-state Uninitialized} *
```

## Garantir une copie Snapshot commune dans un déploiement de copie en miroir

Vous pouvez utiliser le `snapmirror snapshot-owner create` Commande permettant de conserver une copie Snapshot étiquetée sur le système secondaire dans un déploiement mis en miroir-vault. Cela garantit qu'il existe une copie Snapshot commune pour la mise à jour de la relation de coffre-fort.

## Description de la tâche

Si vous utilisez une combinaison de mirror-vault Fan-Out ou de cascade, sachez que les mises à jour échoueront si une copie Snapshot commune n'existe pas sur les volumes source et de destination.

Ce problème ne se pose jamais pour la relation de miroir dans un déploiement de type « fan-out » (fan-out) à base de miroir ou en cascade, car SnapMirror crée toujours une copie Snapshot du volume source avant d'effectuer la mise à jour.

Il peut en revanche s'agir d'un problème pour la relation de copie à distance, puisque SnapMirror ne crée pas de copie Snapshot du volume source lors de la mise à jour d'une relation de copie à distance. Vous devez utiliser le `snapmirror snapshot-owner create` Pour s'assurer qu'il existe au moins une copie Snapshot commune à la fois sur la source et la destination de la relation de coffre-fort.

## Étapes

1. Sur le volume source, attribuez un propriétaire à la copie Snapshot nommée que vous souhaitez conserver :

```
snapmirror snapshot-owner create -vserver <SVM> -volume <volume> -snapshot
<snapshot> -owner <owner>
```

L'exemple suivant affecte ApplicationA en tant que propriétaire du snap1 Copie Snapshot :

```
clust1::> snapmirror snapshot-owner create -vserver vs1 -volume voll
-snapshot snap1 -owner ApplicationA
```

2. Mettez à jour la relation de miroir, comme décrit dans ["Mise à jour manuelle d'une relation de réplication"](#).

Vous pouvez également attendre la mise à jour planifiée de la relation miroir.

3. Transférer la copie Snapshot étiquetée vers la destination du coffre-fort :

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -source-snapshot
snapshot
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).

#### L'exemple suivant transfère le **snap1** La copie Snapshot

```
clust1::> snapmirror update -vserver vs1 -volume voll
-source-snapshot snap1
```

La copie Snapshot nommée sera conservée lors de la mise à jour de la relation de coffre-fort.

4. Sur le volume source, supprimez le propriétaire de la copie Snapshot nommée :

```
snapmirror snapshot-owner delete -vserver SVM -volume volume -snapshot
snapshot -owner owner
```

Les exemples suivants sont supprimés **ApplicationA** en tant que propriétaire du **snap1** Copie Snapshot :

```
clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume voll
-snapshot snap1 -owner ApplicationA
```

## Compatibilité des versions ONTAP pour les relations SnapMirror

Les volumes source et destination doivent exécuter des versions ONTAP compatibles avant de créer une relation de protection des données SnapMirror. Avant de mettre à niveau ONTAP, vérifiez que votre version actuelle de ONTAP est compatible avec votre version cible de ONTAP pour les relations SnapMirror.

### Relations de réplication unifiée

Pour les relations SnapMirror de type « XDP », utilisant des versions sur site ou Cloud Volumes ONTAP.

Depuis ONTAP 9.9 :



- Les versions ONTAP 9.x.0 sont des versions cloud uniquement et prennent en charge les systèmes Cloud Volumes ONTAP. L'astérisque (\*) après la version de la version indique une version en nuage uniquement.
- Les versions ONTAP 9.x.1 sont des versions générales qui prennent en charge à la fois les systèmes sur site et les systèmes Cloud Volumes ONTAP.



L'interopérabilité est bidirectionnelle.

## Interopérabilité pour ONTAP version 9.3 et ultérieure

| Ver<br>sion<br>ON<br>TA<br>P... | Interopérabilité avec ces versions précédentes de ONTAP... |             |            |             |            |             |            |             |            |             |            |             |           |            |     |     |     |     |     |     |
|---------------------------------|------------------------------------------------------------|-------------|------------|-------------|------------|-------------|------------|-------------|------------|-------------|------------|-------------|-----------|------------|-----|-----|-----|-----|-----|-----|
|                                 | 9.1<br>5.1                                                 | 9.1<br>5.0* | 9.1<br>4.1 | 9.1<br>4.0* | 9.1<br>3.1 | 9.1<br>3.0* | 9.1<br>2.1 | 9.1<br>2.0* | 9.1<br>1.1 | 9.1<br>1.0* | 9.1<br>0.1 | 9.1<br>0.0* | 9.9.<br>1 | 9.9.<br>0* | 9.8 | 9.7 | 9.6 | 9.5 | 9.4 | 9.3 |
| 9.1<br>5.1                      | Oui                                                        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui       | Non        | Non | Non | Non | Non | Non | Non |
| 9.1<br>5.0*                     | Oui                                                        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui       | Non        | Non | Non | Non | Non | Non | Non |
| 9.1<br>4.1                      | Oui                                                        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui       | Oui        | Non | Non | Non | Non | Non | Non |
| 9.1<br>4.0*                     | Oui                                                        | Oui         | Oui        | Oui         | Oui        | Non         | Oui        | Non         | Oui        | Non         | Oui        | Non         | Oui       | Non        | Non | Non | Non | Non | Non | Non |
| 9.1<br>3.1                      | Oui                                                        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui       | Oui        | Oui | Non | Non | Non | Non | Non |
| 9.1<br>3.0*                     | Oui                                                        | Oui         | Oui        | Non         | Oui        | Oui         | Oui        | Non         | Oui        | Non         | Oui        | Non         | Oui       | Non        | Oui | Non | Non | Non | Non | Non |
| 9.1<br>2.1                      | Oui                                                        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui       | Oui        | Oui | Oui | Oui | Non | Non | Non |
| 9.1<br>2.0*                     | Oui                                                        | Oui         | Oui        | Non         | Oui        | Non         | Oui        | Oui         | Oui        | Non         | Oui        | Non         | Oui       | Non        | Oui | Oui | Non | Non | Non | Non |
| 9.1<br>1.1                      | Oui                                                        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui       | Oui        | Oui | Oui | Oui | Oui | Non | Non |
| 9.1<br>1.0*                     | Oui                                                        | Oui         | Oui        | Non         | Oui        | Non         | Oui        | Non         | Oui        | Oui         | Oui        | Non         | Oui       | Non        | Oui | Oui | Oui | Oui | Non | Non |
| 9.1<br>0.1                      | Oui                                                        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui        | Oui         | Oui       | Oui        | Oui | Oui | Oui | Oui | Oui | Non |
| 9.1<br>0.0*                     | Oui                                                        | Oui         | Oui        | Non         | Oui        | Non         | Oui        | Non         | Oui        | Non         | Oui        | Oui         | Oui       | Non        | Oui | Oui | Oui | Oui | Non | Non |

|        |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
|--------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 9.9.1  | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Non | Non |
| 9.9.0* | Non | Non | Oui | Non | Oui | Non | Oui | Non | Oui | Non | Oui | Non | Oui | Oui | Oui | Oui | Oui | Oui | Non | Non |
| 9.8    | Non | Non | Non | Non | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Non | Oui |
| 9.7    | Non | Non | Non | Non | Non | Non | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Non | Oui |
| 9.6    | Non | Non | Non | Non | Non | Non | Non | Non | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Non | Oui |
| 9.5    | Non | Non | Non | Non | Non | Non | Non | Non | Non | Non | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| 9.4    | Non | Non | Non | Non | Non | Non | Non | Non | Non | Non | Non | Non | Non | Non | Non | Non | Non | Oui | Oui | Oui |
| 9.3    | Non | Non | Non | Non | Non | Non | Non | Non | Non | Non | Non | Non | Non | Non | Oui | Oui | Oui | Oui | Oui | Oui |

## Relations synchrones SnapMirror



SnapMirror synchrone n'est pas pris en charge par les instances de cloud ONTAP.

| Version ONTAP ... | Interopérabilité avec ces versions précédentes de ONTAP... |        |        |        |        |        |       |     |     |     |     |
|-------------------|------------------------------------------------------------|--------|--------|--------|--------|--------|-------|-----|-----|-----|-----|
|                   | 9.15.1                                                     | 9.14.1 | 9.13.1 | 9.12.1 | 9.11.1 | 9.10.1 | 9.9.1 | 9.8 | 9.7 | 9.6 | 9.5 |
| 9.15.1            | Oui                                                        | Oui    | Oui    | Oui    | Oui    | Oui    | Non   | Non | Non | Non | Non |
| 9.14.1            | Oui                                                        | Oui    | Oui    | Oui    | Oui    | Oui    | Oui   | Oui | Non | Non | Non |
| 9.13.1            | Oui                                                        | Oui    | Oui    | Oui    | Oui    | Oui    | Oui   | Oui | Oui | Non | Non |
| 9.12.1            | Oui                                                        | Oui    | Oui    | Oui    | Oui    | Oui    | Oui   | Oui | Oui | Non | Non |
| 9.11.1            | Oui                                                        | Oui    | Oui    | Oui    | Oui    | Oui    | Oui   | Non | Non | Non | Non |
| 9.10.1            | Oui                                                        | Oui    | Oui    | Oui    | Oui    | Oui    | Oui   | Oui | Non | Non | Non |
| 9.9.1             | Non                                                        | Oui    | Oui    | Oui    | Oui    | Oui    | Oui   | Oui | Oui | Non | Non |
| 9.8               | Non                                                        | Oui    | Oui    | Oui    | Non    | Oui    | Oui   | Oui | Oui | Oui | Non |
| 9.7               | Non                                                        | Non    | Oui    | Oui    | Non    | Non    | Oui   | Oui | Oui | Oui | Oui |
| 9.6               | Non                                                        | Non    | Non    | Non    | Non    | Non    | Non   | Oui | Oui | Oui | Oui |
| 9.5               | Non                                                        | Non    | Non    | Non    | Non    | Non    | Non   | Non | Oui | Oui | Oui |

## Relations de reprise d'activité SVM SnapMirror

### Pour les données de reprise d'activité SVM et la protection des SVM :

La reprise d'activité SVM n'est prise en charge qu'entre les clusters exécutant la même version d'ONTAP.

**L'indépendance de la version n'est pas prise en charge pour la réplication du SVM.**

### Pour la reprise d'activité de SVM pour la migration de SVM :

- La réplication est prise en charge dans une direction unique depuis une version antérieure de ONTAP sur la source vers la même version ou une version ultérieure de ONTAP sur la destination.

- La version ONTAP du cluster cible ne doit pas être plus récente que deux versions majeures sur site ou deux versions majeures de cloud plus récentes, comme illustré dans le tableau ci-dessous.
  - La réplication n'est pas prise en charge pour les cas d'usage de protection des données à long terme.

L'astérisque (\*) après la version de la version indique une version en nuage uniquement.

Pour déterminer la prise en charge, recherchez la version source dans la colonne de gauche du tableau, puis recherchez la version de destination sur la ligne supérieure (DR/migration pour les versions similaires et migration uniquement pour les versions plus récentes).

| Source | Destination                                              |                                                          |                                                          |                                                          |                   |                   |                   |                   |         |        |         |        |         |        |         |        |         |        |         |        |
|--------|----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|-------------------|-------------------|-------------------|-------------------|---------|--------|---------|--------|---------|--------|---------|--------|---------|--------|---------|--------|
|        | 9.3                                                      | 9.4                                                      | 9.5                                                      | 9.6                                                      | 9.7               | 9.8               | 9.9.0*            | 9.9.1             | 9.10.0* | 9.10.1 | 9.11.0* | 9.11.1 | 9.12.0* | 9.12.1 | 9.13.0* | 9.13.1 | 9.14.0* | 9.14.1 | 9.15.0* | 9.15.1 |
| 9.3    | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on |                   |                   |                   |         |        |         |        |         |        |         |        |         |        |         |        |
| 9.4    |                                                          | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on | Mig<br>rati<br>on |                   |                   |         |        |         |        |         |        |         |        |         |        |         |        |
| 9.5    |                                                          |                                                          | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on                                        | Mig<br>rati<br>on | Mig<br>rati<br>on | Mig<br>rati<br>on |                   |         |        |         |        |         |        |         |        |         |        |         |        |
| 9.6    |                                                          |                                                          |                                                          | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on | Mig<br>rati<br>on | Mig<br>rati<br>on | Mig<br>rati<br>on |         |        |         |        |         |        |         |        |         |        |         |        |

|             |  |  |  |  |                                                          |                                                          |                                                          |                                                          |                                                          |                                                          |                   |                   |                   |                   |  |  |  |  |  |
|-------------|--|--|--|--|----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|-------------------|-------------------|-------------------|-------------------|--|--|--|--|--|
| 9.7         |  |  |  |  | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        |                                                          |                   |                   |                   |                   |  |  |  |  |  |
| 9.8         |  |  |  |  |                                                          | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        |                   |                   |                   |                   |  |  |  |  |  |
| 9.9.<br>0*  |  |  |  |  |                                                          |                                                          | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on |                   |                   |                   |  |  |  |  |  |
| 9.9.<br>1   |  |  |  |  |                                                          |                                                          |                                                          | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on | Mig<br>rati<br>on |                   |                   |  |  |  |  |  |
| 9.1<br>0.0* |  |  |  |  |                                                          |                                                          |                                                          |                                                          | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on                                        | Mig<br>rati<br>on | Mig<br>rati<br>on | Mig<br>rati<br>on |                   |  |  |  |  |  |
| 9.1<br>0.1  |  |  |  |  |                                                          |                                                          |                                                          |                                                          |                                                          | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on | Mig<br>rati<br>on | Mig<br>rati<br>on | Mig<br>rati<br>on |  |  |  |  |  |

|             |  |  |  |  |  |  |  |  |  |                                                          |                                                          |                                                          |                                                          |                                                          |                   |                   |                   |                   |  |
|-------------|--|--|--|--|--|--|--|--|--|----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|-------------------|-------------------|-------------------|-------------------|--|
| 9.1<br>1.0* |  |  |  |  |  |  |  |  |  | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        |                   |                   |                   |                   |  |
| 9.1<br>1.1  |  |  |  |  |  |  |  |  |  | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        |                   |                   |                   |                   |  |
| 9.1<br>2.0* |  |  |  |  |  |  |  |  |  |                                                          | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on |                   |                   |                   |  |
| 9.1<br>2.1  |  |  |  |  |  |  |  |  |  |                                                          |                                                          | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on                                        | Mig<br>rati<br>on                                        | Mig<br>rati<br>on | Mig<br>rati<br>on |                   |                   |  |
| 9.1<br>3.0* |  |  |  |  |  |  |  |  |  |                                                          |                                                          |                                                          | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on                                        | Mig<br>rati<br>on | Mig<br>rati<br>on | Mig<br>rati<br>on |                   |  |
| 9.1<br>3.1  |  |  |  |  |  |  |  |  |  |                                                          |                                                          |                                                          |                                                          | Rep<br>rise<br>sur<br>inci<br>den<br>t/mi<br>grat<br>ion | Mig<br>rati<br>on | Mig<br>rati<br>on | Mig<br>rati<br>on | Mig<br>rati<br>on |  |

|             |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                |                                |           |                                |
|-------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--------------------------------|--------------------------------|-----------|--------------------------------|
| 9.1<br>4.0* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Reprise sur incident/migration | Migration                      | Migration | Migration                      |
| 9.1<br>4.1  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Reprise sur incident/migration | Migration                      | Migration |                                |
| 9.1<br>5.0* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                | Reprise sur incident/migration |           | Migration                      |
| 9.1<br>5.1  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                |                                |           | Reprise sur incident/migration |

## Relations de reprise sur incident SnapMirror

Pour les relations SnapMirror de type « DP » et de type de règle « asynchrone-mirror » :



Les miroirs de type DP ne peuvent pas être initialisés depuis ONTAP 9.11.1 et sont complètement obsolètes dans ONTAP 9.12.1. Pour plus d'informations, voir ["Dérecation des relations SnapMirror de protection des données"](#).



Dans le tableau suivant, la colonne de gauche indique la version ONTAP sur le volume source, et la ligne supérieure indique les versions ONTAP que vous pouvez avoir sur le volume de destination.

| Source | Destination |        |       |     |     |     |     |     |     |     |     |     |
|--------|-------------|--------|-------|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|        | 9.11.1      | 9.10.1 | 9.9.1 | 9.8 | 9.7 | 9.6 | 9.5 | 9.4 | 9.3 | 9.2 | 9.1 | 9   |
| 9.11.1 | Oui.        | Non    | Non   | Non | Non | Non | Non | Non | Non | Non | Non | Non |
| 9.10.1 | Oui.        | Oui.   | Non   | Non | Non | Non | Non | Non | Non | Non | Non | Non |



|       |      |      |      |      |      |      |      |      |      |      |      |      |
|-------|------|------|------|------|------|------|------|------|------|------|------|------|
| 9.9.1 | Oui. | Oui. | Oui. | Non  | Non  | Non  | Non  | Non  | Non  | Non  | Non  | Non  |
| 9.8   | Non  | Oui. | Oui. | Oui. | Non  | Non  | Non  | Non  | Non  | Non  | Non  | Non  |
| 9.7   | Non  | Non  | Oui. | Oui. | Oui. | Non  | Non  | Non  | Non  | Non  | Non  | Non  |
| 9.6   | Non  | Non  | Non  | Oui. | Oui. | Oui. | Non  | Non  | Non  | Non  | Non  | Non  |
| 9.5   | Non  | Non  | Non  | Non  | Oui. | Oui. | Oui. | Non  | Non  | Non  | Non  | Non  |
| 9.4   | Non  | Non  | Non  | Non  | Non  | Oui. | Oui. | Oui. | Non  | Non  | Non  | Non  |
| 9.3   | Non  | Non  | Non  | Non  | Non  | Non  | Oui. | Oui. | Oui. | Non  | Non  | Non  |
| 9.2   | Non  | Non  | Non  | Non  | Non  | Non  | Non  | Oui. | Oui. | Oui. | Non  | Non  |
| 9.1   | Non  | Non  | Non  | Non  | Non  | Non  | Non  | Non  | Oui. | Oui. | Oui. | Non  |
| 9     | Non  | Non  | Non  | Non  | Non  | Non  | Non  | Non  | Non  | Oui. | Oui. | Oui. |



L'interopérabilité n'est pas bidirectionnelle.

## SnapMirror limitations

Avant de créer une relation de protection des données, il est recommandé de connaître les limites élémentaires de SnapMirror.

- Un volume de destination ne peut avoir qu'un seul volume source.



Un volume source peut avoir plusieurs volumes de destination. Le volume de destination peut être le volume source pour tout type de relation de réplication SnapMirror.

- Selon le modèle de baie, vous pouvez ventiler jusqu'à huit ou seize volumes de destination à partir d'un seul volume source. Voir la "[Hardware Universe](#)" pour en savoir plus sur votre configuration spécifique.
- Vous ne pouvez pas restaurer de fichiers vers la destination d'une relation SnapMirror DR.
- Les volumes SnapVault source ou de destination ne peuvent pas être de 32 bits.
- Le volume source d'une relation SnapVault ne doit pas être un volume FlexClone.



La relation fonctionnera, mais l'efficacité offerte par les volumes FlexClone ne sera pas préservée.

## Archivage et conformité grâce à la technologie SnapLock

### Qu'est-ce que SnapLock

SnapLock est une solution de conformité hautes performances pour les entreprises qui utilisent le stockage WORM pour conserver les fichiers sous une forme non modifiée à des fins réglementaires et de gouvernance.

SnapLock empêche la suppression, la modification ou la modification des données pour répondre aux réglementations SEC 17a-4, HIPAA, FINRA, CFTC et le RGPD. SnapLock vous permet de créer des volumes spéciaux dans lesquels les fichiers peuvent être stockés et archivés dans un état non effaçable et non

inscriptible pour une période de conservation définie ou indéfiniment. SnapLock permet cette conservation au niveau fichier via des protocoles de fichiers ouverts standard tels que CIFS et NFS. Les protocoles de fichier ouvert pris en charge pour SnapLock sont les suivants : NFS (versions 2, 3 et 4) et CIFS (SMB 1.0, 2.0 et 3.0).

Avec SnapLock, vous archivez des fichiers et des copies Snapshot sur le stockage WORM et définissez des périodes de conservation pour les données protégées WORM. Le stockage WORM SnapLock utilise la technologie NetApp Snapshot et peut exploiter la réplication SnapMirror ainsi que les sauvegardes SnapVault comme technologie de base pour offrir une protection des données de restauration de sauvegarde.

En savoir plus sur le stockage WORM : ["Conformité du stockage WORM avec NetApp SnapLock - TR-4526"](#).

Vous pouvez utiliser une application pour valider les fichiers en mode WORM sur NFS ou CIFS, ou utiliser la fonctionnalité d'autovalidation de SnapLock pour allouer automatiquement les fichiers en mode WORM. Vous pouvez utiliser un fichier *WORM applicable* pour conserver les données écrites de manière incrémentielle, comme les informations de journal. Pour plus d'informations, voir ["Utilisez le mode d'ajout de volumes pour créer des fichiers d'ajout WORM"](#).

SnapLock prend en charge les méthodes de protection des données qui doivent répondre à la plupart des exigences de conformité :

- Vous pouvez utiliser SnapLock pour SnapVault pour protéger les copies Snapshot WORM sur le stockage secondaire. Voir ["Archivage des copies Snapshot en mode WORM"](#).
- Vous pouvez utiliser SnapMirror pour répliquer des fichiers WORM dans un autre emplacement géographique à des fins de reprise après incident. Voir ["Fichiers WORM en miroir"](#).

SnapLock est une fonctionnalité sous licence de NetApp ONTAP. Une seule licence vous donne le droit d'utiliser SnapLock en mode strict conformité, afin de répondre aux exigences externes telles que la règle SEC 17a-4 et un mode perte de l'entreprise, afin de respecter les réglementations internes régissant la protection des ressources numériques. Les licences SnapLock font partie du ["ONTAP One"](#) suite logicielle.

SnapLock est pris en charge sur tous les systèmes AFF, FAS et ONTAP Select. SnapLock n'est pas une solution exclusivement logicielle ; il s'agit d'une solution matérielle et logicielle intégrée. Cette distinction est importante pour les réglementations WORM strictes, telles que la norme SEC 17a-4, qui requièrent une solution matérielle et logicielle intégrée. Pour plus d'informations, reportez-vous à la section ["SEC interprétation : stockage électronique des dossiers des courtiers-concessionnaires"](#).

## Les avantages de SnapLock

Une fois SnapLock configuré, vous pouvez effectuer les tâches suivantes :

- ["Archivage des fichiers en mode WORM"](#)
- ["Archivage des copies Snapshot sur le stockage WORM pour le stockage secondaire"](#)
- ["Mise en miroir des fichiers WORM pour la reprise après incident"](#)
- ["Conservation des fichiers WORM en cas de litiges avec la conservation légale"](#)
- ["Supprimez des fichiers WORM à l'aide de la fonction de suppression privilégiée"](#)
- ["Définissez la période de rétention des fichiers"](#)
- ["Déplacer un volume SnapLock"](#)
- ["Verrouiller une copie Snapshot pour assurer la protection contre les attaques par ransomware"](#)
- ["Vérifiez l'utilisation de SnapLock avec le journal d'audit"](#)
- ["Utilisez les API SnapLock"](#)

## SnapLock Compliance et Enterprise modes

Les modes SnapLock Compliance et Enterprise diffèrent principalement du niveau auquel chaque mode protège les fichiers WORM :

| Mode SnapLock      | Niveau de protection | Suppression du fichier WORM pendant la conservation                                                                |
|--------------------|----------------------|--------------------------------------------------------------------------------------------------------------------|
| Mode de conformité | Au niveau du disque  | Ne peut pas être supprimé                                                                                          |
| Mode entreprise    | Au niveau fichier    | Peut être supprimé par l'administrateur de conformité à l'aide d'une procédure audité de "suppression privilégiée" |

Une fois la période de rétention écoulée, vous êtes responsable de la suppression des fichiers dont vous n'avez plus besoin. Une fois qu'un fichier a été engagé en mode WORM, qu'il soit en mode conformité ou entreprise, il ne peut pas être modifié, même après l'expiration de la période de conservation.

Vous ne pouvez pas déplacer un fichier WORM pendant ou après la période de conservation. Vous pouvez copier un fichier WORM, mais la copie ne conserve pas ses caractéristiques WORM.

Le tableau suivant présente les différences de capacités prises en charge par les modes SnapLock Compliance et Enterprise :

| Fonctionnalité                                                                      | Conformité SnapLock | SnapLock Enterprise                                         |
|-------------------------------------------------------------------------------------|---------------------|-------------------------------------------------------------|
| Activer et supprimer des fichiers à l'aide de la suppression privilégiée            | Non                 | Oui.                                                        |
| Réinitialiser les disques                                                           | Non                 | Oui.                                                        |
| Destruction des agrégats et des volumes SnapLock pendant la période de conservation | Non                 | Oui, à l'exception du volume du journal d'audit de SnapLock |
| Renommer les agrégats ou les volumes                                                | Non                 | Oui.                                                        |
| Utiliser des disques non NetApp                                                     | Non                 | Oui (avec "Virtualisation FlexArray")                       |
| Utilisation du volume SnapLock pour la journalisation des audits                    | Oui.                | Oui, à partir de ONTAP 9.5                                  |

## Fonctionnalités prises en charge et non prises en charge avec SnapLock

Le tableau suivant présente les fonctionnalités prises en charge avec le mode SnapLock Compliance, le mode SnapLock Enterprise ou les deux :

| Fonction                             | Prise en charge par SnapLock Compliance                                                                      | Pris en charge par SnapLock Enterprise                                                                           |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Groupes de cohérence                 | Non                                                                                                          | Non                                                                                                              |
| Volumes chiffrés                     | Oui, à partir de ONTAP 9.2. En savoir plus sur <a href="#">Cryptage et SnapLock</a> .                        | Oui, à partir de ONTAP 9.2. En savoir plus sur <a href="#">Cryptage et SnapLock</a> .                            |
| FabricPool sur les agrégats SnapLock | Non                                                                                                          | Oui, à partir de ONTAP 9.8. En savoir plus sur <a href="#">FabricPool sur les agrégats SnapLock Enterprise</a> . |
| Les agrégats Flash Pool              | Oui, à partir de ONTAP 9.1.                                                                                  | Oui, à partir de ONTAP 9.1.                                                                                      |
| FlexClone                            | Vous pouvez cloner des volumes SnapLock, mais vous ne pouvez pas cloner des fichiers sur un volume SnapLock. | Vous pouvez cloner des volumes SnapLock, mais vous ne pouvez pas cloner des fichiers sur un volume SnapLock.     |
| Volumes FlexGroup                    | Oui, à partir de ONTAP 9.11.1. En savoir plus sur <a href="#">[flexgroup]</a> .                              | Oui, à partir de ONTAP 9.11.1. En savoir plus sur <a href="#">[flexgroup]</a> .                                  |
| LUN                                  | Non En savoir plus sur <a href="#">Prise en charge LUN</a> Avec SnapLock.                                    | Non En savoir plus sur <a href="#">Prise en charge LUN</a> Avec SnapLock.                                        |
| Configurations MetroCluster          | Oui, à partir de ONTAP 9.3. En savoir plus sur <a href="#">Prise en charge de MetroCluster</a> .             | Oui, à partir de ONTAP 9.3. En savoir plus sur <a href="#">Prise en charge de MetroCluster</a> .                 |
| Vérification multiadministrateur     | Oui, à partir de ONTAP 9.13.1. En savoir plus sur <a href="#">Prise en charge MAV</a> .                      | Oui, à partir de ONTAP 9.13.1. En savoir plus sur <a href="#">Prise en charge MAV</a> .                          |
| SAN                                  | Non                                                                                                          | Non                                                                                                              |
| SnapRestore pour un seul fichier     | Non                                                                                                          | Oui.                                                                                                             |
| Synchronisation active SnapMirror    | Non                                                                                                          | Non                                                                                                              |
| SnapRestore                          | Non                                                                                                          | Oui.                                                                                                             |
| SMTape                               | Non                                                                                                          | Non                                                                                                              |
| SnapMirror synchrone                 | Non                                                                                                          | Non                                                                                                              |
| SSD                                  | Oui, à partir de ONTAP 9.1.                                                                                  | Oui, à partir de ONTAP 9.1.                                                                                      |

|                                          |                                                                                                           |                                                                                                           |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Fonctionnalités d'efficacité du stockage | Oui, depuis ONTAP 9.9.1. En savoir plus sur <a href="#">prise en charge de l'efficacité du stockage</a> . | Oui, depuis ONTAP 9.9.1. En savoir plus sur <a href="#">prise en charge de l'efficacité du stockage</a> . |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|

## FabricPool sur les agrégats SnapLock Enterprise

FabricPool est pris en charge sur les agrégats SnapLock Enterprise à partir de ONTAP 9.8. Toutefois, votre équipe de compte doit ouvrir une demande de modification des produits afin de documenter que les données FabricPool hiérarchisées vers un cloud public ou privé ne sont plus protégées par SnapLock, car les administrateurs cloud peuvent les supprimer.



Les données FabricPool placées dans un cloud public ou privé n'sont plus protégées par SnapLock, car les administrateurs cloud peuvent les supprimer.

## Volumes FlexGroup

SnapLock prend en charge les volumes FlexGroup depuis ONTAP 9.11.1, mais les fonctionnalités suivantes ne sont pas prises en charge :

- Obligation légale
- Conservation basée sur les événements
- SnapLock pour SnapVault (prise en charge à partir de ONTAP 9.12.1)

Vous devez également connaître les comportements suivants :

- L'horloge de conformité de volume (VCC) d'un volume FlexGroup est déterminée par le VCC du composant racine. Tous les composants non racines auront leur VCC étroitement synchronisé avec le VCC racine.
- Les propriétés de configuration de SnapLock sont définies uniquement sur la FlexGroup dans son ensemble. Les composants individuels ne peuvent pas avoir des propriétés de configuration différentes, telles que le temps de rétention par défaut et la période de validation automatique.

## Prise en charge LUN

Les LUN ne sont prises en charge dans les volumes SnapLock que dans les cas où les copies Snapshot créées sur un volume non SnapLock sont transférées vers un volume SnapLock pour être protégées dans le cadre de la relation de copie SnapLock. Les LUN ne sont pas prises en charge dans les volumes SnapLock en lecture/écriture. Toutefois, les copies Snapshot inviolables sont prises en charge à la fois sur les volumes source SnapMirror et les volumes de destination qui contiennent des LUN.

## Prise en charge de MetroCluster

La prise en charge de SnapLock dans les configurations MetroCluster diffère entre le mode SnapLock Compliance et le mode SnapLock Enterprise.

## Conformité SnapLock

- Depuis ONTAP 9.3, la conformité SnapLock est prise en charge sur les agrégats MetroCluster sans miroir.
- Depuis ONTAP 9.3, la conformité SnapLock est prise en charge sur les agrégats en miroir, mais uniquement si l'agrégat est utilisé pour héberger les volumes du journal d'audit SnapLock.
- Les configurations SnapLock spécifiques à SVM peuvent être répliquées sur les sites principal et

secondaire à l'aide de MetroCluster.

## SnapLock Enterprise

- Les agrégats SnapLock Enterprise sont pris en charge depuis la version ONTAP 9.
- Depuis ONTAP 9.3, les agrégats SnapLock Enterprise avec suppression privilégiée sont pris en charge.
- Les configurations SnapLock spécifiques à SVM peuvent être répliquées vers les deux sites à l'aide de MetroCluster.

## Configurations MetroCluster et horloges de conformité

Les configurations MetroCluster utilisent deux mécanismes d'horloge de conformité, l'horloge de conformité du volume (VCC) et l'horloge de conformité du système (SCC). Les VCC et SCC sont disponibles dans toutes les configurations SnapLock. Lorsque vous créez un nouveau volume sur un noeud, son VCC est initialisé avec la valeur actuelle du SCC sur ce noeud. Une fois le volume créé, la durée de rétention du volume et du fichier est toujours suivie avec le VCC.

Lorsqu'un volume est répliqué vers un autre site, son VCC est également répliqué. Lors d'un basculement de volume, du site A vers le site B, par exemple, le VCC continue d'être mis à jour sur le site B pendant que le SCC sur le site A s'arrête lorsque le site A passe hors ligne.

Lorsque le site A est remis en ligne et que le rétablissement du volume est effectué, l'horloge du site A SCC redémarre alors que le VCC du volume continue d'être mis à jour. Étant donné que le VCC est mis à jour en permanence, indépendamment des opérations de basculement et de rétablissement, les délais de conservation des fichiers ne dépendent pas des horloges SCC et ne sont pas extensibles.

## Prise en charge de la vérification multiadministrateur

Depuis la version ONTAP 9.13.1, un administrateur de cluster peut explicitement activer la vérification multiadministrateur sur un cluster afin de demander l'approbation du quorum avant l'exécution de certaines opérations SnapLock. Lorsque MAV est activé, les propriétés du volume SnapLock telles que temps-conservation-défaut, temps-conservation-minimum, temps-conservation-maximum, mode-ajout-volume, période-allocation-auto et suppression-privilégiée requièrent l'approbation du quorum. En savoir plus sur ["VAM"](#).

## Efficacité du stockage

Depuis la version ONTAP 9.9.1, SnapLock prend en charge les fonctionnalités d'efficacité du stockage, telles que la compaction des données, la déduplication entre les volumes et la compression adaptative pour les volumes et les agrégats SnapLock. Pour plus d'informations sur l'efficacité du stockage, voir ["Présentation de l'efficacité du stockage ONTAP"](#).

## Le cryptage

ONTAP propose des technologies de cryptage logicielles et matérielles qui permettent de garantir que les données au repos ne peuvent pas être lues si le support de stockage est requalifié, perdu ou volé.

**Avertissement :** NetApp ne peut pas garantir que les fichiers WORM protégés par SnapLock sur des disques ou volumes à autochiffrement seront récupérables en cas de perte de la clé d'authentification ou si le nombre de tentatives d'authentification échouées dépasse la limite spécifiée et entraîne le verrouillage permanent du disque. Vous êtes responsable de vous assurer contre les échecs d'authentification.



Depuis ONTAP 9.2, les volumes chiffrés sont pris en charge sur les agrégats SnapLock.

## Transition depuis la version 7-mode

Vous pouvez migrer des volumes SnapLock de 7-mode vers ONTAP à l'aide de la fonctionnalité de transition basée sur la copie de l'outil de transition 7-mode. Le mode SnapLock du volume de destination, conformité ou entreprise doit correspondre au mode SnapLock du volume source. Vous ne pouvez pas utiliser la transition sans copie pour migrer des volumes SnapLock.

## Configurez SnapLock

### Configurez SnapLock

Avant d'utiliser SnapLock, vous devez configurer SnapLock en exécutant diverses tâches telles que ["Installez la licence SnapLock"](#) Pour chaque nœud qui héberge un agrégat avec un volume SnapLock, initialisez le ["Horloge de conformité"](#), Créez un agrégat SnapLock pour les clusters exécutant des versions ONTAP antérieures à ONTAP 9.10.1, ["Créez et montez un volume SnapLock"](#), et plus encore.

### Initialiser l'horloge de conformité

SnapLock utilise le *volume Compliance Clock* pour éviter toute altération susceptible de modifier la période de conservation des fichiers WORM. Vous devez d'abord initialiser le *système CompléanceClock* sur chaque nœud hébergeant un agrégat SnapLock.

Depuis ONTAP 9.14.1, vous pouvez initialiser ou réinitialiser l'horloge de conformité du système en l'absence de volumes SnapLock ou de volumes sur lesquels le verrouillage des copies Snapshot est activé. La possibilité de réinitialiser permet aux administrateurs système de réinitialiser l'horloge de conformité du système dans les cas où elle a été mal initialisée ou de corriger la dérive de l'horloge sur le système. Dans ONTAP 9.13.1 et les versions antérieures, une fois que vous avez initialisé l'horloge de conformité sur un nœud, vous ne pouvez pas l'initialiser à nouveau.

### Avant de commencer

Pour réinitialiser l'horloge de conformité :

- Tous les nœuds du cluster doivent être en état de santé.
- Tous les volumes doivent être en ligne.
- Aucun volume ne peut être présent dans la file d'attente de récupération.
- Aucun volume SnapLock ne peut être présent.
- Aucun volume sur lequel le verrouillage des copies Snapshot est activé ne peut être présent.

Exigences générales pour l'initialisation de l'horloge de conformité :

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- ["La licence SnapLock doit être installée sur le nœud"](#).

### Description de la tâche

L'heure de l'horloge de conformité du système est héritée par le *volume Compliance Clock*, qui contrôle la période de conservation des fichiers WORM sur le volume. L'horloge de conformité du volume est initialisée automatiquement lorsque vous créez un nouveau volume SnapLock.



Le réglage initial de l'horloge de conformité du système est basé sur l'horloge du système matériel actuel. C'est pourquoi vous devez vérifier que l'heure et le fuseau horaire du système sont corrects avant d'initialiser l'horloge de conformité du système sur chaque nœud. Une fois que vous avez initialisé l'horloge de conformité du système sur un nœud, vous ne pouvez plus l'initialiser lorsque des volumes SnapLock ou des volumes dont le verrouillage est activé sont présents.

## Étapes

Vous pouvez utiliser l'interface de ligne de commande ONTAP pour initialiser l'horloge de conformité ou, à partir de ONTAP 9.12.1, vous pouvez utiliser System Manager pour initialiser l'horloge de conformité.

### System Manager

1. Accédez à **Cluster > Présentation**.
2. Dans la section **nœuds**, cliquez sur **Initialize SnapLock Compliance Clock**.
3. Pour afficher la colonne **horloge de conformité** et vérifier que l'horloge de conformité est initialisée, dans la section **Cluster > Présentation > nœuds**, cliquez sur **Afficher/Masquer** et sélectionnez **horloge de conformité SnapLock**.

### CLI

1. Initialiser l'horloge de conformité du système :

```
snaplock compliance-clock initialize -node node_name
```

La commande suivante initialise l'horloge de conformité du système node1:

```
cluster1::> snaplock compliance-clock initialize -node node1
```

2. Lorsque vous y êtes invité, vérifiez que l'horloge du système est correcte et que vous souhaitez initialiser l'horloge de conformité :

```
Warning: You are about to initialize the secure ComplianceClock of
the node "node1" to the current value of the node's system clock.
This procedure can be performed only once on a given node, so you
should ensure that the system time is set correctly before
proceeding.
```

```
The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016
```

```
Do you want to continue? (y|n): y
```

3. Répétez cette procédure pour chaque nœud qui héberge un agrégat SnapLock.

## Activez la resynchronisation Compliance Clock pour un système configuré en NTP

Vous pouvez activer la fonction de synchronisation de l'heure de l'horloge de conformité SnapLock lorsqu'un



serveur NTP est configuré.

### Ce dont vous avez besoin

- Cette fonction est disponible uniquement au niveau de privilège avancé.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- ["La licence SnapLock doit être installée sur le nœud"](#).
- Cette fonction est disponible uniquement sur les plates-formes Cloud Volumes ONTAP, ONTAP Select et VSIM.

### Description de la tâche

Lorsque le démon d'horloge sécurisée SnapLock détecte une inclinaison au-delà du seuil, ONTAP utilise l'heure système pour réinitialiser les horloges de conformité du système et du volume. Une période de 24 heures est définie comme seuil d'inclinaison. Cela signifie que l'horloge de conformité du système est synchronisée sur l'horloge du système uniquement si l'inclinaison a plus d'un jour.

Le démon d'horloge sécurisée SnapLock détecte une inclinaison et modifie l'horloge de conformité en l'heure système. Toute tentative de modification de l'heure du système pour forcer la synchronisation de l'horloge de conformité avec l'heure du système échoue, car l'horloge de conformité se synchronise avec l'heure du système uniquement si l'heure du système est synchronisée avec l'heure NTP.

### Étapes

1. Activez la fonction de synchronisation de l'heure de l'horloge de conformité SnapLock lorsqu'un serveur NTP est configuré :

```
snaplock compliance-clock ntp
```

La commande suivante active la fonction de synchronisation de l'horloge de conformité du système :

```
cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
```

2. Lorsque vous y êtes invité, vérifiez que les serveurs NTP configurés sont approuvés et que le canal de communication est sécurisé pour activer la fonction :
3. Vérifiez que la fonction est activée :

```
snaplock compliance-clock ntp show
```

La commande suivante vérifie que la fonction de synchronisation de l'horloge de conformité du système est activée :

```
cluster1::*> snaplock compliance-clock ntp show
```

```
Enable clock sync to NTP system time: true
```

### Créer un agrégat SnapLock

Vous utilisez le volume `-snaplock-type` Pour spécifier un type de volume Compliance ou Enterprise SnapLock. Pour les versions antérieures à ONTAP 9.10.1, vous devez

créer un agrégat SnapLock distinct. Depuis ONTAP 9.10.1, les volumes SnapLock et non SnapLock peuvent exister sur le même agrégat. Ainsi, vous n'avez plus besoin de créer un agrégat SnapLock distinct si vous utilisez ONTAP 9.10.1.

#### Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Le SnapLock ["la licence doit être installée"](#) sur le nœud. Cette licence est incluse dans ["ONTAP One"](#).
- ["L'horloge de conformité sur le nœud doit être initialisée"](#).
- Si vous avez partitionné les disques comme « root », « data1 » et « data2 », vous devez vous assurer que les disques de secours sont disponibles.

#### Mise à niveau

Lors de la mise à niveau vers ONTAP 9.10.1, les agrégats SnapLock et non SnapLock existants sont mis à niveau pour prendre en charge la présence de volumes SnapLock et non SnapLock. Cependant, les attributs des volumes SnapLock existants ne sont pas automatiquement mis à jour. Par exemple, les champs de compaction des données, de déduplication entre les volumes et de déduplication entre les volumes en arrière-plan restent inchangés. Les nouveaux volumes SnapLock créés sur des agrégats existants ont les mêmes valeurs par défaut que les volumes qui ne sont pas SnapLock. Les valeurs par défaut des nouveaux volumes et des agrégats dépendent de la plateforme.

#### Ne tenez pas compte des considérations

Pour restaurer une version ONTAP antérieure à la version 9.10.1, vous devez déplacer les volumes SnapLock Compliance, SnapLock Enterprise et SnapLock vers leurs propres agrégats SnapLock.

#### Description de la tâche

- Vous ne pouvez pas créer d'agrégats de conformité pour les LUN FlexArray, mais les agrégats de conformité SnapLock sont pris en charge avec les LUN FlexArray.
- L'option SyncMirror ne permet pas de créer des agrégats de conformité.
- Vous pouvez créer des agrégats de conformité en miroir dans une configuration MetroCluster uniquement si l'agrégat est utilisé pour héberger des volumes du journal d'audit SnapLock.



Dans une configuration MetroCluster, SnapLock Enterprise est pris en charge sur des agrégats en miroir ou non mis en miroir. La conformité SnapLock est prise en charge uniquement sur les agrégats sans miroir.

#### Étapes

1. Créer un agrégat SnapLock :

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

La page man de la commande contient une liste complète d'options.

La commande suivante crée une SnapLock Compliance agrégat nommé aggr1 avec trois disques sur node1:

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1
-diskcount 3 -snaplock-type compliance
```

## Création et montage de volumes SnapLock

Vous devez créer un volume SnapLock pour les fichiers ou les copies Snapshot que vous souhaitez valider en état WORM. Depuis ONTAP 9.10.1, tout volume que vous créez, quel que soit le type d'agrégat, est créé par défaut en tant que volume non SnapLock. Vous devez utiliser le `-snaplock-type` Option permettant de créer explicitement un volume SnapLock en spécifiant Compliance ou Enterprise comme type SnapLock. Par défaut, le type de SnapLock est défini sur `non-snaplock`.

### Avant de commencer

- L'agrégat SnapLock doit être en ligne.
- Vous devriez ["Vérifiez qu'une licence SnapLock est installée"](#). Si aucune licence SnapLock n'est installée sur le nœud, vous devez ["installer"](#) il. Cette licence est incluse avec ["ONTAP One"](#). Avant ONTAP One, la licence SnapLock était incluse dans le bundle sécurité et conformité. Le bundle sécurité et conformité n'est plus proposé, mais reste valide. Bien qu'ils ne soient pas encore requis, les clients existants peuvent choisir de le faire ["Passez à ONTAP One"](#).
- ["L'horloge de conformité sur le nœud doit être initialisée"](#).

### Description de la tâche

Avec les autorisations SnapLock appropriées, vous pouvez détruire ou renommer un volume d'entreprise à tout moment. Vous ne pouvez pas détruire un volume Compliance tant que la période de conservation n'est pas écoulée. Vous ne pouvez jamais renommer un volume Compliance.

Vous pouvez cloner des volumes SnapLock, mais vous ne pouvez pas cloner des fichiers sur un volume SnapLock. Le volume clone sera du même type SnapLock que le volume parent.



Les LUN ne sont pas prises en charge dans les volumes SnapLock. Les LUN ne sont prises en charge dans les volumes SnapLock que dans les cas où les copies Snapshot créées sur un volume non SnapLock sont transférées vers un volume SnapLock pour être protégées dans le cadre de la relation de copie SnapLock. Les LUN ne sont pas prises en charge dans les volumes SnapLock en lecture/écriture. Toutefois, les copies Snapshot inviolables sont prises en charge à la fois sur les volumes source SnapMirror et les volumes de destination qui contiennent des LUN.

Effectuez cette tâche à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes de ONTAP.

## System Manager

Depuis ONTAP 9.12.1, vous pouvez utiliser System Manager pour créer un volume SnapLock.

### Étapes

1. Accédez à **Storage > volumes** et cliquez sur **Add**.
2. Dans la fenêtre **Ajouter un volume**, cliquez sur **plus d'options**.
3. Entrez les informations du nouveau volume, notamment le nom et la taille du volume.
4. Sélectionnez **Activer SnapLock** et choisissez le type SnapLock, conformité ou entreprise.
5. Dans la section **Auto-commit Files**, sélectionnez **Modified** et entrez la durée pendant laquelle un fichier doit rester inchangé avant qu'il ne soit automatiquement engagé. La valeur minimale est de 5 minutes et la valeur maximale est de 10 ans.
6. Dans la section **Data Retention**, sélectionnez la période de rétention minimale et maximale.
7. Sélectionnez la période de rétention par défaut.
8. Cliquez sur **Enregistrer**.
9. Sélectionnez le nouveau volume dans la page **volumes** pour vérifier les paramètres SnapLock.

### CLI

1. Créer un volume SnapLock :

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate
<aggregate_name> -snaplock-type <compliance|enterprise>
```

Pour obtenir la liste complète des options, consultez la page man de la commande. Les options suivantes ne sont pas disponibles pour les volumes SnapLock : `-nvfail`, `-atime-update`, `-is`, `-autobalance-eligible`, `-space-mgmt-try-first`, et `vmalign`.

La commande suivante crée une SnapLock Compliance volume nommé `vol1` marche `aggr1` marche `vs1`:

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
-snaplock-type compliance
```

## Montez un volume SnapLock

Vous pouvez monter un volume SnapLock sur une Junction path dans le SVM namespace pour accéder au client NAS.

### Ce dont vous avez besoin

Le volume SnapLock doit être en ligne.

### Description de la tâche

- Vous pouvez monter un volume SnapLock uniquement sous la racine de la SVM.

- Vous ne pouvez pas monter un volume normal sous un volume SnapLock.

## Étapes

1. Monter un volume SnapLock :

```
volume mount -vserver SVM_name -volume volume_name -junction-path path
```

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante monte un volume SnapLock nommé `vol1` au chemin de jonction `/sales` dans le `vs1` espace de noms :

```
cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
```

## Définissez la durée de rétention

Vous pouvez définir explicitement la durée de conservation d'un fichier ou utiliser la période de rétention par défaut pour le volume afin de définir la durée de conservation. Sauf si vous définissez explicitement la durée de conservation, SnapLock utilise la période de conservation par défaut pour calculer la durée de conservation. Vous pouvez également définir la conservation des fichiers après un événement.

### À propos de la période de conservation et de la durée de conservation

Le paramètre *rétention\_période* pour un fichier WORM spécifie la durée pendant laquelle le fichier doit être conservé après son activation à l'état WORM. Le *temps de rétention* pour un fichier WORM est le temps après lequel le fichier n'a plus besoin d'être conservé. Une période de conservation de 20 ans pour un dossier engagé à l'état WORM le 10 novembre 2020 6 h 00, par exemple, entraînerait un temps de rétention de 10 novembre 2040 6 h 00



Depuis ONTAP 9.10.1, vous pouvez définir une durée de conservation allant jusqu'au 26 octobre 3058 et une période de conservation pouvant aller jusqu'à 100 ans. Lorsque vous prolongez les dates de conservation, les anciennes règles sont automatiquement converties. Dans ONTAP 9.9.1 et versions antérieures, sauf si vous avez défini la période de conservation par défaut sur infinie, la durée maximale de conservation prise en charge est de janvier 19 2071 (GMT).

## Considérations importantes relatives à la réplication

Lorsque vous définissez une relation SnapMirror avec un volume source SnapLock à une date de conservation postérieure au 19 janvier 2071 (GMT), le cluster de destination doit exécuter ONTAP 9.10.1 ou version ultérieure, sinon le transfert SnapMirror échoue.

## Considérations importantes concernant la restauration

ONTAP vous empêche de restaurer un cluster depuis ONTAP 9.10.1 vers une version antérieure de ONTAP

lorsqu'il y a des fichiers avec une période de conservation postérieure à « janvier 19, 2071 8:44:07 ».

**Comprendre les périodes de conservation**

Un volume SnapLock Compliance ou Enterprise a quatre périodes de conservation :

- Durée de conservation minimale (`min`), avec une valeur par défaut de 0
- Durée de conservation maximale (`max`), avec une valeur par défaut de 30 ans
- Période de rétention par défaut, avec une valeur par défaut égale à `min` Pour le mode conformité et le mode entreprise à partir de ONTAP 9.10.1. Dans les versions ONTAP antérieures à ONTAP 9.10.1, la période de conservation par défaut dépend du mode :
  - Pour le mode conformité, la valeur par défaut est égale à `max`.
  - Pour le mode entreprise, la valeur par défaut est égale à `min`.
- Période de conservation non spécifiée.

Depuis ONTAP 9.8, vous pouvez définir la période de conservation des fichiers d'un volume sur `unspecified`, pour activer le fichier à conserver jusqu'à ce que vous ayez défini une durée de conservation absolue. Vous pouvez définir un fichier avec un temps de conservation absolu sur une rétention non spécifiée et revenir à une conservation absolue tant que la nouvelle durée de conservation absolue est postérieure à la durée absolue que vous avez définie précédemment.

Depuis ONTAP 9.12.1, les fichiers WORM dont la période de conservation est définie sur `unspecified` Est garanti que la période de conservation est définie sur la période minimale de conservation configurée pour le volume SnapLock. Lorsque vous modifiez la période de rétention des fichiers de `unspecified` pour une durée de conservation absolue, la nouvelle durée de rétention spécifiée doit être supérieure à la durée de conservation minimale déjà définie sur le fichier.

Ainsi, si vous ne définissez pas explicitement la durée de rétention avant de valider un fichier en mode conformité à l'état WORM et que vous ne modifiez pas les valeurs par défaut, le fichier sera conservé pendant 30 ans. De même, si vous ne définissez pas explicitement la durée de rétention avant de valider un fichier Enterprise-mode à l'état WORM et que vous ne modifiez pas les valeurs par défaut, le fichier sera conservé pendant 0 ans, ou, de manière efficace, pas du tout.

**Définir la période de conservation par défaut**


Vous pouvez utiliser le volume `snaplock modify` Commande pour définir la période de conservation par défaut pour les fichiers d'un volume SnapLock.

**Ce dont vous avez besoin**

Le volume SnapLock doit être en ligne.

**Description de la tâche**

Le tableau suivant indique les valeurs possibles pour l'option de période de conservation par défaut :



La période de conservation par défaut doit être supérieure ou égale à (`>=`) la période de rétention minimale et inférieure ou égale à (`<=`) la période de rétention maximale.

| Valeur    | Unité    | Remarques |
|-----------|----------|-----------|
| 0 - 65535 | secondes |           |

| Valeur       | Unité  | Remarques                                                                                              |
|--------------|--------|--------------------------------------------------------------------------------------------------------|
| 0 - 24       | heures |                                                                                                        |
| 0 - 365      | jours  |                                                                                                        |
| 0 - 12       | mois   |                                                                                                        |
| 0 - 100      | années | À partir d'ONTAP 9.10.1. Pour les versions antérieures de ONTAP, la valeur est comprise entre 0 et 70. |
| capacité     | -      | Utilisez la période de rétention maximale.                                                             |
| minimum      | -      | Utilisez la période de rétention minimale.                                                             |
| illimitée    | -      | Conservez toujours les fichiers.                                                                       |
| non spécifié | -      | Conservez les fichiers jusqu'à ce qu'une période de conservation absolue soit définie.                 |

Les valeurs et les plages des périodes de rétention maximale et minimale sont identiques, sauf pour `max` et `min`, qui ne sont pas applicables. Pour plus d'informations sur cette tâche, voir ["Définissez l'aperçu de la durée de conservation"](#).

Vous pouvez utiliser le `volume snaplock show` commande pour afficher les paramètres de la période de rétention du volume. Pour plus d'informations, consultez la page man de la commande



Une fois qu'un fichier a été engagé à l'état WORM, vous pouvez prolonger mais pas raccourcir la période de rétention.

## Étapes

1. Définissez la période de conservation par défaut pour les fichiers d'un volume SnapLock :

```
volume snaplock modify -vserver SVM_name -volume volume_name -default
-retention-period default_retention_period -minimum-retention-period
min_retention_period -maximum-retention-period max_retention_period
```

Pour obtenir la liste complète des options, consultez la page man de la commande.



Les exemples suivants supposent que les périodes de rétention minimale et maximale n'ont pas été modifiées auparavant.

La commande suivante définit la période de conservation par défaut pour un volume Compliance ou Enterprise sur 20 jours :

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period 20days
```

La commande suivante définit la période de conservation par défaut pour un volume Compliance sur 70 ans :

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
-retention-period 70years
```

La commande suivante définit la période de conservation par défaut pour un volume entreprise sur 10 ans :

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period max -maximum-retention-period 10years
```

Les commandes suivantes définissent la période de conservation par défaut pour un volume entreprise sur 10 jours :

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

La commande suivante définit la période de conservation par défaut d'un volume Compliance sur infinie :

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

### Définissez explicitement la durée de rétention d'un fichier

Vous pouvez définir explicitement la durée de conservation d'un fichier en modifiant son heure de dernier accès. Vous pouvez utiliser n'importe quelle commande ou programme approprié via NFS ou CIFS pour modifier l'heure du dernier accès.

### Description de la tâche

Une fois qu'un fichier a été enregistré sur WORM, vous pouvez prolonger mais pas réduire la durée de conservation. La durée de rétention est stockée dans le `atime` champ du fichier.



Vous ne pouvez pas définir explicitement la durée de conservation d'un fichier sur `infinite`. Cette valeur n'est disponible que lorsque vous utilisez la période de rétention par défaut pour calculer la durée de rétention.

### Étapes



1. Utilisez une commande ou un programme approprié pour modifier l'heure du dernier accès pour le fichier dont vous souhaitez définir la durée de rétention.

Dans un shell UNIX, utilisez la commande suivante pour définir un temps de rétention de 21 novembre 2020 6 h 00 sur un fichier nommé `document.txt`:

```
touch -a -t 202011210600 document.txt
```



Vous pouvez utiliser n'importe quelle commande ou programme approprié pour modifier l'heure du dernier accès dans Windows.

### Définissez la période de rétention des fichiers après un événement

À partir de ONTAP 9.3, vous pouvez définir la durée de conservation d'un fichier après un événement en utilisant la fonction SnapLock *Event Based Retention* (EBR).

#### Ce dont vous avez besoin

- Vous devez être un administrateur SnapLock pour effectuer cette tâche.

["Créez un compte d'administrateur SnapLock"](#)

- Vous devez vous connecter à une connexion sécurisée (SSH, console ou ZAPI).

#### Description de la tâche

La stratégie *Event Retention* définit la période de rétention du fichier après l'événement. La règle peut être appliquée à un seul fichier ou à tous les fichiers d'un répertoire.

- Si un fichier n'est pas un fichier WORM, il est mis à l'état WORM pour la période de conservation définie dans la stratégie.
- Si un fichier est un fichier WORM ou un fichier inscriptible WORM, sa période de conservation sera prolongée par la période de conservation définie dans la stratégie.

Vous pouvez utiliser un volume Compliance-mode ou Enterprise-mode.



Les politiques EBR ne peuvent pas être appliquées aux fichiers en attente légale.

Pour une utilisation avancée, voir ["Stockage WORM conforme avec NetApp SnapLock"](#).

***utilisation d'EBR pour prolonger la période de conservation des fichiers WORM déjà existants***

EBR est pratique lorsque vous souhaitez prolonger la période de conservation des fichiers WORM existants. Par exemple, votre entreprise a peut-être pour politique de conserver les enregistrements W-4 des employés sous forme non modifiée pendant trois ans après que l'employé change de retenue d'impôt. Une autre politique de l'entreprise pourrait exiger que les enregistrements W-4 soient conservés pendant cinq ans après la cessation d'emploi de l'employé.

Dans ce cas, vous pouvez créer une police EBR avec une période de rétention de cinq ans. Une fois l'employé résilié (l'« événement »), vous appliqueriez la politique de l'EBR au registre W-4 de l'employé, ce qui entraînerait la prolongation de sa période de conservation. Ce processus est généralement plus simple que de prolonger manuellement la période de conservation, en particulier lorsqu'un grand nombre de fichiers sont impliqués.

## Étapes

### 1. Créer une règle EBR :

```
snaplock event-retention policy create -vserver SVM_name -name policy_name -retention-period retention_period
```

La commande suivante crée la règle EBR `employee_exit` marche `vs1` avec une période de rétention de dix ans :

```
cluster1::>snaplock event-retention policy create -vserver vs1 -name employee_exit -retention-period 10years
```

### 2. Appliquer une politique EBR :

```
snaplock event-retention apply -vserver SVM_name -name policy_name -volume volume_name -path path_name
```

La commande suivante applique la règle EBR `employee_exit` marche `vs1` à tous les fichiers du répertoire `d1`:

```
cluster1::>snaplock event-retention apply -vserver vs1 -name employee_exit -volume vol1 -path /d1
```

## Créer un journal d'audit

Si vous utilisez ONTAP 9.9.1 ou une version antérieure, vous devez d'abord créer un agrégat SnapLock, puis créer un journal d'audit protégé par SnapLock avant d'effectuer une suppression privilégiée ou un déplacement de volume SnapLock. Le journal d'audit enregistre la création et la suppression de comptes administrateur SnapLock, les modifications du volume du journal, si la suppression privilégiée est activée, les opérations de suppression privilégiée et les opérations de déplacement de volume SnapLock.

Depuis ONTAP 9.10.1, vous ne créez plus d'agrégat SnapLock. Vous devez utiliser l'option `-snaplock-type`

pour "[Créez un volume SnapLock de manière explicite](#)" En spécifiant soit conformité, soit entreprise comme type SnapLock.

### Avant de commencer

Si vous utilisez ONTAP 9.9.1 ou une version antérieure, vous devez être administrateur du cluster pour créer un agrégat SnapLock.

### Description de la tâche

Vous ne pouvez pas supprimer un journal d'audit tant que la période de conservation du fichier journal n'est pas écoulée. Vous ne pouvez pas modifier un journal d'audit même après la période de conservation écoulée. Ceci est vrai pour les modes SnapLock Compliance et Enterprise.



Dans ONTAP 9.4 et versions antérieures, vous ne pouvez pas utiliser un volume SnapLock Enterprise pour la journalisation des audits. Vous devez utiliser un volume SnapLock Compliance. Dans ONTAP 9.5 et versions ultérieures, vous pouvez utiliser un volume SnapLock Enterprise ou un volume SnapLock Compliance pour la journalisation des audits. Dans tous les cas, le volume du journal d'audit doit être monté sur le Junction path `/snaplock_audit_log`. Aucun autre volume ne peut utiliser cette Junction path

Les journaux d'audit SnapLock sont disponibles dans le `/snaplock_log` répertoire sous la racine du volume du journal de vérification, dans les sous-répertoires nommés `privdel_log` (opérations de suppression privilégiée) et `system_log` (autres). Les noms des fichiers journaux d'audit contiennent l'horodatage de la première opération consignée, ce qui facilite la recherche des enregistrements en fonction de l'heure approximative d'exécution des opérations.

- Vous pouvez utiliser le `snaplock log file show` commande pour afficher les fichiers journaux sur le volume du journal d'audit.
- Vous pouvez utiliser le `snaplock log file archive` commande pour archiver le fichier journal actuel et en créer un nouveau, ce qui est utile dans les cas où vous devez enregistrer les informations du journal d'audit dans un fichier distinct.

Pour plus d'informations, consultez les pages de manuels des commandes.



Un volume de protection des données ne peut pas être utilisé comme volume de journal d'audit SnapLock.

### Étapes

1. Créer un agrégat SnapLock.

[Créer un agrégat SnapLock](#)

2. Sur le SVM que vous voulez configurer pour la journalisation d'audit, créez un volume SnapLock.

[Créer un volume SnapLock](#)

3. Configuration du SVM pour la journalisation d'audit :

```
snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log
-size size -retention-period default_retention_period
```



La période de conservation minimale par défaut des fichiers journaux d'audit est de six mois. Si la période de conservation d'un fichier affecté est supérieure à la période de conservation du journal d'audit, la période de conservation du journal hérite de la période de conservation du fichier. Ainsi, si la période de conservation d'un fichier supprimé avec suppression privilégiée est de 10 mois et que la période de conservation du journal d'audit est de 8 mois, la période de conservation du journal est étendue à 10 mois. Pour plus d'informations sur la durée de conservation et la période de rétention par défaut, reportez-vous à la section "[Définissez la durée de rétention](#)".

La commande suivante configure SVM1 Pour la journalisation des audits à l'aide du volume SnapLock logVol. Le journal d'audit a une taille maximale de 20 Go et est conservé pendant huit mois.

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size 20GB -retention-period 8months
```

4. Sur le SVM que vous avez configuré pour la journalisation d'audit, montez le volume SnapLock sur la Junction path /snaplock\_audit\_log.

[Montez un volume SnapLock](#)

## Vérifiez les paramètres SnapLock

Vous pouvez utiliser le volume file fingerprint start et volume file fingerprint dump Commandes permettant d'afficher des informations clés sur les fichiers et volumes, y compris le type de fichier (standard, WORM ou WORM applicable), la date d'expiration du volume, etc.

### Étapes

1. Générer une empreinte de fichier :

```
volume file fingerprint start -vserver SVM_name -file file_path
```

```
svm1::> volume file fingerprint start -vserver svm1 -file /vol/sle/vol/fl
File fingerprint operation is queued. Run "volume file fingerprint show -session-id 16842791" to view the fingerprint session status.
```

La commande génère un ID de session que vous pouvez utiliser comme entrée dans volume file fingerprint dump commande.



Vous pouvez utiliser le volume file fingerprint show Commande avec l'ID de session pour contrôler la progression de l'opération d'empreinte digitale. Assurez-vous que l'opération est terminée avant d'essayer d'afficher l'empreinte digitale.

2. Afficher l'empreinte du fichier :

```
volume file fingerprint dump -session-id session_ID
```

```
svml:> volume file fingerprint dump -session-id 33619976
Vserver:svml
Session-ID:33619976
Volume:slc_vol
Path:/vol/slc_vol/fl
Data
Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH5lCrudOzZYK4r5Cfylg=Metadata

Fingerprint:8iMjqJXiNcqqXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
Algorithm:SHA256
 Fingerprint Scope:data-and-metadata
 Fingerprint Start Time:1460612586
 Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
 Fingerprint Version:3
 SnapLock License:available
 Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
 Volume MSID:2152884007
 Volume DSID:1028
 Hostname:my_host
 Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
 Volume Containing Aggregate:slc_aggr1
 Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
 **SnapLock System ComplianceClock:1460610635
 Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
 Volume SnapLock Type:compliance
 Volume ComplianceClock:1460610635
 Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
 Volume Expiry Date:1465880998**
 Is Volume Expiry Date Wraparound:false
 Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
 Filesystem ID:1028
 File ID:96
 File Type:worm
 File Size:1048576
 Creation Time:1460612515
 Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
 Modification Time:1460612515
 Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
 Changed Time:1460610598
 Is Changed Time Wraparound:false
 Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
 Retention Time:1465880998
 Is Retention Time Wraparound:false
 Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
```

```
Access Time:-
Formatted Access Time:-
Owner ID:0
Group ID:0
Owner SID:-
Fingerprint End Time:1460612586
Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

## Gérer les fichiers WORM

### Gérer les fichiers WORM

Vous pouvez gérer les fichiers WORM de l'une des manières suivantes :

- ["Archivage des fichiers en mode WORM"](#)
- ["Archivage des copies Snapshot sur WORM sur une destination d'archivage sécurisé"](#)
- ["Mise en miroir des fichiers WORM pour la reprise après incident"](#)
- ["Conservation des fichiers WORM en cas de litige"](#)
- ["Supprimez les fichiers WORM"](#)

### Archivage des fichiers en mode WORM

Vous pouvez archiver les fichiers en mode WORM (write once, read many) manuellement ou automatiquement. Vous pouvez également créer des fichiers modifiables WORM.

#### Archivage manuel des fichiers en mode WORM

Vous devez valider manuellement un fichier en mode WORM en le rendant en lecture seule. Vous pouvez utiliser n'importe quelle commande ou programme approprié sur NFS ou CIFS pour changer l'attribut lecture-écriture d'un fichier en lecture seule. Vous pouvez choisir de valider manuellement les fichiers si vous voulez vous assurer qu'une application a terminé l'écriture dans un fichier de sorte que le fichier n'est pas validé prématurément ou qu'il existe des problèmes de mise à l'échelle pour le scanner à validation automatique en raison d'un nombre élevé de volumes.

#### Ce dont vous avez besoin

- Le fichier à valider doit résider sur un volume SnapLock.
- Le fichier doit être accessible en écriture.

#### Description de la tâche

L'heure de la durée de la période de conformité du volume est écrite sur le `ctime` champ du fichier lors de l'exécution de la commande ou du programme. L'heure de la fin de l'horloge détermine quand la durée de conservation du fichier a été atteinte.

#### Étapes

1. Utilisez une commande ou un programme approprié pour modifier l'attribut lecture-écriture d'un fichier en lecture seule.

Dans un shell UNIX, utilisez la commande suivante pour créer un fichier nommé `document.txt` lecture

seule :

```
chmod -w document.txt
```

Dans un shell Windows, utilisez la commande suivante pour créer un fichier nommé `document.txt` lecture seule :

```
attrib +r document.txt
```

### Archivage automatique des fichiers sur WORM

La fonctionnalité d'autovalidation de SnapLock vous permet d'allouer automatiquement les fichiers en mode WORM. La fonction `autocommit` valide un fichier à l'état WORM sur un volume SnapLock si le fichier n'a pas été modifié pendant la période `autocommit` durée. La fonction de validation automatique est désactivée par défaut.

#### Ce dont vous avez besoin

- Les fichiers que vous souhaitez effectuer une validation automatique doivent résider sur un volume SnapLock.
- Le volume SnapLock doit être en ligne.
- Le volume SnapLock doit être un volume en lecture/écriture.



La fonction SnapLock `autocommit` analyse tous les fichiers du volume et valide un fichier s'il répond à l'exigence d'`autocommit`. Il peut y avoir un intervalle de temps entre le moment où le fichier est prêt pour la validation automatique et celui où il est réellement engagé par le scanner SnapLock `autocommit`. Cependant, le fichier est toujours protégé contre les modifications et la suppression par le système de fichiers dès qu'il est éligible à l'auto-validation.

#### Description de la tâche

Le paramètre *`autocommit Period`* spécifie le temps pendant lequel les fichiers doivent rester inchangés avant leur validation automatique. La modification d'un fichier avant que la période de validation automatique ne soit écoulée entraîne le redémarrage de la période de validation automatique du fichier.

Le tableau suivant présente les valeurs possibles pour la période de validation automatique :

| Valeur      | Unité            | Remarques             |
|-------------|------------------|-----------------------|
| Aucune      | -                | La valeur par défaut. |
| 5 - 5256000 | quelques minutes | -                     |
| 1 - 87600   | heures           | -                     |
| 1 - 3650    | jours            | -                     |
| 1 - 120     | mois             | -                     |

| Valeur | Unité  | Remarques |
|--------|--------|-----------|
| 1 - 10 | années | -         |



La valeur minimale est de 5 minutes et la valeur maximale est de 10 ans.

## Étapes

1. Validation automatique des fichiers sur un volume SnapLock vers WORM :

```
volume snaplock modify -vserver SVM_name -volume volume_name -autocommit
-period autocommit_period
```

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante valide automatiquement les fichiers sur le volume `vol1` Du SVM `vs1`, tant que les fichiers restent inchangés pendant 5 heures :

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
-period 5hours
```

## Créez un fichier d'ajout WORM

Un fichier WORM fiable conserve les données écrites de manière incrémentielle, comme les entrées de journal. Vous pouvez utiliser n'importe quelle commande ou programme approprié pour créer un fichier compatible WORM, ou vous pouvez utiliser la fonction SnapLock *volume append mode* pour créer des fichiers compatibles WORM par défaut.

## Utilisez une commande ou un programme pour créer un fichier inscriptible WORM

Vous pouvez utiliser n'importe quelle commande ou programme appropriée sur NFS ou CIFS pour créer un fichier compatible WORM. Un fichier WORM fiable conserve les données écrites de manière incrémentielle, comme les entrées de journal. Les données sont ajoutées au fichier par blocs de 256 Ko. Au fur et à mesure que chaque bloc est écrit, le bloc précédent devient protégé par WORM. Vous ne pouvez pas supprimer le fichier tant que la période de conservation n'est pas écoulée.

## Ce dont vous avez besoin

Le fichier fiable WORM doit résider sur un volume SnapLock.

## Description de la tâche

Les données n'ont pas besoin d'être écrites de manière séquentielle dans le bloc actif de 256 Ko. Lorsque les données sont écrites sur l'octet  $n \times 256 \text{ Ko} + 1$  du fichier, le segment 256 Ko précédent devient protégé par WORM.

Toute écriture non ordonnée au-delà du bloc actif actuel de 256 Ko entraînera la réinitialisation du bloc actif de 256 Ko au dernier décalage et entraînera l'échec des écritures sur les décalages plus anciens avec une erreur du système de fichiers en lecture seule (ROFS). Les décalages d'écriture dépendent de l'application client. Un client qui n'est pas conforme à la sémantique d'écriture du fichier d'ajout WORM peut entraîner une interruption incorrecte du contenu d'écriture. Par conséquent, il est recommandé de s'assurer que le client respecte les restrictions de décalage pour les écritures non ordonnées, ou de garantir les écritures synchrones en montant le système de fichiers en mode synchrone.



## Étapes

1. Utilisez une commande ou un programme approprié pour créer un fichier de longueur nulle avec le temps de rétention souhaité.

Dans un shell UNIX, utilisez la commande suivante pour définir un temps de rétention de 21 novembre 2020 6 h 00 sur un fichier de longueur zéro nommé `document.txt`:

```
touch -a -t 202011210600 document.txt
```

2. Utilisez une commande ou un programme approprié pour modifier l'attribut lecture-écriture du fichier en lecture seule.

Dans un shell UNIX, utilisez la commande suivante pour créer un fichier nommé `document.txt` lecture seule :

```
chmod 444 document.txt
```

3. Utilisez une commande ou un programme approprié pour remettre l'attribut de lecture-écriture du fichier en inscriptible.



Cette étape n'est pas considérée comme un risque de conformité, car aucune donnée n'est présente dans le fichier.

Dans un shell UNIX, utilisez la commande suivante pour créer un fichier nommé `document.txt` inscriptible :

```
chmod 777 document.txt
```

4. Utilisez une commande ou un programme approprié pour commencer à écrire des données dans le fichier.

Dans un shell UNIX, utiliser la commande suivante pour écrire des données sur `document.txt`:

```
echo test data >> document.txt
```



Rétablissez les autorisations de fichier en lecture seule lorsque vous n'avez plus besoin d'ajouter des données au fichier.

## Utilisez le mode d'ajout de volumes pour créer des fichiers d'ajout WORM

Depuis ONTAP 9.3, vous pouvez utiliser la fonctionnalité SnapLock *volume append mode* (VAM) pour créer par défaut des fichiers WORM utilisables. Un fichier WORM fiable conserve les données écrites de manière incrémentielle, comme les entrées de journal. Les données sont ajoutées au fichier par blocs de 256 Ko. Au fur et à mesure que chaque bloc est écrit, le bloc précédent devient protégé par WORM. Vous ne pouvez pas supprimer le fichier tant que la période de conservation n'est pas écoulée.

## Ce dont vous avez besoin

- Le fichier fiable WORM doit résider sur un volume SnapLock.
- Le volume SnapLock doit être démonté et vide des copies Snapshot et des fichiers créés par l'utilisateur.

### Description de la tâche

Les données n'ont pas besoin d'être écrites de manière séquentielle dans le bloc actif de 256 Ko. Lorsque les données sont écrites sur l'octet  $n \times 256 \text{ Ko} + 1$  du fichier, le segment 256 Ko précédent devient protégé par WORM.

Si vous spécifiez une période de validation automatique pour le volume, les fichiers modifiables WORM qui ne sont pas modifiés pour une période supérieure à la période de validation automatique sont validés en mode WORM.



Le mode VAM n'est pas pris en charge sur les volumes des journaux d'audit SnapLock.

### Étapes

1. Activer VAM :

```
volume snaplock modify -vserver SVM_name -volume volume_name -is-volume-append
-mode-enabled true|false
```

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante active le mode VAM sur le volume `vol1` De `SVMvs1`:

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
-append-mode-enabled true
```

2. Utilisez une commande ou un programme approprié pour créer des fichiers avec des autorisations d'écriture.

Les fichiers sont par défaut modifiables.

### Archivage des copies Snapshot sur WORM sur une destination d'archivage sécurisé

Vous pouvez utiliser SnapLock pour SnapVault pour protéger les copies Snapshot WORM sur le stockage secondaire. Vous exécutez toutes les tâches SnapLock de base sur la destination du coffre-fort. Le volume de destination est automatiquement monté en lecture seule. Il est donc inutile de valider de manière explicite les copies Snapshot sur WORM. Ainsi, la création de copies Snapshot planifiées sur le volume de destination à l'aide des règles SnapMirror n'est pas prise en charge.

### Avant de commencer

- Si vous souhaitez utiliser System Manager pour configurer la relation, les clusters source et cible doivent exécuter ONTAP 9.15.1 ou une version ultérieure.
- Sur le cluster de destination :
  - ["Installez la licence SnapLock"](#).
  - ["Initialiser l'horloge de conformité"](#).

- Si vous utilisez l'interface de ligne de commandes avec une version de ONTAP antérieure à la version 9.10.1, ["Créer un agrégat SnapLock"](#).
- La règle de protection doit être de type « coffre-fort ».
- Les agrégats source et de destination doivent être de 64 bits.
- Le volume source ne peut pas être un volume SnapLock.
- Si vous utilisez l'interface de ligne de commandes de ONTAP, les volumes source et de destination doivent être créés dans le ["clusters de peering"](#) et ["SVM"](#).

### Description de la tâche

Le volume source peut utiliser le stockage NetApp ou autre. Pour le stockage non NetApp, vous devez utiliser la virtualisation FlexArray.



Vous ne pouvez pas renommer une copie Snapshot engagée en état WORM.

Vous pouvez cloner des volumes SnapLock, mais vous ne pouvez pas cloner des fichiers sur un volume SnapLock.



Les LUN ne sont pas prises en charge dans les volumes SnapLock. Les LUN ne sont prises en charge dans les volumes SnapLock que dans les cas où les copies Snapshot créées sur un volume non SnapLock sont transférées vers un volume SnapLock pour être protégées dans le cadre de la relation de copie SnapLock. Les LUN ne sont pas prises en charge dans les volumes SnapLock en lecture/écriture. Toutefois, les copies Snapshot inviolables sont prises en charge à la fois sur les volumes source SnapMirror et les volumes de destination qui contiennent des LUN.

Depuis ONTAP 9.10.1, les volumes SnapLock et non SnapLock peuvent exister sur le même agrégat. Ainsi, vous n'avez plus besoin de créer un agrégat SnapLock distinct si vous utilisez ONTAP 9.10.1. Vous pouvez utiliser l'option '-snaplock-type' du volume pour spécifier un type de volume Compliance ou Enterprise SnapLock. Dans les versions ONTAP antérieures à ONTAP 9.10.1, le mode SnapLock, conformité ou entreprise, est hérité de l'agrégat. Les volumes de destination flexibles de la version ne sont pas pris en charge. Le paramètre de langue du volume de destination doit correspondre au paramètre de langue du volume source.

Une période de conservation par défaut est affectée à un volume SnapLock cible du coffre-fort. La valeur pour cette période est initialement définie sur un minimum de 0 ans pour les volumes SnapLock Enterprise et un maximum de 30 ans pour les volumes SnapLock Compliance. À chaque copie NetApp Snapshot, toutes les copies NetApp Snapshot sont conservées pendant cette période de conservation par défaut. La période de conservation peut être prolongée ultérieurement, si nécessaire. Pour plus d'informations, voir ["Aperçu de la durée de conservation"](#).

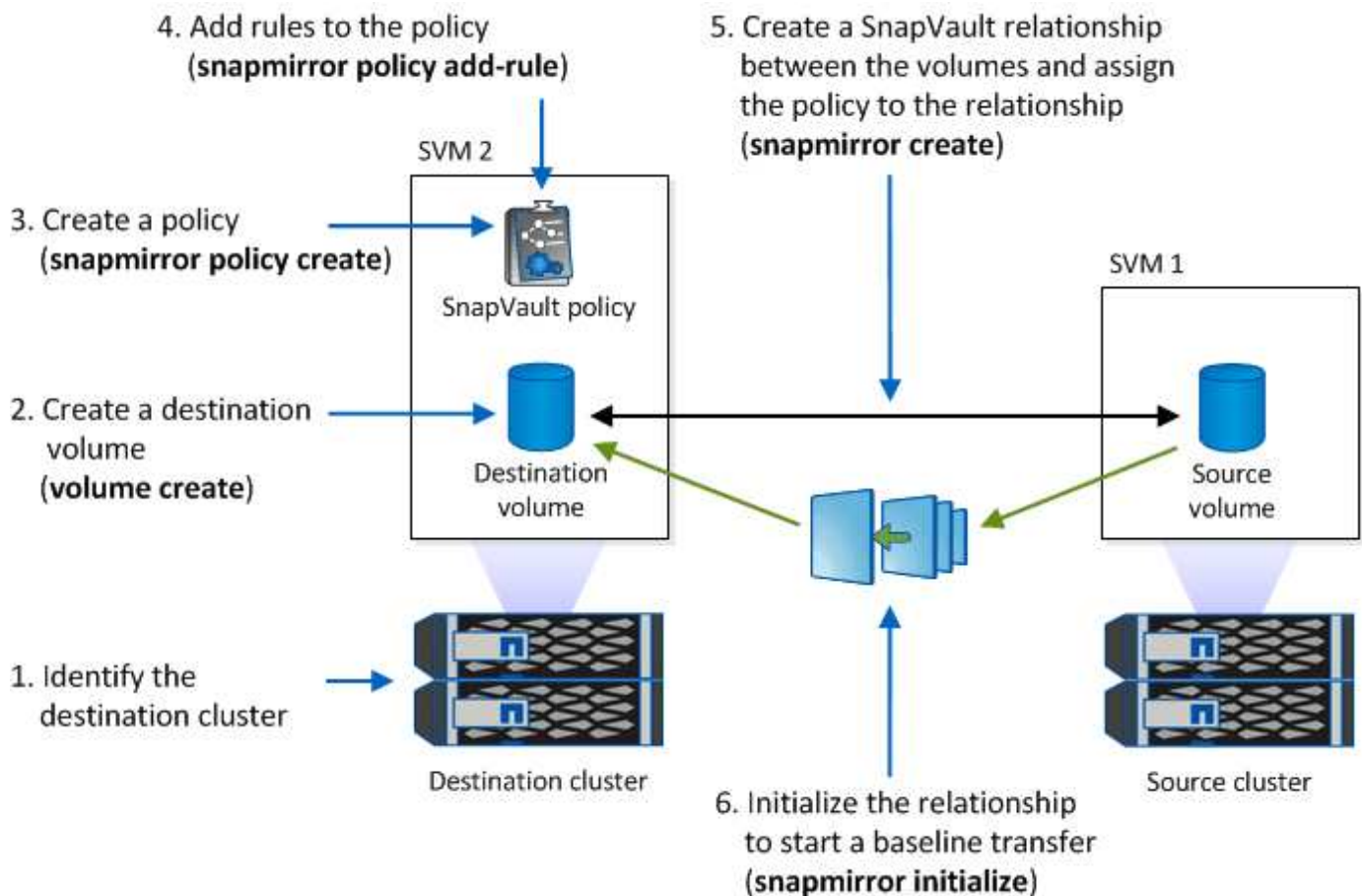
Depuis la version ONTAP 9.14.1, vous pouvez spécifier des périodes de conservation pour des étiquettes SnapMirror spécifiques dans la règle SnapMirror de la relation SnapMirror de sorte que les copies Snapshot répliquées du volume source vers le volume de destination soient conservées pendant la période de conservation spécifiée dans la règle. Si aucune période de conservation n'est spécifiée, la période de rétention par défaut du volume de destination est utilisée.

À partir de ONTAP 9.13.1, vous pouvez restaurer instantanément une copie Snapshot verrouillée sur le volume SnapLock de destination d'une relation de copie SnapLock en créant une copie FlexClone avec `snaplock-type` Défini sur non snaplock et spécifiant la copie Snapshot comme « snapshot-parent » lors de l'exécution de l'opération de création du clone de volume. En savoir plus sur ["Création d'un volume FlexClone avec un type SnapLock"](#).

Pour les configurations MetroCluster, il est important de connaître les éléments suivants :

- Vous pouvez créer une relation SnapVault uniquement entre des SVM source synchrone, et non entre un SVM source synchrone et une SVM de destination synchrone.
- Vous pouvez créer une relation SnapVault depuis un volume d'un SVM source synchrone vers une SVM transmettant les données.
- Vous pouvez créer une relation SnapVault depuis un volume d'une SVM diffusant les données vers un volume DP au sein d'un SVM source synchrone.

L'illustration suivante montre la procédure d'initialisation d'une relation de coffre-fort SnapLock :



### Étapes

Vous pouvez utiliser l'interface de ligne de commandes ONTAP pour créer une relation de copie SnapLock ou, à partir de ONTAP 9.15.1, vous pouvez utiliser System Manager pour créer une relation de copie SnapLock.

## System Manager

1. Naviguez jusqu'à **stockage > volumes** et sélectionnez **Ajouter**.
2. Dans la fenêtre **Ajouter un volume**, choisissez **plus d'options**.
3. Entrez le nom du volume, sa taille, la règle d'export et le nom du partage.
4. Sélectionnez **Verrouiller les instantanés de destination pour empêcher la suppression**, et dans la section **méthode de verrouillage**, choisissez **SnapLock pour SnapVault**. Cette sélection ne s'affiche pas si le type de stratégie sélectionné n'est pas de type « coffre-fort », si la licence SnapLock n'est pas installée ou si l'horloge de conformité n'est pas initialisée.
5. S'il n'est pas déjà activé, sélectionnez **initialiser horloge de conformité SnapLock**.
6. Enregistrez les modifications.

## CLI

1. Sur le cluster de destination, créez un volume de destination SnapLock de type DP taille identique ou supérieure à celle du volume source :

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate
<aggregate_name> -snaplock-type <compliance|enterprise> -type DP
-size <size>
```

La commande suivante crée un volume SnapLock Compliance de 2 Go nommé `dstvolB` dans `SVM2` sur l'agrégat `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

2. Sur le cluster de destination, "[définissez la période de conservation par défaut](#)".
3. "[Créer une nouvelle relation de réplication](#)" Entre la source non SnapLock et la nouvelle destination SnapLock que vous avez créée.

Dans cet exemple, une nouvelle relation SnapMirror est créée avec un volume SnapLock de destination `dstvolB` à l'aide d'une règle de `XDPDefault` Pour archiver les copies Snapshot étiquetées tous les jours et toutes les semaines selon une planification horaire :

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```



"[Création d'une règle de réplication personnalisée](#)" ou un "[planification personnalisée](#)" si les valeurs par défaut disponibles ne sont pas appropriées.

4. Sur le SVM de destination, initialiser la relation SnapVault créée :

```
snapmirror initialize -destination-path <destination_path>
```

La commande suivante initialise la relation entre le volume source `srcvolA` marche SVM1 et le volume de destination `dstvolB` marche SVM2:

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

5. Une fois la relation initialisée et inactive, utilisez le `snapshot show` Sur le volume de destination afin de vérifier l'heure d'expiration du SnapLock appliquée aux copies Snapshot répliquées.

Cet exemple répertorie les copies Snapshot sur le volume `dstvolB` Étiquette SnapMirror et date d'expiration du SnapLock :

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields
snapmirror-label, snaplock-expiry-time
```

### Informations associées

["Cluster et SVM peering"](#)

["Sauvegarde de volume avec SnapVault"](#)

### Mise en miroir des fichiers WORM pour la reprise après incident

Vous pouvez utiliser SnapMirror pour répliquer des fichiers WORM dans un autre emplacement géographique à des fins autres que la reprise après incident. Le volume source et le volume de destination doivent être configurés pour SnapLock et les deux volumes doivent disposer du même mode SnapLock, Compliance ou Enterprise. Toutes les propriétés SnapLock clés du volume et les fichiers sont répliqués.

### Prérequis

Les volumes source et destination doivent être créés dans des clusters associés avec des SVM peering. Pour plus d'informations, voir ["Cluster et SVM peering"](#).

### Description de la tâche

- Depuis ONTAP 9.5, vous pouvez répliquer les fichiers WORM avec la relation SnapMirror de type XDP (protection étendue des données) plutôt qu'avec la relation de type DP (protection des données). Le mode XDP ne dépend pas de la version d'ONTAP. Il peut donc différencier les fichiers stockés dans le même bloc, ce qui facilite la resynchronisation des volumes du mode Compliance répliqué. Pour plus d'informations sur la conversion d'une relation de type DP existante en relation de type XDP, reportez-vous à ["La protection des données"](#).
- Une opération de resynchronisation dans une relation SnapMirror de type DP échoue pour un volume en mode conformité si SnapLock détermine qu'elle entraînera une perte de données. Si une opération de resynchronisation échoue, vous pouvez utiliser le `volume clone create` commande pour créer un clone du volume de destination. Vous pouvez ensuite resynchroniser le volume source avec le clone.
- Une relation SnapMirror de type XDP entre des volumes compatibles SnapLock prend en charge une resynchronisation après une interruption, même si les données de la destination ont divergé de la source après l'arrêt.

Lors d'une resynchronisation, lorsque des divergences de données sont détectées entre la source et la destination au-delà du snapshot commun, un nouvel instantané est coupé sur la destination pour capturer cette divergence. Le nouvel instantané et le snapshot commun sont tous deux verrouillés avec un temps de rétention comme suit :

- Heure d'expiration du volume de la destination
- Si le délai d'expiration du volume est passé ou n'a pas été défini, le snapshot est verrouillé pendant une période de 30 jours
- Si la destination a des raisons juridiques, la période d'expiration réelle du volume est masquée et apparaît comme « indéfinie » ; cependant, l'instantané est verrouillé pendant la durée de la période d'expiration réelle du volume.

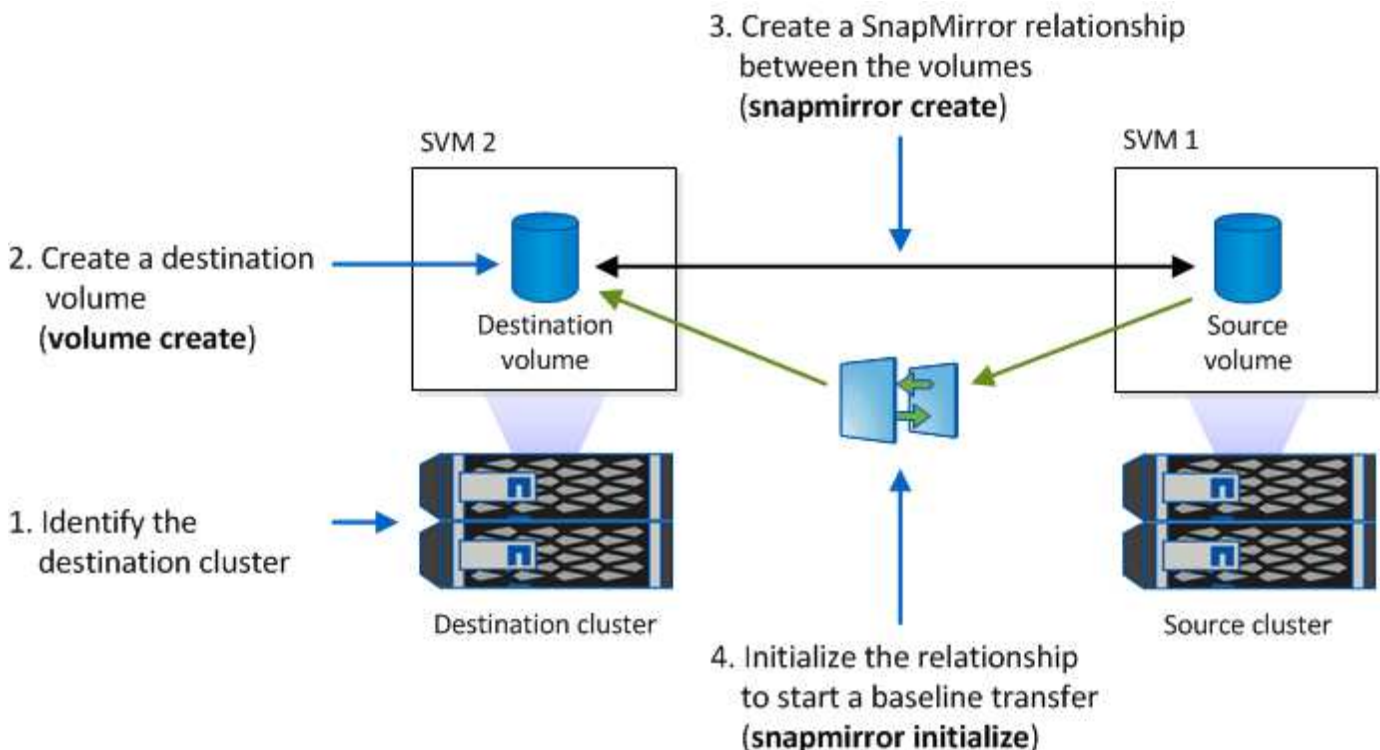
Si le volume de destination a une période d'expiration postérieure à la source, la période d'expiration de destination est conservée et ne sera pas écrasée par la période d'expiration du volume source après la resynchronisation.

Si la destination dispose de mentions légales qui diffèrent de la source, une resynchronisation n'est pas autorisée. La source et la destination doivent disposer de mentions légales identiques ou toutes les mentions légales de la destination doivent être libérées avant toute tentative de resynchronisation.

Une copie Snapshot verrouillée sur le volume de destination créé pour capturer les données divergentes peut être copiée vers la source à l'aide de la CLI en exécutant le `snapmirror update -s snapshot` commande. Une fois copié, le snapshot reste également verrouillé à la source.

- Les relations de protection des données des SVM ne sont pas prises en charge.
- Les relations de protection des données de partage de charge ne sont pas prises en charge.

L'illustration suivante montre la procédure d'initialisation d'une relation SnapMirror :






## System Manager

Depuis ONTAP 9.12.1, System Manager vous permet de configurer la réplication SnapMirror des fichiers WORM.

### Étapes

1. Accédez à **Storage > volumes**.
2. Cliquez sur **Afficher/Masquer** et sélectionnez **Type SnapLock** pour afficher la colonne dans la fenêtre **volumes**.
3. Recherchez un volume SnapLock.
4. Cliquez sur  et sélectionnez **protéger**.
5. Choisir le cluster de destination et la VM de stockage de destination
6. Cliquez sur **plus d'options**.
7. Sélectionnez **Afficher les règles héritées** et **DPDefault (TDA/TDE/s)**.
8. Dans la section **Détails de configuration de destination**, sélectionnez **remplacer le programme de transfert** et sélectionnez **horaire**.
9. Cliquez sur **Enregistrer**.
10. À gauche du nom du volume source, cliquez sur la flèche pour développer les détails du volume, puis, à droite de la page, consultez les informations relatives à la protection SnapMirror distante.
11. Sur le cluster distant, accédez à **protection relations**.
12. Localisez la relation et cliquez sur le nom du volume de destination pour afficher les détails de la relation.
13. Vérifiez que le type de SnapLock du volume de destination et d'autres informations SnapLock.

### CLI

1. Identifier le cluster de destination
2. Sur le cluster de destination, "[Installez la licence SnapLock](#)", "[Initialiser l'horloge de conformité](#)", Et, si vous utilisez une version de ONTAP antérieure à 9.10.1, "[Créer un agrégat SnapLock](#)".
3. Sur le cluster de destination, créez un volume de destination SnapLock de type DP taille identique ou supérieure à celle du volume source :

```
volume create -vserver SVM_name -volume volume_name -aggregate
aggregate_name -snaplock-type compliance|enterprise -type DP -size size
```



Depuis ONTAP 9.10.1, les volumes SnapLock et non SnapLock peuvent exister sur le même agrégat. Ainsi, vous n'avez plus besoin de créer un agrégat SnapLock distinct si vous utilisez ONTAP 9.10.1. Utilisez l'option `volume -snaplock-type` pour spécifier un type de volume Compliance ou Enterprise SnapLock. Dans les versions ONTAP antérieures à ONTAP 9.10.1, le mode SnapLock—Compliance ou Enterprise—est hérité de l'agrégat. Les volumes de destination flexibles de la version ne sont pas pris en charge. Le paramètre de langue du volume de destination doit correspondre au paramètre de langue du volume source.

La commande suivante crée un SnapLock de 2 Go Compliance volume nommé `dstvolB` dans SVM2 sur l'agrégat `node01_aggr`:



```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. Sur le SVM de destination, créer une règle SnapMirror :

```
snapmirror policy create -vserver SVM_name -policy policy_name
```

La commande suivante crée la politique au niveau du SVM SVM1-mirror:

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

5. Sur le SVM de destination, créer une planification SnapMirror :

```
job schedule cron create -name schedule_name -dayofweek day_of_week -hour
hour -minute minute
```

La commande suivante crée une planification SnapMirror nommée weekendcron:

```
SVM2::> job schedule cron create -name weekendcron -dayofweek
"Saturday, Sunday" -hour 3 -minute 0
```

6. Sur le SVM de destination, créer une relation SnapMirror :

```
snapmirror create -source-path source_path -destination-path
destination_path -type XDP|DP -policy policy_name -schedule schedule_name
```

La commande suivante crée une relation SnapMirror entre le volume source srcvolA marche SVM1 et le volume de destination dstvolB marche SVM2, et affecte la stratégie SVM1-mirror et le planning weekendcron:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
weekendcron
```



Le type XDP est disponible dans ONTAP 9.5 et versions ultérieures. Vous devez utiliser le type DP dans ONTAP 9.4 et versions antérieures.

7. Sur le SVM de destination, initialiser la relation SnapMirror :

```
snapmirror initialize -destination-path destination_path
```

Le processus d'initialisation effectue un transfert *baseline* vers le volume de destination. SnapMirror effectue une copie Snapshot du volume source, puis transfère la copie ainsi que tous les blocs de données qu'il renvoie au volume de destination. Il transfère également toutes les autres copies Snapshot du volume source vers le volume de destination.

La commande suivante initialise la relation entre le volume source `srcvolA` marche SVM1 et le volume de destination `dstvolB` marche SVM2:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

### Informations associées

["Cluster et SVM peering"](#)

["Préparation de la reprise après incident de volume"](#)

["Protection des données"](#)

### Conservation des fichiers WORM en cas de litiges avec la conservation légale

À partir de ONTAP 9.3, vous pouvez conserver des fichiers WORM en mode conformité pendant la durée d'un litige en utilisant la fonction *Legal Hold*.

#### Ce dont vous avez besoin

- Vous devez être un administrateur SnapLock pour effectuer cette tâche.

["Créez un compte d'administrateur SnapLock"](#)

- Vous devez vous connecter à une connexion sécurisée (SSH, console ou ZAPI).

#### Description de la tâche

Un fichier placé dans une mise en attente légale se comporte comme un fichier WORM ayant une période de conservation indéfinie. Il est de votre responsabilité de préciser à quel moment la période de conservation légale prend fin.

Le nombre de fichiers que vous pouvez placer sous conservation légale dépend de l'espace disponible sur le volume.

#### Étapes

1. Démarrer une mise en garde légale :

```
snaplock legal-hold begin -litigation-name litigation_name -volume volume_name -path path_name
```

La commande suivante démarre une mise en attente légale pour tous les fichiers dans `vol1`:

```
cluster1::> snaplock legal-hold begin -litigation-name litigation1 -volume vol1 -path /
```

2. Mettre fin à l'attente légale :

```
snaplock legal-hold end -litigation-name litigation_name -volume volume_name -path path_name
```

La commande suivante met fin à la mise en attente légale de tous les fichiers dans voll:

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
voll -path /
```

## Vue d'ensemble de la suppression des fichiers WORM

Vous pouvez supprimer des fichiers WORM en mode entreprise pendant la période de conservation à l'aide de la fonction de suppression privilégiée.

Avant de pouvoir utiliser cette fonction, vous devez créer un compte administrateur SnapLock, puis activer la fonction à l'aide du compte.

### Créez un compte d'administrateur SnapLock

Vous devez disposer des privilèges d'administrateur SnapLock pour effectuer une suppression privilégiée. Ces privilèges sont définis dans le rôle vsadmin-snaplock. Si ce rôle n'est pas encore attribué, vous pouvez demander à l'administrateur du cluster de créer un compte d'administrateur SVM avec le rôle d'administrateur SnapLock.

### Ce dont vous avez besoin

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez vous connecter à une connexion sécurisée (SSH, console ou ZAPI).

### Étapes

1. Créer un compte administrateur SVM avec le rôle d'administrateur SnapLock :

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role role -comment
comment
```

La commande suivante active le compte d'administrateur du SVM SnapLockAdmin avec le prédéfini vsadmin-snaplock rôle d'accès SVM1 utilisation d'un mot de passe :

```
cluster1::> security login create -vserver SVM1 -user-or-group-name
SnapLockAdmin -application ssh -authmethod password -role vsadmin-
snaplock
```

### Activer la fonction de suppression privilégiée

Vous devez activer explicitement la fonction de suppression privilégiée sur le volume entreprise contenant les fichiers WORM que vous souhaitez supprimer.

### Description de la tâche

La valeur du `-privileged-delete` détermine si la suppression privilégiée est activée. Les valeurs possibles sont `enabled`, `disabled`, et `permanently-disabled`.



`permanently-disabled` est l'état du terminal. Vous ne pouvez pas activer la suppression privilégiée sur le volume après avoir défini l'état sur `permanently-disabled`.

## Étapes

1. Activer la suppression privilégiée pour un volume SnapLock Enterprise :

```
volume snaplock modify -vserver SVM_name -volume volume_name -privileged
-delete disabled|enabled|permanently-disabled
```

La commande suivante active la fonction de suppression privilégiée pour le volume entreprise dataVol marche SVM1:

```
SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged
-delete enabled
```

## Supprimez les fichiers WORM en mode entreprise

Vous pouvez utiliser la fonction de suppression privilégiée pour supprimer des fichiers WORM en mode entreprise pendant la période de conservation.

### Ce dont vous avez besoin

- Vous devez être un administrateur SnapLock pour effectuer cette tâche.
- Vous devez avoir créé un journal d'audit SnapLock et activé la fonctionnalité de suppression privilégiée sur le volume entreprise.

### Description de la tâche

Vous ne pouvez pas utiliser une opération de suppression privilégiée pour supprimer un fichier WORM expiré. Vous pouvez utiliser le `volume file retention show` Commande pour afficher la durée de conservation du fichier WORM que vous souhaitez supprimer. Pour plus d'informations, consultez la page man de la commande

### Étape

1. Supprimez un fichier WORM sur un volume d'entreprise :

```
volume file privileged-delete -vserver SVM_name -file file_path
```

La commande suivante supprime le fichier /vol/dataVol/f1 Sur le SVM SVM1:

```
SVM1::> volume file privileged-delete -file /vol/dataVol/f1
```

## Déplacer un volume SnapLock

Depuis ONTAP 9.8, vous pouvez déplacer un volume SnapLock vers un agrégat de destination du même type (entreprise vers entreprise ou conformité vers conformité).

Vous devez avoir le rôle de sécurité SnapLock pour déplacer un volume SnapLock.

### Créez un compte administrateur de sécurité SnapLock

Pour effectuer un déplacement de volume SnapLock, vous devez disposer des privilèges administrateur de sécurité SnapLock. Ce privilège vous est accordé avec le rôle *SnapLock*, introduit dans ONTAP 9.8. Si ce rôle n'est pas encore attribué, vous pouvez demander à votre administrateur de cluster de créer un utilisateur de sécurité SnapLock avec ce rôle de sécurité SnapLock.

#### Ce dont vous avez besoin

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez vous connecter à une connexion sécurisée (SSH, console ou ZAPI).

#### Description de la tâche

Le rôle SnapLock est associé au SVM admin, contrairement au rôle vsadmin-snaplock, qui est associé au SVM de données.

#### Étape

1. Créer un compte administrateur SVM avec le rôle d'administrateur SnapLock :

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role role -comment
comment
```

La commande suivante active le compte d'administrateur du SVM SnapLockAdmin avec le prédéfini snaplock Rôle permettant d'accéder à la SVM d'admin cluster1 utilisation d'un mot de passe :

```
cluster1::> security login create -vserver cluster1 -user-or-group-name
SnapLockAdmin -application ssh -authmethod password -role snaplock
```

### Déplacer un volume SnapLock

Vous pouvez utiliser le `volume move` Commande de déplacement d'un volume SnapLock vers un agrégat de destination.

#### Ce dont vous avez besoin

- Vous devez avoir créé un journal d'audit protégé SnapLock avant d'effectuer le déplacement de volume SnapLock.

["Créer un journal d'audit"](#).

- Si vous utilisez une version de ONTAP antérieure à ONTAP 9.10.1, l'agrégat de destination doit être du même type SnapLock que le volume SnapLock que vous souhaitez déplacer : conformité à la conformité ou entreprise à la norme. Depuis ONTAP 9.10.1, cette restriction est supprimée et un agrégat peut inclure des volumes Compliance et Enterprise SnapLock, ainsi que des volumes non SnapLock.
- Vous devez être un utilisateur ayant le rôle de sécurité SnapLock.

#### Étapes

1. Via une connexion sécurisée, connectez-vous à la LIF de gestion du cluster ONTAP :

```
ssh snaplock_user@cluster_mgmt_ip
```

2. Déplacer un volume SnapLock :

```
volume move start -vserver SVM_name -volume SnapLock_volume_name -destination
-aggregate destination_aggregate_name
```

3. Vérifier l'état de l'opération de déplacement de volume :

```
volume move show -volume SnapLock_volume_name -vserver SVM_name -fields
volume,phase,vserver
```

## Verrouiller une copie Snapshot pour assurer la protection contre les attaques par ransomware

Depuis ONTAP 9.12.1, vous pouvez verrouiller une copie Snapshot sur un volume non SnapLock pour vous protéger des attaques par ransomware. Le verrouillage des copies Snapshot permet de ne pas les supprimer accidentellement ou accidentellement.

La fonction horloge de conformité de SnapLock vous permet de verrouiller les copies Snapshot pendant une période spécifiée, de sorte qu'elles ne puissent pas être supprimées tant que l'heure d'expiration n'est pas atteinte. Le verrouillage des copies Snapshot est inviolable, ce qui les protège contre les menaces de ransomware. Vous pouvez utiliser des copies Snapshot verrouillées pour récupérer des données si un volume est compromis par une attaque par ransomware.

À partir de la version ONTAP 9.14.1, le verrouillage des copies Snapshot prend en charge les copies Snapshot à conservation à long terme sur les destinations des coffres-forts SnapLock et sur les volumes de destination SnapMirror non SnapLock. Le verrouillage des copies Snapshot est activé en définissant la période de conservation à l'aide des règles de règles SnapMirror associées à un [libellé de police existant](#). La règle remplace la période de rétention par défaut définie sur le volume. Si aucune période de conservation n'est associée au label SnapMirror, la période de conservation par défaut du volume est utilisée.

### Exigences et considérations relatives à la non-conformité des copies Snapshot

- Si vous utilisez l'interface de ligne de commandes ONTAP, tous les nœuds du cluster doivent exécuter ONTAP 9.12.1 ou une version ultérieure. Si vous utilisez System Manager, tous les nœuds doivent exécuter ONTAP 9.13.1 ou une version ultérieure.
- ["La licence SnapLock doit être installée sur le cluster"](#). Cette licence est incluse dans ["ONTAP One"](#).
- ["L'horloge de conformité du cluster doit être initialisée"](#).
- Lorsque le verrouillage Snapshot est activé sur un volume, vous pouvez mettre à niveau les clusters vers une version d'ONTAP ultérieure à ONTAP 9.12.1 ; Cependant, vous ne pouvez pas revenir à une version antérieure de ONTAP tant que toutes les copies Snapshot verrouillées n'ont pas atteint leur date d'expiration. Elles sont supprimées et le verrouillage des copies Snapshot est désactivé.
- Lorsqu'un snapshot est verrouillé, la durée d'expiration du volume est définie sur la date d'expiration de la copie Snapshot. Si plusieurs copies Snapshot sont verrouillées, la date d'expiration du volume reflète la date d'expiration la plus élevée parmi toutes les copies Snapshot.
- La période de conservation des copies Snapshot verrouillées est prioritaire sur le nombre de copies Snapshot conservées. En d'autres termes, la limite de conservation des copies Snapshot n'est pas respectée si la période de conservation des copies Snapshot verrouillées n'a pas expiré.
- Dans une relation SnapMirror, vous pouvez définir une période de conservation sur une règle de stratégie de copie en miroir et la période de conservation est appliquée aux copies Snapshot répliquées vers la

destination si le volume de destination est activé pour le verrouillage des copies Snapshot. La période de conservation est prioritaire sur le nombre de copies. Par exemple, les copies Snapshot qui n'ont pas dépassé leur expiration seront conservées même si le nombre de copies à conserver est dépassé.

- Vous pouvez renommer une copie Snapshot sur un volume non SnapLock. Les opérations de renommage de snapshot sur le volume principal d'une relation SnapMirror sont reflétées sur le volume secondaire uniquement si la règle est MirrorAllsnapshots. Pour les autres types de règles, la copie Snapshot renommée n'est pas propagée lors des mises à jour.
- Si vous utilisez l'interface de ligne de commandes de ONTAP, vous pouvez restaurer une copie Snapshot verrouillée avec `volume snapshot restore` Commande uniquement si la copie Snapshot verrouillée est la plus récente. Si des copies Snapshot non expirées sont présentes dans la suite de la restauration, l'opération de restauration de copie Snapshot échoue.

### Fonctionnalités prises en charge par les copies Snapshot inviolables

- "Cloud Volumes ONTAP"
- Volumes FlexGroup

Le verrouillage des copies Snapshot est pris en charge sur les volumes FlexGroup. Le verrouillage des snapshots n'a lieu que sur la copie Snapshot du composant racine. La suppression du volume FlexGroup n'est autorisée que si la durée d'expiration du composant racine est passée.

- Conversion FlexVol en FlexGroup

Vous pouvez convertir un volume FlexVol avec des copies Snapshot verrouillées en un volume FlexGroup. Les copies Snapshot restent verrouillées après la conversion.

- Clone de volume et de fichiers

Vous pouvez créer des clones de volumes et de fichiers à partir d'une copie Snapshot verrouillée.

### Fonctions non prises en charge

Les fonctionnalités suivantes ne sont actuellement pas prises en charge par les copies Snapshot inviolables :

- Groupes de cohérence
- FabricPool
- Volumes FlexCache
- Bande SMtape
- Synchronisation active SnapMirror
- Règle SnapMirror utilisant le `-schedule` paramètre
- SnapMirror synchrone
- Mobilité des données des SVM (utilisé pour la migration ou le déplacement d'un SVM d'un cluster source vers un cluster destination)

### Activez le verrouillage des copies Snapshot lors de la création d'un volume

Depuis ONTAP 9.12.1, vous pouvez activer le verrouillage des copies Snapshot lorsque vous créez un nouveau volume ou que vous modifiez un volume existant à l'aide du `-snapshot-locking-enabled` avec le `volume create` et `volume modify` Dans l'interface de ligne de commande. Depuis la version ONTAP 9.13.1, System Manager permet le verrouillage des copies Snapshot.

## System Manager

1. Naviguez jusqu'à **stockage > volumes** et sélectionnez **Ajouter**.
2. Dans la fenêtre **Ajouter un volume**, choisissez **plus d'options**.
3. Entrez le nom du volume, sa taille, la règle d'export et le nom du partage.
4. Sélectionnez **Activer le verrouillage des instantanés**. Cette sélection ne s'affiche pas si la licence SnapLock n'est pas installée.
5. S'il n'est pas déjà activé, sélectionnez **initialiser horloge de conformité SnapLock**.
6. Enregistrez les modifications.
7. Dans la fenêtre **volumes**, sélectionnez le volume que vous avez mis à jour et choisissez **vue d'ensemble**.
8. Vérifiez que **SnapLock snapshot Copy Locking** affiche **enabled**.

## CLI

1. Pour créer un nouveau volume et activer le verrouillage des copies Snapshot, entrez la commande suivante :

```
volume create -vserver vs1 -volume vol1 -snapshot-locking-enabled true
```

La commande suivante permet de verrouiller les copies Snapshot sur un nouveau volume nommé vol1 :

```
> volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot-locking-enabled true
Warning: Snapshot copy locking is being enabled on volume "vol1" in Vserver "vs1". It cannot be disabled until all locked Snapshot copies are past their expiry time. A volume with unexpired locked Snapshot copies cannot be deleted.
Do you want to continue: {yes|no}: y
[Job 32] Job succeeded: Successful
```

## Activez le verrouillage des copies Snapshot sur un volume existant

Depuis la version ONTAP 9.12.1, vous pouvez activer le verrouillage des copies Snapshot sur un volume existant à l'aide de l'interface de ligne de commande ONTAP. Depuis ONTAP 9.13.1, vous pouvez utiliser System Manager pour activer le verrouillage des copies Snapshot sur un volume existant.



## System Manager

1. Accédez à **Storage > volumes**.
2. Sélectionnez  et choisissez **Modifier > Volume**.
3. Dans la fenêtre **Modifier le volume**, localisez la section Paramètres des copies Snapshot (local) et sélectionnez **Activer le verrouillage des instantanés**.

Cette sélection ne s'affiche pas si la licence SnapLock n'est pas installée.

4. S'il n'est pas déjà activé, sélectionnez **initialiser horloge de conformité SnapLock**.
5. Enregistrez les modifications.
6. Dans la fenêtre **volumes**, sélectionnez le volume que vous avez mis à jour et choisissez **vue d'ensemble**.
7. Vérifiez que **SnapLock snapshot Copy Locking** affiche **enabled**.

## CLI

1. Pour modifier un volume existant afin d'activer le verrouillage des copies Snapshot, entrez la commande suivante :

```
volume modify -vserver vserver_name -volume volume_name -snapshot-locking
-enabled true
```

## Créez une règle de copie Snapshot verrouillée et appliquez la conservation

Depuis ONTAP 9.12.1, vous pouvez créer des règles de copie Snapshot pour appliquer une période de conservation de copies Snapshot et appliquer la règle à un volume afin de verrouiller les copies Snapshot pour la période spécifiée. Vous pouvez également verrouiller une copie Snapshot en définissant manuellement une période de conservation. Depuis ONTAP 9.13.1, System Manager permet de créer des règles de verrouillage des copies Snapshot et de les appliquer à un volume.

### Créer une règle de verrouillage des copies Snapshot

## System Manager

1. Accédez à **Storage > Storage VM** et sélectionnez une VM de stockage.
2. Sélectionnez **Paramètres**.
3. Localisez **stratégies d'instantanés** et sélectionnez ➔.
4. Dans la fenêtre **Ajouter une stratégie d'instantanés**, entrez le nom de la stratégie.
5. Sélectionnez **+ Add**.
6. Fournissez les détails de la planification de la copie Snapshot, notamment le nom de la planification, le nombre maximal de copies Snapshot à conserver et la période de conservation SnapLock.
7. Dans la colonne **SnapLock Retention Period**, entrez le nombre d'heures, de jours, de mois ou d'années pour conserver les copies instantanées. Par exemple, une règle de copie Snapshot avec une période de conservation de 5 jours verrouille une copie Snapshot pendant 5 jours à compter de sa création. Elle ne peut pas être supprimée pendant cette période. Les périodes de conservation suivantes sont prises en charge :
  - Années: 0 - 100
  - Mois: 0 - 1200
  - Jours: 0 - 36500
  - Heures: 0 - 24
8. Enregistrez les modifications.

## CLI

1. Pour créer une règle de copie Snapshot, entrez la commande suivante :

```
volume snapshot policy create -policy policy_name -enabled true -schedule1
schedule1_name -count1 maximum_Snapshot_copies -retention-period1
_retention_period
```


La commande suivante crée une règle de verrouillage des copies Snapshot :

```
cluster1> volume snapshot policy create -policy policy_name -enabled
true -schedule1 hourly -count1 24 -retention-period1 "1 days"
```

Une copie Snapshot n'est pas remplacée si la conservation est active ; autrement dit, le nombre de conservation n'est pas respecté si des copies Snapshot verrouillées n'ont pas encore expiré.

## Application d'une politique de verrouillage à un volume

### System Manager

1. Accédez à **Storage > volumes**.
2. Sélectionnez  et choisissez **Modifier > Volume**.
3. Dans la fenêtre **Edit Volume**, sélectionnez **Schedule Snapshot copies**.
4. Sélectionnez la règle de verrouillage des copies Snapshot dans la liste.
5. Si le verrouillage des copies Snapshot n'est pas déjà activé, sélectionnez **Activer le verrouillage des instantanés**.
6. Enregistrez les modifications.

### CLI

1. Pour appliquer une règle de verrouillage des copies Snapshot à un volume existant, entrez la commande suivante :

```
volume modify -volume volume_name -vserver vserver_name -snapshot-policy policy_name
```

### Appliquez une période de conservation à la création manuelle de copies Snapshot

Vous pouvez appliquer une période de conservation des copies Snapshot lorsque vous créez manuellement une copie Snapshot. Le verrouillage des copies Snapshot doit être activé sur le volume ; sinon, le paramètre de période de conservation est ignoré.

## System Manager

1. Accédez à **stockage > volumes** et sélectionnez un volume.
2. Dans la page de détails du volume, sélectionnez l'onglet **copies Snapshot**.
3. Sélectionnez **+ Add**.
4. Indiquez le nom de la copie Snapshot et la date d'expiration du SnapLock. Vous pouvez sélectionner le calendrier pour choisir la date et l'heure d'expiration de la conservation.
5. Enregistrez les modifications.
6. Sur la page **volumes > copies instantanées**, sélectionnez **Afficher/Masquer** et choisissez **SnapLock expiration Time** pour afficher la colonne **SnapLock expiration Time** et vérifier que la durée de conservation est définie.

## CLI

1. Pour créer une copie Snapshot manuellement et appliquer une période de conservation de verrouillage, entrez la commande suivante :


```
volume snapshot create -volume volume_name -snapshot snapshot_copy_name
-snaplock-expiry-time expiration_date_time
```

La commande suivante crée une nouvelle copie Snapshot et définit la période de conservation :

```
cluster1> volume snapshot create -vserver vs1 -volume voll -snapshot
snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
```

## Appliquez une période de conservation à une copie Snapshot existante

## System Manager

1. Accédez à **stockage > volumes** et sélectionnez un volume.
2. Dans la page de détails du volume, sélectionnez l'onglet **copies Snapshot**.
3. Sélectionnez la copie snapshot, sélectionnez , puis choisissez **Modifier le délai d'expiration SnapLock**. Vous pouvez sélectionner le calendrier pour choisir la date et l'heure d'expiration de la conservation.
4. Enregistrez les modifications.
5. Sur la page **volumes > copies instantanées**, sélectionnez **Afficher/Masquer** et choisissez **SnapLock expiration Time** pour afficher la colonne **SnapLock expiration Time** et vérifier que la durée de conservation est définie.

## CLI

1. Pour appliquer manuellement une période de conservation à une copie Snapshot existante, entrez la commande suivante :

```
volume snapshot modify-snaplock-expiry-time -volume volume_name -snapshot snapshot_copy_name -expiry-time expiration_date_time
```

L'exemple suivant applique une période de conservation à une copie Snapshot existante :

```
cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
-snapshot snap2 -expiry-time "11/10/2022 09:00:00"
```

## Modifiez une stratégie existante pour appliquer la conservation à long terme

Depuis la version ONTAP 9.14.1, vous pouvez modifier une règle SnapMirror existante en ajoutant une règle afin de définir la conservation à long terme des copies Snapshot. La règle permet de remplacer la période de conservation par défaut du volume sur les destinations du coffre-fort SnapLock et sur les volumes de destination non SnapLock SnapMirror.

1. Ajouter une règle à une règle SnapMirror existante :

```
snapmirror policy add-rule -vserver <SVM name> -policy <policy name>
-snapmirror-label <label name> -keep <number of Snapshot copies> -retention
-period [<integer> days|months|years]
```

L'exemple suivant crée une règle qui applique une période de rétention de 6 mois à la stratégie existante appelée « lockvault » :

```
snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror
-label test1 -keep 10 -retention-period "6 months"
```

## Les API SnapLock

Vous pouvez utiliser les API Zephyr pour intégrer la fonctionnalité SnapLock dans les

scripts ou l'automatisation des flux de travail. Les API utilisent la messagerie XML via HTTP, HTTPS et Windows DCE/RPC. Pour plus d'informations, voir "[Documentation sur l'automatisation ONTAP](#)".

#### **abandon-empreinte-fichier**

Annuler une opération d'empreinte digitale de fichier.

#### **fichier-empreinte-dump**

Affiche les informations relatives aux empreintes digitales du fichier.

#### **fichier-empreinte-get-iter**

Affiche l'état des opérations d'empreinte des fichiers.

#### **démarrage de fichier-empreinte-fichier**

Générez une empreinte de fichier.

#### **snaplock-archive-vserver-log**

Archivez le fichier journal d'audit actif.

#### **snaplock-create-vserver-log**

Créer une configuration de journal d'audit pour un SVM.

#### **snaplock-delete-vserver-log**

Supprime une configuration du journal d'audit pour une SVM.

#### **snaplock-file-privileged-delete**

Exécutez une opération de suppression privilégiée.

#### **snaplock-get-file-retention**

Obtenir la période de conservation d'un fichier.

#### **snaplock-get-node-conformité-clock**

Obtenir la date et l'heure de la fin de l'horloge du nœud.

#### **snaplock-get-vserver-active-log-files-iter**

Affiche l'état des fichiers journaux actifs.

#### **snaplock-get-vserver-log-iter**

Afficher la configuration du journal d'audit.

### **snaplock-modify-vsriver-log**

Modifier la configuration du journal d'audit d'un SVM

### **snaplock-set-file-conservation**

Définissez la durée de conservation d'un fichier.

### **snaplock-set-node-compliance-clock**

Définissez la date et l'heure de la fin de l'horloge du nœud.

### **snaplock-volume-set-privileged-delete**

Définissez l'option Privileged-delete sur un volume SnapLock Enterprise.

### **volumes-get-snaplock-attrs**

Obtenir les attributs d'un volume SnapLock.

### **volume-set-snaplock-attrs**

Définissez les attributs d'un volume SnapLock.

## **Groupes de cohérence**

### **Présentation des groupes de cohérence**

Un groupe de cohérence est un ensemble de volumes gérés comme une seule unité. Dans ONTAP, les groupes de cohérence simplifient la gestion et garantissent la protection d'une charge de travail applicative couvrant plusieurs volumes.

Pour simplifier la gestion du stockage, vous pouvez utiliser des groupes de cohérence. Imaginez que vous disposez d'une base de données importante couvrant 20 LUN. Vous pouvez gérer les LUN de manière individuelle ou les traiter comme un jeu de données unique, les organiser au sein d'un même groupe de cohérence.

Les groupes de cohérence facilitent la gestion des charges de travail des applications en fournissant des règles de protection locales et distantes facilement configurées, ainsi que des copies Snapshot cohérentes au niveau des applications ou après panne d'un ensemble de volumes à un point dans le temps. Les copies Snapshot d'un groupe de cohérence permettent de restaurer l'ensemble d'une charge de travail applicative.

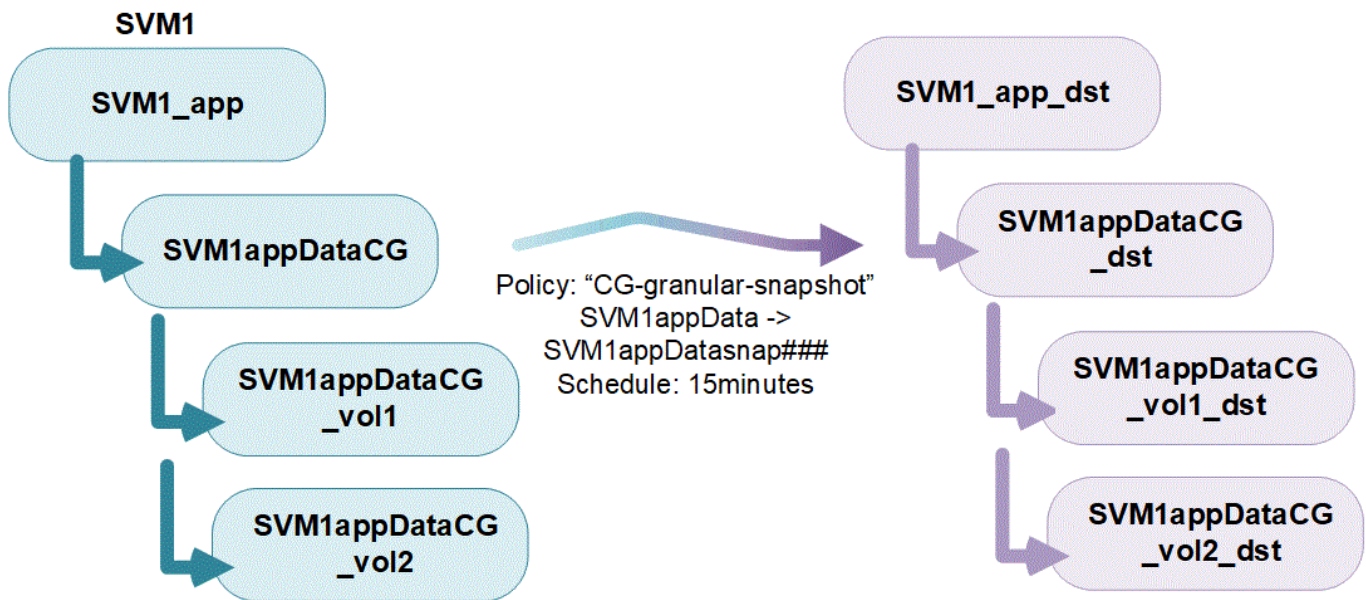
### **En savoir plus sur les groupes de cohérence**

Les groupes de cohérence prennent en charge n'importe quel volume FlexVol, quel que soit le protocole (NAS, SAN ou NVMe). Ils peuvent être gérés via l'API REST de ONTAP ou dans System Manager, dans l'élément de menu **stockage > groupes de cohérence**. Depuis la version ONTAP 9.14.1, la gestion des groupes de cohérence peut s'effectuer via l'interface de ligne de commandes ONTAP.

Les groupes de cohérence peuvent exister sous la forme d'entités individuelles, sous la forme d'un ensemble de volumes, ou dans une relation hiérarchique constituée d'autres groupes de cohérence. Les volumes individuels peuvent disposer de leur propre règle Snapshot granulaire par volume. En outre, des règles Snapshot peuvent être définies au niveau du groupe de cohérence. Le groupe de cohérence ne peut avoir

qu'une relation de synchronisation active SnapMirror et une règle SnapMirror partagée, qui peuvent être utilisées pour restaurer l'ensemble du groupe de cohérence.

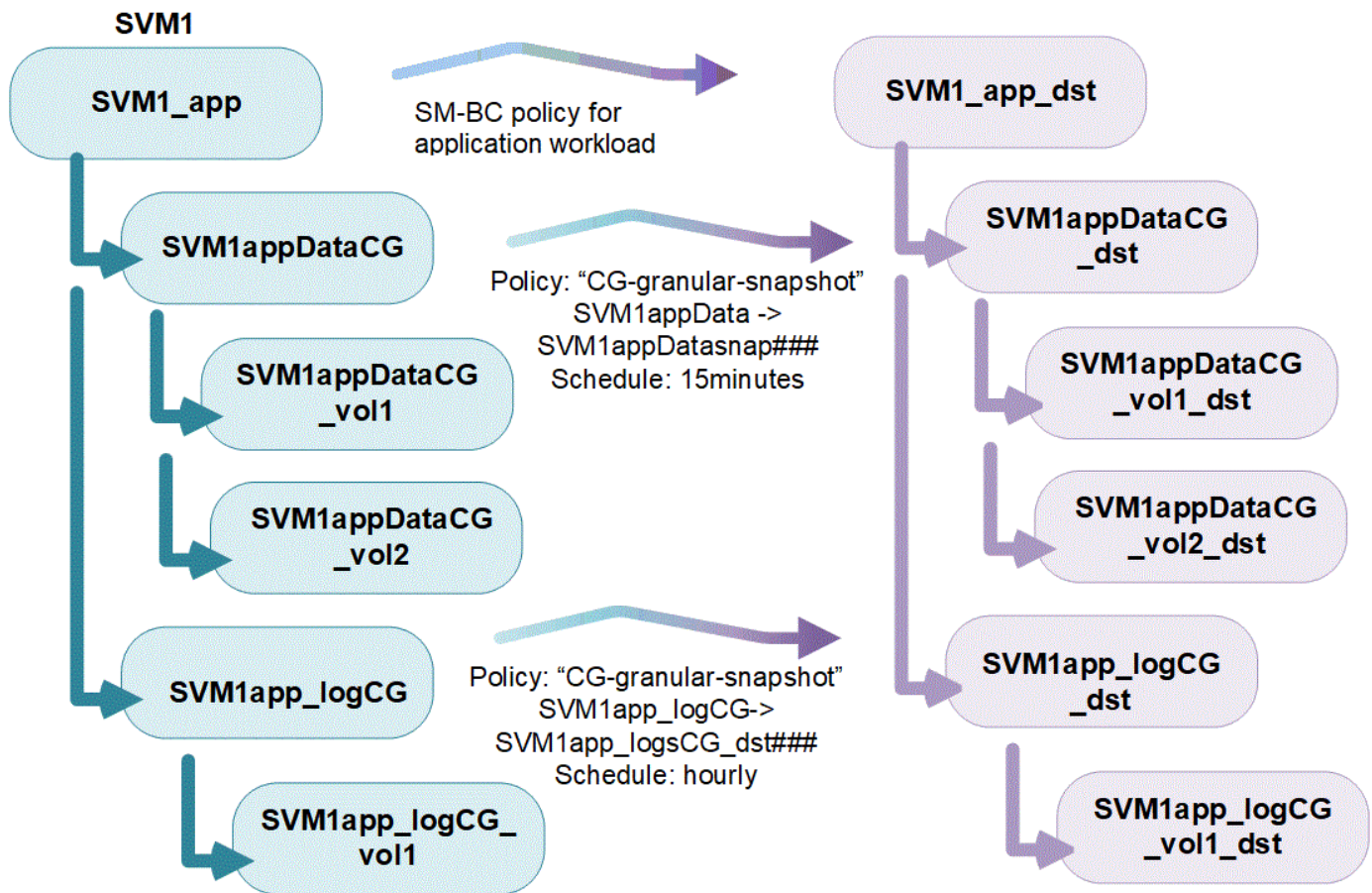
Le graphique suivant illustre l'utilisation possible d'un groupe de cohérence individuel. Données d'une application hébergée sur SVM1 s'étend sur deux volumes : vol1 et vol2. Une règle Snapshot définie sur le groupe de cohérence capture des copies Snapshot des données toutes les 15 minutes.



Des charges de travail applicatives plus importantes peuvent nécessiter plusieurs groupes de cohérence. Dans ce cas, vous pouvez créer des groupes de cohérence hiérarchiques, où un seul groupe de cohérence devient les composants enfants d'un groupe de cohérence parent. Le groupe de cohérence parent peut inclure au maximum cinq groupes de cohérence enfant. Comme dans les groupes de cohérence individuels, une règle de protection de synchronisation active SnapMirror distante peut être appliquée à l'ensemble de la configuration des groupes de cohérence (parents et enfants) afin de restaurer la charge de travail de l'application.

Dans l'exemple suivant, une application est hébergée sur SVM1. L'administrateur a créé un groupe de cohérence parent, SVM1\_app, qui inclut deux groupes de cohérence enfant : SVM1appDataCG pour les données et SVM1app\_logCG pour les journaux. Chaque groupe de cohérence enfant dispose de sa propre règle Snapshot. Copies Snapshot des volumes dans SVM1appDataCG sont prises toutes les 15 minutes. Snapshots de SVM1app\_logCG sont prises toutes les heures. Groupe de cohérence parent SVM1\_app Dispose d'une règle de synchronisation active SnapMirror qui réplique les données pour assurer la continuité de service en cas d'incident.





Depuis la version ONTAP 9.12.1, les groupes de coh rence sont pris en charge [clonage](#) et en modifiant les membres de la coh rence par [ajout ou suppression de volumes](#). Dans System Manager et dans l'API REST de ONTAP. Depuis la version ONTAP 9.12.1, l'API REST ONTAP prend  galement en charge :

- Cr ation de groupes de coh rence avec de nouveaux volumes NFS ou SMB ou espaces de noms NVMe.
- Ajout de volumes NFS ou SMB ou d'espaces de noms NVMe nouveaux ou existants   des groupes de coh rence existants.

Pour plus d'informations sur l'API REST de ONTAP, reportez-vous   ["Documentation de r f rence de l'API REST ONTAP"](#).

## Surveillez les groupes de coh rence

  partir de la version ONTAP 9.13.1, les groupes de coh rence assurent le contr le de la capacit  et des performances en temps r el et historiques, offrant ainsi un aper u des performances des applications et des groupes de coh rence individuels.

Les donn es de surveillance sont actualis es toutes les cinq minutes et sont conserv es jusqu'  un an. Vous pouvez suivre les mesures pour :

- Performances : IOPS, latence et d bit
- Capacit  : taille, logique utilis e, disponible

Vous pouvez afficher les donn es de surveillance dans l'onglet **Pr sentation** du menu Groupe de coh rence dans System Manager ou en les demandant dans l'API REST. Depuis la version ONTAP 9.14.1, vous pouvez afficher les metrics des groupes de coh rence via l'interface de ligne de commandes du syst me

consistency-group metrics show commande.



Dans ONTAP 9.13.1, vous pouvez uniquement récupérer les metrics historiques à l'aide de l'API REST. Depuis la version ONTAP 9.14.1, les indicateurs d'historique sont également disponibles dans System Manager.

## Protégez les groupes de cohérence

Les groupes de cohérence assurent une protection cohérente au niveau des applications, assurant la cohérence de vos données sur plusieurs volumes ou LIF. Lors de la création d'une copie Snapshot d'un groupe de cohérence, une « clôture » est établie sur le groupe de cohérence. Le périmètre lance une file d'attente pour les E/S jusqu'à la fin de l'opération Snapshot, garantissant ainsi la cohérence des données à un point dans le temps entre toutes les entités du groupe de cohérence. Cette barrière peut provoquer un pic passager de latence lors des opérations de création de snapshots, par exemple une règle Snapshot planifiée ou la création d'un Snapshot avec System Manager. Pour plus d'informations dans le cadre de l'API REST et de l'interface de ligne de commandes, reportez-vous à la documentation de l'API REST ONTAP et à la page de manuel de l'interface de ligne de commandes.

La protection est assurée par des groupes de cohérence :

- Règles relatives aux snapshots
- [Synchronisation active SnapMirror](#)
- [\[mcc\]](#) (À partir de ONTAP 9.11.1)
- [Réplication asynchrone SnapMirror](#) (À partir de ONTAP 9.13.1)
- ["Reprise d'activité de SVM"](#) (À partir de ONTAP 9.14.1)

La création d'un groupe de cohérence n'active pas automatiquement la protection. Il est possible de définir des règles de protection locale et à distance lors de la création ou après la création d'un groupe de cohérence.

Pour configurer la protection sur un groupe de cohérence, reportez-vous à la section "[Protéger un groupe de cohérence](#)".

Pour utiliser la protection à distance, vous devez répondre aux exigences de [Synchronisation active SnapMirror](#).



Les relations de synchronisation active SnapMirror ne peuvent pas être établies sur les volumes montés pour l'accès NAS.

## Groupes de cohérence dans les configurations MetroCluster

Depuis ONTAP 9.11.1, vous pouvez provisionner les groupes de cohérence avec de nouveaux volumes sur un cluster dans une configuration MetroCluster. Ces volumes sont provisionnés sur des agrégats en miroir.

Une fois ces agrégats provisionnés, vous pouvez déplacer les volumes associés aux groupes de cohérence entre les agrégats en miroir et non mis en miroir. Les volumes associés à des groupes de cohérence peuvent donc être situés sur des agrégats en miroir, des agrégats sans mise en miroir, ou les deux. Vous pouvez modifier les agrégats en miroir contenant des volumes associés à des groupes de cohérence pour ne plus mettre en miroir. De même, vous pouvez modifier les agrégats non mis en miroir contenant les volumes associés à des groupes de cohérence pour activer la mise en miroir.

Les volumes et les copies Snapshot associés aux groupes de cohérence placés sur des agrégats en miroir sont répliqués sur le site distant (site B). Le contenu des volumes sur le site B garantit l'ordre d'écriture du

groupe de cohérence, ce qui vous permet d'effectuer une restauration depuis le site B en cas d'incident. Vous pouvez accéder aux copies Snapshot de groupe de cohérence à l'aide du groupe de cohérence avec l'API REST et System Manager sur les clusters exécutant ONTAP 9.11.1 ou version ultérieure. Depuis la version ONTAP 9.14.1, vous pouvez également accéder aux copies Snapshot via l'interface de ligne de commandes ONTAP.

Si certains ou l'ensemble des volumes associés à un groupe de cohérence se trouvent sur des agrégats non mis en miroir qui ne sont pas actuellement accessibles, LES opérations D'OBTENTION ou DE SUPPRESSION du groupe de cohérence se comportent comme si les volumes locaux ou les agrégats d'hébergement sont hors ligne.

### Configurations de groupes de cohérence pour la réplication

Si le site B exécute ONTAP 9.10.1 ou une version antérieure, seuls les volumes associés aux groupes de cohérence situés sur les agrégats en miroir sont répliqués sur le site B. Les configurations de groupes de cohérence sont uniquement répliquées vers le site B, si les deux sites exécutent ONTAP 9.11.1 ou une version ultérieure. Une fois le site B mis à niveau vers ONTAP 9.11.1, les données destinées aux groupes de cohérence du site A où tous leurs volumes associés sont répliqués sur le site B.



Pour optimiser les performances et la disponibilité du stockage, il est recommandé de conserver au moins 20 % d'espace libre pour les agrégats en miroir. Bien que la recommandation soit de 10 % pour les agrégats non mis en miroir, le système de fichiers peut utiliser 10 % d'espace supplémentaire pour absorber les modifications incrémentielles. Les modifications incrémentielles augmentent l'utilisation de l'espace pour les agrégats en miroir grâce à l'architecture Snapshot d'ONTAP basée sur la copie en écriture. Le non-respect de ces meilleures pratiques peut avoir un impact négatif sur les performances.

### Mise à niveau

Lors de la mise à niveau vers ONTAP 9.10.1 ou une version ultérieure, les groupes de persistance créés avec la synchronisation active SnapMirror (précédemment appelée SnapMirror Business Continuity) dans ONTAP 9.8 et 9.9.1 sont automatiquement mis à niveau et deviennent gérables sous **stockage > groupes de cohérence** dans System Manager ou l'API REST ONTAP pour plus d'informations sur la mise à niveau à partir de ONTAP 9.8 ou 9.9.1, voir ["Considérations relatives à la mise à niveau et à la restauration de la synchronisation active SnapMirror"](#).

Les copies Snapshot de groupe de cohérence créées dans l'API REST peuvent être gérées via l'interface de groupe de cohérence de System Manager et via les terminaux d'API REST de groupe de cohérence. Depuis la version ONTAP 9.14.1, les snapshots des groupes de cohérence peuvent également être gérés à l'aide de l'interface de ligne de commandes ONTAP.



Copies Snapshot créées à l'aide des commandes ONTAPI `cg-start` et `cg-commit` Sont reconnues comme des copies Snapshot de groupe de cohérence et ne peuvent donc pas être gérées via l'interface de groupe de cohérence de System Manager ou les terminaux de groupe de cohérence de l'API REST ONTAP. Depuis la version ONTAP 9.14.1, ces copies Snapshot peuvent être mises en miroir sur le volume de destination si vous utilisez une règle asynchrone SnapMirror. Pour plus d'informations, voir [Configurer SnapMirror asynchrone](#).

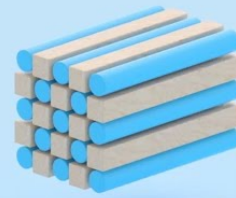
### Fonctionnalités prises en charge par version

|                                                                     | ONTAP<br>9.15.1 | ONTAP<br>9.14.1 | ONTAP<br>9.13.1 | ONTAP<br>9.12.1     | ONTAP<br>9.11.1 | ONTAP<br>9.10.1 |
|---------------------------------------------------------------------|-----------------|-----------------|-----------------|---------------------|-----------------|-----------------|
| Groupes de cohérence hiérarchiques                                  | ✓               | ✓               | ✓               | ✓                   | ✓               | ✓               |
| Protection locale grâce aux copies Snapshot                         | ✓               | ✓               | ✓               | ✓                   | ✓               | ✓               |
| Synchronisation active SnapMirror                                   | ✓               | ✓               | ✓               | ✓                   | ✓               | ✓               |
| Prise en charge de MetroCluster                                     | ✓               | ✓               | ✓               | ✓                   | ✓               |                 |
| Validations en deux phases (API REST uniquement)                    | ✓               | ✓               | ✓               | ✓                   | ✓               |                 |
| Balises d'application et de composant                               | ✓               | ✓               | ✓               | ✓                   |                 |                 |
| Cloner des groupes de cohérence                                     | ✓               | ✓               | ✓               | ✓                   |                 |                 |
| Ajouter et supprimer des volumes                                    | ✓               | ✓               | ✓               | ✓                   |                 |                 |
| Créez un CGS avec de nouveaux volumes NAS                           | ✓               | ✓               | ✓               | API REST uniquement |                 |                 |
| Créez un CGS avec les nouveaux espaces de noms NVMe                 | ✓               | ✓               | ✓               | API REST uniquement |                 |                 |
| Déplacez des volumes entre des groupes de cohérence enfants         | ✓               | ✓               | ✓               |                     |                 |                 |
| Modifier la géométrie du groupe de cohérence                        | ✓               | ✓               | ✓               |                     |                 |                 |
| Contrôle                                                            | ✓               | ✓               | ✓               |                     |                 |                 |
| SnapMirror asynchrone (groupes de cohérence uniques uniquement)     | ✓               | ✓               | ✓               |                     |                 |                 |
| Reprise d'activité de SVM (groupes de cohérence uniques uniquement) | ✓               | ✓               |                 |                     |                 |                 |
| Prise en charge de la CLI                                           | ✓               | ✓               |                 |                     |                 |                 |

## En savoir plus sur les groupes de cohérence

# Consistency Groups for Application Management & Protection

With NetApp ONTAP 9.10.1 + System Manager



© 2022 NetApp, Inc. All rights reserved.

## Plus d'informations

- ["Documentation sur l'automatisation ONTAP"](#)
- [Synchronisation active SnapMirror](#)
- [Notions de base sur la reprise après incident asynchrone SnapMirror](#)
- ["Documentation MetroCluster"](#)

## Limites des groupes de cohérence

Lors de la planification et de la gestion de vos groupes de cohérence, prenez en compte les limites d'objets au sein du cluster et du groupe de cohérence parent ou enfant.

### Limites imposées

Le tableau suivant indique les limites des groupes de cohérence. Des limites séparées s'appliquent aux groupes de cohérence qui utilisent la synchronisation active SnapMirror. Pour plus d'informations, voir ["Limites de synchronisation active SnapMirror"](#).

| Limite                                | Portée  | Minimum | Maximum                                                 |
|---------------------------------------|---------|---------|---------------------------------------------------------|
| Nombre de groupes de cohérence        | Cluster | 0       | Identique au nombre maximal de volumes dans le cluster* |
| Nombre de groupes de cohérence parent | Cluster | 0       | Identique au nombre maximum de volumes dans le cluster  |

|                                                                                                                       |                            |                       |                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------|----------------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nombre de groupes de cohérence individuels et parents                                                                 | Cluster                    | 0                     | Identique au nombre maximum de volumes dans le cluster                                                                                                         |
| Nombre de volumes dans un groupe de cohérence                                                                         | Groupe de cohérence unique | 1 volume              | 80 volumes                                                                                                                                                     |
| Nombre de volumes dans un groupe de cohérence avec SnapMirror asynchrone                                              | Groupe de cohérence unique | 1 volume              | <ul style="list-style-type: none"> <li>• Dans ONTAP 9.15.1 et versions ultérieures : 80 volumes</li> <li>• Dans ONTAP 9.13.1 et 9.14.1 : 16 volumes</li> </ul> |
| Nombre de volumes dans l'enfant d'un groupe de cohérence parent                                                       | Groupe de cohérence parent | 1 volume              | 80 volumes                                                                                                                                                     |
| Nombre de volumes dans un groupe de cohérence enfant                                                                  | Groupe de cohérence enfant | 1 volume              | 80 volumes                                                                                                                                                     |
| Nombre de groupes de cohérence enfants dans un groupe de cohérence parent                                             | Groupe de cohérence parent | 1 groupe de cohérence | 5 groupes de cohérence                                                                                                                                         |
| Nombre de relations de reprise d'activité du SVM où existe un groupe de cohérence (disponible depuis la ONTAP 9.14.1) | Cluster                    | 0                     | 32                                                                                                                                                             |

\* Un maximum de 50 groupes de cohérence activés avec SnapMirror asynchrone peuvent être hébergés sur un cluster.

### Limites non appliquées

La planification minimale prise en charge des copies Snapshot pour les groupes de cohérence est de 30 minutes. Cela est basé sur "[Test des FlexGroups](#)", Qui partagent la même infrastructure Snapshot que les groupes de cohérence.

## Configurez un seul groupe de cohérence

Les groupes de cohérence peuvent être créés avec des volumes existants ou de nouveaux LUN ou volumes (selon la version de ONTAP). Un volume ou une LUN ne peut être associé qu'à un seul groupe de cohérence à la fois.

### Description de la tâche

- Dans les ONTAP 9.10.1 à 9.11.1, la modification des volumes membres d'un groupe de cohérence après sa création n'est pas prise en charge.

Depuis la version ONTAP 9.12.1, vous pouvez modifier les volumes membres d'un groupe de cohérence. Pour plus d'informations sur ce processus, reportez-vous à la section [Modifier un groupe de cohérence](#).

## **Créez un groupe de cohérence avec les nouvelles LUN ou les nouveaux volumes**

Dans ONTAP 9.10.1 à 9.12.1, vous pouvez créer un groupe de cohérence à l'aide de nouvelles LUN. Depuis ONTAP 9.13.1, System Manager prend également en charge la création d'un groupe de cohérence avec de nouveaux namespaces NVMe ou de nouveaux volumes NAS. (Ceci est également pris en charge par l'API REST ONTAP à partir de ONTAP 9.12.1.)



## System Manager

### Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez **+Add**, puis sélectionnez le protocole de votre objet de stockage.

Dans ONTAP 9.10.1 à 9.12.1, la seule option pour un nouvel objet de stockage est **en utilisant de nouvelles LUN**. Depuis ONTAP 9.13.1, System Manager prend en charge la création de groupes de cohérence avec de nouveaux namespaces NVMe et de nouveaux volumes NAS.

3. Nommer le groupe de cohérence. Indiquez le nombre de volumes ou de LUN et la capacité par volume ou LUN.
  - a. **Type d'application** : si vous utilisez ONTAP 9.12.1 ou version ultérieure, sélectionnez un type d'application. Si aucune valeur n'est sélectionnée, le groupe de cohérence se voit attribuer le type de **autre** par défaut. En savoir plus sur la cohérence du balisage dans [Balises d'application et de composant](#). Si vous prévoyez de créer un groupe de cohérence avec une stratégie de protection à distance, vous devez utiliser **Other**.
  - b. Pour **nouveaux LUN** : sélectionnez le système d'exploitation hôte et le format de LUN. Entrez les informations sur l'initiateur hôte.
  - c. Pour **nouveaux volumes NAS** : choisissez l'option d'exportation appropriée (NFS ou SMB/CIFS) en fonction de la configuration NAS de votre SVM.
  - d. Pour **nouveaux espaces de noms NVMe** : sélectionnez le système d'exploitation hôte et le sous-système NVMe.
4. Pour configurer des stratégies de protection, ajoutez un groupe de cohérence enfant ou des autorisations d'accès, sélectionnez **plus d'options**.
5. Sélectionnez **Enregistrer**.
6. Vérifiez que votre groupe de cohérence a été créé en retournant au menu principal du groupe de cohérence sur lequel il apparaîtra une fois le travail terminé. Si vous définissez une stratégie de protection, vous savez qu'elle a été appliquée lorsque vous voyez un bouclier vert sous regarder sous la stratégie appropriée, distant ou local.

### CLI

À partir de la version ONTAP 9.14.1, vous pouvez créer un groupe de cohérence avec les nouveaux volumes via l'interface de ligne de commandes ONTAP. Les paramètres spécifiques dépendent si les volumes sont SAN, NVMe ou NFS.

#### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

#### Créez un groupe de cohérence avec les volumes NFS

1. Créer le groupe de cohérence :

```
consistency-group create -vserver SVM_name -consistency-group consistency-group-name -volume volume-prefix -volume-count number -size size -export-policy policy_name
```

#### Créez un groupe de cohérence avec des volumes SAN



### 1. Créer le groupe de cohérence :

```
consistency-group create -vserver SVM_name -consistency-group consistency-group-name -lun lun_name -size size -lun-count number -igroup igroup_name
```

### Créez un groupe de cohérence avec les namespaces NVMe

#### 1. Créer le groupe de cohérence :

```
consistency-group create -vserver SVM_name -consistency-group consistency_group_name -namespace namespace_name -volume-count number -namespace-count number -size size -subsystem subsystem_name
```

### Après avoir terminé

1. Vérifiez que votre groupe de cohérence a été créé à l'aide de `consistency-group show` commande.

### Créez un groupe de cohérence avec les volumes existants

Vous pouvez utiliser des volumes existants pour créer un groupe de cohérence.

## System Manager

### Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez **+Ajouter** puis **en utilisant des volumes existants**.
3. Nommez le groupe de cohérence et sélectionnez la VM de stockage.
  - a. **Type d'application** : si vous utilisez ONTAP 9.12.1 ou version ultérieure, sélectionnez un type d'application. Si aucune valeur n'est sélectionnée, le groupe de cohérence se voit attribuer le type de **autre** par défaut. En savoir plus sur la cohérence du balisage dans [Balises d'application et de composant](#). Si le groupe de cohérence possède une relation de synchronisation active SnapMirror, vous devez utiliser **Other**.



Dans les versions de ONTAP antérieures à ONTAP 9.15.1, la synchronisation active SnapMirror est appelée SnapMirror Business Continuity.

4. Sélectionnez les volumes existants à inclure. Seuls les volumes qui ne font pas déjà partie d'un groupe de cohérence seront disponibles à la sélection.



Si vous créez un groupe de cohérence avec des volumes existants, le groupe de cohérence prend en charge les volumes FlexVol. Les volumes avec ou relations SnapMirror synchrones ou asynchrones peuvent être ajoutés aux groupes de cohérence, mais ils ne tiennent pas compte des groupes de cohérence. Les groupes de cohérence ne prennent pas en charge les compartiments S3 ni les machines virtuelles de stockage avec des relations SVMDR.

5. Sélectionnez **Enregistrer**.
6. Vérifiez que votre groupe de cohérence a été créé en retournant au menu principal du groupe de cohérence qui s'affiche une fois la tâche ONTAP terminée. Si vous avez choisi une règle de protection, vérifiez qu'elle a été correctement définie en sélectionnant votre groupe de cohérence dans le menu. Si vous définissez une stratégie de protection, vous savez qu'elle a été appliquée lorsque vous voyez un bouclier vert sous regarder sous la stratégie appropriée, distant ou local.

### CLI

Depuis la version ONTAP 9.14.1, vous pouvez créer un groupe de cohérence avec les volumes existants à l'aide de l'interface de ligne de commandes ONTAP.

### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

### Étapes

1. Émettez le `consistency-group create` commande. Le `-volumes` le paramètre accepte une liste de noms de volumes séparés par des virgules.

```
consistency-group create -vserver SVM_name -consistency-group consistency-group-name -volume volumes
```

2. Affichez votre groupe de cohérence à l'aide du `consistency-group show` commande.

## Étapes suivantes

- [Protéger un groupe de cohérence](#)
- [Modifier un groupe de cohérence](#)
- [Cloner un groupe de cohérence](#)

## Configurez un groupe de cohérence hiérarchique

Les groupes de cohérence hiérarchiques vous permettent de gérer des charges de travail volumineuses couvrant plusieurs volumes. En effet, vous créez un groupe de cohérence parent qui sert de parapluie pour les groupes de cohérence enfant.

Les groupes de cohérence hiérarchiques ont un parent qui peut inclure jusqu'à cinq groupes de cohérence individuels. Les groupes de cohérence hiérarchiques peuvent prendre en charge différentes règles Snapshot locales sur plusieurs groupes de cohérence ou volumes individuels. Si vous utilisez une règle de protection à distance, elle s'applique à l'ensemble du groupe de cohérence hiérarchique (parent et enfant).

À partir de ONTAP 9.13.1, vous pouvez [modifier la géométrie de vos groupes de cohérence](#) et [déplacez des volumes entre des groupes de cohérence enfants](#).

Pour connaître les limites d'objets relatives aux groupes de cohérence, reportez-vous à la section [Limites d'objets pour les groupes de cohérence](#).

## Créez un groupe de cohérence hiérarchique avec de nouveaux LUN ou volumes

Lorsque vous créez un groupe de cohérence hiérarchique, vous pouvez le remplir avec de nouvelles LUN. Depuis la version ONTAP 9.13.1, vous pouvez également utiliser de nouveaux espaces de noms NVMe et volumes NAS.

## System Manager

### Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez **+Add**, puis sélectionnez le protocole de votre objet de stockage.

Dans ONTAP 9.10.1 à 9.12.1, la seule option pour un nouvel objet de stockage est **en utilisant de nouvelles LUN**. Depuis ONTAP 9.13.1, System Manager prend en charge la création de groupes de cohérence avec de nouveaux namespaces NVMe et de nouveaux volumes NAS.

3. Nommer le groupe de cohérence. Indiquez le nombre de volumes ou de LUN et la capacité par volume ou LUN.
  - a. **Type d'application** : si vous utilisez ONTAP 9.12.1 ou version ultérieure, sélectionnez un type d'application. Si aucune valeur n'est sélectionnée, le groupe de cohérence se voit attribuer le type de **autre** par défaut. En savoir plus sur la cohérence du balisage dans [Balises d'application et de composant](#). Si vous prévoyez d'utiliser une stratégie de protection à distance, vous devez choisir **autre**.
4. Sélectionnez le système d'exploitation hôte et le format LUN. Entrez les informations sur l'initiateur hôte.
  - a. Pour **nouveaux LUN** : sélectionnez le système d'exploitation hôte et le format de LUN. Entrez les informations sur l'initiateur hôte.
  - b. Pour **nouveaux volumes NAS** : choisissez l'option d'exportation appropriée (NFS ou SMB/CIFS) en fonction de la configuration NAS de votre SVM.
  - c. Pour **nouveaux espaces de noms NVMe** : sélectionnez le système d'exploitation hôte et le sous-système NVMe.
5. Pour ajouter un groupe de cohérence enfant, sélectionnez **plus d'options** puis **+Ajouter un groupe de cohérence enfant**.
6. Sélectionnez le niveau de performance, le nombre de LUN ou de volumes et la capacité par LUN ou volume. Indiquez les configurations d'exportation ou les informations du système d'exploitation appropriées en fonction du protocole que vous utilisez.
7. Vous pouvez également sélectionner une stratégie de snapshot locale et définir les autorisations d'accès.
8. Répétez l'opération pour jusqu'à cinq groupes de cohérence enfant.
9. Sélectionnez **Enregistrer**.
10. Vérifiez que votre groupe de cohérence a été créé en retournant au menu principal du groupe de cohérence sur lequel il apparaîtra une fois le travail ONTAP terminé. Si vous définissez une stratégie de protection, examinez la stratégie appropriée, à distance ou locale, qui doit afficher un bouclier vert avec une coche.

### CLI

#### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

### Étape

1. Créez le nouveau groupe de cohérence à l'aide de `consistency-group create` commande.

Le `volume-count` le paramètre définit le nombre de volumes de chaque groupe de cohérence enfant. Vous pouvez créer un groupe de cohérence parent avec un maximum de cinq groupes de cohérence enfant.

```
consistency-group create -vserver SVM_name -consistency-group
consistency_group_name -parent-consistency-group
parent_consistency_group_name -cg-count number_of_child_consistency_groups
-volume volume_prefix -volume-count number -size size -export-policy
policy_name -storage-service extreme
```

### Créez un groupe de cohérence hiérarchique avec les volumes existants

Vous pouvez organiser des volumes existants en un groupe de cohérence hiérarchique.

## System Manager

### Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez **+Ajouter** puis **en utilisant des volumes existants**.
3. Sélectionnez la VM de stockage.
4. Sélectionnez les volumes existants à inclure. Seuls les volumes qui ne font pas déjà partie d'un groupe de cohérence seront disponibles à la sélection.
5. Pour ajouter un groupe de cohérence enfant, sélectionnez **+Ajouter un groupe de cohérence enfant**. Créez les groupes de cohérence nécessaires, qui seront nommés automatiquement.
  - a. **Type de composant** : si vous utilisez ONTAP 9.12.1 ou version ultérieure, sélectionnez un type de composant "données", "logs" ou "autre". Si aucune valeur n'est sélectionnée, le groupe de cohérence se voit attribuer le type de **autre** par défaut. En savoir plus sur la cohérence du balisage dans [Balises d'application et de composant](#). Si vous prévoyez d'utiliser une stratégie de protection à distance, vous devez utiliser **autre**.
6. Attribuez des volumes existants à chaque groupe de cohérence.
7. Si vous le souhaitez, sélectionnez une règle Snapshot locale.
8. Répétez l'opération pour jusqu'à cinq groupes de cohérence enfant.
9. Sélectionnez **Enregistrer**.
10. Vérifiez que votre groupe de cohérence a été créé en retournant au menu principal du groupe de cohérence sur lequel il apparaîtra une fois le travail ONTAP terminé. Si vous avez choisi une stratégie de protection, vérifiez qu'elle a été correctement définie en sélectionnant votre groupe de cohérence dans le menu ; sous le type de stratégie approprié, vous verrez un bouclier vert avec une coche à l'intérieur de celle-ci.

### CLI

Depuis la version ONTAP 9.14.1, vous pouvez créer un groupe de cohérence hiérarchique à l'aide de l'interface de ligne de commandes.

### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

### Étapes

1. Provisionner un nouveau groupe de cohérence parent et attribuer des volumes à un nouveau groupe de cohérence enfant :

```
consistency-group create -vserver svm_name -consistency-group
child_consistency_group_name -parent-consistency-group
parent_consistency_group_name -volumes volume_names
```

2. Entrez **y** pour confirmer la création d'un groupe de cohérence parent et enfant.

### Étapes suivantes

- [Modifier la géométrie d'un groupe de cohérence](#)

- [Modifier un groupe de cohérence](#)
- [Protéger un groupe de cohérence](#)

## Protégez les groupes de cohérence

Les groupes de cohérence offrent une protection locale et à distance simple à gérer pour les applications SAN, NAS et NVMe couvrant plusieurs volumes.

La création d'un groupe de cohérence n'active pas automatiquement la protection. Les règles de protection peuvent être définies au moment de la création ou après la création du groupe de cohérence. Vous pouvez protéger les groupes de cohérence à l'aide des éléments suivants :

- Copies Snapshot locales
- Synchronisation active SnapMirror (appelée SnapMirror Business Continuity dans les versions de ONTAP d'avant 9.15.1)
- [MetroCluster \(début 9.11.1\)](#)
- SnapMirror asynchrone (début 9.13.1)
- Reprise d'activité asynchrone d'un SVM (début 9.14.1)

Si vous utilisez des groupes de cohérence imbriqués, vous pouvez définir différentes règles de protection pour les groupes de cohérence parent et enfant.

À partir de la version ONTAP 9.11.1, les groupes de cohérence proposent [Création de copies Snapshot de groupe de cohérence en deux phases](#). L'opération Snapshot en deux phases exécute un pré-contrôle, en s'assurant que la copie Snapshot est correctement capturée.

La restauration peut être effectuée pour un groupe de cohérence entier, un seul groupe de cohérence dans une configuration hiérarchique ou pour des volumes individuels dans un groupe de cohérence. La restauration peut être effectuée en sélectionnant le groupe de cohérence à partir duquel vous souhaitez effectuer une restauration, en sélectionnant le type de copie Snapshot, puis en identifiant la copie Snapshot pour laquelle repose la restauration. Pour plus d'informations sur ce processus, voir "[Restaurez un volume à partir d'une copie Snapshot antérieure](#)".

### Configurer une règle Snapshot locale


La définition d'une règle de protection locale des snapshots permet de créer une stratégie couvrant tous les volumes d'un groupe de cohérence.

#### Description de la tâche

La planification minimale prise en charge des copies Snapshot pour les groupes de cohérence est de 30 minutes. Cela est basé sur "[Test des FlexGroups](#)", Qui partagent la même infrastructure Snapshot que les groupes de cohérence.

## System Manager

### Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence que vous avez créé dans le menu Groupe de cohérence.
3. Dans le coin supérieur droit de la page de vue d'ensemble du groupe de cohérence, sélectionnez **Modifier**.
4. Cochez la case en regard de **planifier les copies Snapshot (locales)**.
5. Sélectionnez une règle Snapshot. Pour configurer une nouvelle règle personnalisée, reportez-vous à la section "[Création d'une règle de protection des données personnalisée](#)".
6. Sélectionnez **Enregistrer**.
7. Revenez au menu de présentation du groupe de cohérence. Dans la colonne de gauche sous **copies Snapshot (local)**, l'état indique protégé en regard de .

### CLI

Depuis la version ONTAP 9.14.1, vous pouvez modifier la règle de protection d'un groupe de cohérence à l'aide de l'interface de ligne de commandes.

#### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

### Étape

1. Exécutez la commande suivante pour définir ou modifier la règle de protection :

Si vous modifiez la règle de protection d'une cohérence enfant, vous devez identifier le groupe de cohérence parent à l'aide de `-parent-consistency-group` *parent\_consistency\_group\_name* paramètre.

```
consistency-group modify -vserver svm_name -consistency-group
consistency_group_name -snapshot-policy policy_name
```

## Créer une copie Snapshot à la demande

Si vous devez créer une copie Snapshot de votre groupe de cohérence en dehors d'une règle normalement planifiée, vous pouvez en créer une à la demande.



## System Manager

### Étapes

1. Accédez à **Storage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence pour lequel vous souhaitez créer une copie Snapshot à la demande.
3. Passez à l'onglet **copies instantanées**, puis sélectionnez **+Ajouter**.
4. Indiquez un **Nom** et un **libellé SnapMirror**. Dans le menu déroulant **cohérence**, sélectionnez **cohérence application** ou **cohérence collision**.
5. Sélectionnez **Enregistrer**.

### CLI

Depuis la version ONTAP 9.14.1, vous pouvez créer une copie Snapshot à la demande d'un groupe de cohérence à l'aide de l'interface de ligne de commandes.

### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

### Étape

1. Créer la copie Snapshot :

Par défaut, le type de Snapshot est cohérent après panne. Vous pouvez modifier le type de snapshot avec l'option `-type` paramètre.

```
consistency-group snapshot create -vserver svm_name -consistency-group
consistency_group_name -snapshot snapshot_name
```

## Créez des copies Snapshot de groupe de cohérence en deux phases

Depuis la version ONTAP 9.11.1, les groupes de cohérence prennent en charge les validations en deux phases pour la création des copies Snapshot de groupe de cohérence, qui exécutent un précontrôle avant la validation de la copie Snapshot. Cette fonctionnalité n'est disponible qu'avec l'API REST de ONTAP.

La création de copies Snapshot de groupe de cohérence biphasées est uniquement disponible pour la création de copies Snapshot, et non pour le provisionnement des groupes de cohérence ou la restauration des groupes de cohérence.

Un Snapshot de groupe de cohérence biphasé divise le processus de création des snapshots en deux phases :

1. Dans la première phase, l'API exécute des contrôles préalables et déclenche la création de snapshots. La première phase inclut un paramètre de délai d'expiration, indiquant la durée pendant laquelle la copie Snapshot doit être validée.
2. Si la demande de la phase un s'exécute correctement, vous pouvez appeler la deuxième phase dans l'intervalle désigné à partir de la première phase, en archivant la copie Snapshot sur le terminal approprié.

### Avant de commencer

- Pour utiliser la création Snapshot de groupe de cohérence en deux phases, tous les nœuds du cluster doivent exécuter ONTAP 9.11.1 ou version ultérieure.
- Une seule invocation active d'une opération Snapshot de groupe de cohérence est prise en charge sur une instance de groupe de cohérence à la fois, qu'il s'agisse d'une ou deux phases. Toute tentative d'appel d'une opération de snapshot alors qu'une autre opération est en cours entraîne un échec.
- Lorsque vous appelez la création de Snapshot, vous pouvez définir une valeur de délai d'attente facultative comprise entre 5 et 120 secondes. Si aucune valeur de temporisation n'est fournie, l'opération expire par défaut à 7 secondes. Dans l'API, définissez la valeur du délai d'attente avec le `action_timeout` paramètre. Dans l'interface de ligne de commandes, utilisez `-timeout` drapeau.

## Étapes

Vous pouvez réaliser une copie Snapshot en deux phases avec l'API REST ou, depuis ONTAP 9.14.1, avec l'interface de ligne de commandes ONTAP. Cette opération n'est pas prise en charge dans System Manager.



Si vous appelez la création de Snapshot avec l'API, vous devez valider la copie Snapshot avec l'API. Si vous appelez la création de Snapshot avec l'interface de ligne de commandes, vous devez valider la copie Snapshot avec l'interface de ligne de commandes. Les méthodes de mélange ne sont pas prises en charge.

## CLI

Depuis la version ONTAP 9.14.1, vous pouvez créer une copie Snapshot en deux phases à l'aide de l'interface de ligne de commandes.

### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

### Étapes

1. Lancer l'instantané :

```
consistency-group snapshot start -vserver svm_name -consistency-group
consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds
-write-fence {true|false}]
```

2. Vérifier que l'instantané a été pris :

```
consistency-group snapshot show
```

3. Valider le snapshot :

```
consistency-group snapshot commit svm_name -consistency-group
consistency_group_name -snapshot snapshot_name
```

## API

1. Appelez la création du Snapshot. Envoyez une demande POST au terminal du groupe de cohérence à l'aide de `action=start` paramètre.

```
curl -k -X POST 'https://<IP_address>/application/consistency-
groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H
"accept: application/hal+json" -H "content-type: application/json"
-d '{
 {
 "name": "<snapshot_name>",
 "consistency_type": "crash",
 "comment": "<comment>",
 "snapmirror_label": "<SnapMirror_label>"
 }
'
```

2. Si la demande de POST réussit, le résultat inclut un UUID d'instantané. En utilisant cet UUID, envoyez une demande de CORRECTIF pour valider la copie Snapshot.

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept: application/hal+json" -H "content-type: application/json"
```

For more information about the ONTAP REST API, see [link:https://docs.netapp.com/us-en/ontap-automation/reference/api\\_reference.html](https://docs.netapp.com/us-en/ontap-automation/reference/api_reference.html) [API reference^] or the [link:https://devnet.netapp.com/restapi.php](https://devnet.netapp.com/restapi.php) [ONTAP REST API page^] at the NetApp Developer Network for a complete list of API endpoints.

## Définissez la protection à distance pour un groupe de cohérence

Les groupes de cohérence offrent une protection à distance via la synchronisation active SnapMirror et, à partir de ONTAP 9.13.1, la réplication asynchrone SnapMirror.

### Configurez la protection avec la synchronisation active SnapMirror

Vous pouvez utiliser la synchronisation active SnapMirror pour vous assurer que les copies Snapshot des groupes de cohérence créés dans votre groupe de cohérence sont copiées vers la destination. Pour en savoir plus sur la synchronisation active SnapMirror ou sur la configuration de la synchronisation active SnapMirror à l'aide de l'interface de ligne de commande, reportez-vous à la section [Configuration de la protection pour la continuité de l'activité](#).

### Avant de commencer

- Les relations de synchronisation active SnapMirror ne peuvent pas être établies sur les volumes montés pour l'accès NAS.
- Les étiquettes de règles doivent correspondre dans le cluster source et dans le cluster destination.
- La synchronisation active SnapMirror ne réplique pas les copies Snapshot par défaut, sauf si une règle portant une étiquette SnapMirror est ajoutée au paramètre prédéfini AutomatedFailOver. La règle et les copies Snapshot sont créées avec cette étiquette.

Pour en savoir plus sur ce processus, voir "[Protégez votre infrastructure avec la synchronisation active SnapMirror](#)".


- [Déploiements en cascade](#) Ne sont pas pris en charge avec la synchronisation active SnapMirror.
- À partir de ONTAP 9.13.1, vous pouvez réaliser des opérations sans interruption [ajouter des volumes à un groupe de cohérence](#). Avec une relation de synchronisation active SnapMirror. Toute autre modification apportée à un groupe de cohérence exige que vous rompez la relation de synchronisation active SnapMirror, modifiez le groupe de cohérence, puis rétablissez et resynchronisez la relation.



Pour configurer la synchronisation active SnapMirror avec l'interface de ligne de commandes, reportez-vous à la section [Protégez votre infrastructure avec la synchronisation active SnapMirror](#).

### Étapes pour System Manager

1. Assurez-vous d'avoir rencontré le "[Conditions préalables à l'utilisation de SnapMirror actif Sync](#)".
2. Sélectionnez **stockage > groupes de cohérence**.

3. Sélectionnez le groupe de cohérence que vous avez créé dans le menu Groupe de cohérence.
4. En haut à droite de la page de présentation, sélectionnez **plus** puis **protéger**.
5. System Manager remplit automatiquement les informations côté source. Sélectionnez le cluster et la VM de stockage appropriés pour la destination. Sélectionnez une stratégie de protection. Vérifier que **Initialize relation** est coché.
6. Sélectionnez **Enregistrer**.
7. Le groupe de cohérence doit être initialisé et synchronisé. Vérifiez que la synchronisation s'est bien terminée en retournant au menu **groupe de cohérence**. L'état **SnapMirror (Remote)** s'affiche Protected en regard de .

## Configurer SnapMirror asynchrone

Depuis la version ONTAP 9.13.1, vous pouvez configurer la protection asynchrone SnapMirror pour un groupe de cohérence unique. Depuis la version ONTAP 9.14.1, vous pouvez utiliser la réplication asynchrone SnapMirror pour répliquer des copies Snapshot granulaires par volume vers le cluster de destination à l'aide de la relation de groupe de cohérence.

### Description de la tâche

Pour répliquer des copies Snapshot granulaires par volume, vous devez exécuter ONTAP 9.14.1 ou une version ultérieure. Pour les règles MirrorAndVault et Vault, l'étiquette SnapMirror de la règle Snapshot granulaire des volumes doit correspondre à la règle de règle SnapMirror du groupe de cohérence. Les snapshots granulaires par volume respectent la règle SnapMirror du groupe de cohérence, qui est calculée indépendamment des snapshots du groupe de cohérence. Par exemple, si une règle permet de conserver deux copies Snapshot sur la destination, vous pouvez avoir deux copies Snapshot granulaires au niveau du volume et deux copies Snapshot de groupe de cohérence.

Lors de la resynchronisation de la relation SnapMirror avec des copies Snapshot granulaires par volume, vous pouvez conserver les copies Snapshot granulaires par volume avec le `-preserve` drapeau. Les copies Snapshot granulaires par volume, plus récentes que les copies Snapshot du groupe de cohérence, sont conservées. Si aucune copie Snapshot de groupe de cohérence n'est créée, aucune copie Snapshot granulaire par volume ne peut être transférée lors de l'opération de resynchronisation.

### Avant de commencer

- La protection asynchrone SnapMirror n'est disponible que pour un seul groupe de cohérence. Elle n'est pas prise en charge pour les groupes de cohérence hiérarchiques. Pour convertir un groupe de cohérence hiérarchique en un seul groupe de cohérence, reportez-vous à la section [modifier l'architecture d'un groupe de cohérence](#).
- Les étiquettes de règles doivent correspondre dans le cluster source et dans le cluster destination.
- Vous pouvez interrompre l'activité [ajouter des volumes à un groupe de cohérence](#) Avec une relation asynchrone SnapMirror active. Toute autre modification apportée à un groupe de cohérence exige que vous rompez la relation SnapMirror, modifiez le groupe de cohérence, puis rétablissez et resynchronisez la relation.
- Les groupes de cohérence activés pour la protection avec la réplication asynchrone SnapMirror ont des limites différentes. Pour plus d'informations, voir [Limites des groupes de cohérence](#).
- Si vous avez configuré une relation de protection asynchrone SnapMirror pour plusieurs volumes individuels, vous pouvez convertir ces volumes en groupe de cohérence tout en conservant les copies Snapshot existantes. Pour convertir les volumes avec succès :
  - Il doit y avoir une copie Snapshot commune des volumes.
  - Vous devez interrompre la relation SnapMirror existante, [ajoutez les volumes à un seul groupe de](#)

[cohérence](#), puis resynchronisez la relation à l'aide du flux de travail suivant.


## Étapes

1. Depuis le cluster de destination, sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence que vous avez créé dans le menu Groupe de cohérence.
3. En haut à droite de la page de présentation, sélectionnez **plus** puis **protéger**.
4. System Manager remplit automatiquement les informations côté source. Sélectionnez le cluster et la VM de stockage appropriés pour la destination. Sélectionnez une stratégie de protection. Vérifier que **Initialize relation** est coché.

Lorsque vous sélectionnez une stratégie asynchrone, vous avez la possibilité de **remplacer le programme de transfert**.



La planification minimale prise en charge (objectif de point de récupération, ou RPO) pour les groupes de cohérence avec la réplication asynchrone SnapMirror est de 30 minutes.

5. Sélectionnez **Enregistrer**.
6. Le groupe de cohérence doit être initialisé et synchronisé. Vérifiez que la synchronisation s'est bien terminée en retournant au menu **groupe de cohérence**. L'état **SnapMirror (Remote)** s'affiche Protected en regard de .

## Configuration de la reprise d'activité SVM

À partir de ONTAP 9.14.1, [Reprise d'activité de SVM](#) prend en charge les groupes de cohérence et permet de mettre en miroir les informations relatives aux groupes de cohérence entre le cluster source et le cluster destination.

Si vous activez la reprise d'activité SVM sur un SVM qui contient déjà un groupe de cohérence, suivez les workflows de configuration du SVM pour [System Manager](#) ou le [INTERFACE DE LIGNE DE COMMANDES DE ONTAP](#).

Si vous ajoutez un groupe de cohérence à un SVM figurant dans une relation de reprise d'activité de SVM active et saine, vous devez mettre à jour la relation de SVM DR depuis le cluster destination. Pour plus d'informations, voir [Mettre à jour une relation de réplication manuellement](#). Vous devez mettre à jour la relation chaque fois que vous développez le groupe de cohérence.

## Limites

- La reprise d'activité des SVM ne prend pas en charge les groupes de cohérence hiérarchiques.
- La reprise d'activité pour SVM ne prend pas en charge les groupes de cohérence protégés par la réplication asynchrone SnapMirror. Vous devez rompre la relation SnapMirror avant de configurer la reprise d'activité d'un SVM.
- Les deux clusters doivent exécuter ONTAP 9.14.1 ou une version ultérieure.
- Les relations « Fan-Out » ne sont pas prises en charge pour les configurations de reprise d'activité des SVM contenant des groupes de cohérence.
- Pour les autres limites, voir [limites des groupes de cohérence](#).

## Visualiser les relations

System Manager visualise les mappages de LUN dans le menu **protection > relations**. Lorsque vous sélectionnez une relation source, System Manager affiche une visualisation des relations source. En

sélectionnant un volume, vous pouvez approfondir ces relations pour afficher la liste des LUN et des relations de groupe d'initiateurs. Ces informations peuvent être téléchargées sous forme de classeur Excel à partir de la vue de volume individuelle ; l'opération de téléchargement s'exécute en arrière-plan.

### Informations associées

- ["Cloner un groupe de cohérence"](#)
- ["Configurez les copies Snapshot"](#)
- ["Création de règles personnalisées de protection des données"](#)
- ["Effectuez des restaurations à partir de copies Snapshot"](#)
- ["Restaurez un volume à partir d'une copie Snapshot antérieure"](#)
- ["Présentation de la synchronisation active SnapMirror"](#)
- ["Documentation sur l'automatisation ONTAP"](#)
- [Notions de base sur la reprise après incident asynchrone SnapMirror](#)

## Modifiez les volumes membres d'un groupe de cohérence

À partir de la version ONTAP 9.12.1, vous pouvez modifier un groupe de cohérence en supprimant des volumes ou en ajoutant des volumes (en développant le groupe de cohérence). Depuis la version ONTAP 9.13.1, vous pouvez déplacer des volumes entre des groupes de cohérence enfants s'ils partagent un parent commun.

### Ajouter des volumes à un groupe de cohérence

À partir de ONTAP 9.12.1, vous pouvez ajouter des volumes à un groupe de cohérence sans interruption.

#### Description de la tâche

- Vous ne pouvez pas ajouter des volumes associés à un autre groupe de cohérence.
- Les groupes de cohérence prennent en charge les protocoles NAS, SAN et NVMe.
- Si les ajustements se situent dans l'ensemble, vous pouvez ajouter jusqu'à 16 volumes à la fois à un groupe de cohérence [limites des groupes de cohérence](#).
- Depuis la version ONTAP 9.13.1, vous pouvez ajouter des volumes à un groupe de cohérence sans interruption avec une règle de protection asynchrone SnapMirror active ou SnapMirror.
- Lorsque vous ajoutez des volumes à un groupe de cohérence protégé par la synchronisation active SnapMirror, l'état de la relation de synchronisation active SnapMirror passe à « expansion » jusqu'à ce que la mise en miroir et la protection soient configurées pour le nouveau volume. Si un incident se produit sur le cluster principal avant la fin de ce processus, le groupe de cohérence revient à sa composition d'origine dans le cadre de l'opération de basculement.
- Dans ONTAP 9.12.1 et les versions antérieures, vous *ne pouvez* pas ajouter de volumes à un groupe de cohérence dans une relation de synchronisation active SnapMirror. Vous devez d'abord supprimer la relation de synchronisation active SnapMirror, modifier le groupe de cohérence, puis restaurer la protection avec la synchronisation active SnapMirror.
- Depuis ONTAP 9.12.1, l'API REST de ONTAP prend en charge l'ajout de volumes *New* ou existants à un groupe de cohérence. Pour plus d'informations sur l'API REST de ONTAP, reportez-vous à ["Documentation de référence de l'API REST ONTAP"](#).

Depuis ONTAP 9.13.1, cette fonctionnalité est prise en charge dans System Manager.

- Lors de l'extension d'un groupe de cohérence, les copies Snapshot du groupe de cohérence capturé avant la modification sont considérées comme partielles. Toute opération de restauration basée sur cette copie Snapshot reflète le groupe de cohérence à l'instant T du snapshot.
- Si vous utilisez les ONTAP 9.10.1 à 9.11.1, vous ne pouvez pas modifier un groupe de cohérence. Pour modifier la configuration d'un groupe de cohérence dans les ONTAP 9.10.1 ou 9.11.1, vous devez supprimer ce groupe, puis créer un nouveau groupe de cohérence avec les volumes à inclure.
- Depuis la version ONTAP 9.14.1, vous pouvez répliquer des copies Snapshot granulaires par volume sur le cluster de destination lors de l'utilisation de la réplication asynchrone SnapMirror. Lors de l'extension d'un groupe de cohérence à l'aide de la réplication asynchrone SnapMirror, les snapshots granulaires par volume ne sont répliqués qu'après l'extension du groupe de cohérence lorsque la règle SnapMirror est MirrorAll ou MirrorAndVault. Seuls les snapshots granulaires par volume plus récents que le snapshot du groupe de cohérence de référence sont répliqués.
- Si vous ajoutez des volumes à un groupe de cohérence dans une relation de reprise d'activité de SVM (prise en charge depuis ONTAP 9.14.1), vous devez mettre à jour la relation de reprise d'activité de SVM depuis le cluster de destination après avoir étendu le groupe de cohérence. Pour plus d'informations, reportez-vous à la section [Mettre à jour une relation de réplication manuellement](#).



## Exemple 23. Étapes

### System Manager

Depuis ONTAP 9.12.1, vous pouvez effectuer cette opération avec System Manager.

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence à modifier.
3. Si vous modifiez un seul groupe de cohérence, en haut du menu **volumes**, sélectionnez **plus**, puis **plus** pour ajouter un volume.

Si vous modifiez un groupe de cohérence enfant, identifiez le groupe de cohérence parent à modifier. Cliquez sur le bouton **>** pour afficher les groupes de cohérence enfant, puis sélectionnez **⋮** en regard du nom du groupe de cohérence enfant à modifier. Dans ce menu, sélectionnez **développer**.

4. Sélectionnez jusqu'à 16 volumes à ajouter au groupe de cohérence.
5. Sélectionnez **Enregistrer**. Une fois l'opération terminée, affichez les nouveaux volumes ajoutés dans le menu **volumes** du groupe de cohérence.

### CLI

Depuis la version ONTAP 9.14.1, vous pouvez ajouter des volumes à un groupe de cohérence à l'aide de l'interface de ligne de commandes ONTAP.

### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

### Ajouter des volumes existants

1. Exécutez la commande suivante. Le `-volumes` le paramètre accepte une liste de volumes séparés par une virgule.



Inclure uniquement le `-parent-consistency-group` paramètre si le groupe de cohérence appartient à une relation hiérarchique.

```
consistency-group volume add -vserver svm_name -consistency-group
consistency_group_name -parent-consistency-group parent_consistency_group
-volume volumes
```

### Ajouter de nouveaux volumes

La procédure d'ajout de nouveaux volumes dépend du protocole que vous utilisez.



Inclure uniquement le `-parent-consistency-group` paramètre si le groupe de cohérence appartient à une relation hiérarchique.

- Pour ajouter de nouveaux volumes sans les exporter :

```
consistency-group volume create -vserver SVM_name -consistency-group
child_consistency_group -parent-consistency-group existingParentCg -volume
volume_name -size size
```

- Pour ajouter de nouveaux volumes NFS :

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -volume volume-prefix -volume-count number -size
size -export-policy policy_name
```

- Pour ajouter de nouveaux volumes SAN :

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -lun lun_name -size size -lun-count number -igroup
igroup_name
```

- Pour ajouter de nouveaux espaces de noms NVMe :

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency_group_name -namespace namespace_name -volume-count number
-namespace-count number -size size -subsystem subsystem_name
```

## Supprimez des volumes d'un groupe de cohérence

Les volumes supprimés d'un groupe de cohérence ne sont pas supprimés. Ils restent actifs dans le cluster.

### Description de la tâche

- Vous ne pouvez pas supprimer des volumes d'un groupe de cohérence dans une relation de synchronisation active SnapMirror ou de reprise d'activité de SVM. Vous devez d'abord supprimer la relation SnapMirror active Sync pour modifier le groupe de cohérence, puis rétablir la relation.
- Si un groupe de cohérence ne contient aucun volume après l'opération de suppression, le groupe de cohérence est supprimé.
- Lorsqu'un volume est supprimé d'un groupe de cohérence, les snapshots existants du groupe de cohérence restent considérés comme non valides. Les snapshots existants ne peuvent pas être utilisés pour restaurer le contenu d'un groupe de cohérence. Les snapshots granulaires volume restent valides.
- Si vous supprimez un volume du cluster, il est automatiquement supprimé du groupe de cohérence.
- Pour modifier la configuration d'un groupe de cohérence dans ONTAP 9.10.1 ou 9.11.1, vous devez supprimer ce groupe de cohérence, puis en créer un nouveau avec les volumes membres souhaités.
- La suppression d'un volume du cluster entraîne sa suppression automatique.

## System Manager

Depuis ONTAP 9.12.1, vous pouvez effectuer cette opération avec System Manager.

### Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence enfant ou unique à modifier.
3. Dans le menu **volumes**, sélectionnez les cases à cocher en regard des volumes individuels que vous souhaitez supprimer du groupe de cohérence.
4. Sélectionnez **Supprimer des volumes du groupe de cohérence**.
5. Vérifiez que vous avez bien compris que la suppression des volumes entraîne la non-validité de toutes les copies Snapshot du groupe de cohérence et sélectionnez **Remove**.

### CLI

Depuis la version ONTAP 9.14.1, vous pouvez supprimer des volumes d'un groupe de cohérence à l'aide de l'interface de ligne de commandes.

### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

### Étape

1. Supprimer les volumes. Le `-volumes` le paramètre accepte une liste de volumes séparés par une virgule.

Inclure uniquement le `-parent-consistency-group` paramètre si le groupe de cohérence appartient à une relation hiérarchique.

```
consistency-group volume remove -vserver SVM_name -consistency-group
consistency_group_name -parent-consistency-group
parent_consistency_group_name -volume volumes
```

## Déplacez des volumes entre les groupes de cohérence

Depuis la version ONTAP 9.13.1, vous pouvez déplacer des volumes entre des groupes de cohérence enfants qui partagent un parent.

### Description de la tâche

- Vous pouvez uniquement déplacer des volumes entre des groupes de cohérence imbriqués sous le même groupe de cohérence parent.
- Les snapshots de groupe de cohérence existants sont devenus non valides et ne sont plus accessibles en tant que snapshots de groupe de cohérence. Les snapshots de volumes individuels restent valides.
- Les copies Snapshot du groupe de cohérence parent restent valides.
- Si vous déplacez tous les volumes hors d'un groupe de cohérence enfant, ce groupe de cohérence est supprimé.
- Les modifications apportées à un groupe de cohérence doivent être respectées [limites des groupes de](#)

cohérence.

## System Manager

Depuis ONTAP 9.12.1, vous pouvez effectuer cette opération avec System Manager.

### Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence parent contenant les volumes à déplacer. Recherchez le groupe de cohérence enfant, puis développez le menu **volumes**. Sélectionnez les volumes à déplacer.
3. Sélectionnez **déplacer**.
4. Indiquez si vous souhaitez déplacer les volumes vers un nouveau groupe de cohérence ou un groupe existant.
  - a. Pour déplacer le groupe de cohérence vers un groupe existant, sélectionnez **groupe de cohérence enfant existant**, puis choisissez le nom du groupe de cohérence dans le menu déroulant.
  - b. Pour passer à un nouveau groupe de cohérence, sélectionnez **Nouveau groupe de cohérence enfant**. Indiquez le nom du nouveau groupe de cohérence enfant et sélectionnez un type de composant.
5. Sélectionnez **déplacer**.

### CLI

Depuis la version ONTAP 9.14.1, vous pouvez déplacer des volumes entre des groupes de cohérence à l'aide de l'interface de ligne de commandes ONTAP.

### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

### Déplacez les volumes vers un nouveau groupe de cohérence enfant

1. La commande suivante crée un nouveau groupe de cohérence enfant dans lequel sont situés les volumes désignés.

Lorsque vous créez le nouveau groupe de cohérence, vous pouvez désigner de nouvelles règles de Snapshot, de QoS et de hiérarchisation.

```
consistency-group volume reassign -vserver SVM_name -consistency-group
source_child_consistency_group -parent-consistency-group
parent_consistency_group -volume volumes -new-consistency-group
consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering
-policy policy]
```

### Déplacez les volumes vers un groupe de cohérence enfant existant

1. Réaffectez les volumes. Le `-volumes` le paramètre accepte une liste de noms de volumes séparés par des virgules.

```
consistency-group volume reassign -vserver SVM_name -consistency-group
source_child_consistency_group -parent-consistency-group
parent_consistency_group -volume volumes -to-consistency-group
target_consistency_group
```

## Informations associées

- [Limites des groupes de cohérence](#)
- [Cloner un groupe de cohérence](#)

## Modifier la géométrie du groupe de cohérence

Depuis la version ONTAP 9.13.1, vous pouvez modifier la géométrie d'un groupe de cohérence. La modification de la géométrie d'un groupe de cohérence vous permet de modifier la configuration des groupes de cohérence enfant ou parent sans interrompre les opérations d'E/S en cours.

La modification de la géométrie d'un groupe de cohérence a un impact sur les copies Snapshot existantes du groupe de cohérence. Pour plus de détails, reportez-vous à la modification spécifique de la géométrie que vous souhaitez effectuer.



Vous ne pouvez pas modifier la géométrie d'un groupe de cohérence configuré avec une règle de protection à distance. Vous devez d'abord rompre la relation de protection, modifier la géométrie, puis restaurer la protection à distance.

## Ajouter un nouveau groupe de cohérence enfant

Depuis la version ONTAP 9.13.1, vous pouvez ajouter un nouveau groupe de cohérence enfant à un groupe de cohérence parent existant.

### Description de la tâche

- Un groupe de cohérence parent peut contenir cinq groupes de cohérence enfant au maximum. Voir [limites des groupes de cohérence](#) pour les autres limites.
- Vous ne pouvez pas ajouter un groupe de cohérence enfant à un seul groupe de cohérence. Vous devez d'abord [\[promouvoir\]](#) groupe de cohérence, vous pouvez ensuite ajouter un groupe de cohérence enfant.
- Les copies Snapshot existantes du groupe de cohérence capturé avant l'opération d'extension sont considérées comme partielles. Toute opération de restauration basée sur cette copie Snapshot reflète le groupe de cohérence à l'instant précis de la copie Snapshot.

## Exemple 24. Étapes

### System Manager

Depuis ONTAP 9.13.1, vous pouvez effectuer cette opération avec System Manager.

#### Ajouter un nouveau groupe de cohérence enfant

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence parent auquel vous souhaitez ajouter un groupe de cohérence enfant.
3. En regard du nom du groupe de cohérence parent, sélectionnez **plus** puis **Ajouter un nouveau groupe de cohérence enfant**.
4. Indiquez le nom du groupe de cohérence.
5. Indiquez si vous souhaitez ajouter des volumes nouveaux ou existants.
  - a. Si vous ajoutez des volumes existants, sélectionnez **volumes existants** puis choisissez les volumes dans le menu déroulant.
  - b. Si vous ajoutez de nouveaux volumes, sélectionnez **nouveaux volumes** puis indiquez le nombre de volumes et leur taille.
6. Sélectionnez **Ajouter**.

### CLI

Depuis la version ONTAP 9.14.1, vous pouvez ajouter un groupe de cohérence enfant via l'interface de ligne de commandes ONTAP.

#### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

#### Ajoutez un groupe de cohérence enfant avec les nouveaux volumes

1. Créez le nouveau groupe de cohérence. Indiquez des valeurs pour le nom du groupe de cohérence, le préfixe de volume, le nombre de volumes, la taille du volume, le service de stockage, et nom de la règle d'export :

```
consistency-group create -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
-volume-prefix prefix -volume-count number -size size -storage-service
service -export-policy policy_name
```

#### Ajoutez un groupe de cohérence enfant avec les volumes existants

1. Créez le nouveau groupe de cohérence. Le `volumes` le paramètre accepte une liste de noms de volumes séparés par des virgules.

```
consistency-group create -vserver SVM_name -consistency-group
new_consistency_group -parent-consistency-group parent_consistency_group
-volumes volume
```

## Détacher un groupe de cohérence enfant

Depuis la version ONTAP 9.13.1, vous pouvez supprimer un groupe de cohérence enfant de son groupe de cohérence parent et le convertir en groupe de cohérence individuel.

### Description de la tâche

- Le détachement d'un groupe de cohérence enfant rend les copies Snapshot du groupe de cohérence parent non valides et inaccessibles. Les copies Snapshot granulaires de volume restent valides.
- Les copies Snapshot existantes d'un groupe de cohérence individuel restent valides.
- Cette opération échoue si un groupe de cohérence unique existant porte le même nom que le groupe de cohérence enfant que vous souhaitez détacher. Si ce scénario se produit, vous devez renommer le groupe de cohérence lorsque vous le détachez.

### Exemple 25. Étapes

#### System Manager

Depuis ONTAP 9.13.1, vous pouvez effectuer cette opération avec System Manager.

#### Détacher un groupe de cohérence enfant

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence parent contenant l'enfant à détacher.
3. En regard du groupe de cohérence enfant à détacher, sélectionnez **plus** puis **détacher du parent**.
4. Si vous le souhaitez, renommez le groupe de cohérence et sélectionnez un type d'application.
5. Sélectionnez **détacher**.

#### CLI

Depuis la version ONTAP 9.14.1, vous pouvez détacher un groupe de cohérence enfant à l'aide de l'interface de ligne de commandes ONTAP.

#### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

#### Détacher un groupe de cohérence enfant

1. Détachez le groupe de cohérence. Si vous le souhaitez, renommez le groupe de cohérence détaché avec le `-new-name` paramètre.

```
consistency-group detach -vserver SVM_name -consistency-group
child_consistency_group -parent-consistency-group parent_consistency_group
[-new-name new_name]
```

## Déplacez un groupe de cohérence unique existant sous un groupe de cohérence parent

À partir de la version ONTAP 9.13.1, vous pouvez convertir un groupe de cohérence existant en groupe de cohérence enfant. Au cours de l'opération de déplacement, vous pouvez déplacer le groupe de cohérence sous un groupe de cohérence parent existant ou créer un nouveau groupe de cohérence parent.

### Description de la tâche



- Le groupe de cohérence parent doit avoir au moins quatre enfants. Un groupe de cohérence parent peut contenir cinq groupes de cohérence enfant au maximum. Voir [limites des groupes de cohérence](#) pour les autres limites.
- Les copies Snapshot existantes du groupe de cohérence *parent* capturées avant cette opération sont considérées comme partielles. Toute opération de restauration basée sur l'une de ces copies Snapshot reflète le groupe de cohérence au moment précis de la copie Snapshot.
- Les copies Snapshot de groupe de cohérence existant du groupe de cohérence unique restent valides.

## Exemple 26. Étapes

### System Manager

Depuis ONTAP 9.13.1, vous pouvez effectuer cette opération avec System Manager.

#### Déplacez un groupe de cohérence unique existant sous un groupe de cohérence parent

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence à convertir.
3. Sélectionnez **plus** puis **déplacer sous un autre groupe de cohérence**.
4. Si vous le souhaitez, indiquez un nouveau nom pour le groupe de cohérence et sélectionnez un type de composant. Par défaut, le type de composant sera autre.
5. Indiquez si vous souhaitez migrer vers un groupe de cohérence parent existant ou créer un nouveau groupe de cohérence parent :
  - a. Pour migrer vers un groupe de cohérence parent existant, sélectionnez **groupe de cohérence existant**, puis choisissez le groupe de cohérence dans le menu déroulant.
  - b. Pour créer un nouveau groupe de cohérence parent, sélectionnez **Nouveau groupe de cohérence**, puis indiquez le nom du nouveau groupe de cohérence.
6. Sélectionnez **déplacer**.

### CLI

Depuis la version ONTAP 9.14.1, vous pouvez déplacer un groupe de cohérence unique sous un groupe de cohérence parent à l'aide de l'interface de ligne de commandes ONTAP.

#### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

#### Déplacez un groupe de cohérence sous un nouveau groupe de cohérence parent

1. Créez le groupe de cohérence parent. Le `-consistency-groups` ce paramètre va migrer tous les groupes de cohérence existants vers le nouveau parent.

```
consistency-group attach -vserver svm_name -consistency-group
parent_consistency_group -consistency-groups child_consistency_group
```

#### Déplacez un groupe de cohérence sous un groupe de cohérence existant

1. Déplacer le groupe de cohérence :

```
consistency-group add -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
```

## Promouvoir un groupe de cohérence enfant

Depuis la version ONTAP 9.13.1, vous pouvez promouvoir un groupe de cohérence unique en tant que groupe de cohérence parent. Lorsque vous promouvez le groupe de cohérence unique en parent, vous créez également un nouveau groupe de cohérence enfant qui hérite de tous les volumes du groupe de cohérence unique d'origine.

## Description de la tâche

- Pour convertir un groupe de cohérence enfant en groupe de cohérence parent, vous devez d'abord le faire [\[detach\]](#) le groupe de cohérence enfant doit ensuite suivre la procédure suivante.
- Une fois le groupe de cohérence mis en avant, les copies Snapshot existantes du groupe de cohérence restent valides.

### System Manager

Depuis ONTAP 9.13.1, vous pouvez effectuer cette opération avec System Manager.

#### Promouvoir un groupe de cohérence enfant

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence à promouvoir.
3. Sélectionnez **plus** puis **promouvoir en groupe de cohérence parent**.
4. Entrez un **Nom** et sélectionnez un **Type de composant** pour le groupe de cohérence enfant.
5. Sélectionnez **promouvoir**.

### CLI

Depuis la version ONTAP 9.14.1, vous pouvez déplacer un groupe de cohérence unique sous un groupe de cohérence parent à l'aide de l'interface de ligne de commandes ONTAP.

#### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

#### Promouvoir un groupe de cohérence enfant

1. Promouvoir le groupe de cohérence. Cette commande entraîne la création d'un groupe de cohérence parent et d'un groupe enfant.

```
consistency-group promote -vserver SVM_name -consistency-group
existing_consistency_group -new-name new_child_consistency_group
```

## Rétrograder un parent en un seul groupe de cohérence

Depuis la version ONTAP 9.13.1, vous pouvez rétrograder un groupe de cohérence parent en un seul groupe de cohérence. La rétrogradation du parent aplatit la hiérarchie du groupe de cohérence, supprimant tous les groupes de cohérence enfants associés. Tous les volumes du groupe de cohérence restent dans le nouveau groupe de cohérence unique.

## Description de la tâche

- Les copies Snapshot existantes du groupe de cohérence *parent* restent valides une fois que vous les avez rétrogradés à une cohérence unique. Les copies Snapshot existantes de l'un des groupes de cohérence *child* associés de ce parent deviennent non valides lors de la rétrogradation. Les copies Snapshot de volume individuelles au sein du groupe de cohérence enfant restent accessibles sous forme de copies Snapshot granulaires par volume.

## Exemple 27. Étapes

### System Manager

Depuis ONTAP 9.13.1, vous pouvez effectuer cette opération avec System Manager.

#### Rétrograder un groupe de cohérence

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence parent à rétrograder.
3. Sélectionnez **plus** puis **Rétrograder à un seul groupe de cohérence**.
4. Un avertissement vous informe que tous les groupes de cohérence enfants associés seront supprimés et que leurs volumes seront déplacés dans le nouveau groupe de cohérence unique. Sélectionnez **Rétrograder** pour confirmer que vous comprenez l'impact.

### CLI

Depuis la version ONTAP 9.14.1, vous pouvez rétrograder un groupe de cohérence à l'aide de l'interface de ligne de commandes ONTAP.

#### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

#### Rétrograder un groupe de cohérence

1. Rétrograder le groupe de cohérence. Utilisez l'option `-new-name` paramètre permettant de renommer le groupe de cohérence.

```
consistency-group demote -vserver SVM_name -consistency-group
parent_consistency_group [-new-name new_consistency_group_name]
```

## Modifier les balises d'application et de composant

Depuis la version ONTAP 9.12.1, les groupes de cohérence prennent en charge le balisage des composants et des applications. Les balises d'application et de composant sont un outil de gestion qui vous permet de filtrer et d'identifier différentes charges de travail dans vos groupes de cohérence.

### Description de la tâche

Les groupes de cohérence proposent deux types de balises :

- **Balises d'application** : elles s'appliquent aux groupes de cohérence individuel et parent. Les balises d'application fournissent un étiquetage pour les charges de travail telles que MongoDB, Oracle ou SQL Server. La balise d'application par défaut pour les groupes de cohérence est autre.
- **Balises de composant**: Les enfants des groupes de cohérence hiérarchiques ont des balises de composant au lieu de balises d'application. Les options pour les balises de composant sont « données », « journaux » ou « autre ». La valeur par défaut est autre.

Lors de la création de groupes de cohérence ou après la création de groupes de cohérence, vous pouvez appliquer les balises.



Si le groupe de cohérence possède une relation de synchronisation active SnapMirror, vous devez utiliser **Other** comme balise d'application ou de composant.

## Étapes

Depuis ONTAP 9.12.1, vous pouvez modifier les balises d'application et de composant à l'aide de System Manager. Depuis ONTAP 9.14.1, vous pouvez modifier les balises d'application et de composant à l'aide de l'interface de ligne de commande ONTAP.

### System Manager

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence dont vous souhaitez modifier la balise. Sélectionnez **:** en regard du nom du groupe de cohérence, puis **Edit**.
3. Dans le menu déroulant, choisissez la balise d'application ou de composant appropriée.
4. Sélectionnez **Enregistrer**.

### CLI

Depuis la version ONTAP 9.14.1, vous pouvez modifier la balise d'application ou de composant d'un groupe de cohérence existant à l'aide de l'interface de ligne de commandes ONTAP.

#### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

#### Modifier la balise d'application

1. Les balises d'application acceptent un nombre limité de chaînes prédéfinies. Pour afficher la liste des chaînes acceptées, exécutez la commande suivante :  

```
consistency-group modify -vserver svm_name -consistency-group consistency_group -application-type ?
```
2. Choisissez la chaîne appropriée dans le résultat, puis modifiez le groupe de cohérence :  

```
consistency-group modify -vserver svm_name -consistency-group consistency_group -application-type application_type
```

#### Modifier la balise du composant

1. Modifier le type de composant. Le type de composant peut être données, journaux ou autre. Si vous utilisez la synchronisation active SnapMirror, celle-ci doit être « autre ».  

```
consistency-group modify -vserver svm -consistency-group child_consistency_group -parent-consistency-group parent_consistency_group -application-component-type [data|logs|other]
```

## Cloner un groupe de cohérence

Depuis la version ONTAP 9.12.1, vous pouvez cloner un groupe de cohérence pour créer une copie du groupe de cohérence et de son contenu. Le clonage d'un groupe de cohérence crée une copie de la configuration de groupe de cohérence, de ses métadonnées telles que le type d'application, et de tous les volumes et leur contenu tels

que les fichiers, les répertoires, les LUN ou les espaces de noms NVMe.

### Description de la tâche

Lors du clonage d'un groupe de cohérence, vous pouvez le cloner avec sa configuration actuelle, mais avec un contenu de volume tel qu'ils sont ou basé sur un Snapshot de groupe de cohérence existant.

Le clonage d'un groupe de cohérence est pris en charge uniquement pour l'ensemble du groupe de cohérence. Vous ne pouvez pas cloner un groupe de cohérence enfant individuel dans une relation hiérarchique : seule la configuration complète des groupes de cohérence peut être clonée.

Lorsque vous clonez un groupe de cohérence, les composants suivants ne sont pas clonés :

- IGroups
- Mappages de LUN
- Sous-systèmes NVMe
- Mappages de sous-systèmes d'espace de noms NVMe

### Avant de commencer

- Lorsque vous clonez un groupe de cohérence, ONTAP ne crée pas de partages SMB pour les volumes clonés si aucun nom de partage n'est spécifié. \* Les groupes de cohérence clonés ne sont pas montés si aucun chemin de jonction n'est spécifié.
- Si vous tentez de cloner un groupe de cohérence à partir d'une copie Snapshot qui ne reflète pas les volumes constitutants actuels du groupe de cohérence, l'opération échoue.
- Une fois que vous avez cloné un groupe de cohérence, vous devez effectuer l'opération de mappage appropriée.

Reportez-vous à la section [Mappez les igroups sur plusieurs LUN](#) ou [Mappez un namespace NVMe à un sous-système](#) pour en savoir plus.

- Le clonage d'un groupe de cohérence n'est pas pris en charge pour un groupe de cohérence dans une relation de synchronisation active SnapMirror ou avec des volumes DP associés.

## System Manager

### Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence à cloner dans le menu **Groupe de cohérence**.
3. En haut à droite de la page de présentation du groupe de cohérence, sélectionnez **Clone**.
4. Indiquez un nom pour le nouveau groupe de cohérence cloné ou acceptez le nom par défaut.
  - a. Choisissez si vous souhaitez activer **"Provisionnement fin"**.
  - b. Choisissez **Split Clone** si vous souhaitez dissocier le groupe de cohérence de sa source et allouer de l'espace disque supplémentaire au groupe de cohérence cloné.
5. Pour cloner le groupe de cohérence dans son état actuel, choisissez **Ajouter une nouvelle copie Snapshot**.

Pour cloner le groupe de cohérence à partir d'un snapshot, choisissez **utiliser une copie Snapshot existante**. La sélection de cette option ouvre un nouveau sous-menu. Sélectionnez la copie Snapshot que vous souhaitez utiliser comme base de l'opération de clonage.

6. Sélectionnez **Clone**.
7. Retournez au menu **Groupe de cohérence** pour confirmer que votre groupe de cohérence a été cloné.

### CLI

Depuis la version ONTAP 9.14.1, vous pouvez cloner un groupe de cohérence à l'aide de l'interface de ligne de commandes et des informations d'identification d'administrateur du cluster.

### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

### Cloner un groupe de cohérence

1. Le `consistency-group clone create` la commande clone le groupe de cohérence à l'état instantané actuel. Pour baser l'opération de clonage sur un snapshot, incluez le `-source-snapshot` paramètre.

```
consistency-group clone create -vserver svm_name -consistency-group
clone_name -source-consistency-group consistency_group_name [-source-
snapshot snapshot_name]
```

### Étapes suivantes

- [Mappez les igroups sur plusieurs LUN](#)
- [Mappez un namespace NVMe à un sous-système](#)

## Supprimez un groupe de cohérence


Si vous décidez de ne plus avoir besoin d'un groupe de cohérence, vous pouvez le supprimer.

## Description de la tâche

- La suppression d'un groupe de cohérence supprime l'instance du groupe de cohérence et n'a \_pas d'impact sur les volumes ou les LUN constitutifs. La suppression d'un groupe de cohérence n'entraîne pas la suppression des snapshots présents sur chaque volume, mais ils ne sont plus accessibles en tant que snapshots de groupe de cohérence. Toutefois, les snapshots peuvent continuer à être gérés comme des snapshots granulaires de volume ordinaires.
- ONTAP supprime automatiquement un groupe de cohérence si tous les volumes du groupe de cohérence sont supprimés.
- La suppression d'un groupe de cohérence parent entraîne la suppression de tous les groupes de cohérence enfant associés.
- Si vous utilisez une version de ONTAP comprise entre 9.10.1 et 9.12.0, les volumes ne peuvent être supprimés d'un groupe de cohérence que si le volume lui-même est supprimé, auquel cas le volume est automatiquement supprimé du groupe de cohérence. Depuis la version ONTAP 9.12.1, vous pouvez supprimer des volumes d'un groupe de cohérence sans le supprimer. Pour plus d'informations sur ce processus, reportez-vous à la section [Modifier un groupe de cohérence](#).

## Exemple 28. Étapes

### System Manager

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence à supprimer.
3. En regard du nom du groupe de cohérence, sélectionnez , puis **Delete**.

### CLI

Depuis la version ONTAP 9.14.1, vous pouvez supprimer un groupe de cohérence à l'aide de l'interface de ligne de commandes.

### Avant de commencer

- Vous devez avoir le niveau de privilège admin pour effectuer cette tâche.
- Dans ONTAP 9.14.1, vous devez être administrateur de cluster ou SVM pour effectuer cette tâche. Depuis ONTAP 9.15.1, tout utilisateur au niveau de privilège admin peut effectuer cette tâche.

### Supprimez un groupe de cohérence

1. Supprimez le groupe de cohérence :

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

# Synchronisation active SnapMirror

## Introduction

### Présentation de la synchronisation active SnapMirror

La synchronisation active SnapMirror (également appelée SnapMirror Business Continuity [SM-BC]) permet aux services de l'entreprise de continuer à fonctionner même en cas de défaillance complète du site. Les applications peuvent ainsi basculer en toute



transparence grâce à une copie secondaire. Une intervention manuelle, ainsi que des scripts personnalisés sont requis pour déclencher un basculement avec la synchronisation active SnapMirror.

Disponible à partir de ONTAP 9.9.1, la synchronisation active SnapMirror est prise en charge sur les clusters AFF, les clusters ASA et C-Series (AFF ou ASA). Les clusters principal et secondaire doivent être du même type : ASA ou AFF. La synchronisation active SnapMirror protège les applications avec des LUN iSCSI ou FCP.

À partir de la version ONTAP 9.15.1, SnapMirror active Sync prend en charge un [capacité active/active symétrique](#), Activation des opérations de lecture et d'écriture d'E/S à partir des deux copies d'un LUN protégé avec réplication synchrone bidirectionnelle, ce qui permet aux deux copies de LUN de traiter les opérations d'E/S localement. Avant ONTAP 9.15.1, la synchronisation active SnapMirror prend uniquement en charge les configurations actif-actif asymétriques, dans lesquelles les données du site secondaire sont proxys vers un LUN.



Depuis juillet 2024, le contenu des rapports techniques publiés au format PDF a été intégré à la documentation produit de ONTAP. La documentation relative à la synchronisation active de SnapMirror ONTAP inclut désormais du contenu de *TR-4878: SnapMirror active sync*.

## Avantages

La synchronisation active SnapMirror offre les avantages suivants :

- Disponibilité sans interruption pour les applications stratégiques.
- Possibilité d'héberger alternativement des applications critiques à partir de sites principaux et secondaires.
- Gestion simplifiée des applications grâce à l'utilisation de groupes de cohérence pour assurer la cohérence des ordres d'écriture dépendants.
- Capacité à tester le basculement pour chaque application.
- Création instantanée de clones en miroir sans impact sur la disponibilité des applications.
- La possibilité de déployer des charges de travail protégées et non protégées dans le même cluster ONTAP.
- L'identité des LUN reste la même, de sorte que l'application les considère comme un périphérique virtuel partagé.
- Possibilité de réutiliser des clusters secondaires avec flexibilité pour créer des clones instantanés pour l'utilisation des applications à des fins de développement et de test UAT ou de création de rapports, sans impact sur la disponibilité ou les performances des applications.

La synchronisation active SnapMirror vous permet de protéger vos LUN de données. Ainsi, les applications peuvent basculer en toute transparence afin d'assurer la continuité de l'activité en cas d'incident. Pour plus d'informations, voir "[Cas d'utilisation](#)".

## Concepts clés

La synchronisation active SnapMirror exploite des groupes de cohérence et le médiateur ONTAP pour assurer la réplication et le traitement de vos données, même en cas d'incident. Lors de la planification du déploiement de la synchronisation active SnapMirror, il est important de comprendre les concepts essentiels de la synchronisation active SnapMirror et de son architecture.

## Asymétrie et symétrie

La synchronisation active SnapMirror prend en charge les solutions asymétriques et, à partir de ONTAP 9.15.1, actives/actives symétriques. Ces options font référence à la façon dont les hôtes accèdent aux chemins de stockage et écrivent des données. Dans une configuration asymétrique, les données du site secondaire sont proxys vers un LUN. Dans une configuration actif-actif symétrique, les deux sites peuvent accéder au stockage local pour les E/S actives

Le mode actif-actif symétrique est optimisé pour les applications en cluster, notamment VMware VMSC, le cluster de basculement Windows avec SQL et Oracle RAC.

Pour plus d'informations, voir [Architecture de synchronisation active SnapMirror](#).

### Groupe de cohérence

A "[groupe de cohérence](#)" Est un ensemble de volumes FlexVol qui garantit la cohérence de la charge de travail applicative et qui doit être protégé pour la continuité de l'activité.

L'objectif d'un groupe de cohérence est de prendre des images Snapshot simultanées de plusieurs volumes, ce qui garantit des copies cohérentes après panne d'un ensemble de volumes à un moment donné. Un groupe de cohérence garantit que tous les volumes d'un dataset sont suspendus, puis aimantés précisément au même point dans le temps. Cela offre un point de restauration cohérent avec les données sur l'ensemble des volumes prenant en charge le dataset. Un groupe de cohérence conserve ainsi une cohérence dépendante de l'ordre d'écriture. Si vous décidez de protéger les applications pour la continuité de l'activité, le groupe de volumes correspondant à cette application doit être ajouté à un groupe de cohérence de sorte qu'une relation de protection des données soit établie entre un groupe de cohérence source et un groupe de cohérence de destination. La cohérence source et destination doit contenir le même nombre et le même type de volumes.

### Composant

LUN ou volume individuel faisant partie du groupe de cohérence protégé dans la relation de synchronisation active SnapMirror.

### Médiateur de ONTAP

Le "[Médiateur de ONTAP](#)" Reçoit des informations de santé sur les clusters et les nœuds ONTAP de peering, qui s'orchestrent entre les deux et déterminent si chaque nœud/cluster est en bon état et s'il est en cours d'exécution. Le médiateur ONTAP fournit des informations de santé sur :

- Clusters Peer ONTAP
- Nœuds de cluster Peer ONTAP
- Groupes de cohérence (qui définissent les unités de basculement dans une relation de synchronisation active SnapMirror) ; les informations suivantes sont fournies pour chaque groupe de cohérence :
  - État de la réplication : non initialisé, en synchronisation ou désynchronisé
  - Quel cluster héberge la copie principale
  - Contexte d'opération (utilisé pour le basculement planifié)

Grâce à ces informations sur l'état de santé du médiateur ONTAP, les clusters peuvent différencier différents types de défaillances et déterminer s'il faut effectuer un basculement automatique. Le médiateur ONTAP est l'un des trois intervenants du quorum de synchronisation active SnapMirror avec les deux clusters ONTAP (principal et secondaire). Pour parvenir à un consensus, au moins deux parties au quorum doivent accepter une certaine opération.



Depuis la version ONTAP 9.15.1, System Manager affiche l'état de votre relation de synchronisation active SnapMirror depuis l'un ou l'autre cluster. Vous pouvez également surveiller l'état du médiateur ONTAP depuis l'un des clusters dans System Manager. Dans les versions précédentes de ONTAP, System Manager affiche l'état des relations de synchronisation active SnapMirror depuis le cluster source.

### Basculement planifié

Opération manuelle pour modifier le rôle des copies dans une relation de synchronisation active SnapMirror. Les sites principaux deviennent les sites secondaires, et le site secondaire devient le site principal.

### Polarisation primaire en premier et primaire

La synchronisation active SnapMirror utilise un principe prioritaire qui donne la préférence à la copie principale pour traiter les E/S en cas de partition réseau.

Le principal biais est une implémentation spéciale de quorum qui améliore la disponibilité d'un dataset protégé par synchronisation active SnapMirror. Si la copie principale est disponible, le biais principal entre en vigueur lorsque le médiateur ONTAP n'est pas accessible depuis les deux clusters.

Le principal et le principal biais sont pris en charge dans la synchronisation active SnapMirror à partir de ONTAP 9.15.1. Les copies primaires sont désignées dans System Manager et sortent avec l'API REST et l'interface de ligne de commandes.

### Basculement automatique non planifié (AUFO)

Opération automatique pour effectuer un basculement vers la copie miroir. L'opération nécessite l'aide du médiateur ONTAP pour détecter que la copie principale n'est pas disponible.

### Non synchronisé (OOS)

Lorsque les E/S de l'application ne sont pas répliquées sur le système de stockage secondaire, elles sont signalées comme **hors synchronisation**. L'état « non synchronisé » signifie que les volumes secondaires ne sont pas synchronisés avec le volume primaire (source) et que la réplication SnapMirror n'est pas en cours.

Si l'état du miroir est `SnapshotMirrored`, indique un échec ou un échec de transfert dû à une opération non prise en charge.

La synchronisation active SnapMirror prend en charge la resynchronisation automatique qui permet le retour des copies à un état insync.

À partir de la version ONTAP 9.15.1, SnapMirror active Sync est pris en charge ["reconfiguration automatique dans les configurations « fan-out »"](#).

### Configuration uniforme et non uniforme

- **Accès hôte uniforme** signifie que les hôtes des deux sites sont connectés à tous les chemins vers les clusters de stockage sur les deux sites. Les chemins intersites sont étirés sur toute la distance.
- **Accès hôte non uniforme** signifie que les hôtes de chaque site sont connectés uniquement au cluster du même site. Les chemins intersites et les chemins étendus ne sont pas connectés.



Un accès uniforme à l'hôte est pris en charge pour tout déploiement SnapMirror à synchronisation active. L'accès non uniforme à l'hôte n'est pris en charge que pour les déploiements actif-actif symétriques.

### RPO nul

L'objectif RPO correspond à l'objectif de point de récupération, qui correspond à la quantité de perte de

données jugée acceptable au cours d'une période donnée. La valeur RPO de zéro signifie qu'aucune perte de données n'est acceptable.

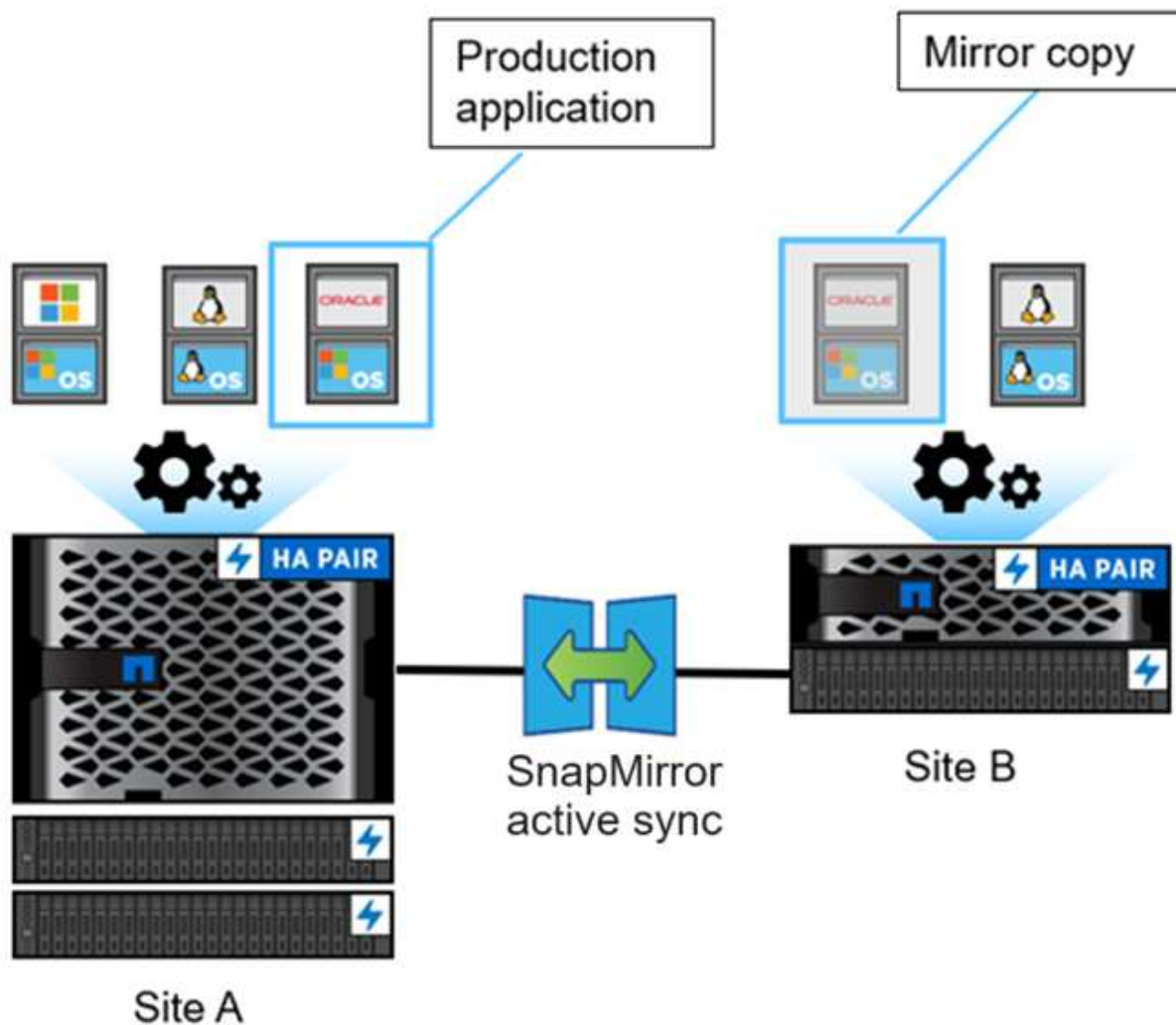
### **Le RTO nul**

L'objectif RTO désigne l'objectif de délai de restauration, qui correspond au temps jugé acceptable pour une application de reprendre son activité normale sans interruption suite à une panne, une défaillance ou tout autre événement de perte de données. La valeur zéro RTO indique qu'aucune interruption n'est acceptable.

### **Architecture de synchronisation active SnapMirror**

Grâce à l'architecture de synchronisation active SnapMirror, les charges de travail actives peuvent être traitées simultanément depuis les deux clusters afin de traiter les charges de travail principales. Dans certains pays, la réglementation applicable aux institutions financières exige également la maintenance périodique des entreprises à partir de leurs data centers secondaires. Les déploiements « Tick-Tock » sont également pris en charge par la synchronisation active SnapMirror.

La relation de protection des données à protéger pour la continuité de l'activité est créée entre le système de stockage source et le système de stockage de destination, en ajoutant au groupe de cohérence des LUN spécifiques à l'application provenant de différents volumes d'une machine virtuelle de stockage (SVM). Dans des conditions normales, l'application d'entreprise écrit sur le groupe de cohérence principal, qui réplique ces E/S de manière synchrone sur le groupe de cohérence du miroir.



Bien qu'il existe deux copies distinctes des données dans la relation de protection des données, étant donné que la synchronisation active SnapMirror conserve la même identité de LUN, l'hôte d'application la considère comme un périphérique virtuel partagé avec plusieurs chemins d'accès, alors qu'une seule copie de LUN est en cours d'écriture à la fois. Lorsqu'une panne met le système de stockage principal hors ligne, ONTAP détecte cette défaillance et utilise le médiateur pour la reconfirmation. Si ni ONTAP ni le médiateur ne peuvent envoyer d'requête ping au site principal, ONTAP effectue l'opération de basculement automatique. Ce processus entraîne le basculement d'une application spécifique uniquement, sans intervention manuelle ni script nécessaire auparavant pour le basculement.

Autres points à prendre en compte :

- Les volumes sans miroir qui sont en dehors de la protection pour la continuité de l'activité sont pris en charge.
- Une seule autre relation SnapMirror asynchrone est prise en charge pour les volumes protégés pour la continuité de l'activité.
- Les topologies en cascade ne sont pas prises en charge avec la protection pour la continuité de l'activité.

#### Médiateur de ONTAP

ONTAP Mediator est installé dans un troisième domaine de défaillance, distinct des deux clusters ONTAP. Son

rôle principal est de servir de témoin passif des copies actives de synchronisation SnapMirror. En cas de partition réseau ou d'indisponibilité d'une copie, le système SnapMirror Active Sync utilise Mediator pour déterminer quelle copie continue à transmettre les E/S, tout en interrompant les E/S sur l'autre copie. Cette configuration comprend trois composants clés :

- Cluster ONTAP principal hébergeant le groupe de cohérence principal de synchronisation active SnapMirror
- Cluster ONTAP secondaire hébergeant le groupe de cohérence miroir
- Médiateur de ONTAP

Le médiateur ONTAP joue un rôle crucial dans les configurations de synchronisation active SnapMirror en tant que témoin de quorum passif. Il assure la maintenance du quorum et facilite l'accès aux données en cas de défaillance. Il agit comme un proxy ping pour les contrôleurs afin de déterminer la vivacité des contrôleurs homologues. Bien que le Mediator ne déclenche pas activement les opérations de basculement, il fournit une fonction essentielle en permettant au nœud survivant de vérifier l'état de son partenaire pendant les problèmes de communication réseau. Dans son rôle de témoin de quorum, le médiateur ONTAP fournit un chemin alternatif (servant effectivement de proxy) au cluster homologue.

De plus, il permet aux clusters d'obtenir ces informations dans le cadre du processus de quorum. Il utilise la LIF node management et la LIF cluster management à des fins de communication. Il établit des connexions redondantes via plusieurs chemins afin de différencier les pannes de site et les défaillances de liaison ISL (interswitch Link). Lorsqu'un cluster perd la connexion avec le logiciel ONTAP Mediator et tous ses nœuds en raison d'un événement, il est considéré comme inaccessible. Cela déclenche une alerte et permet un basculement automatique vers le groupe de cohérence du miroir (CG) sur le site secondaire, ce qui garantit une continuité d'E/S pour le client. Le chemin d'accès aux données de réplication repose sur un mécanisme de pulsation. Si un problème de réseau ou un événement persiste au-delà d'une certaine période, cela peut entraîner des défaillances de pulsation, ce qui entraîne une désynchronisation de la relation. Toutefois, la présence de chemins redondants, comme le basculement de LIF vers un autre port, peut maintenir le signal de détection et éviter de telles perturbations.

Pour résumer, le médiateur ONTAP est utilisé aux fins suivantes :

- Établir un quorum
- Disponibilité continue via basculement automatique (AUFO)
- Basculements planifiés (PFO)



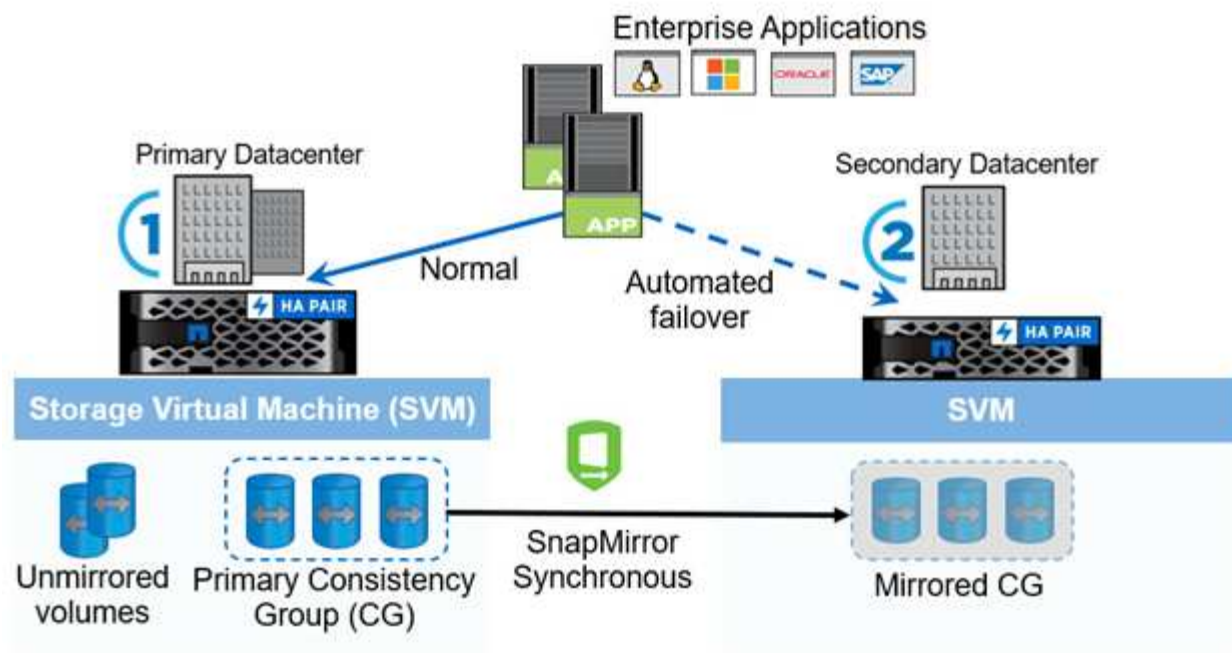
ONTAP Mediator 1.7 peut gérer dix paires de clusters à des fins de continuité de l'activité.



Lorsque le médiateur ONTAP n'est pas disponible, vous ne pouvez pas effectuer de basculements planifiés ou automatisés. La réplication synchrone des données d'application se poursuit sans interruption sur et sans aucune perte de données.

## Exploitation

La figure suivante illustre la conception générale de la synchronisation active SnapMirror.



Le schéma représente une application d'entreprise hébergée sur une machine virtuelle de stockage (SVM) au niveau du data Center principal. La SVM contient cinq volumes, dont trois font partie d'un groupe de cohérence. Les trois volumes du groupe de cohérence sont mis en miroir sur un data Center secondaire. Dans des circonstances normales, toutes les opérations d'écriture sont effectuées sur le data Center principal. Dans les faits, ce data Center sert de source pour les opérations d'E/S, tandis que le data Center secondaire sert de destination.

En cas d'incident au niveau du data Center principal, ONTAP charge le data Center secondaire d'agir comme le data Center principal, et de traiter toutes les opérations d'E/S. Seuls les volumes mis en miroir dans le groupe de cohérence sont gérés. Toutes les opérations relatives aux deux autres volumes du SVM sont affectées par le sinistre.

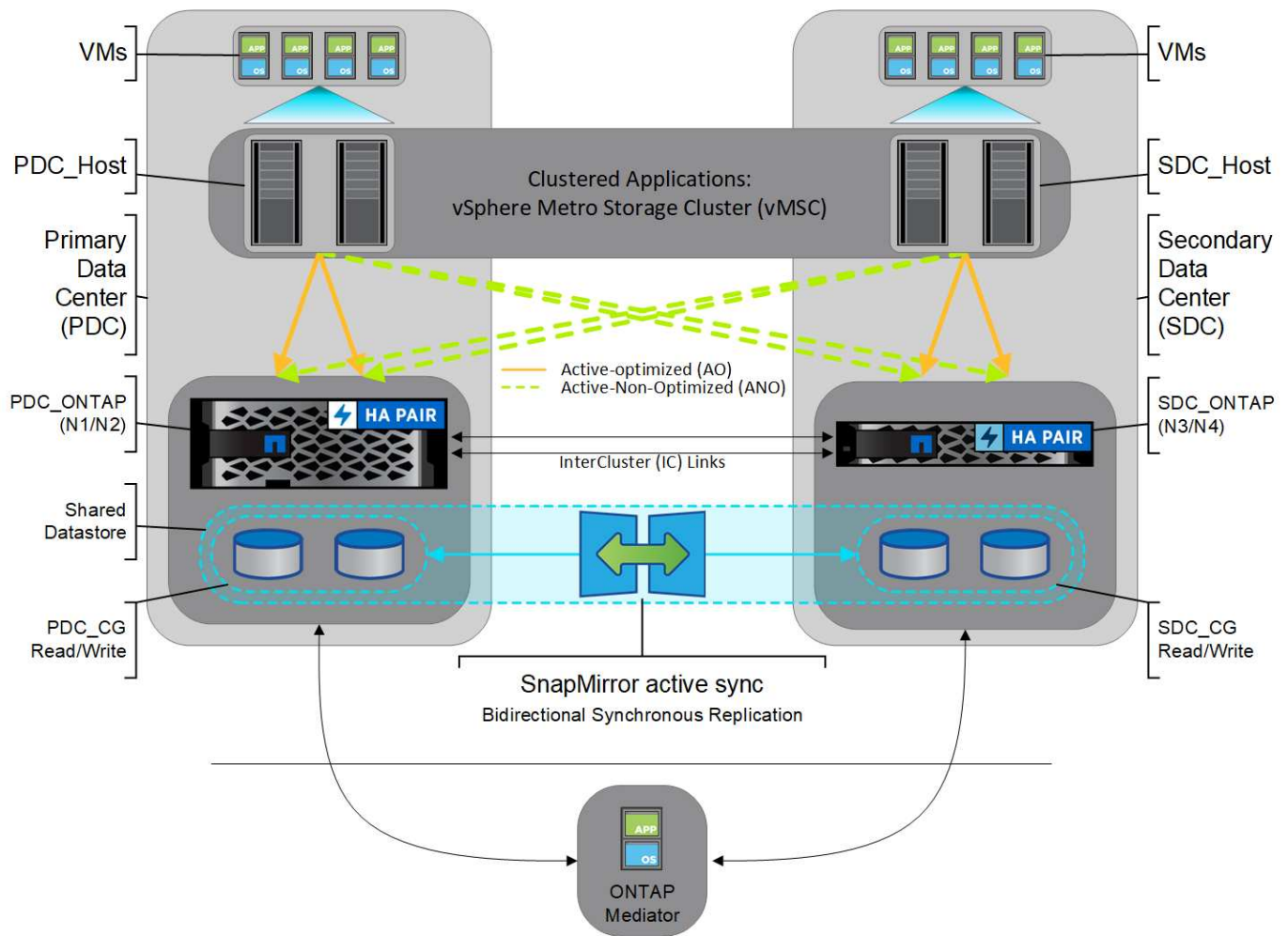
### Symétrie actif-actif

SnapMirror Active Sync offre des solutions asymétriques.

Dans les configurations *asymétriques*, la copie de stockage primaire expose un chemin optimisé pour le mode actif et traite activement les E/S du client. Le site secondaire utilise un chemin distant pour les E/S. Les chemins de stockage du site secondaire sont considérés comme actifs-non optimisés. L'accès à la LUN d'écriture est proxy depuis le site secondaire.

Dans les configurations *active/active symétriques*, les chemins optimisés pour le mode actif sont exposés sur les deux sites, sont spécifiques à l'hôte et sont configurables. Ainsi, les hôtes de chaque côté peuvent accéder au stockage local pour les E/S actives.





Le mode actif-actif symétrique est destiné aux applications en cluster, notamment VMware Metro Storage Cluster, Oracle RAC et Windows Failover Clustering avec SQL.

### Cas d'utilisation de la synchronisation active SnapMirror

Les exigences d'un environnement professionnel connecté à l'échelle mondiale exigent une restauration rapide des données des applications stratégiques sans aucune perte de données en cas de perturbation, par exemple une cyberattaque, une panne de courant ou une catastrophe naturelle. Ces exigences s'intensifient sur des domaines tels que les finances et le respect des obligations réglementaires telles que le Règlement général de l'Union européenne sur la protection des données (RGPD).

Les utilisations de SnapMirror Active Sync sont les suivantes :

#### Déploiement des applications pour un objectif de délai de restauration (RTO) nul

Dans un déploiement SnapMirror actif, vous disposez d'un cluster principal et d'un cluster secondaire. Une LUN dans le cluster principal **L1P** a un miroir (**L1S**) Sur le serveur secondaire ; les deux LUN partagent le même ID de série et sont signalées comme des LUN de lecture-écriture à l'hôte. En revanche, les opérations de lecture et d'écriture sont uniquement gérées sur le LUN principal, **L1P**. Toutes les écritures sont effectuées sur le miroir **L1S** sont servis par proxy.

#### Déploiement des applications sans RTO ni TAF

TAF est basé sur le basculement de chemin MPIO hôte basé sur le logiciel pour permettre un accès au



stockage sans interruption. Les deux copies de LUN (par exemple, primaire (L1P) et copie miroir (L1S) ont la même identité (numéro de série) et sont signalées comme accessibles en lecture-écriture à l'hôte. Toutefois, les lectures et écritures sont uniquement gérées par le volume primaire. Les E/S émises vers la copie miroir sont proxyés à la copie principale. Le chemin d'accès privilégié de l'hôte vers L1 est VS1:N1 basé sur l'état d'accès ALUA (Asymmetric Logical Unit Access) Active Optimized (A/O). ONTAP Mediator est nécessaire dans le cadre du déploiement, principalement pour effectuer un basculement (planifié ou non) en cas de panne du stockage primaire.

La synchronisation active SnapMirror utilise le protocole ALUA, qui permet à un logiciel de chemins d'accès multiples d'hôte d'application d'établir les chemins avec les priorités et la disponibilité d'accès pour la communication entre l'hôte d'application et la baie de stockage. Le protocole ALUA marque les chemins optimisés actifs vers les contrôleurs propriétaires de la LUN et d'autres comme chemins actifs non optimisés, utilisés uniquement en cas de défaillance du chemin principal.

### **Applications en cluster**

Les applications en cluster, notamment VMware Metro Storage Cluster, Oracle RAC et Windows Failover Clustering avec SQL, nécessitent un accès simultané afin que les VM puissent basculer vers un autre site sans impact sur les performances. La fonction actif-actif symétrique de SnapMirror sert les E/S localement avec la réplication bidirectionnelle afin de répondre aux exigences des applications en cluster.

### **Scénario d'incident**

Répliquez plusieurs volumes de manière synchrone pour une application entre des sites situés dans des sites dispersés géographiquement. En cas d'interruption du stockage primaire, vous pouvez basculer automatiquement vers la copie secondaire, assurant ainsi la continuité de l'activité pour les applications de niveau 1. Lorsque le site hébergeant le cluster principal rencontre un incident, le logiciel de chemins d'accès multiples hôte marque tous les chemins à travers le cluster comme descendant et utilise les chemins depuis le cluster secondaire. Il en résulte un basculement sans interruption activé par le médiateur ONTAP vers la copie miroir.

### **Basculement Windows**

La synchronisation active SnapMirror assure la flexibilité grâce à une granularité au niveau des applications et à un basculement automatique faciles à utiliser. La solution SnapMirror Active Sync utilise la réplication synchrone SnapMirror sur réseau IP pour répliquer des données à des vitesses élevées sur un réseau LAN ou WAN. Vous bénéficiez ainsi d'une haute disponibilité des données et d'une réplication rapide des données pour vos applications stratégiques, comme Oracle ou Microsoft SQL Server, dans des environnements physiques et virtuels.

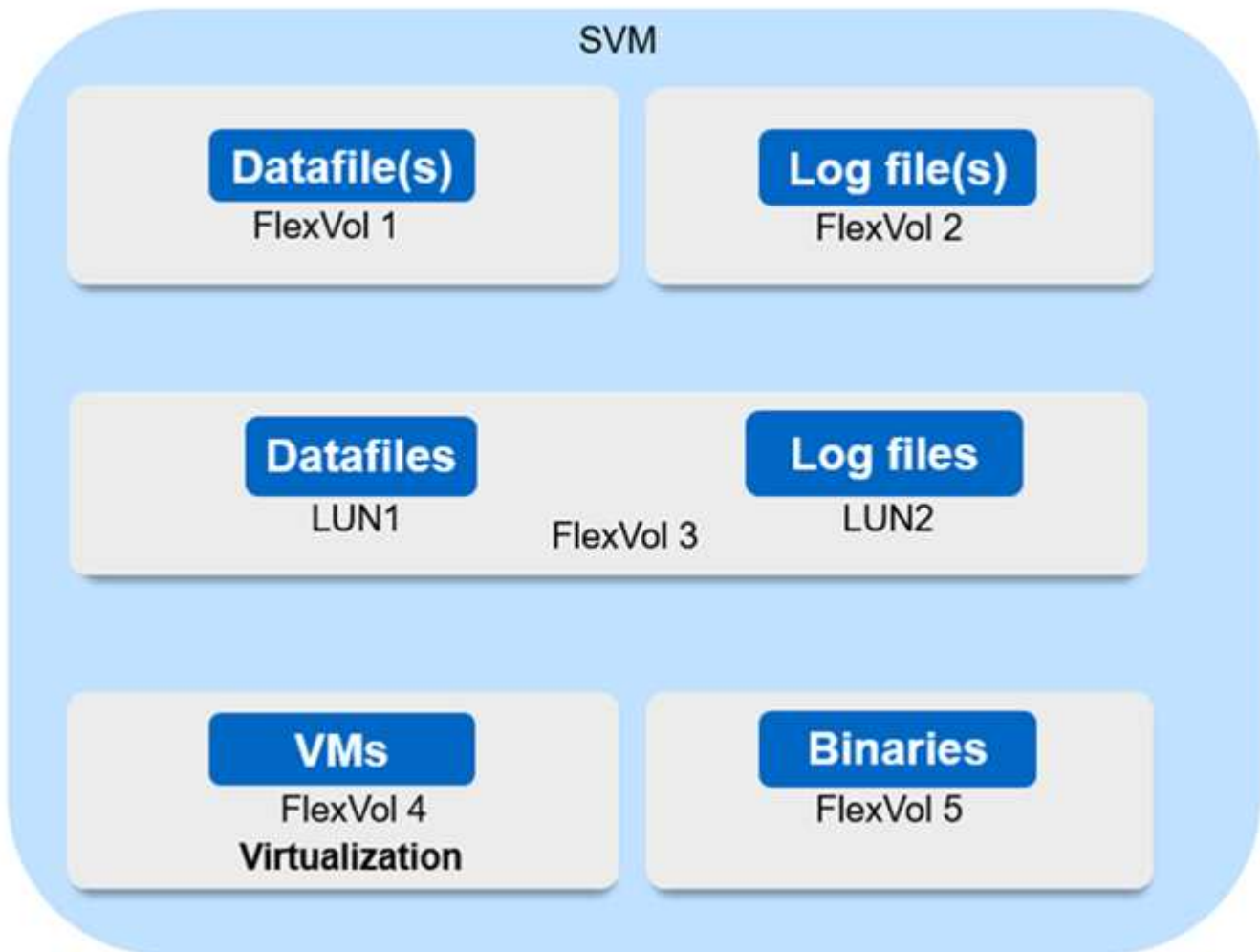
La synchronisation active SnapMirror assure le fonctionnement continu des services stratégiques, même en cas de défaillance complète du site, avec une mise au point automatique sur la copie secondaire. Aucune intervention manuelle ou aucun script supplémentaire n'est nécessaire pour déclencher ce basculement.

### **Stratégie de déploiement et bonnes pratiques pour la synchronisation active SnapMirror**

Il est important que votre stratégie de protection des données identifie clairement les workloads qui doivent être protégés pour assurer la continuité de l'activité. L'étape la plus critique de votre stratégie de protection des données est d'avoir une meilleure disposition des données des applications d'entreprise pour pouvoir décider de la manière dont vous distribuez les volumes et protégez la continuité de l'activité. Étant donné que le basculement a lieu au niveau des groupes de cohérence par application, veillez à ajouter les volumes de données nécessaires au groupe de cohérence.

## Configuration d'un SVM

Le diagramme représente la configuration recommandée pour les machines virtuelles de stockage (SVM) pour la synchronisation active SnapMirror.



- Pour les volumes de données :
  - Les charges de travail de lecture aléatoire sont isolées des écritures séquentielles. Par conséquent, selon la taille de la base de données, les données et les fichiers journaux sont généralement placés sur des volumes distincts.
    - Pour les grandes bases de données critiques, le fichier de données unique se trouve sur FlexVol 1 et son fichier journal correspondant sur FlexVol 2.
    - Pour une meilleure consolidation, les bases de données non stratégiques de petite à moyenne taille sont regroupées de manière à ce que tous les fichiers de données se trouvent sur FlexVol 1 et que les fichiers journaux correspondants se trouvent sur FlexVol 2. Cependant, vous perdrez la granularité au niveau de l'application par le biais de ce regroupement.
  - Une autre variante est d'avoir tous les fichiers dans le même FlexVol 3, avec les fichiers de données dans LUN1 et ses fichiers journaux dans le LUN 2.
- Si votre environnement est virtualisé, toutes les machines virtuelles des diverses applications d'entreprise sont partagées dans un datastore. En général, les VM et les binaires d'application sont répliqués de manière asynchrone à l'aide de SnapMirror.

## Planification

### Prérequis

Lors de la planification de votre déploiement de synchronisation active SnapMirror, assurez-vous de répondre aux différentes exigences en matière de matériel, de logiciels et de configuration système.

### Sous-jacent

- Seuls les clusters haute disponibilité à deux nœuds sont pris en charge
- Les deux clusters doivent être des baies AFF (y compris AFF C-Series) ou SAN 100 % Flash (ASA, y compris C-Series). Le mélange n'est pas pris en charge.

### Logiciel

- ONTAP 9.9.1 ou version ultérieure
- ONTAP Mediator 1.2 ou version ultérieure
- Un serveur Linux ou une machine virtuelle pour le médiateur ONTAP exécutant l'un des éléments suivants :

| Version du médiateur ONTAP | Versions Linux prises en charge                                                                                                                               |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.8                        | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux : 8.6, 8.7, 8.8, 8.9, 8.10, 9.2, 9.3 et 9.4</li><li>• Rocky Linux 8 et 9</li></ul>           |
| 1.7                        | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux : 8.5, 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2 et 9.3</li><li>• Rocky Linux 8 et 9</li></ul>       |
| 1.6                        | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux : 8.4, 8.5, 8.6, 8.7, 8.8, 9.0, 9.1, 9.2</li><li>• Rocky Linux 8 et 9</li></ul>              |
| 1.5                        | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul> |
| 1.4                        | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul> |
| 1.3                        | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul>           |
| 1.2                        | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 8.1</li><li>• CentOS: 7.6, 7.7, 7.8</li></ul>                               |

## Licences

- Une licence synchrone SnapMirror doit être appliquée aux deux clusters.
- Une licence SnapMirror doit être appliquée aux deux clusters.



Si vous avez acheté vos systèmes de stockage ONTAP avant juin 2019, consultez la page ["Clés de licence principales pour ONTAP NetApp"](#) Pour obtenir la licence synchrone SnapMirror requise.

## Environnement de mise en réseau

- Le temps de réponse aller-retour de latence entre clusters doit être inférieur à 10 millisecondes.
- À partir de ONTAP 9.14.1, ["Réservations persistantes SCSI-3"](#) Sont pris en charge avec la synchronisation active SnapMirror.

## Protocoles pris en charge

- Seuls les protocoles SAN sont pris en charge (pas NFS/SMB).
- Seuls les protocoles Fibre Channel et iSCSI sont pris en charge.
- L'IPspace par défaut est requis par SnapMirror Active Sync pour les relations entre clusters. L'IPspace personnalisé n'est pas pris en charge.

## Style de sécurité NTFS

La sécurité NTFS est **non** prise en charge sur les volumes SnapMirror actif sync.

## Médiateur de ONTAP

- Le médiateur ONTAP doit être provisionné en externe et connecté à ONTAP pour un basculement transparent des applications.
- Pour fonctionner entièrement et permettre un basculement non planifié automatique, le médiateur ONTAP externe doit être provisionné et configuré avec des clusters ONTAP.
- Le médiateur ONTAP doit être installé dans un troisième domaine de défaillance, distinct des deux clusters ONTAP.
- Lors de l'installation du médiateur ONTAP, vous devez remplacer le certificat auto-signé par un certificat valide signé par une autorité de certification grand public fiable.
- Pour plus d'informations sur le médiateur ONTAP, reportez-vous à la section ["Préparez-vous à installer le service ONTAP Mediator"](#).

## Volumes de destination en lecture/écriture

- Les relations de synchronisation active SnapMirror ne sont pas prises en charge sur les volumes de destination en lecture-écriture. Avant de pouvoir utiliser un volume en lecture-écriture, vous devez le convertir en volume DP en créant une relation SnapMirror au niveau du volume, puis en supprimant la relation. Pour plus de détails, voir ["Convertir une relation SnapMirror existante en synchronisation active SnapMirror"](#).

## Plus d'informations

- ["Hardware Universe"](#)

- ["Présentation du médiateur ONTAP"](#)

## Interopérabilité de la synchronisation active SnapMirror

La synchronisation active SnapMirror est compatible avec de nombreux systèmes d'exploitation, hôtes d'application et autres fonctionnalités d'ONTAP.



Pour obtenir des informations spécifiques sur la compatibilité et l'interopérabilité qui ne sont pas abordées ici, consultez la matrice d'interopérabilité ("[IMT](#)").

### Hôtes d'applications

La synchronisation active SnapMirror prend en charge les hôtes d'applications, notamment Hyper-V, Red Hat Enterprise Linux (RHEL), VMware, VMware vSphere Metro Storage Cluster (vMSC), Windows Server, et, depuis ONTAP 9.14.1, le cluster de basculement Windows Server.

### Systèmes d'exploitation

La synchronisation active SnapMirror est prise en charge par de nombreux systèmes d'exploitation, notamment :

- AIX via PVR (à partir de ONTAP 9.11.1)
- HP-UX (à partir de ONTAP 9.10.1)
- Solaris 11.4 (à partir de ONTAP 9.10.1)

### AIX

À partir de ONTAP 9.11.1, AIX est pris en charge avec la synchronisation active SnapMirror via PVR.

La synchronisation active SnapMirror peut assurer une protection des données avec un RPO nul, mais le processus de basculement avec AIX nécessite des étapes supplémentaires pour reconnaître le changement de chemin. Les LUN qui ne font pas partie d'un groupe de volumes racine subissent une pause d'E/S jusqu'à `cfgmgr` la commande est exécutée. Cette fonctionnalité peut être automatisée et la plupart des applications reprennent leurs opérations sans interruption supplémentaire.

Les LUN faisant partie d'un groupe de volumes root ne doivent généralement pas être protégées avec la synchronisation active SnapMirror. Il n'est pas possible d'exécuter `cfgmgr` Commande après un basculement, ce qui signifie qu'un redémarrage est nécessaire pour reconnaître les modifications apportées aux chemins SAN. Vous pouvez toujours assurer la protection des données avec un RPO nul au sein du groupe de volumes root, mais le basculement entraînera des perturbations.

Pour plus d'informations sur la synchronisation active de SnapMirror avec AIX, consultez votre équipe de compte NetApp.

### HP-UX

Depuis ONTAP 9.10.1, la synchronisation active SnapMirror pour HP-UX est prise en charge.

### Basculement automatique non planifié avec HP-UX

Un événement de basculement automatique non planifié (AUFO) sur le cluster maître isolé peut être causé par une défaillance de double événement lorsque la connexion entre le cluster principal et le cluster secondaire est perdue et que la connexion entre le cluster principal et le médiateur est également perdue. Ce phénomène est considéré comme un événement rare, contrairement à d'autres événements AUFO.

- Dans ce scénario, la reprise des E/S sur l'hôte HP-UX peut prendre plus de 120 secondes. Selon les applications en cours d'exécution, il se peut que cela n'entraîne aucune interruption d'E/S ni aucun message d'erreur.
- Pour résoudre ce problème, vous devez redémarrer les applications sur l'hôte HP-UX dont la tolérance d'interruption est inférieure à 120 secondes.

## Solaris

À partir de ONTAP 9.10.1, la synchronisation active SnapMirror prend en charge Solaris 11.4.

Pour vous assurer que les applications client Solaris ne sont pas perturbatrices lorsqu'un basculement de site non planifié se produit dans un environnement de synchronisation active SnapMirror, modifiez les paramètres par défaut du système d'exploitation Solaris. Pour configurer Solaris avec les paramètres recommandés, reportez-vous à l'article de la base de connaissances ["Prise en charge de l'hôte Solaris Paramètres recommandés dans la synchronisation active SnapMirror"](#).

## Interopérabilité ONTAP

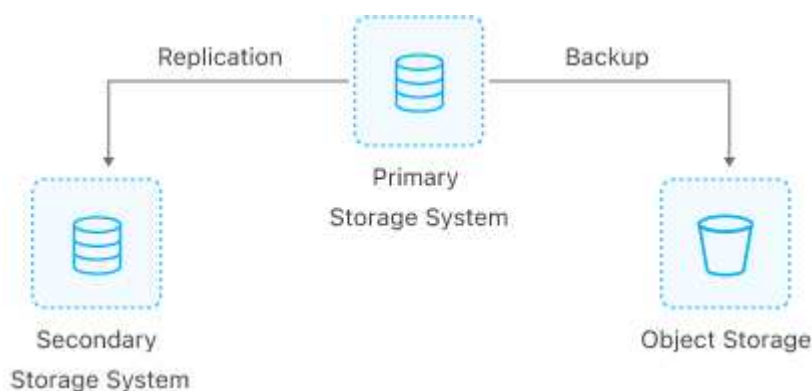
SnapMirror Active Sync s'intègre avec des composants de ONTAP afin d'étendre ses fonctions de protection des données.

## FabricPool

La synchronisation active SnapMirror prend en charge les volumes source et de destination sur les agrégats FabricPool avec des règles de Tiering aucune, Snapshot ou Auto. La synchronisation active SnapMirror ne prend pas en charge les agrégats FabricPool au moyen d'une règle de Tiering.

## Configurations « Fan-Out »

Dans [configurations « fan-out »](#), Votre volume source peut être mis en miroir vers un terminal de destination de synchronisation actif SnapMirror et vers une ou plusieurs relations asynchrones SnapMirror.



Prise en charge de la synchronisation active SnapMirror [configurations « fan-out »](#) avec le `MirrorAllSnapshots` Et, à partir de ONTAP 9.11.1, le `MirrorAndVault` politique. Les configurations « Fan-Out » ne sont pas prises en charge dans la synchronisation active SnapMirror avec le `XDPDefault` politique.

Depuis la version ONTAP 9.15.1, la synchronisation active SnapMirror prend en charge la reconfiguration automatique dans le segment « Fan-Out » après un événement de basculement. Si le basculement du site principal vers le site secondaire a réussi, le site tertiaire est automatiquement reconfiguré pour traiter le site secondaire comme la source. La reconfiguration est déclenchée par un basculement planifié ou non planifié. La reconfiguration a également lieu lors du retour arrière vers le site principal.

Pour plus d'informations sur la gestion de votre configuration de « Fan-Out » dans les versions précédentes de ONTAP, reportez-vous à la section [reprendre la protection dans la configuration du « fan-out »](#).

## Restauration NDMP

À partir de ONTAP 9.13.1, vous pouvez utiliser [NDMP pour copier et restaurer les données](#) Avec la synchronisation active SnapMirror. L'utilisation de NDMP permet de déplacer des données vers la source de synchronisation active SnapMirror pour effectuer une restauration sans interrompre la protection. Cette fonctionnalité est particulièrement utile dans les configurations « Fan-Out ».

## SnapCenter

SnapCenter prend en charge la synchronisation active SnapMirror à partir de "[SnapCenter 5.0](#)". SnapCenter permet de créer des snapshots qui peuvent être utilisés pour protéger et restaurer des applications et des machines virtuelles, ce qui permet de proposer des solutions de stockage toujours disponibles avec une granularité au niveau des applications.

## SnapRestore

La synchronisation active SnapMirror prend en charge les SnapRestore de fichier partiel et unique.

### SnapRestore à fichier unique

ONTAP 9.11.1 et [SnapRestore pour un seul fichier](#) Est pris en charge pour les volumes SnapMirror actifs synchronisés. Vous pouvez restaurer un fichier unique à partir d'une copie Snapshot répliquée à partir de la source de synchronisation active SnapMirror vers la destination. Étant donné que les volumes peuvent contenir une ou plusieurs LUN, cette fonctionnalité vous permet de mettre en œuvre une opération de restauration moins disruptive en restaurant de façon granulaire une seule LUN sans interrompre les autres LUN. Single File SnapRestore propose deux options : sur place et hors place.

### Fichier partiel SnapRestore

À partir de ONTAP 9.12.1, "[Restauration partielle de LUN](#)" Est pris en charge pour les volumes SnapMirror actifs synchronisés. Vous pouvez restaurer des données à partir de copies Snapshot créées par les applications et répliquées entre les volumes SnapMirror source (volume) de synchronisation active et cible (copie Snapshot). Une restauration partielle des LUN ou des fichiers peut s'avérer nécessaire si vous devez restaurer une base de données sur un hôte qui stocke plusieurs bases de données sur la même LUN. Pour utiliser cette fonctionnalité, vous devez connaître le décalage d'octets de départ des données et du nombre d'octets.

## Des LUN de grande taille et de grands volumes

La prise en charge de LUN et de volumes importants (supérieurs à 100 To) dépend de la version de ONTAP que vous utilisez et de votre plateforme.

### ONTAP 9.12.1P2 et versions ultérieures

- Pour ONTAP 9.12.1 P2 et versions ultérieures, la synchronisation active SnapMirror prend en charge des LUN de grande taille et des volumes de plus de 100 To sur ASA et AFF (y compris C-Series).



Pour les versions ONTAP 9.12.1P2 et ultérieures, vous devez vous assurer que les clusters principal et secondaire sont des baies SAN 100 % Flash (ASA) ou des baies 100 % Flash (AFF), et que ONTAP 9.12.1 P2 ou version ultérieure est installé sur les deux. Si le cluster secondaire exécute une version antérieure à ONTAP 9.12.1P2 ou si le type de baie n'est pas le même que le cluster principal, la relation synchrone peut être désynchronisée si le volume primaire dépasse 100 To.

### ONTAP 9.9.1 - 9.12.1P1

- Pour les versions ONTAP comprises entre ONTAP 9.9.1 et 9.12.1 P1 (inclus), les LUN de grande taille et les volumes de grande taille supérieurs à 100 To sont pris en charge uniquement sur les baies SAN 100 % Flash.



Pour les versions ONTAP comprises entre ONTAP 9.9.1 et 9.12.1 P2, vous devez vous assurer que les clusters principal et secondaire sont des baies SAN 100 % Flash, et que ONTAP 9.9.1 ou version ultérieure est installé sur les deux. Si le cluster secondaire exécute une version antérieure à ONTAP 9.9.1 ou s'il ne s'agit pas d'une baie SAN 100 % Flash, la relation synchrone peut être désynchronisée si le volume principal dépasse les 100 To.

### Plus d'informations

- ["Comment configurer un hôte AIX pour la synchronisation active SnapMirror"](#)

### Limites d'objet pour la synchronisation active SnapMirror

Lorsque vous vous préparez à utiliser la synchronisation active SnapMirror, tenez compte des limites d'objet suivantes.

#### Groupes de cohérence dans un cluster

Les limites de groupe de cohérence d'un cluster avec SnapMirror actif Sync sont calculées en fonction des relations et dépendent de la version de ONTAP utilisée. Les limites sont indépendantes de la plateforme.

| Version ONTAP                        | Nombre maximal de relations |
|--------------------------------------|-----------------------------|
| ONTAP 9.11.1 et versions ultérieures | 50                          |
| ONTAP 9.10.1                         | 20                          |
| ONTAP 9.9.1                          | 5                           |

#### Volumes par groupe de cohérence

Le nombre maximal de volumes par groupe de cohérence avec la synchronisation active SnapMirror est indépendant de la plateforme.



| Version ONTAP                        | Nombre maximal de volumes pris en charge dans une relation de groupe de cohérence |
|--------------------------------------|-----------------------------------------------------------------------------------|
| ONTAP 9.15.1 et versions ultérieures | 80                                                                                |
| ONTAP 9.10.1-9.14.1                  | 16                                                                                |
| ONTAP 9.9.1                          | 12                                                                                |

## Volumes

Dans SnapMirror, les limites de volume de la synchronisation active sont calculées sur la base du nombre de terminaux, et non du nombre de relations. Un groupe de cohérence de 12 volumes contribue à hauteur de 12 terminaux sur le cluster principal et le cluster secondaire. La synchronisation active SnapMirror et les relations synchrones SnapMirror contribuent toutes deux au nombre total de terminaux.

Le nombre maximum de terminaux par plateforme est inclus dans le tableau suivant.

| S. Non | Plateforme | Terminals par haute disponibilité pour la synchronisation active SnapMirror |              |             | Terminals de synchronisation actifs SnapMirror et de synchronisation globaux pour chaque haute disponibilité |              |             |
|--------|------------|-----------------------------------------------------------------------------|--------------|-------------|--------------------------------------------------------------------------------------------------------------|--------------|-------------|
|        |            | ONTAP 9.11.1 et versions ultérieures                                        | ONTAP 9.10.1 | ONTAP 9.9.1 | ONTAP 9.11.1 et versions ultérieures                                                                         | ONTAP 9.10.1 | ONTAP 9.9.1 |
| 1      | AFF        | 400                                                                         | 200          | 60          | 400                                                                                                          | 200          | 80          |
| 2      | ASA        | 400                                                                         | 200          | 60          | 400                                                                                                          | 200          | 80          |

## Limites D'objets SAN

Les limites des objets SAN sont incluses dans le tableau suivant. Les limites s'appliquent quelle que soit la plate-forme.

| Objet dans une relation de synchronisation active SnapMirror                    | Nombre                                                                                                                                              |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| LUN par volume                                                                  | 256                                                                                                                                                 |
| Mappages de LUN par nœud                                                        | <ul style="list-style-type: none"> <li>• 4096 (ONTAP 9.10 et versions ultérieures)</li> <li>• 2048 (ONTAP 9.9.1 et versions antérieures)</li> </ul> |
| Mappages de LUN par cluster                                                     | <ul style="list-style-type: none"> <li>• 8192 (ONTAP 9.10 et versions ultérieures)</li> <li>• 4096 (ONTAP 9.9.1 et versions antérieures)</li> </ul> |
| LIFs par SVM (avec au moins un volume dans une relation SnapMirror active Sync) | 256                                                                                                                                                 |
| LIF inter-cluster par nœud                                                      | 4                                                                                                                                                   |
| LIF inter-cluster par cluster                                                   | 8                                                                                                                                                   |

## Informations associées

- ["Hardware Universe"](#)
- ["Limites des groupes de cohérence"](#)

## Configurer

### Configurer le médiateur ONTAP et les clusters pour la synchronisation active SnapMirror

La synchronisation active SnapMirror utilise des clusters à peering pour assurer la disponibilité de vos données en cas de basculement. Le médiateur ONTAP est une ressource clé qui assure la continuité de l'activité et surveille l'état de santé de chaque cluster. Pour configurer la synchronisation active SnapMirror, vous devez d'abord installer le médiateur ONTAP et vous assurer que vos clusters principal et secondaire sont correctement configurés.

Une fois que vous avez installé le médiateur ONTAP et configuré vos clusters, vous devez le faire [\[initialize-the-ontap-mediator\]](#) Le médiateur ONTAP à utiliser avec la synchronisation active SnapMirror. Vous devez alors [Créer, initialisez et mappez le groupe de cohérence pour la synchronisation active SnapMirror.](#)

#### Médiateur de ONTAP

Le médiateur ONTAP fournit un magasin persistant et cloisonné pour les métadonnées haute disponibilité utilisées par les clusters ONTAP dans une relation de synchronisation active SnapMirror. De plus, ONTAP Mediator fournit une fonctionnalité de requête d'intégrité de nœud synchrone pour faciliter la détermination du quorum et sert de proxy ping pour la détection de la vivacité du contrôleur.

#### Conditions requises pour le médiateur ONTAP

- Le médiateur ONTAP comprend son propre ensemble de prérequis. Vous devez remplir ces conditions préalables avant d'installer le médiateur.

Pour plus d'informations, voir ["Préparez-vous à installer le service ONTAP Mediator"](#).

- Par défaut, le médiateur ONTAP fournit un service via le port TCP 31784. Assurez-vous que le port 31784 est ouvert et disponible entre les clusters ONTAP et le médiateur.

#### Installer le médiateur ONTAP et confirmer la configuration du cluster

Suivez chacune des étapes suivantes. Pour chaque étape, vous devez confirmer que la configuration spécifique a été effectuée. Utilisez le lien fourni après chaque étape pour obtenir plus d'informations si nécessaire.

#### Étapes

1. Installez le service Mediator ONTAP avant de vous assurer que vos clusters source et destination sont correctement configurés.

[Préparez l'installation ou la mise à niveau du service Mediator ONTAP](#)

2. Vérifier qu'une relation de peering de cluster existe entre les clusters



L'IPspace par défaut est requis par SnapMirror Active Sync pour les relations entre clusters. Un IPspace personnalisé n'est pas pris en charge.

[Configurer les relations de pairs](#)

3. Vérifier que les machines virtuelles de stockage sont créées sur chaque cluster

#### [Création d'un SVM](#)

4. Vérifiez qu'il existe une relation homologue entre les machines virtuelles de stockage de chaque cluster.

#### [Création d'une relation de SVM peering](#)

5. Vérifiez que les volumes existent pour vos LUN.

#### [Création d'un volume](#)

6. Confirmer qu'au moins une LIF SAN est créée sur chaque nœud du cluster

#### ["Considérations relatives aux LIF dans un environnement SAN de cluster"](#)

#### ["Création d'une LIF"](#)

7. Vérifiez que les LUN nécessaires sont créées et mappées sur un groupe initiateur, qui est utilisé pour mapper les LUN sur l'initiateur sur l'hôte d'application.

#### [Créer des LUN et mapper des igroups](#)

8. Relancez l'analyse de l'hôte de l'application pour détecter toute nouvelle LUN.

### **Initialiser le médiateur ONTAP pour la synchronisation active SnapMirror à l'aide de certificats auto-signés**

Une fois que vous avez installé le médiateur ONTAP et confirmé la configuration du cluster, vous devez initialiser le médiateur ONTAP pour la surveillance du cluster. Vous pouvez initialiser le médiateur ONTAP à l'aide du Gestionnaire système ou de l'interface de ligne de commande ONTAP.

## System Manager

Avec System Manager, vous pouvez configurer le serveur ONTAP Mediator pour un basculement automatisé. Vous pouvez également remplacer le SSL et l'autorité de certification auto-signés par le certificat SSL et l'autorité de certification validés par un tiers si vous ne l'avez pas déjà fait.

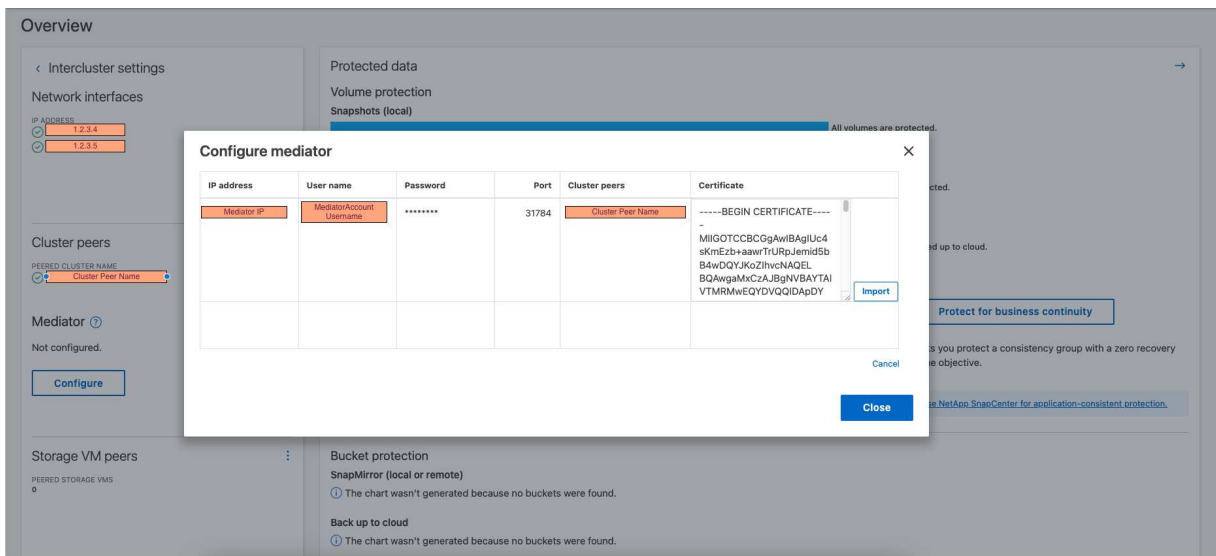


De ONTAP 9.8 à 9.14.1, la synchronisation active SnapMirror est appelée SnapMirror Business Continuity (SM-BC).

### Étapes

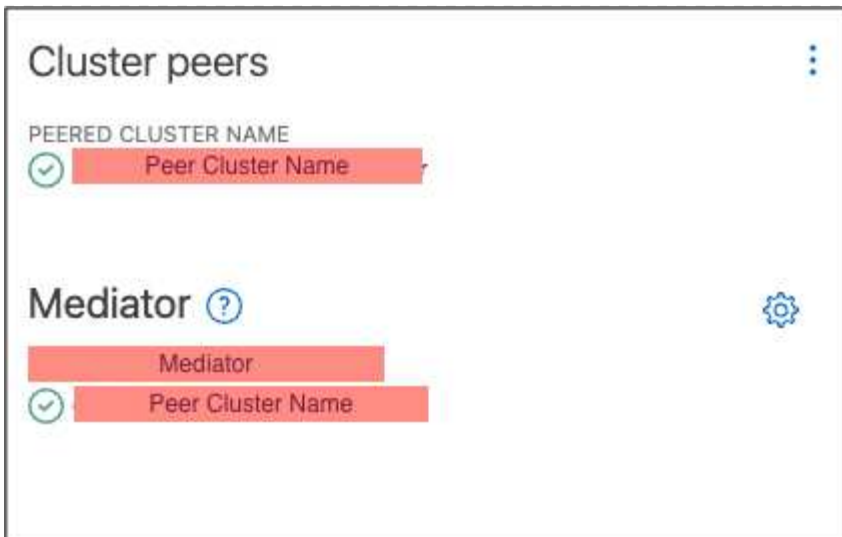
1. Accédez à **protection > vue d'ensemble > Médiateur > configurer**.
2. Sélectionnez **Ajouter** et entrez les informations suivantes sur le serveur ONTAP Mediator :
  - Adresse IPv4
  - Nom d'utilisateur
  - Mot de passe
  - Certificat
3. Vous pouvez fournir l'entrée de certificat de deux manières :
  - **Option (a)** : sélectionnez **Importer** pour accéder à l' `.crt` et importez-le.
  - **Option (b)** : copier le contenu du `.crt` Classez et collez-les dans le champ **Certificate**.

Lorsque tous les détails sont saisis correctement, le certificat fourni est installé sur tous les clusters homologues.



Une fois l'ajout du certificat terminé, le médiateur ONTAP est ajouté au cluster ONTAP.

L'image suivante montre une configuration réussie du médiateur ONTAP :



## CLI

Vous pouvez initialiser le médiateur ONTAP à partir du cluster principal ou secondaire à l'aide de l'interface de ligne de commande ONTAP. Lorsque vous émettez le `mediator add` Sur un cluster, le médiateur ONTAP est automatiquement ajouté sur l'autre cluster.

Le médiateur ONTAP ne peut pas être initialisé dans ONTAP sans un certificat d'autorité de certification valide. Par conséquent, vous devez ajouter une autorité de certification valide au magasin de certificats pour les clusters à peering.

## Étapes

1. Recherchez le certificat de l'autorité de certification du médiateur ONTAP à l'emplacement d'installation du logiciel hôte/VM ONTAP Mediator Linux `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. Ajoutez une autorité de certification valide au magasin de certificats sur le cluster peering.

## Exemple

```
[root@ontap-mediator server_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
BAoMDE5ldEFwcCwgSW5jLjJELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
...
p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----
```

3. Ajoutez le certificat de l'autorité de certification du médiateur ONTAP à un cluster ONTAP. Lorsque vous y êtes invité, insérez le certificat de l'autorité de certification obtenu auprès du médiateur ONTAP. Répétez les étapes sur tous les clusters homologues :

```
security certificate install -type server-ca -vserver <vserver_name>
```

## Exemple

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@ontap-mediator server_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFtATBgNV
BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAGMCkNhbgGlm3Ju
...
p+jdg5bG6lcxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----
```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster
```

Please enter Certificate: Press when done

```
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFtATBgNV
BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAGMCkNhbgGlm3Ju
...
p+jdg5bG6lcxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----
```

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

```
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX
```

The certificate's generated name for reference: ONTAPMediatorCA

```
C1_test_cluster::*>
```

4. Afficher le certificat d'autorité de certification auto-signé installé à l'aide du nom généré du certificat :

```
security certificate show -common-name <common_name>
```

### Exemple

```

C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver Serial Number Certificate Name
Type

C1_test_cluster
 6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
 ONTAPMediatorCA
server-ca
 Certificate Authority: ONTAP Mediator CA
 Expiration Date: Thu Feb 15 14:35:25 2029

```

5. Initialisez le médiateur ONTAP sur l'un des clusters. Le médiateur ONTAP est automatiquement ajouté pour l'autre cluster :

```

snapmirror mediator add -mediator-address <ip_address> -peer-cluster
<peer_cluster_name> -username user_name

```

#### Exemple

```

C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: *****
Enter the password again: *****

```

6. Vérifier l'état de la configuration du médiateur ONTAP :

```

snapmirror mediator show

```

| Mediator Address | Peer Cluster    | Connection Status | Quorum Status |
|------------------|-----------------|-------------------|---------------|
| 1.2.3.4          | C2_test_cluster | connected         | true          |

Quorum Status Indique si les relations du groupe de cohérence SnapMirror sont synchronisées avec le médiateur ONTAP ; le statut est true indique une synchronisation réussie.

#### Réinitialiser le médiateur ONTAP avec des certificats tiers

Vous devrez peut-être réinitialiser le service de médiateur ONTAP. Il peut y avoir des situations qui nécessitent la réinitialisation du service de médiateur ONTAP, telles qu'une modification de l'adresse IP du médiateur ONTAP, l'expiration du certificat, etc.

La procédure suivante illustre la réinitialisation du médiateur ONTAP pour un cas spécifique lorsqu'un certificat auto-signé doit être remplacé par un certificat tiers.

### **Description de la tâche**

Vous devez remplacer les certificats auto-signés du cluster SM-BC par des certificats tiers, supprimer la configuration du médiateur ONTAP de ONTAP, puis ajouter le médiateur ONTAP.



## System Manager

Avec System Manager, vous devez supprimer du cluster ONTAP le médiateur ONTAP configuré avec l'ancien certificat auto-signé et reconfigurer le cluster ONTAP avec le nouveau certificat tiers.

### Étapes

1. Sélectionnez l'icône des options de menu et sélectionnez **Supprimer** pour supprimer le Mediator ONTAP.



Cette étape ne supprime pas le serveur autosigné Server-ca du cluster ONTAP. NetApp recommande d'accéder à l'onglet **certificat** et de le supprimer manuellement avant d'effectuer l'étape suivante ci-dessous pour ajouter un certificat tiers :

| IP address        | User name | Password | Port  | Cluster peers     | Certificate |
|-------------------|-----------|----------|-------|-------------------|-------------|
| Mediator IP       |           |          | 31784 | Peer Cluster Name |             |
| <div>Remove</div> |           |          |       |                   |             |
| <div>+ Add</div>  |           |          |       |                   |             |

Close

2. Ajoutez à nouveau le médiateur ONTAP avec le bon certificat.

Le médiateur ONTAP est maintenant configuré avec le nouveau certificat auto-signé par un tiers.

Overview

Intercluster settings

Protected data

Configure mediator

| IP address  | User name                | Password | Port  | Cluster peers     | Certificate                                                                                                                                           |
|-------------|--------------------------|----------|-------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mediator IP | MediatorAccount Username | *****    | 31784 | Cluster Peer Name | -----BEGIN CERTIFICATE-----<br>MIIGOTCCBCGgAwIBAgIUc4<br>sKmiEzb+awwTRUpJemid5b<br>B4wDQYJKoZIhvcNAQEL<br>BQAwgMxKZAJBgNVBAYTAI<br>VTMRMwEQYDVQIDApDY |

Import

Cancel

Close

## CLI

Vous pouvez réinitialiser le médiateur ONTAP à partir du cluster principal ou secondaire en utilisant

l'interface de ligne de commande ONTAP pour remplacer le certificat auto-signé par le certificat tiers.

## Étapes

1. Supprimez l'auto-signature `ca.crt` installé plus tôt lorsque vous avez utilisé des certificats auto-signés pour tous les clusters. Dans l'exemple ci-dessous, il y a deux clusters :

### Exemple

```
C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
2 entries were deleted.

C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
2 entries were deleted.
```

2. Supprimez le médiateur ONTAP précédemment configuré du cluster SM-BC à l'aide de `-force true`:

### Exemple

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster Connection Status Quorum Status

1.2.3.4 C2_test_cluster connected true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
 exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. Reportez-vous aux étapes décrites dans la section ["Remplacez les certificats auto-signés par des certificats tiers approuvés"](#) sur la façon d'obtenir des certificats de l'autorité de certification subordonnée, appelée `ca.crt`. Remplacez les certificats auto-signés par des certificats tiers approuvés



Le `ca.crt` Possède certaines propriétés qu'il dérive de la demande qui doit être envoyée à l'autorité PKI, définie dans le fichier `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/open_ssl_ca.cnf`.

4. Ajoutez le nouveau certificat d'autorité de certification ONTAP Mediator tiers `ca.crt` À partir de l'emplacement d'installation du logiciel hôte/VM ONTAP Mediator Linux :

#### Exemple

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator server_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAGMCkNhbGlm3Ju
...
p+jdg5bG6lcxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----
```

5. Ajoutez le `ca.crt` dans le cluster peering. Répétez cette étape pour tous les clusters homologues :

#### Exemple

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster
```

Please enter Certificate: Press when done

```
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAGMCkNhbGlm3Ju
...
p+jdg5bG6lcxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----
```

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

CA: ONTAP Mediator CA  
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

```
C1_test_cluster::*>
```

6. Supprimez le médiateur ONTAP précédemment configuré du cluster de synchronisation active SnapMirror :

**Exemple**

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster Connection Status Quorum Status

1.2.3.4 C2_test_cluster connected true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. Ajoutez de nouveau le médiateur ONTAP :

**Exemple**

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster Connection Status Quorum Status

1.2.3.4 C2_test_cluster connected true
```

Quorum Status Indique si les relations de groupe de cohérence SnapMirror sont synchronisées avec le médiateur ; le statut est true indique une synchronisation réussie.

**Protégez votre infrastructure avec la synchronisation active SnapMirror**

La synchronisation active SnapMirror offre une protection asymétrique et, à partir de ONTAP 9.15.1, une protection actif-actif symétrique.

## Configurer la protection asymétrique

Configurer la protection asymétrique à l'aide de SnapMirror Active Sync implique de sélectionner des LUN sur le cluster source ONTAP et de les ajouter à un groupe de cohérence.

### Avant de commencer

- Vous devez disposer d'une licence SnapMirror synchrone.
- Vous devez être un administrateur de cluster ou de machines virtuelles de stockage.
- Tous les volumes constitutifs d'un groupe de cohérence doivent se trouver dans une seule VM de stockage (SVM).
  - Les LUN peuvent résider sur des volumes différents.
- Le cluster source et le cluster destination ne peuvent pas être identiques.
- Vous ne pouvez pas établir de relations de groupe de cohérence avec la synchronisation active SnapMirror entre les clusters ASA et les clusters non-ASA.
- L'IPspace par défaut est requis par SnapMirror Active Sync pour les relations entre clusters. L'IPspace personnalisé n'est pas pris en charge.
- Le nom du groupe de cohérence doit être unique.
- Les volumes du cluster secondaire (destination) doivent être de type DP.
- Les SVM primaire et secondaire doivent être en relation de peering.

### Étapes

Vous pouvez configurer un groupe de cohérence via l'interface de ligne de commandes ONTAP ou System Manager.

Depuis ONTAP 9.10.1, ONTAP propose un menu et un terminal de groupe de cohérence dans System Manager, ainsi que des utilitaires de gestion supplémentaires. Si vous utilisez ONTAP 9.10.1 ou une version ultérieure, reportez-vous à la section "[Configurer un groupe de cohérence](#)" ensuite "[configurer la protection](#)". Pour créer une relation synchrone active SnapMirror.



De ONTAP 9.8 à 9.14.1, la synchronisation active SnapMirror est appelée SnapMirror Business Continuity (SM-BC).

## System Manager

1. Sur le cluster principal, accédez à **protection > Présentation > protéger pour la continuité de l'activité > protéger les LUN**.
2. Sélectionnez les LUN que vous souhaitez protéger et ajoutez-les à un groupe de protection.
3. Sélectionner le cluster de destination et le SVM.
4. **Initialize relation** est sélectionné par défaut. Cliquez sur **Save** pour commencer la protection.
5. Accédez à **Tableau de bord > performances** pour vérifier l'activité IOPS des LUN.
6. Sur le cluster de destination, utilisez System Manager pour vérifier que la protection de la relation de continuité de l'activité est en mode synchrone : **protection > relations**.

## CLI

1. Créez une relation de groupe de cohérence à partir du cluster destination.  
`destination::> snapmirror create -source-path source-path -destination-path destination-path -cg-item-mappings volume-paths -policy policy-name`

Vous pouvez mapper jusqu'à 12 volumes constitutifs à l'aide du `cg-item-mappings` sur le `snapmirror create` commande.

La création de deux groupes de cohérence dans l'exemple suivant : `cg_src_` on the source with ``vol1` et `vol2` et un groupe de cohérence de destination en miroir, `cg_dst`.

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
```

2. Depuis le cluster de destination, initialisez le groupe de cohérence.

```
destination::> snapmirror initialize -destination-path destination-
consistency-group
```

3. Confirmer que l'opération d'initialisation a réussi. Le statut doit être de `InSync`.

```
snapmirror show
```

4. Sur chaque cluster, créez un groupe initiateur afin de mapper les LUN sur l'initiateur de l'hôte d'application.  
`lun igroup create -igroup name -protocol fc|iscsi -ostype os -initiator initiator_name`

5. Sur chaque cluster, mappez les LUN sur le groupe initiateur :

```
lun map -path path_name -igroup igroup_name
```

6. Vérifiez que le mappage de LUN a réussi avec le `lun map` commande. Vous pouvez ensuite détecter les nouveaux LUN sur l'hôte d'application.

## Configurer la protection actif-actif symétrique

Vous pouvez établir une protection symétrique à l'aide de System Manager ou de l'interface de ligne de

commande de ONTAP. Dans les deux interfaces, il existe différentes étapes pour [configurations uniformes et non uniformes](#).

#### **Avant de commencer**

- Les deux clusters doivent exécuter ONTAP 9.15.1 ou une version ultérieure.
- Les configurations actif-actif symétriques nécessitent le AutomatedFailoverDuplex règles de protection. Sinon, vous pouvez [Créez une règle SnapMirror personnalisée](#) à condition que le `-type` est `automated-failover-duplex`.

## Exemple 29. Étapes

### System Manager

#### Étapes pour une configuration uniforme

1. Sur le site principal, "[Créez un groupe de cohérence à l'aide des nouvelles LUN.](#)"
  - a. Lors de la création du groupe de cohérence, spécifiez les initiateurs hôtes à créer des igroups.
  - b. Cochez la case **Activer SnapMirror** puis choisissez le `AutomatedFailoverDuplex` politique.
  - c. Dans la boîte de dialogue qui s'affiche, cochez la case **répliquer les groupes initiateurs** pour répliquer les groupes initiateurs. Dans **Edit proximal settings**, définissez les SVM proximales pour vos hôtes.
  - d. Sélectionnez **Enregistrer**.

#### Étapes d'une configuration non uniforme

1. Sur le site principal, "[Créez un groupe de cohérence à l'aide des nouvelles LUN.](#)"
  - a. Lors de la création du groupe de cohérence, spécifiez les initiateurs hôtes à créer des igroups.
  - b. Cochez la case **Activer SnapMirror** puis choisissez le `AutomatedFailoverDuplex` politique.
  - c. Sélectionnez **Save** pour créer les LUN, le groupe de cohérence, le groupe initiateur, la relation SnapMirror et le mappage des groupes initiateur.
2. Sur le site secondaire, créez un groupe initiateur et mappez les LUN.
  - a. Accédez à **hosts > SAN Initiator Groups**.
  - b. Sélectionnez **+Ajouter** pour créer un nouveau groupe initiateur.
  - c. Indiquez un **Nom**, sélectionnez le **système d'exploitation hôte**, puis choisissez **membres du groupe initiateur**.
  - d. Sélectionnez **Enregistrer**.
3. Mappez le nouveau groupe initiateur sur les LUN de destination.
  - a. Accédez à **stockage > LUN**.
  - b. Sélectionnez toutes les LUN à mapper sur le groupe initiateur.
  - c. Sélectionnez **plus** puis **Mapper sur les groupes initiateurs**.

### CLI

#### Étapes pour une configuration uniforme

1. Créez une nouvelle relation SnapMirror regroupant tous les volumes de l'application. Assurez-vous de désigner le `AutomatedFailOverDuplex` règle d'établissement de la réplication synchrone bidirectionnelle.

```
snapmirror create -source-path source_path -destination-path
destination_path -cg-item-mappings source_volume:@destination_volume
-policy AutomatedFailOverDuplex
```

2. Confirmer que l'opération a réussi en attendant le `Mirrored State` pour afficher sous SnapMirrored et le `Relationship Status` comme `Insync`.

```
snapmirror show -destination-path destination_path
```

3. Sur votre hôte, configurez la connectivité hôte avec l'accès à chaque cluster en fonction de vos



besoins.

4. Établissement de la configuration du groupe initiateur. Définissez les chemins d'accès préférés des initiateurs sur le cluster local. Spécifiez l'option permettant de répliquer la configuration vers l'affinité inverse du cluster homologue.

```
SiteA::> igroup create -vserver svm_name -os-type os_type -igroup
igroup_name -replication-peer peer_svm_name -initiator host
```

```
SiteA::> igroup add -vserver svm_name -igroup igroup_name -os-type os_type
-initiator host
```

5. Depuis l'hôte, détectez les chemins et vérifiez que les hôtes disposent d'un chemin actif/optimisé vers la LUN de stockage à partir du cluster préféré.
6. Déployez l'application et distribuez les charges de travail des machines virtuelles entre les clusters pour atteindre l'équilibrage de charge requis.

### Étapes d'une configuration non uniforme

1. Créez une nouvelle relation SnapMirror regroupant tous les volumes de l'application. Assurez-vous de désigner la stratégie 'AutomatedFailOverDuplex' pour établir une réplication de synchronisation bidirectionnelle.

```
snapmirror create -source-path source_path -destination-path
destination_path -cg-item-mappings source_volume:@destination_volume
-policy AutomatedFailOverDuplex
```

2. Confirmer que l'opération a réussi en attendant le Mirrored State pour afficher sous SnapMirrored et le Relationship Status comme Insync.

```
snapmirror show -destination-path destination_path
```

3. Sur votre hôte, configurez la connectivité hôte avec l'accès à chaque cluster en fonction de vos besoins.
4. Établissement des configurations de groupe initiateur sur le cluster source et le cluster destination

```
primary site
SiteA::> igroup create -vserver svm_name -igroup igroup_name -initiator
host_1_name
```

```
secondary site
SiteB::> igroup create -vserver svm_name -igroup igroup_name -initiator
host_2_name
```

5. Depuis l'hôte, détectez les chemins et vérifiez que les hôtes disposent d'un chemin actif/optimisé vers la LUN de stockage à partir du cluster préféré.
6. Déployez l'application et distribuez les charges de travail des machines virtuelles entre les clusters pour atteindre l'équilibrage de charge requis.

### Convertir une relation SnapMirror existante en relation SnapMirror active Sync

Si vous avez configuré la protection SnapMirror, vous pouvez convertir la relation en

synchronisation active SnapMirror. À partir de ONTAP 9.15.1, vous pouvez convertir la relation pour utiliser une protection active/active symétrique.

#### Convertir une relation SnapMirror existante en relation SnapMirror active Sync asymétrique

Si vous avez déjà une relation synchrone SnapMirror entre un cluster source et un cluster destination, vous pouvez la convertir en relation synchrone SnapMirror asymétrique. Vous pouvez ainsi associer les volumes en miroir à un groupe de cohérence, garantissant ainsi un RPO nul sur une charge de travail à plusieurs volumes. En outre, vous pouvez conserver les snapshots SnapMirror existants si vous devez revenir à un point dans le temps avant d'établir la relation de synchronisation active SnapMirror.

#### Description de la tâche

- Vous devez être administrateur du cluster et SVM sur les clusters principal et secondaire.
- Vous ne pouvez pas convertir le RPO nul en synchronisation RTO zéro en modifiant la règle SnapMirror.
- Vous devez vous assurer que le mappage des LUN est annulé avant d'émettre le `snapmirror create` commande.

Si les LUN existantes du volume secondaire sont mappées et l'AutomatedFailover la règle est configurée, le `snapmirror create` la commande déclenche une erreur.

#### Avant de commencer

- Une relation synchrone de SnapMirror avec RPO nul doit exister entre le cluster principal et le cluster secondaire.
- Avant de pouvoir créer la relation SnapMirror avec un objectif RTO nul, toutes les LUN du volume de destination doivent être démappées.
- La synchronisation active SnapMirror prend uniquement en charge les protocoles SAN (pas NFS/CIFS). Assurez-vous qu'aucun composant du groupe de cohérence n'est monté pour l'accès au NAS.

#### Étapes

1. Depuis le cluster secondaire, effectuer une mise à jour SnapMirror sur la relation existante :

```
SiteB::>snapmirror update -destination-path vs1_dst:vol1
```

2. Vérifier que la mise à jour SnapMirror a été correctement effectuée :

```
SiteB::>snapmirror show
```

3. Mettez en pause chacune des relations synchrones avec RPO nul :

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1
```

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. Supprimez chacune des relations synchrones RPO zéro :

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol1
```

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol2
```

5. Relâcher la relation SnapMirror source mais conserver les copies Snapshot courantes :

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol1
```

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol2
```

#### 6. Créer une relation SnapMirror synchrone à objectif de durée de restauration nul :

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailover
```

#### 7. Resynchroniser le groupe de cohérence :

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

#### 8. Relancez les chemins d'E/S de la LUN hôte pour restaurer tous les chemins d'accès aux LUN.

### Convertir une relation SnapMirror en relation actif-actif symétrique

Depuis la version ONTAP 9.15.1, vous pouvez convertir une relation SnapMirror existante en relation actif-actif symétrique SnapMirror synchrone.

#### Avant de commencer

- Vous devez exécuter ONTAP 9.15.1 ou une version ultérieure.
- Une relation synchrone de SnapMirror avec RPO nul doit exister entre le cluster principal et le cluster secondaire.
- Avant de pouvoir créer la relation SnapMirror avec un objectif RTO nul, toutes les LUN du volume de destination doivent être démappées.
- La synchronisation active SnapMirror prend uniquement en charge les protocoles SAN (pas NFS/CIFS). Assurez-vous qu'aucun composant du groupe de cohérence n'est monté pour l'accès au NAS.

#### Étapes

##### 1. Depuis le cluster secondaire, effectuer une mise à jour SnapMirror sur la relation existante :

```
SiteB::>snapmirror update -destination-path vs1_dst:vol1
```

##### 2. Vérifier que la mise à jour SnapMirror a été correctement effectuée :

```
SiteB::>snapmirror show
```

##### 3. Mettez en pause chacune des relations synchrones avec RPO nul :

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1
```

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
```

##### 4. Supprimez chacune des relations synchrones RPO zéro :

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol1
```

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol2
```

5. Relâcher la relation SnapMirror source mais conserver les copies Snapshot courantes :

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol1
```

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol2
```

6. Créez une relation synchrone SnapMirror RTO zéro avec la règle AutomatedFailoverDuplex :

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailoverDuplex
```

7. Si les hôtes existants sont locaux du cluster principal, ajoutez l'hôte au cluster secondaire et établissez la connectivité avec l'accès respectif à chaque cluster.
8. Sur le site secondaire, supprimez les mappages de LUN sur les groupes initiateurs associés aux hôtes distants.



Assurez-vous que le groupe initiateur ne contient pas de mappages pour les LUN non répliqués.

```
SiteB::> lun mapping delete -vserver svm_name -igroup igroup -path <>
```

9. Sur le site principal, modifiez la configuration de l'initiateur pour les hôtes existants afin de définir le chemin proximal des initiateurs sur le cluster local.

```
SiteA::> igroup initiator add-proximal-vserver -vserver svm_name -initiator
host -proximal-vserver server
```

10. Ajoutez un groupe initiateur et un initiateur pour les nouveaux hôtes et définissez la proximité de l'hôte pour l'affinité avec l'hôte sur son site local. Réplication igroup exécutable pour répliquer la configuration et inverser la localisation de l'hôte sur le cluster distant.

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator host2
-proximal-vserver vsB
```

11. Découvrez les chemins sur les hôtes et vérifiez que les hôtes disposent d'un chemin Active/Optimized vers la LUN de stockage à partir du cluster préféré
12. Déployez l'application et distribuez les workloads des machines virtuelles entre les clusters.
13. Resynchroniser le groupe de cohérence :

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

14. Relancez les chemins d'E/S de la LUN hôte pour restaurer tous les chemins d'accès aux LUN.

## Convertir le type de relation de synchronisation active SnapMirror

À partir de ONTAP 9.15.1, vous pouvez convertir des types de protection SnapMirror actif en mode synchrone en mode actif-actif symétrique et inversement.

### Convertir en relation active/active symétrique

Vous pouvez convertir une relation de synchronisation active SnapMirror avec une protection asynchrone pour utiliser une fonction active/active symétrique.

#### Avant de commencer

- Les deux clusters doivent exécuter ONTAP 9.15.1 ou une version ultérieure.
- Les configurations actif-actif symétriques nécessitent le AutomatedFailoverDuplex règles de protection. Sinon, vous pouvez [Créez une règle SnapMirror personnalisée](#) a condition que le `-type` est `automated-failover-duplex`.

## System Manager

### Étapes pour une configuration uniforme

1. Supprimez le groupe initiateur de destination :
  - a. Sur le cluster de destination, accédez à **hosts > SAN Initiator Groups**.
  - b. Sélectionnez le groupe initiateur avec la relation SnapMirror, puis **Delete**.
  - c. Dans la boîte de dialogue, sélectionnez la case **Annuler le mappage des LUN associées**, puis **Supprimer**.
2. Editez la relation synchrone active SnapMirror.
  - a. Accédez à **protection > relations**.
  - b. Sélectionnez le menu kabob en regard de la relation que vous voulez modifier, puis **Modifier**.
  - c. Modifiez la **protection Policy** sur AutomatedFailoverDuplex.
  - d. Sélection `AutoMatedFailoverDuplex` invite une boîte de dialogue à modifier les paramètres de proximité de l'hôte. Pour les initiateurs, sélectionnez l'option appropriée pour **initiateur proximal** à puis **Enregistrer**.
  - e. Sélectionnez **Enregistrer**.
3. Dans le menu **protection**, confirmez que l'opération a réussi lorsque la relation s'affiche comme `InSync`.

### Étapes d'une configuration non uniforme

1. Supprimez le groupe initiateur de destination :
  - a. Sur le site secondaire, accédez à **hosts > SAN Initiator Groups**.
  - b. Sélectionnez le groupe initiateur avec la relation SnapMirror, puis **Delete**.
  - c. Dans la boîte de dialogue, sélectionnez la case **Annuler le mappage des LUN associées**, puis **Supprimer**.
2. Créer un groupe initiateur :
  - a. Dans le menu **SAN Initiator Groups** du site de destination, sélectionnez **Add**.
  - b. Indiquez un **Nom**, sélectionnez le **système d'exploitation hôte**, puis choisissez **membres du groupe initiateur**.
  - c. Sélectionnez **Enregistrer**.
3. Mappez le nouveau groupe initiateur sur les LUN de destination.
  - a. Accédez à **stockage > LUN**.
  - b. Sélectionnez toutes les LUN à mapper sur le groupe initiateur.
  - c. Sélectionnez **plus** puis **Mapper sur les groupes initiateurs**.
4. Editez la relation synchrone active SnapMirror.
  - a. Accédez à **protection > relations**.
  - b. Sélectionnez le menu kabob en regard de la relation que vous voulez modifier, puis **Modifier**.
  - c. Modifiez la **protection Policy** sur AutomatedFailoverDuplex.
  - d. La sélection de `AutoMatedFailoverDuplex` permet de modifier les paramètres de proximité de l'hôte. Pour les initiateurs, sélectionnez l'option appropriée pour **initiateur proximal** à puis **Enregistrer**.

e. Sélectionnez **Enregistrer**.

5. Dans le menu **protection**, confirmez que l'opération a réussi lorsque la relation s'affiche comme InSync.

## CLI

### Étapes pour une configuration uniforme

1. Modifier la règle SnapMirror depuis AutomatedFailover à AutomatedFailoverDuplex:

```
snapmirror modify -destination-path destination_path -policy
AutomatedFailoverDuplex
```

2. La modification de la règle déclenche une resynchronisation. Attendez la fin de la resynchronisation et confirmez que la relation est Insync:

```
snapmirror show -destination-path destination_path
```

3. Si les hôtes existants sont locaux du cluster principal, ajoutez l'hôte au second cluster et établissez la connectivité avec l'accès respectif à chaque cluster.
4. Sur le site secondaire, supprimez les mappages de LUN sur les groupes initiateurs associés aux hôtes distants.



Assurez-vous que le groupe initiateur ne contient pas de mappages pour les LUN non répliquées.

```
SiteB::> lun mapping delete -vserver svm_name -igroup igroup -path <>
```

5. Sur le site principal, modifiez la configuration de l'initiateur pour les hôtes existants afin de définir le chemin proximal des initiateurs sur le cluster local.

```
SiteA::> igroup initiator add-proximal-vserver -vserver svm_name -initiator
host -proximal-vserver server
```

6. Ajoutez un groupe initiateur et un initiateur pour les nouveaux hôtes et définissez la proximité de l'hôte pour l'affinité avec l'hôte sur son site local. Réplication igroup exécutable pour répliquer la configuration et inverser la localisation de l'hôte sur le cluster distant.

```
SiteA::> igroup modify -vserver vsA -igroup igl -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator
host2 -proximal-vserver vsB
```

7. Découvrez les chemins sur les hôtes et vérifiez que les hôtes disposent d'un chemin Active/Optimized vers la LUN de stockage à partir du cluster préféré
8. Déployez l'application et distribuez les workloads des machines virtuelles entre les clusters.

### Étapes d'une configuration non uniforme

1. Modifier la règle SnapMirror depuis AutomatedFailover à AutomatedFailoverDuplex:

```
snapmirror modify -destination-path destination_path -policy
AutomatedFailoverDuplex
```

2. La modification de la règle déclenche une resynchronisation. Attendez la fin de la resynchronisation et confirmez que la relation est Insync:

```
snapmirror show -destination-path destination_path
```

3. Si les hôtes existants sont locaux au cluster principal, ajoutez l'hôte au second cluster et établissez la connectivité avec l'accès respectif à chaque cluster.
4. Sur le site secondaire, supprimez les mappages de LUN sur les groupes initiateurs associés aux hôtes distants.



Assurez-vous que le groupe initiateur ne contient pas de mappages pour les LUN non répliquées.

```
SiteB::> lun mapping delete -vserver svm_name -igroup igroup -path <>
```

5. Sur le site principal, modifiez la configuration de l'initiateur pour les hôtes existants afin de définir le chemin proximal des initiateurs sur le cluster local.

```
SiteA::> igroup initiator add-proximal-vserver -vserver Svm_name -initiator
host -proximal-vserver server
```

6. Sur le site secondaire, ajoutez un nouveau groupe initiateur et un initiateur pour les nouveaux hôtes et définissez la proximité de l'hôte pour l'affinité avec l'hôte sur son site local. Mappez les LUN sur le groupe initiateur.

```
SiteB::> igroup create -vserver svm_name -igroup igroup_name
SiteB::> igroup add -vserver svm_name -igroup igroup_name -initiator
host_name
SiteB::> lun mapping create -igroup igroup_name -path path_name
```

7. Découvrez les chemins sur les hôtes et vérifiez que les hôtes disposent d'un chemin Active/Optimized vers la LUN de stockage à partir du cluster préféré
8. Déployez l'application et distribuez les workloads des machines virtuelles entre les clusters.

### Conversion d'une relation symétrique actif/actif à une relation asymétrique

Si vous avez configuré la protection actif-actif symétrique, vous pouvez la convertir en protection asymétrique à l'aide de l'interface de ligne de commande ONTAP.

#### Étapes

1. Déplacez toutes les charges de travail des machines virtuelles vers l'hôte local du cluster source.
2. Supprimez la configuration du groupe initiateur pour les hôtes qui ne gèrent pas les instances de VM et modifiez la configuration du groupe initiateur pour mettre fin à la réplication du groupe initiateur.

code

3. Sur le site secondaire, annulez le mappage des LUN.

```
SiteB::> lun mapping delete -vserver svm_name -igroup igroup_name -path <>
```



4. Sur le site secondaire, supprimez la relation actif-actif symétrique.

```
SiteB::> snapmirror delete -destination-path destination_path
```

5. Sur le site primaire, relâchez la relation actif-actif symétrique.

```
SiteA::> snapmirror release -destination-path destination_path -relationship
-info-only true
```

6. Depuis le site secondaire, créez une relation avec le même ensemble de volumes avec AutomatedFailover policy : resynchronisez la relation.

```
SiteB::> snapmirror create -source-path source_path -destination-path
destination_path -cg-item-mappings source:@destination -policy
AutomatedFailover
SiteB::> snapmirror resync -destination-path vs1:/cg/cg1_dst
```



Le groupe de cohérence sur le site secondaire doit être mis en place **"à supprimer"** avant de recréer la relation. Les volumes de destination **"Doit être converti en type DP"**.

7. Vérifiez que l'état miroir de la relation est Snapmirrored Le statut de la relation est Insync.

```
snapmirror show -destination-path destination_path
```

8. Redécouvrez les chemins depuis l'hôte.

## Gérer la synchronisation active SnapMirror et protéger les données

### Créer une copie Snapshot commune

Outre les opérations de copie Snapshot planifiées régulièrement, vous pouvez créer manuellement une commune **"La copie Snapshot"** Entre les volumes du groupe de cohérence SnapMirror principal et les volumes du groupe de cohérence SnapMirror secondaire.

#### Description de la tâche

L'intervalle de création d'un Snapshot planifié est de 12 heures.

#### Avant de commencer

- La relation de groupe SnapMirror doit être en mode synchrone.

#### Étapes

1. Créer une copie Snapshot commune :

```
destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
```

2. Surveiller la progression de la mise à jour :

```
destination::>snapmirror show -fields -newest-snapshot
```

## **Effectuer un basculement planifié des clusters dans une relation de synchronisation active SnapMirror**

Lors d'un basculement planifié des clusters ONTAP dans une relation de synchronisation active SnapMirror, vous basculez les rôles des clusters principal et secondaire, de sorte que le cluster secondaire remplace le cluster principal. Lors d'un basculement, ce qui est généralement le cluster secondaire traite les demandes d'entrée et de sortie localement sans interrompre les opérations client.

Vous pouvez effectuer un basculement planifié pour tester l'état de santé de votre configuration de reprise sur incident ou pour effectuer des opérations de maintenance sur le cluster principal.

### **Description de la tâche**

Un basculement planifié est initié par l'administrateur du cluster secondaire. L'opération nécessite le basculement des rôles principal et secondaire afin que le cluster secondaire prenne le relais du cluster principal. Le nouveau cluster principal peut alors commencer à traiter les demandes d'entrée et de sortie localement, sans interrompre les opérations client.

### **Avant de commencer**

- La relation de synchronisation active SnapMirror doit être synchronisée.
- Vous ne pouvez pas lancer de basculement planifié lorsqu'une opération sans interruption est en cours. La continuité de l'activité inclut les déplacements de volumes, les transferts d'agrégats et les basculements de stockage.
- Le médiateur ONTAP doit être configuré, connecté et en quorum.

### **Étapes**

Vous pouvez effectuer un basculement planifié via l'interface de ligne de commande ONTAP ou System Manager.

## System Manager



De ONTAP 9.8 à 9.14.1, la synchronisation active SnapMirror est appelée SnapMirror Business Continuity (SM-BC).

1. Dans System Manager, sélectionnez **protection > vue d'ensemble > relations**.
2. Identifiez la relation de synchronisation active SnapMirror que vous souhaitez basculer. En regard de son nom, sélectionnez le ... À côté du nom de la relation, puis sélectionnez **basculement**.
3. Pour surveiller l'état du basculement, utilisez `snapmirror failover show` Dans l'interface de ligne de commandes ONTAP.

## CLI

1. Depuis le cluster de destination, lancer l'opération de basculement :

```
destination::>snapmirror failover start -destination-path
vs1_dst:/cg/cg_dst
```

2. Surveiller la progression du basculement :

```
destination::>snapmirror failover show
```

3. Une fois l'opération de basculement terminée, vous pouvez contrôler l'état de la relation de protection synchrone SnapMirror depuis la destination :

```
destination::>snapmirror show
```

## Restaurez vos données après des opérations automatiques de basculement non planifié

Une opération automatique de basculement non planifié (AUFO) se produit lorsque le cluster principal est en panne ou isolé. Le médiateur ONTAP détecte les basculements et exécute un basculement automatique non planifié vers le cluster secondaire. Le cluster secondaire est converti en cluster principal et commence à servir les clients. Cette opération est effectuée uniquement avec l'aide du médiateur ONTAP.



Après le basculement automatique non planifié, il est important d'analyser à nouveau les chemins d'E/S des LUN hôtes afin d'éviter toute perte de chemins d'E/S.

## Rétablir la relation de protection après un basculement non planifié

Vous pouvez rétablir la relation de protection à l'aide de System Manager ou de l'interface de ligne de commandes ONTAP.

## System Manager



### Étapes

De ONTAP 9.8 à 9.14.1, la synchronisation active SnapMirror est appelée SnapMirror Business Continuity (SM-BC).

1. Accédez à **protection > relations** et attendez que l'état de la relation affiche "insync".
2. Pour reprendre les opérations sur le cluster source d'origine, cliquez sur et sélectionnez **basculement**.

### CLI

Vous pouvez surveiller l'état du basculement automatique non planifié à l'aide du `snapmirror failover show` commande.

Par exemple :

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
 Source Path: vs1:/cg/scg3
 Destination Path: vs3:/cg/dcg3
 Failover Status: completed
 Error Reason:
 End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
 Failover Type: unplanned
Error Reason codes: -
```

Reportez-vous à la "[Référence EMS](#)" pour en savoir plus sur les messages d'événement et sur les actions correctives à mener.

## Reprise de la protection dans une configuration « Fan-Out » après le basculement

Depuis la version ONTAP 9.15.1, la synchronisation active SnapMirror prend en charge la reconfiguration automatique dans le segment « Fan-Out » après un événement de basculement. Pour plus d'informations, voir "[configurations « fan-out »](#)".

Si vous utilisez ONTAP 9.14.1 ou une version antérieure et que vous rencontrez un basculement sur le cluster secondaire dans la relation de synchronisation active SnapMirror, la destination asynchrone SnapMirror devient défectueuse. Vous devez restaurer manuellement la protection en supprimant et en créant la relation avec le terminal asynchrone SnapMirror.

### Étapes

1. Vérifiez que le basculement s'est terminé correctement :  
`snapmirror failover show`
2. Sur le point de terminaison asynchrone SnapMirror, supprimez le point de terminaison « Fan-Out » :  
`snapmirror delete -destination-path destination_path`

3. Sur le troisième site, créez des relations asynchrones SnapMirror entre le nouveau volume primaire de synchronisation active SnapMirror et le volume de destination asynchrone « Fan-Out » :  

```
snapmirror create -source-path source_path -destination-path destination_path
-policy MirrorAllSnapshots -schedule schedule
```
4. Resynchroniser la relation :  

```
snapmirror resync -destination-path destination_path
```
5. Vérifiez l'état et l'état de la relation :  

```
snapmirror show
```

## Surveillez les opérations de synchronisation active SnapMirror

Vous pouvez contrôler les opérations de synchronisation active SnapMirror suivantes pour vérifier l'état de votre configuration de synchronisation active SnapMirror :

- Médiateur de ONTAP
- Opérations de basculement planifiées
- Opérations de basculement non planifiées automatiques
- Disponibilité de la synchronisation active SnapMirror



Depuis la version ONTAP 9.15.1, System Manager affiche l'état de votre relation de synchronisation active SnapMirror depuis l'un ou l'autre cluster. Vous pouvez également surveiller l'état du médiateur ONTAP depuis l'un des clusters dans System Manager.

### Médiateur de ONTAP

En fonctionnement normal, l'état du médiateur ONTAP doit être connecté. S'il est dans un autre état, cela peut indiquer une condition d'erreur. Vous pouvez consulter le "[Messages du système de gestion des événements \(EMS\)](#)" pour déterminer l'erreur et les actions correctives appropriées.

### Opérations de basculement planifiées

Vous pouvez surveiller l'état et la progression d'une opération de basculement planifié à l'aide de l'`snapmirror failover show` commande. Par exemple :

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Une fois l'opération de basculement terminée, vous pouvez contrôler l'état de la protection SnapMirror depuis le nouveau cluster de destination. Par exemple :

```
ClusterA::> snapmirror show
```

Reportez-vous à la "[Référence EMS](#)" pour en savoir plus sur les messages d'événement et les actions correctives à mener.

### Opérations de basculement non planifiées automatiques

Lors d'un basculement automatique non planifié, vous pouvez surveiller l'état de l'opération à l'aide du

snapmirror failover show commande.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
 Source Path: vs1:/cg/scg3
 Destination Path: vs3:/cg/dcg3
 Failover Status: completed
 Error Reason:
 End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
 Failover Type: unplanned
Error Reason codes: -
```

Reportez-vous à la ["Référence EMS"](#) pour en savoir plus sur les messages d'événement et sur les actions correctives à mener.

#### **Disponibilité de la synchronisation active SnapMirror**

Vous pouvez vérifier la disponibilité de la relation de synchronisation active SnapMirror à l'aide d'une série de commandes situées sur le cluster principal, le cluster secondaire ou les deux.

Les commandes que vous utilisez incluent `snapmirror mediator show` commande sur le cluster principal et le cluster secondaire pour vérifier le statut de connexion et de quorum, le `snapmirror show` et la `volume show` commande. Par exemple :

```

SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster Connection Status Quorum Status

10.236.172.86 SMBC_B connected true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster Connection Status Quorum Status

10.236.172.86 SMBC_A connected true

SMBC_B::*> snapmirror show -expand

Progress
Source Destination Mirror Relationship Total
Last
Path Type Path State Status Progress Healthy
Updated

vs0:/cg/cg1 XDP vs1:/cg/cg1_dp Snapmirrored Insync - true -
vs0:vol1 XDP vs1:vol1_dp Snapmirrored Insync - true -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus

vs0 vol1 true false Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus

vs1 vol1_dp false true No-consensus

```

### Permet d'ajouter ou de supprimer des volumes à un groupe de cohérence

À mesure que les exigences des charges de travail applicatives évoluent, vous devrez peut-être ajouter ou supprimer des volumes d'un groupe de cohérence pour assurer la continuité de l'activité. Le processus d'ajout et de suppression de volumes dans une relation de synchronisation active SnapMirror dépend de la version de ONTAP que vous utilisez.

Dans la plupart des cas, il s'agit d'un processus perturbateur qui vous oblige à supprimer la relation SnapMirror, à modifier le groupe de cohérence, puis à reprendre la protection. Depuis la version ONTAP 9.13.1, l'ajout de volumes à un groupe de cohérence avec une relation SnapMirror active n'entraîne aucune

interruption.

### Description de la tâche

- Dans ONTAP 9.9.1, vous pouvez ajouter ou supprimer des volumes à un groupe de cohérence à l'aide de l'interface de ligne de commandes ONTAP.
- Depuis ONTAP 9.10.1, il est recommandé de le gérer "[groupes de cohérence](#)" Via System Manager ou avec l'API REST ONTAP.

Si vous souhaitez modifier la composition du groupe de cohérence en ajoutant ou en supprimant un volume, vous devez d'abord supprimer la relation d'origine, puis créer à nouveau le groupe de cohérence avec la nouvelle composition.

- À partir de ONTAP 9.13.1, vous pouvez ajouter des volumes à un groupe de cohérence sans interruption avec une relation SnapMirror active depuis la source ou la destination.

La suppression de volumes est une opération disruptive. Vous devez supprimer la relation SnapMirror avant de supprimer des volumes.



## ONTAP 9.9.1-9.13.0

### Avant de commencer

- Vous ne pouvez pas commencer à modifier le groupe de cohérence tant qu'il se trouve dans le groupe InSync état.
- Le volume de destination doit être de type DP.
- Le nouveau volume que vous ajoutez pour développer le groupe de cohérence doit disposer d'une paire de copies Snapshot communes entre les volumes source et de destination.

### Étapes

Les exemples présentés dans deux mappages de volume :  $\text{vol\_src1} \longleftrightarrow \text{vol\_dst1}$  et  $\text{vol\_src2} \longleftrightarrow \text{vol\_dst2}$ , dans une relation de groupe de cohérence entre les points d'extrémité  $\text{vs1\_src}:/\text{cg}/\text{cg\_src}$  et  $\text{vs1\_dst}:/\text{cg}/\text{cg\_dst}$ .

1. Sur le cluster source et le cluster destination, vérifiez qu'il existe un Snapshot commun entre le cluster source et le cluster destination avec la commande `snapshot show -vserver svm_name -volume volume_name -snapshot snapmirror`

```
source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot snapmirror*
```

```
destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot snapmirror*
```

2. Si aucune copie Snapshot n'existe déjà, créez et initialisez une relation FlexVol SnapMirror :

```
destination::>snapmirror initialize -source-path vs1_src:vol_src3
-destination-path vs1_dst:vol_dst3
```

3. Supprimez la relation de groupe de cohérence :

```
destination::>snapmirror delete -destination-path vs1_dst:vol_dst3
```

4. Libérer la relation SnapMirror source et conserver les copies Snapshot courantes :

```
source::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol_dst3
```

5. Annulez le mappage des LUN et supprimez la relation de groupe de cohérence existante :

```
destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup
<igroup_name>
```



Les LUN de destination ne sont pas mappées, tandis que les LUN présentes sur la copie primaire continuent de servir les E/S de l'hôte

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
-relationship-info-only true
```

6. Si vous utilisez ONTAP 9.10.1 à 9.13.0, supprimez et recréez le groupe de cohérence sur la source avec la composition correcte. Suivez les étapes de la section [Supprimez un groupe de cohérence](#) puis [Configurez un seul groupe de cohérence](#). Dans ONTAP 9.10.1 et les versions ultérieures, vous devez effectuer les opérations de suppression et de création dans System Manager ou avec l'API REST ONTAP ; il n'existe pas de procédure d'interface de ligne de commandes.

**Si vous utilisez ONTAP 9.9.1, passez à l'étape suivante.**

7. Créez le nouveau groupe de cohérence sur la destination avec la nouvelle composition :

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. Resynchroniser la relation de groupe de cohérence RTO zéro pour garantir qu'elle est synchronisée :

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. Remappage des LUN que vous n'avez pas mappées à l'étape 5 :

```
destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
```

10. Relancez les chemins d'E/S de la LUN hôte pour restaurer tous les chemins d'accès aux LUN.

#### ONTAP 9.13.1 et versions ultérieures


À partir de ONTAP 9.13.1, vous pouvez ajouter des volumes à un groupe de cohérence sans interruption avec une relation active SnapMirror synchrone. La synchronisation active SnapMirror prend en charge l'ajout de volumes à la fois depuis la source et la destination.



De ONTAP 9.8 à 9.14.1, la synchronisation active SnapMirror est appelée SnapMirror Business Continuity (SM-BC).

Pour plus d'informations sur l'ajout de volumes provenant du groupe de cohérence source, reportez-vous à la section [Modifier un groupe de cohérence](#).

#### Ajout d'un volume depuis le cluster de destination

1. Sur le cluster de destination, sélectionnez **protection > relations**.
2. Recherchez la configuration SnapMirror à laquelle vous souhaitez ajouter des volumes. Sélectionnez , puis **développer**.
3. Sélectionnez les relations de volume dont les volumes doivent être ajoutés au groupe de cohérence
4. Sélectionnez **développer**.

#### Mettez à niveau et restaurez ONTAP avec la synchronisation active SnapMirror

La synchronisation active SnapMirror est prise en charge à partir de ONTAP 9.9.1. La mise à niveau et la restauration du cluster ONTAP ont des implications sur vos relations de synchronisation active SnapMirror, selon la version de ONTAP vers laquelle vous effectuez la mise à niveau ou la restauration.

## Mettez à niveau ONTAP avec SnapMirror Active Sync

Pour utiliser la synchronisation active SnapMirror, tous les nœuds des clusters source et destination doivent exécuter ONTAP 9.9.1 ou une version ultérieure.

Lorsque vous mettez à niveau ONTAP avec des relations actives SnapMirror synchronisées, vous devez utiliser [Mise à niveau automatisée sans interruption \(ANDU\)](#). Grâce à ANDU, vos relations de synchronisation active SnapMirror sont synchronisées et fonctionnent correctement lors du processus de mise à niveau.

Il n'y a pas d'étape de configuration pour préparer les déploiements de synchronisation active SnapMirror en vue des mises à niveau de ONTAP. Cependant, il est recommandé de vérifier, avant et après la mise à niveau :

- Les relations de synchronisation active SnapMirror sont synchronisées.
- Il n'y a pas d'erreur liée à SnapMirror dans le journal des événements.
- Le Mediator est en ligne et sain à partir des deux clusters.
- Tous les hôtes peuvent voir tous les chemins correctement pour protéger les LUN.



Lorsque vous mettez à niveau des clusters de ONTAP 9.9.1 ou 9.9.1 vers ONTAP 9.10.1 et versions ultérieures, ONTAP crée de nouvelles données [groupes de cohérence](#) Sur les clusters source et destination des relations de synchronisation active SnapMirror qui peuvent être configurées à l'aide de System Manager.



Le `snapmirror quiesce` et `snapmirror resume` Les commandes ne sont pas prises en charge avec la synchronisation active SnapMirror.

## Restaurez ONTAP 9.9.1 à partir de ONTAP 9.10.1

Pour rétablir les relations de la version 9.10.1 à la version 9.9.1, les relations de synchronisation active SnapMirror doivent être supprimées, suivies de l'instance de groupe de cohérence 9.10.1. Impossible de supprimer les groupes de cohérence avec une relation active SnapMirror synchrone. Tout volume FlexVol mis à niveau vers la version 9.10.1 précédemment associé à une autre application de conteneur intelligent ou d'entreprise en 9.9.1 ou version antérieure ne sera plus associé à la restauration. La suppression des groupes de cohérence ne supprime pas les volumes constitutifs ou les snapshots granulaires volume. Reportez-vous à la section ["Supprimez un groupe de cohérence"](#) Pour plus d'informations sur cette tâche dans ONTAP 9.10.1 et versions ultérieures.

## Revenir de ONTAP 9.9.1



La synchronisation active SnapMirror n'est pas prise en charge avec les clusters ONTAP mixtes par rapport aux versions antérieures à ONTAP 9.9.1.

Lorsque vous revenez de ONTAP 9.9.1 à une version antérieure de ONTAP, vous devez prendre connaissance des points suivants :

- Si le cluster héberge une destination de synchronisation active SnapMirror, le rétablissement vers ONTAP 9.8 ou version antérieure n'est pas autorisé tant que la relation n'est pas rompue et supprimée.
- Si le cluster héberge une source de synchronisation active SnapMirror, le rétablissement vers ONTAP 9.8 ou version antérieure n'est pas autorisé tant que la relation n'est pas validée.
- Toutes les règles de synchronisation active SnapMirror personnalisées créées par l'utilisateur doivent être supprimées avant de revenir à ONTAP 9.8 ou à une version antérieure.

Pour répondre à ces exigences, reportez-vous à la section ["Supprime une configuration de synchronisation active SnapMirror"](#).

## Étapes

1. Vérifiez que vous êtes prêt à revenir à la version précédente en saisissant la commande suivante depuis l'un des clusters de la relation de synchronisation active SnapMirror :

```
cluster::> system node revert-to -version 9.7 -check-only
```

L'exemple de résultat suivant montre un cluster qui n'est pas prêt à revenir avec des instructions de nettoyage.

```
cluster::> system node revert-to -version 9.7 -check-only
Error: command failed: The revert check phase failed. The following
issues must be resolved before revert can be completed. Bring the data
LIFs down on running vservers. Command to list the running vservers:
vserver show -admin-state running Command to list the data LIFs that are
up: network interface show -role data -status-admin up Command to bring
all data LIFs down: network interface modify {-role data} -status-admin
down
Disable snapshot policies.
 Command to list snapshot policies: "snapshot policy show".
 Command to disable snapshot policies: "snapshot policy modify
-vserver
 * -enabled false"

 Break off the initialized online data-protection (DP) volumes and
delete
 Uninitialized online data-protection (DP) volumes present on the
local
node.
 Command to list all online data-protection volumes on the local
node:
 volume show -type DP -state online -node <local-node-name>
 Before breaking off the initialized online data-protection volumes,
quiesce and abort transfers on associated SnapMirror relationships
and
 wait for the Relationship Status to be Quiesced.
 Command to quiesce a SnapMirror relationship: snapmirror quiesce
 Command to abort transfers on a SnapMirror relationship: snapmirror
abort
 Command to see if the Relationship Status of a SnapMirror
relationship
is Quiesced: snapmirror show
 Command to break off a data-protection volume: snapmirror break
 Command to break off a data-protection volume which is the
destination
```

```

of a SnapMirror relationship with a policy of type "vault":
snapmirror
break -delete-snapshots
 Uninitialized data-protection volumes are reported by the
"snapmirror
break" command when applied on a DP volume.
 Command to delete volume: volume delete

Delete current version snapshots in advanced privilege level.
 Command to list snapshots: "snapshot show -fs-version 9.9.1"
 Command to delete snapshots: "snapshot prepare-for-revert -node
<nodename>"

Delete all user-created policies of the type active-strict-sync-
mirror
and active-sync-mirror.
 The command to see all active-strict-sync-mirror and active-sync-
mirror
type policies is:
 snapmirror policy show -type
active-strict-sync-mirror,active-sync-mirror
 The command to delete a policy is :
 snapmirror policy delete -vserver <SVM-name> -policy <policy-name>

```

2. Une fois que vous avez satisfait aux exigences de la vérification de restauration, reportez-vous à la section ["Restaurez la ONTAP"](#).

## Supprime une configuration de synchronisation active SnapMirror

Si vous n'avez plus besoin de protection synchrone SnapMirror avec objectif RTO nul, vous pouvez supprimer votre relation de synchronisation active SnapMirror.

### Supprimer une configuration asymétrique

- Avant de supprimer la relation de synchronisation active SnapMirror, toutes les LUN du cluster de destination doivent être démappées.
- Une fois que les LUN sont démappées et que l'hôte est réanalysé, la cible SCSI informe les hôtes que l'inventaire des LUN a changé. Les LUN existantes sur les volumes secondaires RTO de zéro sont modifiées pour refléter une nouvelle identité après la suppression de la relation RTO de zéro. Les hôtes découvrent les LUN du volume secondaire en tant que nouveaux LUN sans relation avec les LUN du volume source.
- Les volumes secondaires restent des volumes DP une fois la relation supprimée. Vous pouvez lancer le `snapmirror break` pour les convertir en lecture/écriture.
- La suppression de la relation n'est pas autorisée à l'état d'échec lorsque la relation n'est pas inversée.

### Étapes

1. Depuis le cluster secondaire, supprimez la relation SnapMirror Active Sync Consistency group entre le terminal source et le terminal de destination :

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

2. Depuis le cluster principal, relationer la relation de groupe de cohérence et les copies Snapshot créées pour la relation :

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
```

3. Effectuez une nouvelle analyse de l'hôte pour mettre à jour l'inventaire des LUN.
4. Depuis la version ONTAP 9.10.1, la suppression de la relation SnapMirror ne supprime pas le groupe de cohérence. Pour supprimer le groupe de cohérence, vous devez utiliser System Manager ou l'API REST de ONTAP. Voir [Supprimez un groupe de cohérence](#) pour en savoir plus.

### **Supprime une configuration actif-actif symétrique**

Vous pouvez supprimer une configuration symétrique au moyen de System Manager ou de l'interface de ligne de commandes ONTAP. Dans les deux interfaces, il existe différentes étapes pour [configurations uniformes et non uniformes](#).

## System Manager

### Étapes pour une configuration uniforme

1. Sur le site principal, supprimez les hôtes distants du groupe initiateur et mettez fin à la réplication.
  - a. Accédez à **hosts > SAN Initiator Groups**.
  - b. Sélectionnez le groupe initiateur à modifier, puis **Modifier**.
  - c. Supprimez l'initiateur distant et mettez fin à la réplication du groupe initiateur. Sélectionnez **Enregistrer**.
2. Sur le site secondaire, supprimez la relation répliquée en démappant les LUN.
  - a. Accédez à **hosts > SAN Initiator Groups**.
  - b. Sélectionnez le groupe initiateur avec la relation SnapMirror, puis **Delete**.
  - c. Dans la boîte de dialogue, sélectionnez la case **Annuler le mappage des LUN associées**, puis **Supprimer**.
  - d. Accédez à **protection > relations**.
  - e. Sélectionnez la relation de synchronisation active SnapMirror, puis **Release** pour supprimer les relations.

### Étapes d'une configuration non uniforme

1. Sur le site principal, supprimez les hôtes distants du groupe initiateur et mettez fin à la réplication.
  - a. Accédez à **hosts > SAN Initiator Groups**.
  - b. Sélectionnez le groupe initiateur à modifier, puis **Modifier**.
  - c. Supprimez l'initiateur distant et mettez fin à la réplication du groupe initiateur. Sélectionnez **Enregistrer**.
2. Sur le site secondaire, supprimez la relation de synchronisation active SnapMirror.
  - a. Accédez à **protection > relations**.
  - b. Sélectionnez la relation de synchronisation active SnapMirror, puis **Release** pour supprimer les relations.

## CLI

### Étapes pour une configuration uniforme

1. Déplacez toutes les charges de travail de machine virtuelle vers le cluster hôte local à source de la synchronisation active SnapMirror.
2. Sur le cluster source, supprimez les initiateurs du groupe initiateur et modifiez la configuration du groupe initiateur pour mettre fin à la réplication.

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -initiator <host2>
SiteA::> igroup modify -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -replication-peer "-"
```

3. Sur le site secondaire, supprimez le mappage de LUN et supprimez la configuration du groupe initiateur :

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. Sur le site secondaire, supprimez la relation de synchronisation active SnapMirror.

```
SiteB::> snapmirror delete -destination-path destination_path
```

5. Sur le site primaire, relationship actif SnapMirror depuis le site primaire.

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. Redécouvrez les chemins pour vérifier que seul le chemin local est disponible pour l'hôte.

### Étapes d'une configuration non uniforme

1. Déplacez toutes les charges de travail de machine virtuelle vers le cluster hôte local à source de la synchronisation active SnapMirror.
2. Sur le cluster source, supprimez les initiateurs du groupe initiateur.

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -initiator
<host2>
```

3. Sur le site secondaire, supprimez le mappage de LUN et supprimez la configuration du groupe initiateur :

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. Sur le site secondaire, supprimez la relation de synchronisation active SnapMirror.

```
SiteB::> snapmirror delete -destination-path <destination_path>
```

5. Sur le site primaire, relationship actif SnapMirror depuis le site primaire.

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. Redécouvrez les chemins pour vérifier que seul le chemin local est disponible pour l'hôte.

## Supprimer le médiateur ONTAP

Si vous souhaitez supprimer une configuration de médiateur ONTAP existante de vos clusters ONTAP, vous pouvez le faire à l'aide du `snapmirror mediator remove` commande.

### Étapes

1. Supprimer un médiateur ONTAP :

```
snapmirror mediator remove -mediator-address 12.345.678.90 -peer-cluster
cluster_xyz
```

## Résoudre les problèmes



## L'opération de suppression de SnapMirror a échoué lors du basculement

### Problème :

Lorsque ONTAP 9.9.1 est installé sur un cluster, exécutant le `snapmirror delete`  
Échec de la commande lorsqu'une relation de groupe de cohérence de synchronisation active SnapMirror est à l'état basculement.

```
C2_cluster::> snapmirror delete vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

### Solution

Lorsque les nœuds d'une relation de synchronisation active SnapMirror sont à l'état basculement, effectuez l'opération de suppression et de libération de SnapMirror avec l'option «-force » définie sur « true ».

```
C2_cluster::> snapmirror delete vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
 "vs1:/cg/dd" will be deleted, however the items of the
destination
 Consistency Group might not be made writable, deletable, or
modifiable
 after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

## Échec de la création d'une relation SnapMirror et initialisation du groupe de cohérence

### Problème :

La création de la relation SnapMirror et l'initialisation du groupe de cohérence échouent.

### Solution :

Vérifiez que vous n'avez pas dépassé la limite des groupes de cohérence par cluster. Dans SnapMirror, les limites des groupes de cohérence sont indépendantes de la plateforme et diffèrent en fonction de la version de ONTAP. Voir "[Limites d'objets](#)" Pour obtenir des conseils spécifiques à votre version de ONTAP.

### Erreur :

Si le groupe de cohérence reste en cours d'initialisation, vérifiez l'état des initialisations de groupes de cohérence avec l'API REST de ONTAP, System Manager ou la commande `sn show -expand`.




De ONTAP 9.8 à 9.14.1, la synchronisation active SnapMirror est appelée SnapMirror Business Continuity (SM-BC).

### Solution :

Si l'initialisation de ces groupes de cohérence échoue, supprimez la relation SnapMirror active Sync,

supprimez le groupe de cohérence, recréez la relation et initialisez-la. Ce flux de travail diffère selon la version de ONTAP que vous utilisez.

| Si vous utilisez ONTAP 9.9.1                                                                                                                                                                                                                                           | Si vous utilisez ONTAP 9.10.1 ou version ultérieure                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. <a href="#">"Supprimez la configuration de la synchronisation active SnapMirror"</a></li> <li>2. <a href="#">"Créer une relation de groupe de cohérence, puis initialiser la relation de groupe de cohérence"</a></li> </ol> | <ol style="list-style-type: none"> <li>1. Sous <b>protection &gt; relations</b>, recherchez la relation de synchronisation active SnapMirror dans le groupe de cohérence. Sélectionnez , puis <b>Delete</b> pour supprimer la relation de synchronisation active SnapMirror.</li> <li>2. <a href="#">"Supprimez le groupe de cohérence"</a></li> <li>3. <a href="#">"Configurer le groupe de cohérence"</a></li> </ol> |

## Échec du basculement planifié

### Problème :

Après avoir exécuté le `snapmirror failover start` commande, sortie de `snapmirror failover show` commande affiche un message indique qu'une opération sans interruption est en cours.

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason

vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.

08:35:04
```

### Cause :

Un basculement planifié ne peut pas commencer lorsqu'une opération sans interruption est en cours, notamment le déplacement de volumes, le déplacement d'agrégats et le basculement du stockage.

### Solution :

Attendez la fin de l'opération sans interruption et réessayez l'opération de basculement.

## Le médiateur ONTAP est inaccessible ou l'état du quorum du médiateur est faux

### Problème :

Après avoir exécuté le `snapmirror failover start` commande, sortie de `snapmirror failover show` Affiche un message indiquant que le médiateur ONTAP n'est pas configuré.

Voir ["Configurer le médiateur ONTAP et les clusters pour la synchronisation active SnapMirror"](#).

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason

vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

#### Cause :

Le médiateur n'est pas configuré ou il existe des problèmes de connectivité réseau.

#### Solution :

Si le médiateur ONTAP n'est pas configuré, vous devez configurer le médiateur ONTAP avant de pouvoir établir une relation de synchronisation active SnapMirror. Résolvez tous les problèmes de connectivité réseau. Vérifiez que Mediator est connecté et que l'état du quorum est défini sur le site source et le site de destination à l'aide de la commande `snapmirror médiateur show`. Pour plus d'informations, voir ["Configurez le médiateur ONTAP"](#).

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster Connection Status Quorum Status

10.234.10.143 cluster2 connected true
```

### Basculément non planifié automatique non déclenché sur le site B

#### Problème :

Une défaillance sur le site A ne déclenche pas de basculement non planifié sur le site B.

#### Cause possible n° 1 :

Le médiateur ONTAP n'est pas configuré. Pour déterminer si c'est la cause, lancez le `snapmirror mediator show` Commande sur le cluster site B.

```
Cluster2::*> snapmirror mediator show
This table is currently empty.
```

Cet exemple indique que le médiateur ONTAP n'est pas configuré sur le site B.

#### Solution :

Assurez-vous que ONTAP Mediator est configuré sur les deux clusters, que l'état est connecté et que le quorum est défini sur vrai.

#### Cause possible n°2 :

Le groupe de cohérence SnapMirror est désynchronisé. Pour déterminer s'il en est ainsi, consultez le journal des événements pour savoir si le groupe de cohérence était en cours de synchronisation au moment où le site

A défaillant.

```
cluster::*> event log show -event *out.of.sync*
```

| Time               | Node                | Severity | Event                                                                                                                                                                                                                                                                          |
|--------------------|---------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -----              |                     |          |                                                                                                                                                                                                                                                                                |
| 10/1/2020 23:26:12 | sti42-vsims-ucs511w | ERROR    | sms.status.out.of.sync:<br>Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume<br>"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-<br>ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:<br>"Transfer failed." |

### Solution :

Procédez comme suit pour effectuer un basculement forcé sur le site B.

1. Annulez le mappage de toutes les LUN appartenant au groupe de cohérence à partir du site B.
2. Supprimez la relation de groupe de cohérence SnapMirror à l'aide du `force` option.
3. Entrez le `snapmirror break` Commande sur les volumes constitutifs du groupe de cohérence pour convertir les volumes DP en R/W, afin d'activer les E/S à partir du site B.
4. Démarrez les nœuds du site A pour créer une relation RTO zéro du site B au site A.
5. Libérez le groupe de cohérence avec `relationship-info-only` Sur le site A pour conserver la copie Snapshot commune et annuler le mappage des LUN appartenant au groupe de cohérence.
6. Convertissez les volumes du site A de la lecture/écriture en DP en configurant une relation de niveau volume en utilisant la règle de synchronisation ou la stratégie asynchrone.
7. Émettez le `snapmirror resync` pour synchroniser les relations.
8. Supprimez les relations SnapMirror avec la règle de synchronisation sur le site A.
9. Libérer les relations SnapMirror avec la règle de synchronisation à l'aide de `relationship-info-only true` Sur le site B.
10. Créer une relation de groupe de cohérence entre le site B et le site A.
11. Effectuez une resynchronisation de groupe de cohérence à partir du site A, puis vérifiez que le groupe de cohérence est en cours de synchronisation.
12. Relancez les chemins d'E/S de la LUN hôte pour restaurer tous les chemins d'accès aux LUN.

### Lien entre le site B et le médiateur vers le bas et le site A vers le bas

Pour vérifier la connexion du médiateur ONTAP, utilisez le `snapmirror mediator show` commande. Si l'état de la connexion est injoignable et que le site B ne parvient pas à atteindre le site A, vous aurez une sortie similaire à celle ci-dessous. Suivez les étapes de la solution pour restaurer la connexion

```

cluster::*> snapmirror mediator show
Mediator Address Peer Cluster Connection Status Quorum Status

10.237.86.17 C1_cluster unreachable true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::*> snapmirror show -expand
Source Destination Mirror Relationship Total
Last
Path Type Path State Status Progress Healthy
Updated

vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::*> cluster peer show
Peer Cluster Name Cluster Serial Number Availability
Authentication

C1_cluster 1-80-000011 Unavailable ok

```

## Solution

Forcer un basculement pour activer les E/S depuis le site B, puis établir une relation RTO nul entre le site B et le site A. Procédez comme suit pour effectuer un basculement forcé sur le site B.

1. Annulez le mappage de toutes les LUN appartenant au groupe de cohérence à partir du site B.
2. Supprimez la relation de groupe de cohérence SnapMirror à l'aide de l'option force.
3. Entrez la commande SnapMirror break (`snapmirror break -destination_path svm:_volume_`)  
Sur les volumes constitutifs du groupe de cohérence pour convertir les volumes de DP en RW, afin d'activer les E/S à partir du site B.

Vous devez lancer la commande SnapMirror break pour chaque relation du groupe de cohérence. Par exemple, si le groupe de cohérence contient trois volumes, vous exécutez la commande pour chaque volume.

4. Démarrez les nœuds du site A pour créer une relation RTO zéro du site B au site A.
5. Libérer le groupe de cohérence avec les informations uniquement sur le site A pour conserver la copie Snapshot commune et annuler le mappage des LUN appartenant au groupe de cohérence.
6. Convertissez les volumes du site A de RW en DP en configurant une relation au niveau du volume à l'aide de la règle de synchronisation ou de la stratégie asynchrone.
7. Émettez le `snapmirror resync` pour synchroniser les relations.
8. Supprimez les relations SnapMirror avec la règle de synchronisation sur le site A.
9. Établissez les relations SnapMirror avec la règle de synchronisation à l'aide de `Relationship-info-only true` sur le site B.
10. Créer une relation de groupe de cohérence entre le site B et le site A.
11. Depuis le cluster source, resynchronisez le groupe de cohérence. Vérifiez que l'état du groupe de cohérence est synchronisé.
12. Relancez la recherche des chemins d'E/S de la LUN hôte pour restaurer tous les chemins vers les LUN.

### Lien entre le site A et le médiateur vers le bas et le site B vers le bas

Lorsque vous utilisez la synchronisation active SnapMirror, vous risquez de perdre la connectivité entre le médiateur ONTAP ou vos clusters peering. Vous pouvez diagnostiquer le problème en vérifiant la connexion, la disponibilité et l'état de consensus des différentes parties de la relation de synchronisation active SnapMirror, puis en revoquant la connexion avec force.

| Que vérifier                                                    | Commande CLI                                                | Indicateur                                                                |
|-----------------------------------------------------------------|-------------------------------------------------------------|---------------------------------------------------------------------------|
| Médiateur du site A                                             | <code>snapmirror mediator show</code>                       | L'état de la connexion s'affiche comme <code>unreachable</code>           |
| Connectivité du site B.                                         | <code>cluster peer show</code>                              | La disponibilité s'affiche sous la forme <code>unavailable</code>         |
| État de consensus du volume actif de synchronisation SnapMirror | <code>volume show volume_name -fields smbc-consensus</code> | Le <code>sm-bc consensus</code> s'affiche <code>Awaiting-consensus</code> |

Pour plus d'informations sur le diagnostic et la résolution de ce problème, reportez-vous à l'article de la base de connaissances ["Liaison entre le site A et le médiateur en panne et le site B en cas d'utilisation de la synchronisation active SnapMirror"](#).

### L'opération de suppression SnapMirror échoue lorsque la clôture est définie sur le volume de destination

#### Problème :

L'opération de suppression de SnapMirror échoue lorsque l'un des volumes de destination a une barrière de redirection définie.

#### Solution

Effectuer les opérations suivantes pour réessayer la redirection et supprimer la clôture du volume de destination.

- Resynchronisation de SnapMirror

- Mise à jour SnapMirror

## **Opération de déplacement de volume bloquée lorsque le volume principal est en baisse**

### **Problème :**

Une opération de déplacement de volume est bloquée indéfiniment dans un état de mise en service différée lorsque le site principal est en panne dans une relation de synchronisation active SnapMirror.

Lorsque le site principal est en panne, le site secondaire effectue un basculement automatique non planifié (AUFO). Lorsqu'une opération de déplacement de volume est en cours lorsque l'AUFO est déclenché, le déplacement de volume devient bloqué.

### **Solution :**

Interrompez l'instance de déplacement de volume bloquée et redémarrez l'opération de déplacement de volume.

## **Échec de la version de SnapMirror lorsqu'il est impossible de supprimer la copie Snapshot**

### **Problème :**

L'opération de version de SnapMirror échoue lorsque la copie Snapshot ne peut pas être supprimée.

### **Solution :**

La copie Snapshot contient une balise transitoire. Utilisez le `snapshot delete` commande avec `-ignore-owners` Option pour supprimer la copie Snapshot transitoire.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners true -force true
```

Réessayez `snapmirror release` commande.

## **Le déplacement de volume la copie Snapshot de référence s'affiche comme la plus récente**

### **Problème :**

Après avoir effectué une opération de déplacement de volume sur un volume de groupe de cohérence, la copie Snapshot de référence du déplacement de volume peut s'afficher de manière incorrecte comme la plus récente pour la relation SnapMirror.

Vous pouvez afficher la dernière copie Snapshot avec la commande suivante :

```
snapmirror show -fields newest-snapshot status -expand
```

### **Solution :**

Effectuez manuellement une opération `snapmirror resync` ou attendez la resynchronisation automatique suivante une fois l'opération de déplacement du volume terminée.

# Service médiateur pour MetroCluster et SnapMirror actif Sync

## Présentation du médiateur ONTAP

Le Mediator ONTAP offre plusieurs fonctions pour les fonctionnalités ONTAP :

- Magasin persistant et cloisonné pour les métadonnées haute disponibilité.
- Sert de proxy ping pour la vivacité du contrôleur.
- Fournit une fonctionnalité de requête d'intégrité de nœud synchrone pour aider à déterminer le quorum.

Le médiateur ONTAP fournit deux services `systemctl` supplémentaires :

- **`ontap_mediator.service`**

Gère le serveur API REST pour la gestion des relations ONAP.

- **`mediator-scst.service`**

Contrôle le démarrage et l'arrêt du module iSCSI (SCST).

## Outils fournis à l'administrateur système

Outils fournis à l'administrateur système :

- **`/usr/local/bin/mediator_change_password`**

Définit un nouveau mot de passe d'API lorsque le nom d'utilisateur et le mot de passe d'API actuels sont fournis.

- **`/usr/local/bin/mediator_change_user`**

Définit un nouveau nom d'utilisateur d'API lorsque le nom d'utilisateur et le mot de passe d'API actuels sont fournis.

- **`/usr/local/bin/mediator_generate_support_bundle`**

Génère un fichier tgz local contenant toutes les informations de support utiles qui sont nécessaires à la communication avec le support client NetApp. Cela inclut la configuration de l'application, les journaux et certaines informations système. Les bundles sont générés sur le disque local et peuvent être transférés manuellement, si nécessaire. Emplacement de stockage : `/opt/netapp/data/support_bundles/`

- **`/usr/local/bin/uninstall_ontap_mediator`**

Supprime le progiciel ONTAP Mediator et le module du noyau SCST. Cela inclut la configuration, les journaux et les données de boîte aux lettres.

- **`/usr/local/bin/mediator_unlock_user`**

Libère un verrouillage sur le compte utilisateur de l'API si la limite de tentatives d'authentification a été atteinte. Cette fonction est utilisée pour empêcher la dérivation de mot de passe par force brute. Il invite l'utilisateur à entrer le nom d'utilisateur et le mot de passe corrects.



- `/usr/local/bin/mediator_add_user`

(Support uniquement) utilisé pour ajouter l'utilisateur de l'API lors de l'installation.

## Notes spéciales

ONTAP Mediator s'appuie sur SCST pour fournir iSCSI (voir <http://scst.sourceforge.net/index.html>). Ce paquet est un module de noyau qui est compilé lors de l'installation spécifiquement pour le noyau. Toute mise à jour du noyau peut nécessiter la réinstallation de SCST. Vous pouvez également désinstaller puis réinstaller le médiateur ONTAP, puis reconfigurer la relation ONTAP.



Toute mise à jour du noyau du système d'exploitation du serveur doit être coordonnée avec une fenêtre de maintenance dans ONTAP.

## Nouveautés du médiateur ONTAP

De nouvelles améliorations du médiateur ONTAP sont fournies avec chaque version. Voici les nouveautés.

### Améliorations

| Version du médiateur ONTAP | Améliorations                                                                                                                                                                                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.8                        | <ul style="list-style-type: none"> <li>• Prise en charge de RHEL 8.6, 8.7, 8.8, 8.9, 8.10, 9.2, 9.3 et 9.4</li> <li>• Prise en charge de Rocky Linux 8 et 9</li> </ul>                                                                                                                                                     |
| 1.7                        | <ul style="list-style-type: none"> <li>• Prise en charge de RHEL 8.5, 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2 et 9.3</li> <li>• Prise en charge de Rocky Linux 8 et 9</li> <li>• Prise en charge des données SAN (Subject alternative Name) dans les certificats auto-signés et les certificats signés par des tiers.</li> </ul> |
| 1.6                        | <ul style="list-style-type: none"> <li>• Mises à jour Python 3.9.</li> <li>• Prise en charge de RHEL 8.4-8.8, 9.0-9.2, Rocky Linux 8 et 9.</li> <li>• Support interrompu pour RHEL 7.x/CentOS toutes les versions.</li> </ul>                                                                                              |
| 1.5                        | <ul style="list-style-type: none"> <li>• Optimisation de la vitesse pour les systèmes SnapMirror à plus grande échelle.</li> <li>• Signature de code cryptographique ajoutée au programme d'installation.</li> <li>• Inclut des avertissements de dérécupération pour RHEL 7.x / CentOS 7.x.</li> </ul>                    |
| 1.4                        | <ul style="list-style-type: none"> <li>• Prise en charge de RHEL 8.4 et 8.5.</li> <li>• Inclut SCST version 3.6.0.</li> <li>• Ajout de la prise en charge de Secure Boot (SB) du micrologiciel basé sur UEFI.</li> </ul>                                                                                                   |

|     |                                                                                                                                                                                                                          |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.3 | <ul style="list-style-type: none"> <li>• Prise en charge de RHEL/CentOS 8.2 et 8.3.</li> <li>• Inclut SCST version 3.5.0.</li> </ul>                                                                                     |
| 1.2 | <ul style="list-style-type: none"> <li>• Prise en charge des boîtes aux lettres HTTPS.</li> <li>• À utiliser avec ONTAP 9.8+ MCC-IP AUSO et SnapMirror actif sync ZRTO.</li> <li>• Inclut SCST version 3.4.0.</li> </ul> |
| 1.1 | <ul style="list-style-type: none"> <li>• Prise en charge de RHEL/CentOS 7.6, 7.7, 8.0 et 8.1.</li> <li>• Élimine les dépendances Perl.</li> <li>• Inclut SCST version 3.4.0.</li> </ul>                                  |
| 1.0 | <ul style="list-style-type: none"> <li>• Prise en charge des boîtes aux lettres iSCSI.</li> <li>• A utiliser avec ONTAP 9.7+ MCC-IP AUSO.</li> <li>• Prise en charge de RHEL/CentOS 7.6.</li> </ul>                      |

### Matrice de prise en charge du se

| Système d'exploitation pour le médiateur ONTAP | 1.8      | 1.7      | 1.6      | 1.5  | 1.4  | 1.3  | 1.2       | 1.1  | 1.0                   |
|------------------------------------------------|----------|----------|----------|------|------|------|-----------|------|-----------------------|
| 7.6                                            | Obsolète | Obsolète | Obsolète | Oui. | Oui. | Oui. | Oui.      | Oui. | Oui (RHEL uniquement) |
| 7.7                                            | Obsolète | Obsolète | Obsolète | Oui. | Oui. | Oui. | Oui.      | Non  | Non                   |
| 7.8                                            | Obsolète | Obsolète | Obsolète | Oui. | Oui. | Oui. | Oui.      | Non  | Non                   |
| 7.9                                            | Obsolète | Obsolète | Obsolète | Oui. | Oui. | Oui. | Implicite | Non  | Non                   |
| RHEL 8.0                                       | Obsolète | Obsolète | Obsolète | Oui. | Oui. | Oui. | Oui.      | Oui. | Non                   |
| RHEL 8.1                                       | Obsolète | Obsolète | Obsolète | Oui. | Oui. | Oui. | Oui.      | Non  | Non                   |
| RHEL 8.2                                       | Obsolète | Obsolète | Obsolète | Oui. | Oui. | Oui. | Non       | Non  | Non                   |
| RHEL 8.3                                       | Obsolète | Obsolète | Obsolète | Oui. | Oui. | Oui. | Non       | Non  | Non                   |
| RHEL 8.4                                       | Oui.     | Oui.     | Oui.     | Oui. | Oui. | Non  | Non       | Non  | Non                   |

|                  |      |           |      |      |      |     |     |     |     |
|------------------|------|-----------|------|------|------|-----|-----|-----|-----|
| RHEL 8.5         | Oui. | Oui.      | Oui. | Oui. | Oui. | Non | Non | Non | Non |
| RHEL 8.6         | Oui. | Oui.      | Oui. | Non  | Non  | Non | Non | Non | Non |
| RHEL 8.7         | Oui. | Oui.      | Oui. | Non  | Non  | Non | Non | Non | Non |
| RHEL 8.8         | Oui. | Oui.      | Oui. | Non  | Non  | Non | Non | Non | Non |
| RHEL 8.9         | Oui. | À DÉFINIR | Non  | Non  | Non  | Non | Non | Non | Non |
| RHEL 8.10        | Oui. | Non       | Non  | Non  | Non  | Non | Non | Non | Non |
| RHEL 9.0         | Oui. | Oui.      | Oui. | Non  | Non  | Non | Non | Non | Non |
| RHEL 9.1         | Oui. | Oui.      | Oui. | Non  | Non  | Non | Non | Non | Non |
| RHEL 9.2         | Oui. | Oui.      | Oui. | Non  | Non  | Non | Non | Non | Non |
| RHEL 9.3         | Oui. | À DÉFINIR | Non  | Non  | Non  | Non | Non | Non | Non |
| RHEL 9.4         | Oui. | Non       | Non  | Non  | Non  | Non | Non | Non | Non |
| CentOS 8 et flux | Non  | Non       | Non  | Non  | Non  | Non | S/O | S/O | S/O |
| Rocky Linux 8    | Oui. | Oui.      | Oui. | S/O  | S/O  | S/O | S/O | S/O | S/O |
| Rocky Linux 9    | Oui. | Oui.      | Oui. | S/O  | S/O  | S/O | S/O | S/O | S/O |

- Sauf mention contraire, le système d'exploitation fait référence aux versions RedHat et CentOS.
- « Non » signifie que le système d'exploitation et le médiateur ONTAP ne sont pas compatibles.
- CentOS 8 a été retiré pour toutes les versions en raison de sa ramification. CentOS Stream a été considéré comme un OS cible de production non approprié. Aucun support n'est planifié.
- ONTAP Mediator 1.5 était la dernière version prise en charge pour les systèmes d'exploitation de succursale RHEL 7.x.
- ONTAP Mediator 1.6 ajoute la prise en charge de Rocky Linux 8 et 9.

### Matrice de prise en charge SCST

Le tableau suivant indique la version SCST prise en charge pour chaque version du Mediator ONTAP.

| Version du médiateur ONTAP | Version SCST prise en charge |
|----------------------------|------------------------------|
| Médiateur ONTAP 1.8        | scst-3.8.0.tar.bz2           |
| Médiateur ONTAP 1.7        | scst-3.7.0.tar.bz2           |
| Médiateur ONTAP 1.6        | scst-3.7.0.tar.bz2           |
| Médiateur ONTAP 1.5        | scst-3.6.0.tar.bz2           |
| Médiateur ONTAP 1.4        | scst-3.6.0.tar.bz2           |
| Médiateur ONTAP 1.3        | scst-3.5.0.tar.bz2           |
| Médiateur ONTAP 1.2        | scst-3.4.0.tar.bz2           |
| Médiateur ONTAP 1.1        | scst-3.4.0.tar.bz2           |
| Médiateur ONTAP 1.0        | scst-3.3.0.tar.bz2           |

## Résolution des problèmes

| Modifier l’ID | Description                                                                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6995122       | Lorsqu’une incompatibilité de noyau est détectée, un message d’avertissement est émis et le processus d’installation du Mediator ONTAP se poursuit sans interruption.       |
| 7062227       | Des modifications ont été mises en œuvre pour garantir que le processus d’installation du Mediator ONTAP s’arrête lorsque des échecs de vérification OpenSSL se produisent. |
| 6912810       | Ajout de la prise en charge des événements de vérification de l’état du Mediator ONTAP et des opérations de support ONTAP.                                                  |
| 7028815       | Mise à niveau du <code>scst</code> pour supprimer les fichiers de correctifs inutiles, utilisez la version 3.8.0.                                                           |
| 7097014       | Introduction d’un nouveau script pour valider les certificats utilisés par le médiateur ONTAP 1.8.                                                                          |

## Installer ou mettre à niveau

### Préparez l’installation ou la mise à niveau du service Mediator ONTAP

Pour installer le service ONTAP Mediator, vous devez vous assurer que toutes les conditions préalables sont remplies, récupérer le package d’installation et exécuter le programme d’installation sur l’hôte. Cette procédure est utilisée pour une installation ou une mise à niveau d’une installation existante.

### Description de la tâche

- À partir de ONTAP 9.7, vous pouvez utiliser n’importe quelle version du Mediator ONTAP pour contrôler une configuration IP MetroCluster.

- Depuis ONTAP 9.8, vous pouvez utiliser n'importe quelle version du médiateur ONTAP pour surveiller une relation de synchronisation active SnapMirror.

## Avant de commencer

Vous devez remplir les conditions suivantes.



Le service ONTAP Mediator n'est pas compatible avec le mode Red Hat Enterprise Linux FIPS et l'empêche de s'installer correctement. Vous pouvez vérifier si le mode FIPS est activé à l'aide de la `fips-mode-setup --check` commande. Vous pouvez désactiver le mode FIPS à l'aide de la `fips-mode-setup --disable` commande. Redémarrez le système après avoir désactivé le mode FIPS pour installer correctement le service ONTAP Mediator.

| Version du médiateur ONTAP | Versions Linux prises en charge                                                                                                                                  |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.8                        | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux : 8.6, 8.7, 8.8, 8.9, 8.10, 9.2, 9.3 et 9.4</li> <li>• Rocky Linux 8 et 9</li> </ul>           |
| 1.7                        | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux : 8.5, 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2 et 9.3</li> <li>• Rocky Linux 8 et 9</li> </ul>       |
| 1.6                        | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux : 8.4, 8.5, 8.6, 8.7, 8.8, 9.0, 9.1, 9.2</li> <li>• Rocky Linux 8 et 9</li> </ul>              |
| 1.5                        | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5</li> <li>• CentOS: 7.6, 7.7, 7.8, 7.9</li> </ul> |
| 1.4                        | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5</li> <li>• CentOS: 7.6, 7.7, 7.8, 7.9</li> </ul> |
| 1.3                        | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3</li> <li>• CentOS: 7.6, 7.7, 7.8, 7.9</li> </ul>           |
| 1.2                        | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 8.1</li> <li>• CentOS: 7.6, 7.7, 7.8</li> </ul>                               |



La version du noyau doit correspondre à la version du système d'exploitation.

- installation physique 64 bits ou machine virtuelle
- 8 GO DE RAM
- 1 Go d'espace disque (utilisé pour l'installation des applications, les journaux du serveur et la base de données)
- Utilisateur : accès racine

Tous les packages de bibliothèque, à l'exception du noyau, peuvent être mis à jour en toute sécurité, mais ils peuvent nécessiter un redémarrage pour prendre effet dans l'application ONTAP Mediator. Une fenêtre de

service est recommandée lorsqu'un redémarrage est nécessaire.

Si vous installez le `yum-utils` vous pouvez utiliser le `needs-restarting` commande.

Le noyau du noyau peut être mis à jour s'il est mis à jour vers une version qui est toujours prise en charge par la matrice de version du médiateur ONTAP. Un redémarrage est obligatoire, une fenêtre de maintenance est donc nécessaire.

Le module du noyau SCST doit être désinstallé avant le redémarrage, puis réinstallé après le redémarrage.



La mise à niveau vers un noyau au-delà de la version du système d'exploitation prise en charge pour la version spécifique du Mediator ONTAP n'est pas prise en charge. (Cela indique probablement que le module SCST testé ne se compile pas).

### Enregistrez une clé de sécurité lorsque le démarrage sécurisé UEFI est activé

Si le démarrage sécurisé UEFI est activé, pour installer le médiateur ONTAP, vous devez enregistrer une clé de sécurité avant de pouvoir démarrer le service du médiateur ONTAP. Pour déterminer si le système est activé pour UEFI et si l'amorçage sécurisé est activé, effectuez les opérations suivantes :

#### Étapes

1. Si `mokutil` n'est pas installé, exécutez la commande suivante :

```
yum install mokutil
```

2. Pour déterminer si le démarrage sécurisé UEFI est activé sur votre système, exécutez la commande suivante :

```
mokutil --sb-state
```

Les résultats indiquent si le démarrage sécurisé UEFI est activé sur ce système.



ONTAP Mediator 1.2.0 et les versions précédentes ne prennent pas en charge ce mode.

### Désactivez le démarrage sécurisé UEFI

Vous pouvez également choisir de désactiver le démarrage sécurisé UEFI avant d'installer le médiateur ONTAP.

#### Étapes

1. Dans les paramètres du BIOS de la machine physique, désactivez l'option « démarrage sécurisé UEFI ».
2. Dans les paramètres VMware de la machine virtuelle, désactivez l'option « démarrage sécurisé » pour vSphere 6.x ou l'option « démarrage sécurisé » pour vSphere 7.x.

### Mettez à niveau le système d'exploitation hôte, puis le médiateur ONTAP

Pour mettre à niveau le système d'exploitation hôte pour ONTAP Mediator vers une version ultérieure, vous devez d'abord désinstaller ONTAP Mediator.

#### Avant de commencer

Les meilleures pratiques d'installation de Red Hat Enterprise Linux ou Rocky Linux et des référentiels associés sur votre système sont répertoriées ci-dessous. Les systèmes installés ou configurés différemment peuvent

nécessiter des étapes supplémentaires.

- Vous devez installer Red Hat Enterprise Linux ou Rocky Linux conformément aux meilleures pratiques de Red Hat. En raison de la fin de vie des versions CentOS 8.x, les versions compatibles de CentOS 8.x ne sont pas recommandées.
- Lors de l'installation du service ONTAP Mediator sur Red Hat Enterprise Linux ou Rocky Linux, le système doit avoir accès au référentiel approprié pour que le programme d'installation puisse accéder à toutes les dépendances logicielles requises et les installer.
- Pour que le programme d'installation de yum trouve des logiciels dépendants dans les référentiels Red Hat Enterprise Linux, vous devez avoir enregistré le système pendant l'installation de Red Hat Enterprise Linux ou ultérieurement en utilisant un abonnement Red Hat valide.

Pour plus d'informations sur le Gestionnaire d'abonnement Red Hat, reportez-vous à la documentation Red Hat.

- Les ports suivants doivent être inutilisés et disponibles pour le médiateur :
  - 31784
  - 3260
- Si vous utilisez un pare-feu tiers : reportez-vous à la ["Exigences relatives au pare-feu pour le médiateur ONTAP"](#)
- Si l'hôte Linux se trouve dans un emplacement sans accès à Internet, vous devez vous assurer que les packages requis sont disponibles dans un référentiel local.

Si vous utilisez le protocole LACP (Link Aggregation Control Protocol) dans un environnement Linux, vous devez configurer correctement le noyau et vous assurer que le `sysctl net.ipv4.conf.all.arp_ignore` est réglé sur « 2 ».

**Ce dont vous avez besoin**

Les packages suivants sont requis par le service ONTAP Mediator :

| Toutes les versions de RHEL/CentOS                                                                                                                                                                                                                                                                                                | Packages supplémentaires pour RHEL 8.x / Rocky Linux 8                                                                                                                                                     | Packages supplémentaires pour RHEL 9.x / Rocky Linux 9                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• openssl</li><li>• openssl-devel</li><li>• kernel-devel-\$ (nom_underscore -r)</li><li>• gcc</li><li>• marque</li><li>• libselinux-utils</li><li>• correctif</li><li>• bzip2</li><li>• perl-Data-Dumper</li><li>• perl-ExtUtils-MakeMaker</li><li>• efibootmgr</li><li>• mokutil</li></ul> | <ul style="list-style-type: none"><li>• python3-pip</li><li>• elfutils-libelf-devel</li><li>• politiqueutils-python-utils</li><li>• red hat-lsb-core</li><li>• python39</li><li>• python39-devel</li></ul> | <ul style="list-style-type: none"><li>• python3-pip</li><li>• elfutils-libelf-devel</li><li>• politiqueutils-python-utils</li><li>• python3</li><li>• python3-devel</li></ul> |

Le package d'installation Mediator est un fichier tar compressé auto-extractible qui comprend :

- Un fichier RPM contenant toutes les dépendances qui ne peuvent pas être obtenues du référentiel de la version prise en charge.
- Un script d'installation.

Une certification SSL valide est recommandée.

### Description de la tâche

Lorsque vous mettez à niveau le système d'exploitation hôte pour ONTAP Mediator vers une version majeure ultérieure (par exemple, de 7.x à 8.x) à l'aide de l'outil de mise à niveau leapp, Vous devez désinstaller ONTAP Mediator car l'outil tente de détecter les nouvelles versions de tous les RPM installés dans les référentiels enregistrés avec le système.

Comme un fichier .rpm a été installé dans le cadre du programme d'installation de ONTAP Mediator, il est inclus dans cette recherche. Cependant, comme ce fichier .rpm a été décompressé dans le cadre du programme d'installation et n'a pas été téléchargé à partir d'un référentiel enregistré, une mise à niveau est introuvable. Dans ce cas, l'outil de mise à niveau leapp désinstalle le package.

Afin de conserver les fichiers journaux, qui seront utilisés pour trier les dossiers de support, vous devez sauvegarder les fichiers avant de procéder à une mise à niveau du système d'exploitation et les restaurer après une réinstallation du progiciel ONTAP Mediator. Étant donné que le médiateur ONTAP est en cours de réinstallation, tous les clusters ONTAP qui y sont connectés devront être reconnectés après la nouvelle installation.



Les étapes suivantes doivent être effectuées dans l'ordre. Immédiatement après la réinstallation du médiateur ONTAP, vous devez arrêter le service ontap\_médiateur, remplacer les fichiers journaux et redémarrer le service. Cela permet de s'assurer que les journaux ne seront pas perdus.

### Étapes

1. Sauvegardez les fichiers journaux.

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. Effectuez une mise à niveau avec l'outil de mise à niveau leapp.



```
[rootmediator-host ~]# leapp preupgrade --target 8.4
....
....
[rootmediator-host ~]# leapp upgrade --target 8.4
....
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

### 3. Réinstallez le médiateur ONTAP.



Effectuez le reste des étapes immédiatement après la réinstallation du médiateur ONTAP pour éviter la perte des fichiers journaux.

```
[rootmediator-host ~]# ontap-mediator-1.6.0/ontap-mediator-1.6.0

ONTAP Mediator: Self Extracting Installer

....
[rootmediator-host ~]#
```

### 4. Arrêtez le service ontap\_médiateur.

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

### 5. Remplacez les fichiers journaux.

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

### 6. Démarrez le service ontap\_médiateur.

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

### 7. Reconnectez tous les clusters ONTAP au médiateur ONTAP mis à niveau

```

siteA::> metrocluster configuration-settings mediator show
Mediator IP Port Node Configuration
Connection
Status Status

172.31.40.122
31784 siteA-node2 true false
 siteA-nod1 true false
 siteB-node2 true false
 siteB-node2 true false

siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover.
It may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP Port Node Configuration
Connection
Status Status

172.31.40.122
31784 siteA-node2 true true
 siteA-nod1 true true
 siteB-node2 true true
 siteB-node2 true true

siteA::>

```

## Procédure de synchronisation active SnapMirror

Pour la synchronisation active SnapMirror, si vous avez installé votre certificat TLS en dehors du répertoire /opt/netapp, vous n'avez pas besoin de le réinstaller. Si vous utilisez le certificat auto-signé généré par défaut ou si vous placez votre certificat personnalisé dans le répertoire /opt/netapp, vous devez le sauvegarder et le restaurer.

```
peer1::> snapmirror mediator show
```

| Mediator Address | Peer Cluster | Connection Status | Quorum Status |
|------------------|--------------|-------------------|---------------|
| 172.31.49.237    | peer2        | unreachable       | true          |

```
peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2
```

```
Info: [Job 39] 'mediator remove' job queued
```

```
peer1::> job show -id 39
```

| Job ID | Name            | Owning Vserver | Node        | State   |
|--------|-----------------|----------------|-------------|---------|
| 39     | mediator remove | peer1          | peer1-node1 | Success |

Description: Removing entry in mediator

```
peer1::> security certificate show -common-name ONTAPMediatorCA
```

| Vserver | Serial Number                            | Certificate Name | Type      |
|---------|------------------------------------------|------------------|-----------|
| peer1   | 4A790360081F41145E14C5D7CE721DC6C210007F | ONTAPMediatorCA  | server-ca |

```
peer1
```

```
4A790360081F41145E14C5D7CE721DC6C210007F
```

```
ONTAPMediatorCA
```

```
server-
```

```
ca
```

```
Certificate Authority: ONTAP Mediator CA
```

```
Expiration Date: Mon Apr 17 10:27:54 2073
```

```
peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.
```

```
peer1::> security certificate install -type server-ca -vserver peer1
```

```
Please enter Certificate: Press <Enter> when done
```

```
..<snip ONTAP Mediator CA public key>..
```

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

```
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254
```

The certificate's generated name for reference: ONTAPMediatorCA

```
peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.
```

```
peer2::> security certificate install -type server-ca -vserver peer2
```

```
Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..
```

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

```
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254
```

The certificate's generated name for reference: ONTAPMediatorCA

```
peer1::> snapmirror mediator add -mediator-address 172.31.49.237 -peer
-cluster peer2 -username mediatoradmin
```

Notice: Enter the mediator password.

```
Enter the password:
Enter the password again:
```

Info: [Job: 43] 'mediator add' job queued

```
peer1::> job show -id 43
```

| Job | ID | Name                                   | Owning<br>Vserver | Node        | State   |
|-----|----|----------------------------------------|-------------------|-------------|---------|
| 43  |    | mediator add                           | peer1             | peer1-node2 | Success |
|     |    | Description: Creating a mediator entry |                   |             |         |

```
peer1::> snapmirror mediator show
```

| Mediator      | Address | Peer  | Cluster | Connection | Status | Quorum | Status |
|---------------|---------|-------|---------|------------|--------|--------|--------|
| 172.31.49.237 |         | peer2 |         | connected  |        | true   |        |

```
peer1::>
```

## Autoriser l'accès aux référentiels

Vous devez activer l'accès aux référentiels pour que le médiateur ONTAP puisse accéder aux packages requis pendant le processus d'installation

### Étapes

1. Déterminez les référentiels à accéder, comme indiqué dans le tableau suivant :

| Si votre système d'exploitation est... | Vous devez donner l'accès à ces référentiels...                                                                            |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| RHEL 7.x                               | <ul style="list-style-type: none"><li>• rhel-7-server-optional-rpms</li></ul>                                              |
| RHEL 8.x                               | <ul style="list-style-type: none"><li>• rhel-8-for-x86_64-baseos-rpms</li><li>• rhel-8-for-x86_64-appstream-rpms</li></ul> |
| RHEL 9.x                               | <ul style="list-style-type: none"><li>• rhel-9-for-x86_64-baseos-rpms</li><li>• rhel-9-for-x86_64-appstream-rpms</li></ul> |
| CentOS 7.x                             | <ul style="list-style-type: none"><li>• C7.6.1810 - référentiel de base</li></ul>                                          |
| Rocky Linux 8                          | <ul style="list-style-type: none"><li>• appstream</li><li>• bases</li></ul>                                                |
| Rocky Linux 9                          | <ul style="list-style-type: none"><li>• appstream</li><li>• bases</li></ul>                                                |

2. Utilisez l'une des procédures suivantes pour activer l'accès aux référentiels répertoriés ci-dessus afin que ONTAP Mediator puisse accéder aux packages requis pendant le processus d'installation.



Si le médiateur ONTAP a des dépendances sur les modules Python présents dans les référentiels "extras" et "facultatifs", il peut avoir besoin d'accéder au `rhel-X-for-x86_64-extras-rpms` et `rhel-X-for-x86_64-optional-rpms` fichiers.

## Procédure pour le système d'exploitation RHEL 7.x.

Utilisez cette procédure si votre système d'exploitation est **RHEL 7.x** pour activer l'accès aux référentiels :

### Étapes

1. Abonnez-vous au référentiel requis :

```
subscription-manager repos --enable rhel-7-server-optional-rpms
```

L'exemple suivant montre l'exécution de cette commande :

```
[root@localhost ~]# subscription-manager repos --enable rhel-7-
server-optional-rpms
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
```

2. Exécutez le `yum repolist` commande.

L'exemple suivant montre l'exécution de cette commande. Le référentiel "rhel-7-Server-optional-rpms" devrait apparaître dans la liste.

```
[root@localhost ~]# yum repolist
Loaded plugins: product-id, search-disabled-repos, subscription-
manager
rhel-7-server-optional-rpms | 3.2 kB 00:00:00
rhel-7-server-rpms | 3.5 kB 00:00:00
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
| 26 kB 00:00:00
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
| 2.5 MB 00:00:00
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
| 8.3 MB 00:00:01
repo id repo name
status
rhel-7-server-optional-rpms/7Server/x86_64 Red Hat Enterprise
Linux 7 Server - Optional (RPMs) 19,447
rhel-7-server-rpms/7Server/x86_64 Red Hat Enterprise
Linux 7 Server (RPMs) 26,758
repolist: 46,205
[root@localhost ~]#
```

## Procédure pour le système d'exploitation RHEL 8.x.

Utilisez cette procédure si votre système d'exploitation est **RHEL 8.x** pour activer l'accès aux référentiels :

### Étapes

1. Abonnez-vous au référentiel requis :

```
subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
```

L'exemple suivant montre l'exécution de cette commande :

```
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this system.
```

2. Exécutez le `yum repolist` commande.

Les nouveaux référentiels auxquels vous êtes abonné doivent apparaître dans la liste.

## Procédure pour le système d'exploitation RHEL 9.x.

Utilisez cette procédure si votre système d'exploitation est **RHEL 9.x** pour activer l'accès aux référentiels :

### Étapes

1. Abonnez-vous au référentiel requis :

```
subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
```

L'exemple suivant montre l'exécution de cette commande :

```
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this system.
```

2. Exécutez le `yum repolist` commande.

Les nouveaux référentiels auxquels vous êtes abonné doivent apparaître dans la liste.



## Procédure pour le système d'exploitation CentOS 7.x.

Utilisez cette procédure si votre système d'exploitation est **CentOS 7.x** pour activer l'accès aux référentiels :



Les exemples suivants montrent un référentiel pour CentOS 7.6 et peuvent ne pas fonctionner pour d'autres versions de CentOS. Utilisez le référentiel de base pour votre version de CentOS.

### Étapes

1. Ajoutez le référentiel C7.6.1810 - base. Le référentiel de coffre-fort C7.6.1810 - base contient le paquet "kernel-devel" nécessaire pour le Mediator ONTAP.
2. Ajoutez les lignes suivantes à /etc/yum.repos.d/CentOS-Vault.repo.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. Exécutez le `yum repolist` commande.

L'exemple suivant montre l'exécution de cette commande. Le référentiel CentOS-7.6.1810 - base doit apparaître dans la liste.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: distro.ibiblio.org
* extras: distro.ibiblio.org
* updates: ewr.edge.kernel.org
C7.6.1810-base | 3.6 kB 00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz | 166 kB 00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db | 6.0 MB 00:00:04
repo id repo name status
C7.6.1810-base/x86_64 CentOS-7.6.1810 - Base 10,019
base/7/x86_64 CentOS-7 - Base 10,097
extras/7/x86_64 CentOS-7 - Extras 307
updates/7/x86_64 CentOS-7 - Updates 1,010
repolist: 21,433
[root@localhost ~]#
```

## Procédure pour les systèmes d'exploitation Rocky Linux 8 ou 9

Utilisez cette procédure si votre système d'exploitation est **Rocky Linux 8** ou **Rocky Linux 9** pour permettre l'accès aux référentiels :

### Étapes

1. Abonnez-vous aux référentiels requis :

```
dnf config-manager --set-enabled baseos

dnf config-manager --set-enabled appstream
```

2. Exécutez un clean fonctionnement :

```
dnf clean all
```

3. Vérifiez la liste des référentiels :

```
dnf repolist
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id repo name
appstream Rocky Linux 8 - AppStream
baseos Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id repo name
appstream Rocky Linux 9 - AppStream
baseos Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

## Téléchargez le package d'installation du Mediator

Téléchargez le package d'installation Mediator dans le cadre du processus d'installation.

### Étapes

1. Téléchargez le progiciel d'installation du médiateur à partir de la page ONTAP Mediator.

["Page de téléchargement du médiateur ONTAP"](#)

2. Vérifiez que le package d'installation du Mediator se trouve dans le répertoire de travail actuel :

```
[root@sdot-r730-0003a-d6 ~]# ls ontap-mediator-1.8.0.tgz
```



Pour ONTAP Mediator versions 1.4 et antérieures, le programme d'installation est nommé `ontap-mediator`.

Si vous êtes à un endroit sans accès à Internet, vous devez vous assurer que le programme d'installation a accès aux packages requis.

3. Si nécessaire, déplacez le package d'installation du Mediator du répertoire de téléchargement vers le répertoire d'installation de l'hôte Linux Mediator.

4. Décompressez le programme d'installation :

```
tar xvfz ontap-mediator-1.8.0.tgz
```

```
ontap-mediator-1.8.0/
ontap-mediator-1.8.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.8.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.8.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.8.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.8.0/ONTAP-Mediator-production.pub
ontap-mediator-1.8.0/ontap-mediator-1.8.0
ontap-mediator-1.8.0/ontap-mediator-1.8.0.sig.tsr
ontap-mediator-1.8.0/ontap-mediator-1.8.0.tsr
ontap-mediator-1.8.0/ontap-mediator-1.8.0.sig
```

## Vérifiez la signature du code du médiateur ONTAP

Vous devez vérifier la signature de code du médiateur ONTAP avant d'installer le progiciel d'installation du médiateur ONTAP.

### Avant de commencer

Avant de vérifier la signature du code du médiateur ONTAP, votre système doit répondre aux exigences suivantes.

- openssl versions 1.0.2 à 3.0 pour la vérification de base
- openssl version 1.1.0 ou ultérieure pour les opérations TSA (Time Stamping Authority)
- Accès public Internet pour vérification OCSP

Le pack de téléchargement contient les fichiers suivants :

| Fichier                           | Description                                                                                          |
|-----------------------------------|------------------------------------------------------------------------------------------------------|
| ONTAP-Mediator-production.pub     | Clé publique utilisée pour vérifier la signature                                                     |
| csc-prod-chain-ONTAP-Mediator.pem | La chaîne de confiance de l'autorité de certification publique                                       |
| csc-prod-ONTAP-Mediator.pem       | Certificat utilisé pour générer la clé                                                               |
| ontap-mediator-1.8.0              | Exécutable d'installation du produit pour la version 1.8.0                                           |
| ontap-mediator-1.8.0.sig          | Le SHA-256 a été écrasé, puis signé par RSA à l'aide de la clé csc-prod, signature de l'installateur |
| ontap-mediator-1.8.0.sig.tsr      | La demande de révocation que OCSCP doit utiliser pour la signature de l'installateur                 |
| ontap-mediator-1.8.0.tsr          | Fichier de requête de signature d'horodatage                                                         |
| tsa-prod-ONTAP-Mediator.pem       | Le certificat public pour le TSR                                                                     |
| tsa-prod-chain-ONTAP-Mediator.pem | La chaîne CA du certificat public pour le TSR                                                        |

## Étapes

1. Effectuez la vérification de révocation sur `csc-prod-ONTAP-Mediator.pem` Via le protocole OCSP (Online Certificate Status Protocol).
  - a. Recherchez l'URL OCSP utilisée pour enregistrer le certificat car les certificats de développeur ne fournissent pas nécessairement d'uri.

```
openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
```

- b. Générez une demande OCSP pour le certificat.

```
openssl ocsf -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout req.der
```

- c. Connectez-vous au OCSP Manager pour envoyer la demande OCSP :

```
openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-chain-ONTAP-Mediator.pem
```

2. Vérifiez la chaîne de confiance du CSC et sa date d'expiration par rapport à l'hôte local :

```
openssl verify
```



Le openssl La version du CHEMIN d'ACCÈS doit être valide cert.pem (pas auto-signé).

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath ${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem # Failure action: The Code-Signature-Check certificate has expired or is invalid. Download a newer version of the ONTAP Mediator.
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath ${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem # Failure action: The Time-Stamp certificate has expired or is invalid. Download a newer version of the ONTAP Mediator.
```

3. Vérifiez le ontap-mediator-1.8.0.sig.tsr et ontap-mediator-1.8.0.tsr fichiers utilisant les certificats associés :

```
openssl ts -verify
```



.tsr les fichiers contiennent la réponse de l'horodatage associée au programme d'installation et à la signature du code. Le traitement confirme que l'horodatage a une signature valide de TSA et que votre fichier d'entrée n'a pas changé. La vérification est effectuée localement sur votre machine. De façon indépendante, il n'est pas nécessaire d'accéder aux serveurs TSA.

```
openssl ts -verify -data ontap-mediator-1.8.0.sig -in ontap-mediator-1.8.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-ONTAP-Mediator.pem
openssl ts -verify -data ontap-mediator-1.8.0 -in ontap-mediator-1.8.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-ONTAP-Mediator.pem
```

4. Vérifiez les signatures par rapport à la clé :

```
openssl -dgst -verify
```

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.8.0.sig ontap-mediator-1.8.0
```

## Exemple de vérification de la signature de code du médiateur ONTAP (sortie console)

```
[root@scspa2695423001 ontap-mediator-1.8.0]# pwd
/root/ontap-mediator-1.8.0
[root@scspa2695423001 ontap-mediator-1.8.0]# ls -l
total 63660
-r--r--r-- 1 root root 8582 Feb 19 15:02 csc-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root 2373 Feb 19 15:02 csc-prod-ONTAP-
Mediator.pem
-r-xr-xr-- 1 root root 65132818 Feb 20 15:17 ontap-mediator-1.8.0
-rw-r--r-- 1 root root 384 Feb 20 15:17 ontap-mediator-1.8.0.sig
-rw-r--r-- 1 root root 5437 Feb 20 15:17 ontap-mediator-
1.8.0.sig.tsr
-rw-r--r-- 1 root root 5436 Feb 20 15:17 ontap-mediator-1.8.0.tsr
-r--r--r-- 1 root root 625 Feb 19 15:02 ONTAP-Mediator-
production.pub
-r--r--r-- 1 root root 3323 Feb 19 15:02 tsa-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root 1740 Feb 19 15:02 tsa-prod-ONTAP-
Mediator.pem
[root@scspa2695423001 ontap-mediator-1.8.0]#
[root@scspa2695423001 ontap-mediator-1.8.0]#
/root/verify_ontap_mediator_signatures.sh
++ openssl version -d
++ cut -d '"' -f2
+ OPENSSLDIR=/etc/pki/tls
+ openssl version
OpenSSL 1.1.1k FIPS 25 Mar 2021
++ openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
+ ocsp_uri=http://ocsp.entrust.net
+ echo http://ocsp.entrust.net
http://ocsp.entrust.net
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout
req.der
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url
http://ocsp.entrust.net -resp_text -respout resp.der -verify_other csc-
prod-chain-ONTAP-Mediator.pem
OCSP Response Data:
 OCSP Response Status: successful (0x0)
 Response Type: Basic OCSP Response
 Version: 1 (0x0)
 Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
```

Produced At: Feb 28 05:01:00 2023 GMT

Responses:

Certificate ID:

Hash Algorithm: sha1

Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A

Issuer Key Hash: CE894F8251AA15A28462CA312361D261F8FE78

Serial Number: 511A542B57522AEB7295A640DC6200E5

Cert Status: good

This Update: Feb 28 05:00:00 2023 GMT

Next Update: Mar 4 04:59:59 2023 GMT

Signature Algorithm: sha512WithRSAEncryption

3c:1d:49:b0:93:62:37:3e:c7:38:e3:9f:9f:62:82:73:ed:f4:  
ea:00:6b:f1:01:cd:79:57:92:f1:9d:5d:85:9b:60:59:f8:6c:  
e6:f4:50:51:f3:4c:8a:51:dd:50:68:16:8f:20:24:7e:39:b0:  
44:94:8d:b0:61:da:b9:08:36:74:2d:44:55:62:fb:92:be:4a:  
e7:6c:8c:49:dd:0c:fd:d8:ce:20:08:0d:0f:5a:29:a3:19:03:  
9f:d3:df:41:f4:89:0f:73:18:3f:ac:bb:a7:a3:96:7d:c5:70:  
4c:57:cd:17:17:c6:8a:60:d1:37:c9:2d:81:07:2a:d7:a6:02:  
ee:ce:88:16:22:db:e3:43:64:1e:9b:0d:4d:31:66:fa:ab:a5:  
52:99:94:4a:4a:d0:52:c5:34:f5:18:c7:15:5b:ce:74:c2:fc:  
61:ea:55:aa:f1:2f:82:a3:6a:95:8d:7e:2b:38:49:4f:bf:b1:  
68:7b:1b:24:8b:1f:4d:c5:77:f0:71:af:9c:34:c8:7a:82:50:  
09:a2:19:6e:c6:30:4f:da:a2:79:08:f9:d0:ff:85:d9:2a:84:  
cf:0c:aa:75:8f:72:c9:a7:a2:83:e8:8b:cf:ed:0c:69:75:b6:  
2a:7b:6b:58:99:01:d8:34:ad:e1:89:25:27:1b:fa:d9:6d:32:  
97:3a:0b:0a:8e:a3:9e:e3:f4:e0:d6:1a:c9:b5:14:8c:3e:54:  
3b:37:17:1a:93:44:84:8b:4a:87:97:1e:76:43:3e:d3:ec:8b:  
7e:56:4a:3f:01:31:c0:e5:58:fb:50:ce:6f:b1:e7:35:f9:b7:  
a3:ef:6b:3b:21:95:37:a6:5b:8f:f0:15:18:36:65:89:a1:9c:  
9b:69:00:b4:b1:65:6a:bc:11:2d:d4:9b:b4:97:cc:cb:7a:0c:  
16:11:c1:75:58:7e:13:ab:56:3c:3f:93:5b:95:24:c6:54:52:  
1f:86:a9:16:ce:d9:ea:8b:3a:f3:4f:c4:8f:ad:de:e8:3e:3c:  
d2:51:51:ad:33:7f:d8:c5:33:24:26:f1:2d:9d:0e:9f:55:d0:  
68:bf:af:bd:68:4a:40:08:bc:92:a0:62:54:7d:16:7b:36:29:  
15:b1:cd:58:8e:fb:4a:f2:3e:94:8b:fe:56:95:cc:24:32:af:  
5f:71:99:18:ed:0c:64:94:f7:54:48:87:48:d0:6d:b3:42:04:  
96:03:73:a2:8e:8a:6a:b2:af:ee:56:19:a1:c6:35:12:59:ad:  
19:6a:fe:e0:f1:27:cc:96:4e:f0:4f:fb:6a:bd:ce:05:2c:aa:  
79:7c:df:02:5c:ca:53:7d:60:12:88:7c:ce:15:c7:d4:02:27:  
c1:ab:cf:71:30:1e:14:ba

WARNING: no nonce in response

Response verify OK

csc-prod-ONTAP-Mediator.pem: good

This Update: Feb 28 05:00:00 2023 GMT

Next Update: Mar 4 04:59:59 2023 GMT



```

+ openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls csc-prod-ONTAP-Mediator.pem
csc-prod-ONTAP-Mediator.pem: OK
+ openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls tsa-prod-ONTAP-Mediator.pem
tsa-prod-ONTAP-Mediator.pem: OK
+ openssl ts -verify -data ontap-mediator-1.8.0.sig -in ontap-mediator-
1.8.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl ts -verify -data ontap-mediator-1.8.0 -in ontap-mediator-
1.8.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.8.0.sig ontap-mediator-1.8.0
Verified OK
[root@scspa2695423001 ontap-mediator-1.8.0]#

```

## Installez le package d'installation du Mediator ONTAP

Pour installer le service ONTAP Mediator, vous devez obtenir le package d'installation et exécuter le programme d'installation sur l'hôte.

### Étapes

1. Exécutez le programme d'installation et répondez aux invites si nécessaire :

```
./ontap-mediator-1.8.0/ontap-mediator-1.8.0 -y
```

```
[root@scs000099753 ~]# ./ontap-mediator-1.8.0/ontap-mediator-1.8.0 -y
```

Le processus d'installation permet de créer les comptes requis et d'installer les packages requis. Si une version antérieure de Mediator est installée sur l'hôte, vous serez invité à confirmer la mise à niveau.

2. À partir de ONTAP Mediator 1.4, le mécanisme de démarrage sécurisé est activé sur les systèmes UEFI. Lorsque le démarrage sécurisé est activé, vous devez suivre les étapes supplémentaires pour enregistrer la clé de sécurité après l'installation :

- Suivez les instructions du fichier README pour signer le module de noyau SCST. :

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
signing
```

- Repérez les touches requises :

/opt/netapp/lib/ontap\_mediator/ontap\_mediator/SCST\_mod\_keys



Une fois l'installation terminée, les fichiers README et l'emplacement des clés sont également fournis dans la sortie du système.

## Exemple d'installation du Mediator ONTAP (sortie console)

```
[root@sdot-r730-0003a-d6 ~]# ontap-mediator-1.8.0/ontap-mediator-1.8.0
-y

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
 Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
Error querying OCSP responder
 WARNING: The OCSP check failed while attempting to test the Code-
Signature-Check certificate
 SKIPPING: Code signature check, manual override due to lack of OCSP
response
+ Unpacking the ONTAP Mediator installer
ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode
The installer will change the SELinux context type of
/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi from type 'lib_t' to
'bin_t'.

+ Checking for default Linux firewall
success
success
success

#####
Preparing for installation of ONTAP Mediator packages.

+ Installing required packages.
```

Updating Subscription Management repositories.

Unable to read consumer identity

This system is not registered with an entitlement server. You can use subscription-manager to register.

Last metadata expiration check: 272 days, 23:59:05 ago on Thu 07 Sep 2023 11:37:05 AM EDT.

Package openssl-1:1.1.1k-9.el8\_7.x86\_64 is already installed.

Package libselinux-utils-2.9-8.el8.x86\_64 is already installed.

Package perl-Data-Dumper-2.167-399.el8.x86\_64 is already installed.

Package bzip2-1.0.6-26.el8.x86\_64 is already installed.

Package efibootmgr-16-1.el8.x86\_64 is already installed.

Package mokutil-1:0.3.0-12.el8.x86\_64 is already installed.

Package python3-pip-9.0.3-23.el8.noarch is already installed.

Package polycoreutils-python-utils-2.9-24.el8.noarch is already installed.

Dependencies resolved.

```
=====
=====
=====
=====
Package
Architecture Version
Repository Size
=====
=====
=====
=====
```

Installing:

```
elfutils-libelf-devel
x86_64 0.189-3.el8
Local-BaseOS 62 k
gcc
x86_64 8.5.0-20.el8
Local-AppStream 23 M
kernel-devel
x86_64 4.18.0-513.el8
Local-BaseOS 24 M
make
x86_64 1:4.2.1-11.el8
Local-BaseOS 498 k
openssl-devel
x86_64 1:1.1.1k-9.el8_7
Local-BaseOS 2.3 M
patch
```

|                                 |              |
|---------------------------------|--------------|
| x86_64                          | 2.7.6-11.el8 |
| Local-BaseOS                    | 138 k        |
| perl-ExtUtils-MakeMaker         |              |
| noarch                          | 1:7.34-1.el8 |
| Local-AppStream                 | 301 k        |
| python39                        |              |
| x86_64                          | 3.9.17-      |
| 2.module+el8.9.0+19644+d68f775d |              |
| Local-AppStream                 | 34 k         |
| python39-devel                  |              |
| x86_64                          | 3.9.17-      |
| 2.module+el8.9.0+19644+d68f775d |              |
| Local-AppStream                 | 229 k        |
| redhat-lsb-core                 |              |
| x86_64                          | 4.1-47.el8   |
| Local-AppStream                 | 45 k         |
| Installing dependencies:        |              |
| annobin                         |              |
| x86_64                          | 11.13-2.el8  |
| Local-AppStream                 | 972 k        |
| cpp                             |              |
| x86_64                          | 8.5.0-20.el8 |
| Local-AppStream                 | 10 M         |
| dwz                             |              |
| x86_64                          | 0.12-10.el8  |
| Local-AppStream                 | 109 k        |
| efi-srpm-macros                 |              |
| noarch                          | 3-3.el8      |
| Local-AppStream                 | 22 k         |
| gcc-plugin-annobin              |              |
| x86_64                          | 8.5.0-20.el8 |
| Local-AppStream                 | 36 k         |
| ghc-srpm-macros                 |              |
| noarch                          | 1.4.2-7.el8  |
| Local-AppStream                 | 9.4 k        |
| glibc-devel                     |              |
| x86_64                          | 2.28-236.el8 |
| Local-BaseOS                    | 84 k         |
| glibc-headers                   |              |
| x86_64                          | 2.28-236.el8 |
| Local-BaseOS                    | 489 k        |
| go-srpm-macros                  |              |
| noarch                          | 2-17.el8     |
| Local-AppStream                 | 13 k         |
| isl                             |              |
| x86_64                          | 0.16.1-6.el8 |

|                      |                     |
|----------------------|---------------------|
| Local-AppStream      | 841 k               |
| kernel-headers       |                     |
| x86_64               | 4.18.0-513.el8      |
| Local-BaseOS         | 11 M                |
| keyutils-libs-devel  |                     |
| x86_64               | 1.5.10-9.el8        |
| Local-BaseOS         | 48 k                |
| krb5-devel           |                     |
| x86_64               | 1.18.2-25.el8_8     |
| Local-BaseOS         | 562 k               |
| libcom_err-devel     |                     |
| x86_64               | 1.45.6-5.el8        |
| Local-BaseOS         | 39 k                |
| libkadm5             |                     |
| x86_64               | 1.18.2-25.el8_8     |
| Local-BaseOS         | 188 k               |
| libselinux-devel     |                     |
| x86_64               | 2.9-8.el8           |
| Local-BaseOS         | 200 k               |
| libsepol-devel       |                     |
| x86_64               | 2.9-3.el8           |
| Local-BaseOS         | 87 k                |
| libverto-devel       |                     |
| x86_64               | 0.3.2-2.el8         |
| Local-BaseOS         | 18 k                |
| libxcrypt-devel      |                     |
| x86_64               | 4.1.1-6.el8         |
| Local-BaseOS         | 25 k                |
| libzstd-devel        |                     |
| x86_64               | 1.4.4-1.el8         |
| Local-BaseOS         | 44 k                |
| m4                   |                     |
| x86_64               | 1.4.18-7.el8        |
| Local-BaseOS         | 223 k               |
| mailx                |                     |
| x86_64               | 12.5-29.el8         |
| Local-BaseOS         | 257 k               |
| ncurses-compat-libs  |                     |
| x86_64               | 6.1-10.20180224.el8 |
| Local-BaseOS         | 329 k               |
| ocaml-srpm-macros    |                     |
| noarch               | 5-4.el8             |
| Local-AppStream      | 9.5 k               |
| openblas-srpm-macros |                     |
| noarch               | 2-2.el8             |
| Local-AppStream      | 8.0 k               |

|                        |                  |       |
|------------------------|------------------|-------|
| pcr2-devel             |                  |       |
| x86_64                 | 10.32-3.el8_6    |       |
| Local-BaseOS           |                  | 605 k |
| pcr2-utf16             |                  |       |
| x86_64                 | 10.32-3.el8_6    |       |
| Local-BaseOS           |                  | 229 k |
| pcr2-utf32             |                  |       |
| x86_64                 | 10.32-3.el8_6    |       |
| Local-BaseOS           |                  | 220 k |
| perl-CPAN-Meta-YAML    |                  |       |
| noarch                 | 0.018-397.el8    |       |
| Local-AppStream        |                  | 34 k  |
| perl-ExtUtils-Command  |                  |       |
| noarch                 | 1:7.34-1.el8     |       |
| Local-AppStream        |                  | 19 k  |
| perl-ExtUtils-Install  |                  |       |
| noarch                 | 2.14-4.el8       |       |
| Local-AppStream        |                  | 46 k  |
| perl-ExtUtils-Manifest |                  |       |
| noarch                 | 1.70-395.el8     |       |
| Local-AppStream        |                  | 37 k  |
| perl-ExtUtils-ParseXS  |                  |       |
| noarch                 | 1:3.35-2.el8     |       |
| Local-AppStream        |                  | 83 k  |
| perl-JSON-PP           |                  |       |
| noarch                 | 1:2.97.001-3.el8 |       |
| Local-AppStream        |                  | 68 k  |
| perl-Test-Harness      |                  |       |
| noarch                 | 1:3.42-1.el8     |       |
| Local-AppStream        |                  | 279 k |
| perl-devel             |                  |       |
| x86_64                 | 4:5.26.3-422.el8 |       |
| Local-AppStream        |                  | 600 k |
| perl-srpm-macros       |                  |       |
| noarch                 | 1-25.el8         |       |
| Local-AppStream        |                  | 11 k  |
| perl-version           |                  |       |
| x86_64                 | 6:0.99.24-1.el8  |       |
| Local-AppStream        |                  | 67 k  |
| postfix                |                  |       |
| x86_64                 | 2:3.5.8-7.el8    |       |
| Local-BaseOS           |                  | 1.5 M |
| python-rpm-macros      |                  |       |
| noarch                 | 3-45.el8         |       |
| Local-AppStream        |                  | 16 k  |
| python-srpm-macros     |                  |       |

```

noarch 3-45.el8
Local-AppStream 16 k
 python3-pyparsing
noarch 2.1.10-7.el8
Local-BaseOS 142 k
 python3-rpm-macros
noarch 3-45.el8
Local-AppStream 15 k
 python39-libs
x86_64 3.9.17-
2.module+el8.9.0+19644+d68f775d
Local-AppStream 8.2 M
 python39-pip-wheel
noarch 20.2.4-
8.module+el8.9.0+19644+d68f775d
Local-AppStream 1.1 M
 python39-setuptools-wheel
noarch 50.3.2-
4.module+el8.9.0+19644+d68f775d
Local-AppStream 497 k
 qt5-srpm-macros
noarch 5.15.3-1.el8
Local-AppStream 11 k
 redhat-lsb-submod-security
x86_64 4.1-47.el8
Local-AppStream 22 k
 redhat-rpm-config
noarch 131-1.el8
Local-AppStream 91 k
 rust-srpm-macros
noarch 5-2.el8
Local-AppStream 9.3 k
 spax
x86_64 1.5.3-13.el8
Local-BaseOS 217 k
 systemtap-sdt-devel
x86_64 4.9-3.el8
Local-AppStream 88 k
 zlib-devel
x86_64 1.2.11-25.el8
Local-BaseOS 59 k
Installing weak dependencies:
 bison
x86_64 3.0.4-10.el8
Local-AppStream 688 k
 flex

```



```

x86_64 2.6.1-9.el8
Local-AppStream 320 k
 perl-CPAN-Meta
noarch 2.150010-396.el8
Local-AppStream 191 k
 perl-CPAN-Meta-Requirements
noarch 2.140-396.el8
Local-AppStream 37 k
 perl-Encode-Locale
noarch 1.05-
10.module+el8.3.0+6498+9eecfe51
Local-AppStream 22 k
 perl-Time-HiRes
x86_64 4:1.9758-2.el8
Local-AppStream 61 k
 python39-pip
noarch 20.2.4-
8.module+el8.9.0+19644+d68f775d
Local-AppStream 1.9 M
 python39-setuptools
noarch 50.3.2-
4.module+el8.9.0+19644+d68f775d
Local-AppStream 871 k
Enabling module streams:
 python39
3.9

Transaction Summary
=====
=====
=====
=====
Install 71 Packages

Total size: 95 M
Installed size: 224 M
Is this ok [y/N]: y
Downloading Packages:
Red Hat Enterprise Linux 9 - BaseOS
45 kB/s | 5.0 kB 00:00
Importing GPG key 0xFD431D51:
 Userid : "Red Hat, Inc. (release key 2) <security@redhat.com>"
 Fingerprint: 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51
 From : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Is this ok [y/N]: y
Key imported successfully

```

```

Importing GPG key 0xD4082792:
 Userid : "Red Hat, Inc. (auxiliary key) <security@redhat.com>"
 Fingerprint: 6A6A A7C9 7C88 90AE C6AE BFE2 F76F 66C3 D408 2792
 From : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Is this ok [y/N]: y
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
 Preparing :
1/1
 Installing : python-srpm-macros-3-45.el8.noarch
1/71
 Installing : perl-version-6:0.99.24-1.el8.x86_64
2/71
 Installing : m4-1.4.18-7.el8.x86_64
3/71
 Running scriptlet: m4-1.4.18-7.el8.x86_64
3/71
 Installing : perl-CPAN-Meta-Requirements-2.140-396.el8.noarch
4/71
 Installing : python-rpm-macros-3-45.el8.noarch
5/71
 Installing : python3-rpm-macros-3-45.el8.noarch
6/71
 Installing : perl-Time-HiRes-4:1.9758-2.el8.x86_64
7/71
 Installing : perl-JSON-PP-1:2.97.001-3.el8.noarch
8/71
 Installing : perl-ExtUtils-ParseXS-1:3.35-2.el8.noarch
9/71
 Installing : zlib-devel-1.2.11-25.el8.x86_64
10/71
 Installing : make-1:4.2.1-11.el8.x86_64
11/71
 Running scriptlet: make-1:4.2.1-11.el8.x86_64
11/71
 Installing : perl-Test-Harness-1:3.42-1.el8.noarch
12/71
 Installing : bison-3.0.4-10.el8.x86_64
13/71
 Running scriptlet: bison-3.0.4-10.el8.x86_64
13/71
 Installing : flex-2.6.1-9.el8.x86_64

```

```
14/71
Running scriptlet: flex-2.6.1-9.el8.x86_64
14/71
Installing : rust-srpm-macros-5-2.el8.noarch
15/71
Installing : redhat-lsb-submod-security-4.1-47.el8.x86_64
16/71
Installing : qt5-srpm-macros-5.15.3-1.el8.noarch
17/71
Installing : python39-setuptools-wheel-50.3.2-
4.module+el8.9.0+19644+d68f775d.noarch
18/71
Installing : python39-pip-wheel-20.2.4-
8.module+el8.9.0+19644+d68f775d.noarch
19/71
Installing : python39-libs-3.9.17-
2.module+el8.9.0+19644+d68f775d.x86_64
20/71
Installing : python39-3.9.17-
2.module+el8.9.0+19644+d68f775d.x86_64
21/71
Running scriptlet: python39-3.9.17-
2.module+el8.9.0+19644+d68f775d.x86_64
21/71
Installing : python39-setuptools-50.3.2-
4.module+el8.9.0+19644+d68f775d.noarch
22/71
Running scriptlet: python39-setuptools-50.3.2-
4.module+el8.9.0+19644+d68f775d.noarch
22/71
Installing : python39-pip-20.2.4-
8.module+el8.9.0+19644+d68f775d.noarch
23/71
Running scriptlet: python39-pip-20.2.4-
8.module+el8.9.0+19644+d68f775d.noarch
23/71
Installing : perl-srpm-macros-1-25.el8.noarch
24/71
Installing : perl-ExtUtils-Manifest-1.70-395.el8.noarch
25/71
Installing : perl-ExtUtils-Command-1:7.34-1.el8.noarch
26/71
Installing : perl-Encode-Locale-1.05-
10.module+el8.3.0+6498+9eecfe51.noarch
27/71
Installing : perl-CPAN-Meta-YAML-0.018-397.el8.noarch
```

```
28/71
 Installing : perl-CPAN-Meta-2.150010-396.el8.noarch
29/71
 Installing : openblas-srpm-macros-2-2.el8.noarch
30/71
 Installing : ocaml-srpm-macros-5-4.el8.noarch
31/71
 Installing : isl-0.16.1-6.el8.x86_64
32/71
 Running scriptlet: isl-0.16.1-6.el8.x86_64
32/71
 Installing : go-srpm-macros-2-17.el8.noarch
33/71
 Installing : ghc-srpm-macros-1.4.2-7.el8.noarch
34/71
 Installing : efi-srpm-macros-3-3.el8.noarch
35/71
 Installing : dwz-0.12-10.el8.x86_64
36/71
 Installing : cpp-8.5.0-20.el8.x86_64
37/71
 Running scriptlet: cpp-8.5.0-20.el8.x86_64
37/71
 Installing : spax-1.5.3-13.el8.x86_64
38/71
 Running scriptlet: spax-1.5.3-13.el8.x86_64
38/71
 Installing : python3-pyparsing-2.1.10-7.el8.noarch
39/71
 Installing : systemtap-sdt-devel-4.9-3.el8.x86_64
40/71
 Running scriptlet: postfix-2:3.5.8-7.el8.x86_64
41/71
 Installing : postfix-2:3.5.8-7.el8.x86_64
41/71
 Running scriptlet: postfix-2:3.5.8-7.el8.x86_64
41/71
 Installing : pcre2-utf32-10.32-3.el8_6.x86_64
42/71
 Installing : pcre2-utf16-10.32-3.el8_6.x86_64
43/71
 Installing : pcre2-devel-10.32-3.el8_6.x86_64
44/71
 Installing : patch-2.7.6-11.el8.x86_64
45/71
 Installing : ncurses-compat-libs-6.1-10.20180224.el8.x86_64
```

```
46/71
 Installing : mailx-12.5-29.el8.x86_64
47/71
 Installing : libzstd-devel-1.4.4-1.el8.x86_64
48/71
 Installing : elfutils-libelf-devel-0.189-3.el8.x86_64
49/71
 Installing : libverto-devel-0.3.2-2.el8.x86_64
50/71
 Installing : libsepol-devel-2.9-3.el8.x86_64
51/71
 Installing : libselinux-devel-2.9-8.el8.x86_64
52/71
 Installing : libkadm5-1.18.2-25.el8_8.x86_64
53/71
 Installing : libcom_err-devel-1.45.6-5.el8.x86_64
54/71
 Installing : keyutils-libs-devel-1.5.10-9.el8.x86_64
55/71
 Installing : krb5-devel-1.18.2-25.el8_8.x86_64
56/71
 Installing : openssl-devel-1:1.1.1k-9.el8_7.x86_64
57/71
 Installing : kernel-headers-4.18.0-513.el8.x86_64
58/71
 Running scriptlet: glibc-headers-2.28-236.el8.x86_64
59/71
 Installing : glibc-headers-2.28-236.el8.x86_64
59/71
 Installing : libxcrypt-devel-4.1.1-6.el8.x86_64
60/71
 Installing : glibc-devel-2.28-236.el8.x86_64
61/71
 Running scriptlet: glibc-devel-2.28-236.el8.x86_64
61/71
 Installing : gcc-8.5.0-20.el8.x86_64
62/71
 Running scriptlet: gcc-8.5.0-20.el8.x86_64
62/71
 Installing : annobin-11.13-2.el8.x86_64
63/71
 Installing : gcc-plugin-annobin-8.5.0-20.el8.x86_64
64/71
 Installing : redhat-rpm-config-131-1.el8.noarch
65/71
 Running scriptlet: redhat-rpm-config-131-1.el8.noarch
```

```

65/71
 Installing : perl-ExtUtils-Install-2.14-4.el8.noarch
66/71
 Installing : perl-devel-4:5.26.3-422.el8.x86_64
67/71
 Installing : perl-ExtUtils-MakeMaker-1:7.34-1.el8.noarch
68/71
 Installing : kernel-devel-4.18.0-513.el8.x86_64
69/71
 Running scriptlet: kernel-devel-4.18.0-513.el8.x86_64
69/71
 Installing : redhat-lsb-core-4.1-47.el8.x86_64
70/71
 Installing : python39-devel-3.9.17-
2.module+el8.9.0+19644+d68f775d.x86_64
71/71
 Running scriptlet: python39-devel-3.9.17-
2.module+el8.9.0+19644+d68f775d.x86_64
71/71
 Verifying : elfutils-libelf-devel-0.189-3.el8.x86_64
1/71
 Verifying : glibc-devel-2.28-236.el8.x86_64
2/71
 Verifying : glibc-headers-2.28-236.el8.x86_64
3/71
 Verifying : kernel-devel-4.18.0-513.el8.x86_64
4/71
 Verifying : kernel-headers-4.18.0-513.el8.x86_64
5/71
 Verifying : keyutils-libs-devel-1.5.10-9.el8.x86_64
6/71
 Verifying : krb5-devel-1.18.2-25.el8_8.x86_64
7/71
 Verifying : libcom_err-devel-1.45.6-5.el8.x86_64
8/71
 Verifying : libkadm5-1.18.2-25.el8_8.x86_64
9/71
 Verifying : libselinux-devel-2.9-8.el8.x86_64
10/71
 Verifying : libsepol-devel-2.9-3.el8.x86_64
11/71
 Verifying : libverto-devel-0.3.2-2.el8.x86_64
12/71
 Verifying : libxcrypt-devel-4.1.1-6.el8.x86_64
13/71
 Verifying : libzstd-devel-1.4.4-1.el8.x86_64

```

```
14/71
 Verifying : m4-1.4.18-7.el8.x86_64
15/71
 Verifying : mailx-12.5-29.el8.x86_64
16/71
 Verifying : make-1:4.2.1-11.el8.x86_64
17/71
 Verifying : ncurses-compat-libs-6.1-10.20180224.el8.x86_64
18/71
 Verifying : openssl-devel-1:1.1.1k-9.el8_7.x86_64
19/71
 Verifying : patch-2.7.6-11.el8.x86_64
20/71
 Verifying : pcre2-devel-10.32-3.el8_6.x86_64
21/71
 Verifying : pcre2-utf16-10.32-3.el8_6.x86_64
22/71
 Verifying : pcre2-utf32-10.32-3.el8_6.x86_64
23/71
 Verifying : postfix-2:3.5.8-7.el8.x86_64
24/71
 Verifying : python3-pyparsing-2.1.10-7.el8.noarch
25/71
 Verifying : spax-1.5.3-13.el8.x86_64
26/71
 Verifying : zlib-devel-1.2.11-25.el8.x86_64
27/71
 Verifying : annobin-11.13-2.el8.x86_64
28/71
 Verifying : bison-3.0.4-10.el8.x86_64
29/71
 Verifying : cpp-8.5.0-20.el8.x86_64
30/71
 Verifying : dwz-0.12-10.el8.x86_64
31/71
 Verifying : efi-srpm-macros-3-3.el8.noarch
32/71
 Verifying : flex-2.6.1-9.el8.x86_64
33/71
 Verifying : gcc-8.5.0-20.el8.x86_64
34/71
 Verifying : gcc-plugin-annobin-8.5.0-20.el8.x86_64
35/71
 Verifying : ghc-srpm-macros-1.4.2-7.el8.noarch
36/71
 Verifying : go-srpm-macros-2-17.el8.noarch
```

```

37/71
 Verifying : isl-0.16.1-6.el8.x86_64
38/71
 Verifying : ocaml-srpm-macros-5-4.el8.noarch
39/71
 Verifying : openblas-srpm-macros-2-2.el8.noarch
40/71
 Verifying : perl-CPAN-Meta-2.150010-396.el8.noarch
41/71
 Verifying : perl-CPAN-Meta-Requirements-2.140-396.el8.noarch
42/71
 Verifying : perl-CPAN-Meta-YAML-0.018-397.el8.noarch
43/71
 Verifying : perl-Encode-Locale-1.05-
10.module+el8.3.0+6498+9eecfe51.noarch
44/71
 Verifying : perl-ExtUtils-Command-1:7.34-1.el8.noarch
45/71
 Verifying : perl-ExtUtils-Install-2.14-4.el8.noarch
46/71
 Verifying : perl-ExtUtils-MakeMaker-1:7.34-1.el8.noarch
47/71
 Verifying : perl-ExtUtils-Manifest-1.70-395.el8.noarch
48/71
 Verifying : perl-ExtUtils-ParseXS-1:3.35-2.el8.noarch
49/71
 Verifying : perl-JSON-PP-1:2.97.001-3.el8.noarch
50/71
 Verifying : perl-Test-Harness-1:3.42-1.el8.noarch
51/71
 Verifying : perl-Time-HiRes-4:1.9758-2.el8.x86_64
52/71
 Verifying : perl-devel-4:5.26.3-422.el8.x86_64
53/71
 Verifying : perl-srpm-macros-1-25.el8.noarch
54/71
 Verifying : perl-version-6:0.99.24-1.el8.x86_64
55/71
 Verifying : python-rpm-macros-3-45.el8.noarch
56/71
 Verifying : python-srpm-macros-3-45.el8.noarch
57/71
 Verifying : python3-rpm-macros-3-45.el8.noarch
58/71
 Verifying : python39-3.9.17-
2.module+el8.9.0+19644+d68f775d.x86_64

```



```
59/71
 Verifying : python39-devel-3.9.17-
2.module+el8.9.0+19644+d68f775d.x86_64
60/71
 Verifying : python39-libs-3.9.17-
2.module+el8.9.0+19644+d68f775d.x86_64
61/71
 Verifying : python39-pip-20.2.4-
8.module+el8.9.0+19644+d68f775d.noarch
62/71
 Verifying : python39-pip-wheel-20.2.4-
8.module+el8.9.0+19644+d68f775d.noarch
63/71
 Verifying : python39-setuptools-50.3.2-
4.module+el8.9.0+19644+d68f775d.noarch
64/71
 Verifying : python39-setuptools-wheel-50.3.2-
4.module+el8.9.0+19644+d68f775d.noarch
65/71
 Verifying : qt5-srpm-macros-5.15.3-1.el8.noarch
66/71
 Verifying : redhat-lsb-core-4.1-47.el8.x86_64
67/71
 Verifying : redhat-lsb-submod-security-4.1-47.el8.x86_64
68/71
 Verifying : redhat-rpm-config-131-1.el8.noarch
69/71
 Verifying : rust-srpm-macros-5-2.el8.noarch
70/71
 Verifying : systemtap-sdt-devel-4.9-3.el8.x86_64
71/71
Installed products updated.

Installed:
 annobin-11.13-2.el8.x86_64
 bison-3.0.4-10.el8.x86_64
 cpp-8.5.0-20.el8.x86_64
 dwz-0.12-10.el8.x86_64
 efi-srpm-macros-3-3.el8.noarch
 elfutils-libelf-devel-0.189-3.el8.x86_64
 flex-2.6.1-9.el8.x86_64
 gcc-8.5.0-20.el8.x86_64
 gcc-plugin-annobin-8.5.0-20.el8.x86_64
 ghc-srpm-macros-1.4.2-7.el8.noarch
 glibc-devel-2.28-236.el8.x86_64
 glibc-headers-2.28-236.el8.x86_64
```

```
go-srpm-macros-2-17.el8.noarch
isl-0.16.1-6.el8.x86_64
kernel-devel-4.18.0-513.el8.x86_64
kernel-headers-4.18.0-513.el8.x86_64
keyutils-libs-devel-1.5.10-9.el8.x86_64
krb5-devel-1.18.2-25.el8_8.x86_64
libcom_err-devel-1.45.6-5.el8.x86_64
libkadm5-1.18.2-25.el8_8.x86_64
libselinux-devel-2.9-8.el8.x86_64
libsepol-devel-2.9-3.el8.x86_64
libverto-devel-0.3.2-2.el8.x86_64
libxcrypt-devel-4.1.1-6.el8.x86_64
libzstd-devel-1.4.4-1.el8.x86_64
m4-1.4.18-7.el8.x86_64
mailx-12.5-29.el8.x86_64
make-1:4.2.1-11.el8.x86_64
ncurses-compat-libs-6.1-10.20180224.el8.x86_64
ocaml-srpm-macros-5-4.el8.noarch
openblas-srpm-macros-2-2.el8.noarch
openssl-devel-1:1.1.1k-9.el8_7.x86_64
patch-2.7.6-11.el8.x86_64
pcre2-devel-10.32-3.el8_6.x86_64
pcre2-utf16-10.32-3.el8_6.x86_64
pcre2-utf32-10.32-3.el8_6.x86_64
perl-CPAN-Meta-2.150010-396.el8.noarch
perl-CPAN-Meta-Requirements-2.140-396.el8.noarch
perl-CPAN-Meta-YAML-0.018-397.el8.noarch
perl-Encode-Locale-1.05-10.module+el8.3.0+6498+9eecfe51.noarch
perl-ExtUtils-Command-1:7.34-1.el8.noarch
perl-ExtUtils-Install-2.14-4.el8.noarch
perl-ExtUtils-MakeMaker-1:7.34-1.el8.noarch
perl-ExtUtils-Manifest-1.70-395.el8.noarch
perl-ExtUtils-ParseXS-1:3.35-2.el8.noarch
perl-JSON-PP-1:2.97.001-3.el8.noarch
perl-Test-Harness-1:3.42-1.el8.noarch
perl-Time-HiRes-4:1.9758-2.el8.x86_64
perl-devel-4:5.26.3-422.el8.x86_64
perl-srpm-macros-1-25.el8.noarch
perl-version-6:0.99.24-1.el8.x86_64
postfix-2:3.5.8-7.el8.x86_64
python-rpm-macros-3-45.el8.noarch
python-srpm-macros-3-45.el8.noarch
python3-pyparsing-2.1.10-7.el8.noarch
python3-rpm-macros-3-45.el8.noarch
python39-3.9.17-2.module+el8.9.0+19644+d68f775d.x86_64
python39-devel-3.9.17-2.module+el8.9.0+19644+d68f775d.x86_64
```

```
python39-libs-3.9.17-2.module+el8.9.0+19644+d68f775d.x86_64
python39-pip-20.2.4-8.module+el8.9.0+19644+d68f775d.noarch
python39-pip-wheel-20.2.4-8.module+el8.9.0+19644+d68f775d.noarch
python39-setuptools-50.3.2-4.module+el8.9.0+19644+d68f775d.noarch
python39-setuptools-wheel-50.3.2-4.module+el8.9.0+19644+d68f775d.noarch
qt5-srpm-macros-5.15.3-1.el8.noarch
redhat-lsb-core-4.1-47.el8.x86_64
redhat-lsb-submod-security-4.1-47.el8.x86_64
redhat-rpm-config-131-1.el8.noarch
rust-srpm-macros-5-2.el8.noarch
spax-1.5.3-13.el8.x86_64
systemtap-sdt-devel-4.9-3.el8.x86_64
zlib-devel-1.2.11-25.el8.x86_64
```

Complete!

OS package installations finished

+ Installing ONTAP Mediator. (Log: /root/ontap\_mediator.MRjxkr/ontap-mediator-1.8.0/ontap-mediator-1.8.0/install\_20240606113556.log)

This step will take several minutes. Use the log file to view progress.

Sudoer config verified

ONTAP Mediator rsyslog and logging rotation enabled

+ Install successful. (Moving log to /opt/netapp/lib/ontap\_mediator/log/install\_20240606113556.log)

+ WARNING: This system supports UEFI

Secure Boot (SB) is currently disabled on this system.

If SB is enabled in the future, SCST will not work unless the following action is taken:

Using the keys in

/opt/netapp/lib/ontap\_mediator/ontap\_mediator/SCST\_mod\_keys follow instructions in

/opt/netapp/lib/ontap\_mediator/ontap\_mediator/SCST\_mod\_keys/README.module-signing

to sign the SCST kernel module. Note that reboot will be needed.

SCST will not start automatically when Secure Boot is enabled and not configured properly.

+ Note: ONTAP Mediator generated a self-signed server certificate for temporary use on

this host. If the DNS name or IP address for the host is changed, the certificate

will no longer be valid. The default certificates should be replaced with secure

trusted certificates signed by a known certificate authority prior to use for production.

For more information, see `/opt/netapp/lib/ontap_mediator/README`

+ Note: ONTAP Mediator uses a kernel module compiled specifically for the current

OS. Using 'yum update' to upgrade the kernel might cause service interruption.

For more information, see `/opt/netapp/lib/ontap_mediator/README`

## Vérifiez l'installation

Une fois le médiateur ONTAP installé, vous devez vérifier que les services du médiateur ONTAP sont en cours d'exécution.

### Étapes

1. Afficher l'état des services du médiateur ONTAP :

a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
└─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
Main PID: 286662 (iscsi-scstd)
Tasks: 1 (limit: 49473)
Memory: 1.2M
CGroup: /system.slice/mediator-scst.service
└─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

## 2. Vérifiez les ports utilisés par le service ONTAP Mediator :

netstat

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

tcp 0 0 0.0.0.0:31784 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:3260 0.0.0.0:* LISTEN
tcp6 0 0 :::3260 :::* LISTEN
```

## Configuration post-installation

Une fois le service ONTAP Mediator installé et en cours d'exécution, des tâches de configuration supplémentaires doivent être effectuées dans le système de stockage ONTAP pour utiliser les fonctions du Mediator :

- Pour utiliser le service médiateur ONTAP dans une configuration IP MetroCluster, reportez-vous à la section ["Configuration du service médiateur ONTAP à partir d'une configuration IP MetroCluster"](#).
- Pour utiliser la synchronisation active SnapMirror, reportez-vous à la section ["Installez le service médiateur ONTAP et confirmez la configuration du cluster ONTAP"](#).

## Configurer les stratégies de sécurité du médiateur ONTAP

Le serveur ONTAP Mediator prend en charge plusieurs paramètres de sécurité configurables. Les valeurs par défaut pour tous les paramètres sont fournies dans un fichier `basse_space_Threshold_mib: 10read-only` :

`/opt/netapp/lib/ontap_mediator/server_config/ontap_mediator.user_config.yaml`

Toutes les valeurs placées dans le `ontap_mediator.user_config.yaml` Remplace les valeurs par défaut

et sera conservé dans toutes les mises à niveau du Mediator ONTAP.

Après modification `ontap_mediator.user_config.yaml`, Redémarrez le service ONTAP Mediator :

```
systemctl restart ontap_mediator
```

### Modifier les attributs du médiateur ONTAP

Les attributs suivants peuvent être configurés :



Autres valeurs par défaut dans `ontap_mediator.config.yaml` ne doit pas être modifié.

- **Paramètres utilisés pour installer des certificats SSL tiers en remplacement des certificats auto-signés par défaut**

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
tor_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
tor_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
cert_valid_days: '1095' # Used to set the expiration
on client certs to 3 years
x509_passin_pwd: 'pass:ontap' # passphrase for the signed
client cert
```

- **Paramètres qui fournissent des protections contre les attaques de devinettes de mots de passe par force brute**

Pour activer la fonction, définissez une valeur pour `window_seconds` et le `retry_limit`

Exemples :

- Fournissez une fenêtre de 5 minutes pour les hypothèses, puis réinitialisez le compte à zéro échec :

```
authentication_lock_window_seconds: 300
```

- Verrouiller le compte si cinq défaillances se produisent dans la période de la fenêtre :

```
authentication_retry_limit: 5
```

- Réduisez l'impact des attaques par tâtonnements de mots de passe par force brute en définissant un délai qui se produit avant le rejet de chaque tentative, ce qui ralentit les attaques.

```
authentication_failure_delay_seconds: 5
```

```
authentication_failure_delay_seconds: 0 # seconds (float) to delay
failed auth attempts prior to response, 0 = no delay
authentication_lock_window_seconds: null # seconds (int) since the
oldest failure before resetting the retry counter, null = no window
authentication_retry_limit: null # number of retries to
allow before locking API access, null = unlimited
```

- **Champs qui contrôlent les règles de complexité du mot de passe du compte utilisateur de l'API ONTAP Mediator**

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0 # min. uppercase characters
password_lowercase_chars: 1 # min. lowercase character
password_special_chars: 1 # min. non-letter, non-digit
password_nonletter_chars: 2 # min. non-letter characters (digits,
specials, anything)
```

- **Paramètre qui contrôle l'espace libre requis sur le /opt/netapp/lib/ontap\_mediator disque.**

Si l'espace est inférieur au seuil défini, le service émet un avertissement.

```
low_space_threshold_mib: 10
```

- **Paramètre qui contrôle RESERVE\_LOG\_SPACE.**

L'installation par défaut du serveur ONTAP Mediator crée un espace disque distinct pour les journaux. Le programme d'installation crée un nouveau fichier de taille fixe avec un total de 700 Mo d'espace disque à utiliser explicitement pour la journalisation Mediator.

Pour désactiver cette fonction et utiliser l'espace disque par défaut, effectuez les opérations suivantes :

- a. Dans le fichier suivant, remplacez la valeur de RESERVE\_LOG\_SPACE de "1" à "0" :

```
/opt/netapp/lib/ontap_mediator/tools/mediator_env
```

- b. Redémarrez le Mediator :

- i. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep`

```
"RESERVE_LOG_SPACE"
```

```
RESERVE_LOG_SPACE=0
```

ii. `systemctl restart ontap_mediator`

Pour réactiver la fonction, changez la valeur de « 0 » à « 1 » et redémarrez le Mediator.



Le basculement entre les espaces disque ne purge pas les journaux existants. Tous les journaux précédents sont sauvegardés puis déplacés vers l'espace disque actuel après avoir basculé et redémarré le Mediator.

## Gérez le service ONTAP médiateur

Gérer le service ONTAP Mediator, y compris la modification des informations d'identification de l'utilisateur, l'arrêt et la réactivation du service, la vérification de son intégrité et l'installation ou la désinstallation de SCST pour la maintenance de l'hôte. Vous pouvez également gérer des certificats, tels que la régénération de certificats auto-signés, leur remplacement par des certificats tiers approuvés et le dépannage des problèmes liés aux certificats.

### Modifiez le nom d'utilisateur

Vous pouvez modifier le nom d'utilisateur en procédant comme suit.

#### Description de la tâche

Effectuez cette tâche sur l'hôte Linux sur lequel le service ONTAP Mediator est installé.

Si vous ne pouvez pas atteindre cette commande, il vous faudra peut-être exécuter la commande en utilisant le chemin d'accès complet, comme illustré dans l'exemple suivant :

```
/usr/local/bin/mediator_username
```

#### Étapes

Modifiez le nom d'utilisateur en choisissant l'une des options suivantes :

- **Option (a)** : exécutez la commande `mediator_change_user` et répondez aux invites comme indiqué dans l'exemple suivant :

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
 Mediator API User Name: mediatoradmin
 Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```



- **Option (b)** : exécutez la commande suivante :

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME=mediatoradmin
mediator_change_user
The account username has been modified successfully.
[root@mediator-host ~]#
```

## Changer le mot de passe

Vous pouvez modifier le mot de passe à l'aide de la procédure suivante.

### Description de la tâche

Effectuez cette tâche sur l'hôte Linux sur lequel le service ONTAP Mediator est installé.

Si vous ne pouvez pas atteindre cette commande, il vous faudra peut-être exécuter la commande en utilisant le chemin d'accès complet, comme illustré dans l'exemple suivant :

```
/usr/local/bin/mediator_change_password
```

### Étapes

Modifiez le mot de passe en choisissant l'une des options suivantes :

- **Option (a)** : exécutez le `mediator_change_password` commande et répond aux invites, comme illustré dans l'exemple suivant :

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
Mediator API User Name: mediatoradmin
Old Password:
New Password:
Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- **Option (b)** : exécutez la commande suivante :

```
MEDIATOR_USERNAME=mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

L'exemple montre que le mot de passe passe de "mediator1" à "mediator2".

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
The password has been updated successfully.
[root@mediator-host ~]#
```

## Arrêtez le service ONTAP Mediator

Pour arrêter le service du médiateur ONTAP, effectuez les opérations suivantes :

### Étapes

1. Arrêter le médiateur ONTAP :

```
systemctl stop ontap_mediator
```

2. Arrêt SCST :

```
systemctl stop mediator-scst
```

3. Désactivez le médiateur ONTAP et le SCST :

```
systemctl disable ontap_mediator mediator-scst
```

## Réactiver le service ONTAP Mediator

Pour réactiver le service ONTAP Mediator, effectuez les opérations suivantes :

### Étapes

1. Activer le médiateur ONTAP et le SCST :

```
systemctl enable ontap_mediator mediator-scst
```

2. Démarrer SCST :

```
systemctl start mediator-scst
```

3. Démarrer le médiateur ONTAP :

```
systemctl start ontap_mediator
```

## Vérifiez que le médiateur ONTAP fonctionne correctement

Une fois le médiateur ONTAP installé, vous devez vérifier que les services du médiateur ONTAP sont en cours d'exécution.

### Étapes

1. Afficher l'état des services du médiateur ONTAP :

- a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
└─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst

Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
Main PID: 286662 (iscsi-scstd)
Tasks: 1 (limit: 49473)
Memory: 1.2M
CGroup: /system.slice/mediator-scst.service
└─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Vérifiez les ports utilisés par le service ONTAP Mediator :

`netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'
```

```
tcp 0 0 0.0.0.0:31784 0.0.0.0:* LISTEN
```

```
tcp 0 0 0.0.0.0:3260 0.0.0.0:* LISTEN
```

```
tcp6 0 0 :::3260 :::* LISTEN
```

## Désinstallez manuellement SCST pour effectuer la maintenance de l'hôte

Pour désinstaller SCST, vous avez besoin du paquet tar SCST utilisé pour la version installée de ONTAP Mediator.

### Étapes

1. Téléchargez l'ensemble SCST approprié (comme indiqué dans le tableau suivant) et décompressez-le.

| Pour cette version ... | Utiliser ce paquet tar... |
|------------------------|---------------------------|
| Médiateur ONTAP 1.8    | scst-3.8.0.tar.bz2        |
| Médiateur ONTAP 1.7    | scst-3.7.0.tar.bz2        |
| Médiateur ONTAP 1.6    | scst-3.7.0.tar.bz2        |
| Médiateur ONTAP 1.5    | scst-3.6.0.tar.bz2        |
| Médiateur ONTAP 1.4    | scst-3.6.0.tar.bz2        |
| Médiateur ONTAP 1.3    | scst-3.5.0.tar.bz2        |
| Médiateur ONTAP 1.1    | scst-3.4.0.tar.bz2        |
| Médiateur ONTAP 1.0    | scst-3.3.0.tar.bz2        |

2. Exécutez les commandes suivantes dans le répertoire « scst » :

- a. `systemctl stop mediator-scst`
- b. `make scstadm_uninstall`
- c. `make iscsi_uninstall`
- d. `make usr_uninstall`
- e. `make scst_uninstall`
- f. `depmod`

## Installez manuellement SCST pour effectuer la maintenance de l'hôte

Pour installer manuellement le SCST, vous devez disposer du paquet tar SCST utilisé pour la version installée du Mediator ONTAP (voir le [tableau ci-dessus](#)).

1. Exécutez les commandes suivantes dans le répertoire « scst » :

- a. `make 2release`
- b. `make scst_install`
- c. `make usr_install`
- d. `make iscsi_install`
- e. `make scstadm_install`
- f. `depmod`
- g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
- h. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
- i. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`

2. Si vous le souhaitez, si le démarrage sécurisé est activé, effectuez les opérations suivantes avant de redémarrer :

a. Déterminez chaque nom de fichier pour les modules "scst\_vdisk", "scst" et "iscsi\_scst" :

```
[root@localhost ~]# modinfo -n scst_vdisk
[root@localhost ~]# modinfo -n scst
[root@localhost ~]# modinfo -n iscsi_scst
```

b. Déterminez la version du noyau :

```
[root@localhost ~]# uname -r
```

c. Signez chaque fichier avec le noyau :

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-
file \sha256 \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.priv \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.der \
module-filename
```

d. Installez la clé correcte avec le micrologiciel UEFI.

Les instructions d'installation de la clé UEFI se trouvent à l'adresse suivante :

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing
```

La clé UEFI générée se trouve à l'emplacement suivant :

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.der
```

### 3. Redémarrer :

```
reboot
```

## Désinstallez le service ONTAP Mediator

Si nécessaire, vous pouvez supprimer le service ONTAP Mediator.

### Avant de commencer

Le Mediator ONTAP doit être déconnecté de ONTAP avant de supprimer le service ONTAP Mediator.

### Description de la tâche

Vous devez effectuer cette tâche sur l'hôte Linux sur lequel le service ONTAP Mediator est installé.

Si vous ne pouvez pas atteindre cette commande, il vous faudra peut-être exécuter la commande en utilisant le chemin d'accès complet, comme illustré dans l'exemple suivant :

```
/usr/local/bin/uninstall_ontap_mediator
```

### Étape

#### 1. Désinstallez le service ONTAP Mediator :

```
uninstall_ontap_mediator
```

```
[root@mediator-host ~]# uninstall_ontap_mediator

ONTAP Mediator: Self Extracting Uninstaller

+ Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
+ Remove successful.
[root@mediator-host ~]#
```

## Régénérez un certificat auto-signé temporaire

À partir de ONTAP Mediator 1.7, vous pouvez régénérer un certificat auto-signé temporaire en suivant la procédure suivante.



Cette procédure n'est prise en charge que sur les systèmes exécutant ONTAP Mediator 1.7 ou version ultérieure.

## Description de la tâche

- Vous effectuez cette tâche sur l'hôte Linux sur lequel le service ONTAP Mediator est installé.
- Vous pouvez effectuer cette tâche uniquement si les certificats auto-signés générés sont devenus obsolètes en raison de modifications apportées au nom d'hôte ou à l'adresse IP de l'hôte après l'installation du médiateur ONTAP.
- Une fois que le certificat auto-signé temporaire a été remplacé par un certificat tiers approuvé, vous devez *ne pas* utiliser cette tâche pour régénérer un certificat. L'absence d'un certificat auto-signé entraînera l'échec de cette procédure.

## Étape

Pour régénérer un nouveau certificat auto-signé temporaire pour l'hôte actuel, effectuez l'étape suivante :

1. Redémarrez le service ONTAP Mediator :

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
.....
.....++++
.....++++
e is 65537 (0x010001)
Generating a RSA private key
.....++++
.....
.....+++
+
writing new private key to 'ontap_mediator_server.key'

Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

## Remplacez les certificats auto-signés par des certificats tiers approuvés

S'il est pris en charge, vous pouvez remplacer les certificats auto-signés par des certificats tiers approuvés.

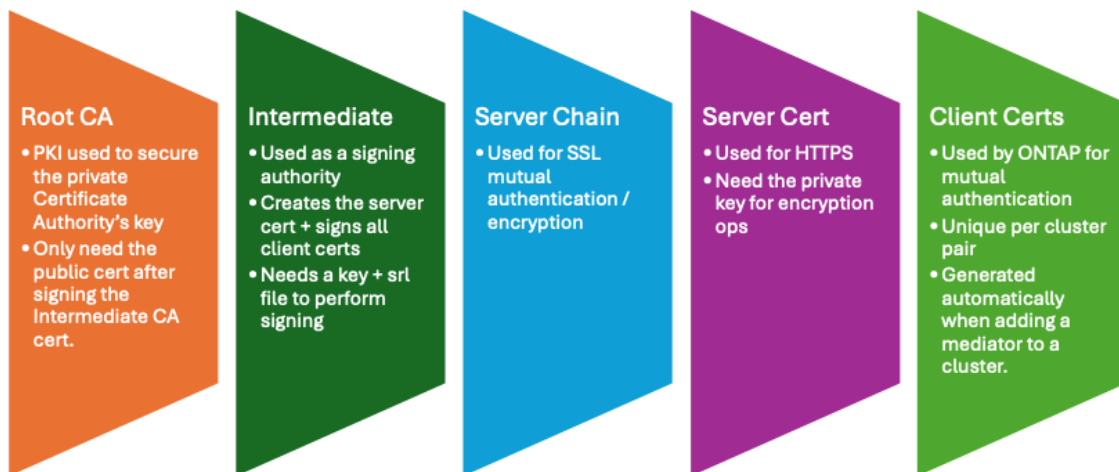


- Les certificats tiers ne sont pris en charge qu'avec le médiateur ONTAP sur certaines versions de ONTAP. Voir "[Bugs NetApp ID de bug en ligne CONTAP-243278](#)".
- Les certificats tiers ne sont pris en charge que sur les systèmes exécutant ONTAP Mediator 1.7 ou version ultérieure.

### Description de la tâche

- Vous effectuez cette tâche sur l'hôte Linux sur lequel le service ONTAP Mediator est installé.
- Vous pouvez effectuer cette tâche si les certificats auto-signés générés doivent être remplacés par des certificats obtenus auprès d'une autorité de certification subordonnée de confiance. Pour ce faire, vous devez avoir accès à une infrastructure à clé publique (PKI) fiable.
- L'image suivante montre les objectifs de chaque certificat de Mediator ONTAP.

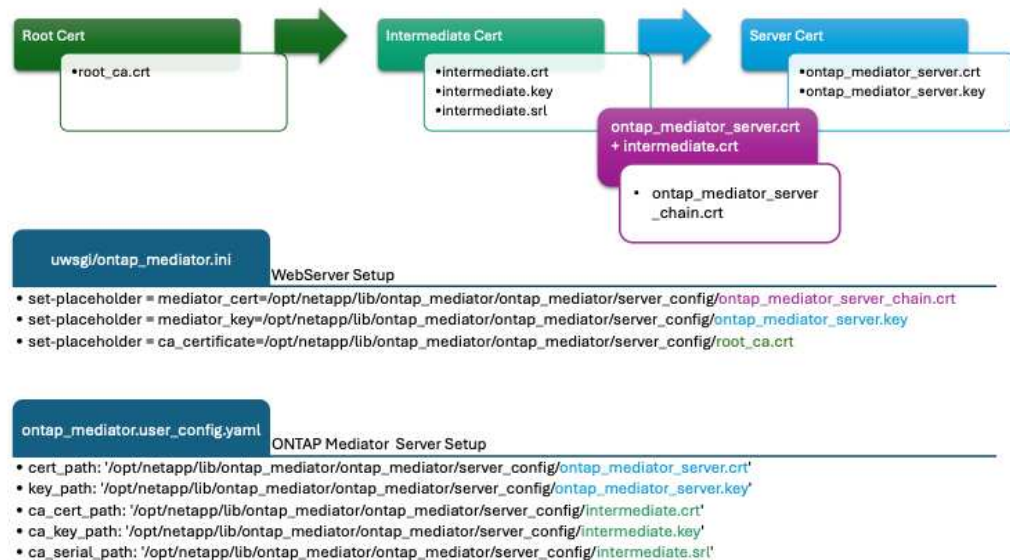
## ONTAP Mediator Certificate Purposes



- L'image suivante montre la configuration du serveur Web et de la configuration du serveur ONTAP Mediator.



# ONTAP Mediator Certificates



## Étape 1 : obtenir un certificat d'un tiers émettant un certificat d'autorité de certification

Vous pouvez obtenir un certificat auprès d'une autorité PKI en suivant la procédure suivante.

L'exemple suivant illustre le remplacement des acteurs de certificat auto-signés, à savoir `ca.key`, `ca.csr`, `ca.srl`, et `ca.crt` situé à `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/` avec les acteurs de certificat tiers.



L'exemple illustre les critères nécessaires pour les certificats requis pour le service ONTAP Mediator. Vous pouvez obtenir les certificats auprès d'une autorité PKI d'une manière qui peut être différente de cette procédure. Ajustez la procédure en fonction des besoins de votre entreprise.

## Étapes

1. Créez une clé privée `ca.key` et un fichier de configuration `openssl_ca.cnf` Qui sera consommé par l'autorité PKI pour générer un certificat.

- a. Générez la clé privée `ca.key`:

### Exemple

```
openssl genrsa -aes256 -out ca.key 4096
```

- a. Le fichier de configuration `openssl_ca.cnf` (situé à `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) définit les propriétés que le certificat généré doit avoir.
2. Utilisez la clé privée et le fichier de configuration pour créer une demande de signature de certificat `ca.csr`:

### Exemple:

```
openssl req -key <private_key_name>.key -new -out <certificate_csr_name>.csr
-config <config_file_name>.cnf
```

```
[root@scs000216655 server_config]# openssl req -key ca.key -new -config
openssl_ca.cnf -out ca.csr
Enter pass phrase for ca.key:
[root@scs000216655 server_config]# cat ca.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIE6TCCAtECAQAwgaMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlh
...
erARKhY9z0e8BHPl3g==
-----END CERTIFICATE REQUEST-----
```

3. Envoyez la demande de signature de certificat `ca.csr` À une autorité PKI pour leur signature.

L'autorité PKI vérifie la demande et signe le , générant le `.csr`certificat `ca.crt`. De plus, vous devez obtenir le `root_ca.crt` certificat qui a signé le `ca.crt` certificat auprès de l'autorité PKI.



Pour les clusters SnapMirror Business Continuity (SM-BC), vous devez ajouter les `ca.crt` certificats et `root_ca.crt` à un cluster ONTAP. Voir ["Configurer le médiateur ONTAP et les clusters pour la synchronisation active SnapMirror"](#).

## Étape 2 : générez un certificat de serveur en signant avec une certification d'autorité de certification tierce

Un certificat de serveur doit être signé par la clé privée `ca.key` et le certificat tiers `ca.crt`. De plus, le fichier de configuration

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf`  
Contient certains attributs qui spécifient les propriétés requises pour les certificats de serveur émis par OpenSSL.

Les commandes suivantes peuvent générer un certificat de serveur.

### Étapes

1. Pour générer une requête de signature de certificat de serveur (CSR), exécutez la commande suivante à partir du `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` dossier :

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
ontap_mediator_server.csr
```

2. pour générer un certificat de serveur à partir de la RSC, exécutez la commande suivante à partir du `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` dossier :



Les `ca.crt` fichiers et `ca.key` ont été obtenus d'une autorité de l'ICP. Si vous utilisez un nom de certificat différent, par exemple, `intermediate.crt` et `intermediate.key`, remplacez `ca.crt` et `ca.key` par `intermediate.crt` et `intermediate.key` respectivement.

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA ca.crt -CAkey
ca.key -CAcreateserial -sha512 -days 1095 -req -in ontap_mediator_server.csr
-out ontap_mediator_server.crt
```

- L' -CAcreateserial option est utilisée pour générer les ca.srl fichiers ou intermediate.srl , en fonction du nom de certificat que vous utilisez.

### Étape 3 : remplacez le nouveau certificat d'autorité de certification tiers et le certificat de serveur dans la configuration du médiateur ONTAP

La configuration du certificat est fournie au service Mediator ONTAP dans le fichier de configuration situé à l'adresse

/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.config.yaml. Le fichier comprend les attributs suivants :

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediato
r_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediato
r_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- cert\_path et key\_path sont des variables de certificat de serveur.
- ca\_cert\_path, ca\_key\_path, et ca\_serial\_path Sont des variables de certificat CA.

### Étapes

1. Remplacez tous les ca.\* fichiers par les certificats tiers.
2. Créez une chaîne de certificats à partir des ca.crt certificats et ontap\_mediator\_server.crt :

```
cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
```

3. Mettre à jour le /opt/netapp/lib/ontap\_mediator/uwsgi/ontap\_mediator.ini fichier.

Mettre à jour les valeurs de mediator\_cert,, mediator\_key`et `ca\_certificate:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_ser
ver_chain.crt
```

```
set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_ser
ver.key
```

```
set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- La mediator\_cert valeur est le chemin du ontap\_mediator\_server\_chain.crt fichier.
- Le mediator\_key value est le chemin d'accès de la clé dans le ontap\_mediator\_server.crt fichier, qui est ontap\_mediator\_server.key.
- La ca\_certificate valeur est le chemin du root\_ca.crt fichier.

4. Vérifiez que les attributs suivants des certificats nouvellement générés sont définis correctement :

- Propriétaire du groupe Linux : netapp:netapp
- Autorisations Linux : 600

5. Redémarrez le médiateur ONTAP :

```
systemctl restart ontap_mediator
```

#### Étape 4 : si vous le souhaitez, utilisez un chemin ou un nom différent pour vos certificats tiers

Vous pouvez utiliser des certificats tiers portant un nom différent de ca.\* ou stockez les certificats tiers dans un emplacement différent.

#### Étapes

1. Configurez le

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml
```

 fichier pour remplacer les valeurs de variable par défaut dans le ontap\_mediator.config.yaml fichier.

Si vous avez obtenu intermediate.crt d'une autorité PKI et que vous stockez sa clé privée intermediate.key à l'emplacement

/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config, le ontap\_mediator.user\_config.yaml fichier devrait ressembler à l'exemple suivant :



Si vous avez utilisé intermediate.crt pour signer le ontap\_mediator\_server.crt certificat, le intermediate.srl fichier est généré. Voir [Étape 2 : générez un certificat de serveur en signant avec une certification d'autorité de certification tierce](#) pour plus d'informations.

```
[root@scs000216655 server_config]# cat ontap_mediator.user_config.yaml

This config file can be used to override the default settings in
ontap_mediator.config.yaml
To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
set the property to the desired value. e.g.,
#
The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
To override this value with 6 mailboxes per target, add the following
key/value pair
below this comment:
#
'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediat
e.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediat
e.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediat
e.srl'
```

- a. Si vous utilisez une structure de certificat où le `root_ca.crt` certificat fournit un certificat qui signe le `certificat intermediate.crt` `ontap_mediator_server.crt`, créez une chaîne de certificats à partir du `intermediate.crt` et des `ontap_mediator_server.crt` certificats :



**Vous devez avoir obtenu les `intermediate.crt` certificats et `ontap_mediator_server.crt` d'une autorité PKI plus tôt dans la procédure.**

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

- b. Mettre à jour le `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` fichier.

Mettre à jour les valeurs de `mediator_cert,,mediator_key`et `ca_certificate:`

```

set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_s
erver_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_s
erver.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt

```

- La `mediator_cert` valeur est le chemin du `ontap_mediator_server_chain.crt` fichier.
- La `mediator_key` valeur est le chemin d'accès de la clé dans le `ontap_mediator_server.crt` fichier, qui est `ontap_mediator_server.key`.
- La `ca_certificate` valeur est le chemin du `root_ca.crt` fichier.



Pour les clusters SnapMirror Business Continuity (SM-BC), vous devez ajouter les `intermediate.crt` certificats et `root_ca.crt` à un cluster ONTAP. Voir ["Configurer le médiateur ONTAP et les clusters pour la synchronisation active SnapMirror"](#).

c. Vérifiez que les attributs suivants des certificats nouvellement générés sont définis correctement :

- Propriétaire du groupe Linux : `netapp:netapp`
- Autorisations Linux : `600`

2. Redémarrez le médiateur ONTAP lorsque les certificats sont mis à jour dans le fichier de configuration :

```
systemctl restart ontap_mediator
```

## Résoudre les problèmes liés aux certificats

Vous pouvez vérifier certaines propriétés des certificats.

### Vérifiez l'expiration du certificat

Utiliser la commande suivante pour identifier la plage de validité du certificat :

```

[root@scs000216982 server_config]# openssl x509 -in ca.crt -text -noout
Certificate:
 Data:
 ...
 Validity
 Not Before: Feb 22 19:57:25 2024 GMT
 Not After : Feb 15 19:57:25 2029 GMT

```

### Vérifier les extensions X509v3 dans la certification CA

Utilisez la commande suivante pour vérifier les extensions X509v3 dans la certification CA.

Les propriétés définies dans **v3\_ca** dans `openssl_ca.cnf` s'affichent sous la forme X509v3 extensions dans `ca.crt`.

```
[root@scs000216982 server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@scs000216982 server_config]# cat openssl_ca.cnf
...
[v3_ca]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@scs000216982 server_config]# openssl x509 -in ca.crt -text -noout
Certificate:
 Data:
 ...
 X509v3 extensions:
 X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
 X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

 X509v3 Basic Constraints: critical
 CA:TRUE
 X509v3 Key Usage: critical
 Digital Signature, Certificate Sign, CRL Sign
```

**Vérifiez les extensions X509v3 dans le certificat de serveur et les noms Alt d'objet**

Le `v3_req` propriétés définies dans `openssl_server.cnf` le fichier de configuration s'affiche sous la forme X509v3 extensions dans le certificat.

Dans l'exemple suivant, vous pouvez obtenir les variables dans `alt_names` en exécutant les commandes `hostname -A` et `hostname -I` Sur la machine virtuelle Linux sur laquelle le Mediator ONTAP est installé.

Vérifiez auprès de votre administrateur réseau les valeurs correctes des variables.

```

[root@scs000216982 server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@scs000216982 server_config]# cat openssl_server.cnf
...
[v3_req]
basicConstraints = CA:false
extendedKeyUsage = serverAuth
keyUsage = keyEncipherment, dataEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@scs000216982 server_config]# openssl x509 -in ca.crt -text -noout
Certificate:
 Data:
 ...

 X509v3 extensions:
 X509v3 Basic Constraints:
 CA:FALSE
 X509v3 Extended Key Usage:
 TLS Web Server Authentication
 X509v3 Key Usage:
 Key Encipherment, Data Encipherment
 X509v3 Subject Alternative Name:
 DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd

```

### Vérifiez qu'une clé privée correspond à un certificat

Vous pouvez vérifier si une clé privée particulière correspond à un certificat.

Utilisez les commandes OpenSSL suivantes sur la clé et le certificat respectivement :



```
[root@scs000216982 server_config]# openssl rsa -noout -modulus -in
intermediate.key | openssl md5
Enter pass phrase for intermediate.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@scs000216982 server_config]# openssl x509 -noout -modulus -in
intermediate.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

Si le `-modulus` attribut pour les deux correspondances, il indique que la clé privée et la paire de certificats sont compatibles et peuvent fonctionner l'une avec l'autre.

#### **Vérifiez qu'un certificat de serveur est créé à partir d'un certificat d'autorité de certification particulier**

Vous pouvez utiliser la commande suivante pour vérifier que le certificat du serveur est créé à partir d'un certificat d'autorité de certification spécifique.

```
[root@scs000216982 server_config]# openssl verify -CAfile ca.crt
ontap_mediator_server.crt
ontap_mediator_server.crt: OK
```

Si la validation OCSP (Online Certificate Status Protocol) est utilisée, utilisez la commande ["openssl-verify"](#).

## **Maintenir l'hôte du système d'exploitation pour le médiateur ONTAP**

Pour des performances optimales, vous devez maintenir régulièrement le système d'exploitation hôte pour ONTAP Mediator.

### **Redémarrez l'hôte**

Redémarrez l'hôte lorsque les clusters fonctionnent correctement. Bien que le médiateur ONTAP soit hors ligne, les clusters risquent de ne pas pouvoir réagir correctement aux pannes. Une fenêtre de service est recommandée si un redémarrage est nécessaire.

Le médiateur ONTAP reprend automatiquement au cours du redémarrage et entre de nouveau les relations qui avaient été précédemment configurées avec les clusters ONTAP.

### **Mises à jour du package hôte**

N'importe quelle bibliothèque ou paquets yum (à l'exception du noyau) peut être mis à jour en toute sécurité, mais peut nécessiter un redémarrage pour prendre effet. Une fenêtre de service est recommandée si un redémarrage est nécessaire.

Si vous installez le `yum-utils` utiliser le `needs-restarting` commande permettant de détecter si des modifications de pack nécessitent un redémarrage.

Vous devez redémarrer si l'une des dépendances du médiateur ONTAP est mise à jour car elles ne prendront pas effet immédiatement sur les processus en cours d'exécution.

## Mises à niveau mineures du noyau du système d'exploitation hôte

SCST doit être compilé pour le noyau utilisé. Pour mettre à jour le système d'exploitation, une fenêtre de maintenance est requise.

### Étapes

Procédez comme suit pour mettre à niveau le noyau du système d'exploitation hôte.

1. Arrêtez le médiateur ONTAP
2. Désinstallez le progiciel SCST. (SCST ne fournit pas de mécanisme de mise à niveau.)
3. Mettez à niveau le système d'exploitation, puis redémarrez.
4. Réinstallez le progiciel SCST.
5. Réactiver les services du médiateur ONTAP.

## L'hôte modifie le nom d'hôte ou l'adresse IP

### Description de la tâche

- Vous effectuez cette tâche sur l'hôte Linux sur lequel le service ONTAP Mediator est installé.
- Vous pouvez effectuer cette tâche uniquement si les certificats auto-signés générés sont devenus obsolètes en raison de modifications apportées au nom d'hôte ou à l'adresse IP de l'hôte après l'installation du médiateur ONTAP.
- Une fois que le certificat auto-signé temporaire a été remplacé par un certificat tiers approuvé, vous devez *ne pas* utiliser cette tâche pour régénérer un certificat. L'absence d'un certificat auto-signé entraînera l'échec de cette procédure.

### Étape

Pour régénérer un nouveau certificat auto-signé temporaire pour l'hôte actuel, effectuez l'étape suivante :

1. Redémarrez le médiateur ONTAP :

```
./make_self_signed_certs.sh overwrite
```

```

[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
.....
.....++++
.....++++
e is 65537 (0x010001)
Generating a RSA private key
.....++++
.....
.....+++
+
writing new private key to 'ontap_mediator_server.key'

Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator

```

## Gérez des sites MetroCluster avec System Manager

### Présentation de la gestion de site MetroCluster avec System Manager

Depuis ONTAP 9.8, System Manager peut être utilisé comme interface simplifiée pour gérer une configuration d'une configuration MetroCluster.

Une configuration MetroCluster permet aux deux clusters de mettre en miroir les données les uns aux autres. Ainsi, si un cluster tombe en panne, les données ne sont pas perdues.

En général, une entreprise configure les clusters dans deux emplacements géographiques distincts. Un administrateur situé sur chaque emplacement configure un cluster et le configure. Ensuite, l'un des administrateurs peut configurer le peering entre les clusters afin que ceux-ci puissent partager les données.

L'entreprise peut également installer un médiateur ONTAP dans un troisième emplacement. Le service ONTAP Mediator surveille l'état de chaque cluster. Lorsque l'un des clusters détecte qu'il ne peut pas communiquer avec le cluster partenaire, il demande au moniteur de déterminer si l'erreur est un problème avec le système

de cluster ou avec la connexion réseau.

Si le problème vient de la connexion réseau, l'administrateur système effectue des méthodes de dépannage pour corriger l'erreur et se reconnecter. Si le cluster partenaire est défaillant, l'autre cluster démarre un processus de basculement pour contrôler les E/S de données pour les deux clusters.

Vous pouvez également effectuer un basculement pour arrêter l'un des systèmes du cluster dans le cadre d'une maintenance planifiée. Le cluster partenaire gère toutes les opérations d'E/S des données pour les deux clusters jusqu'à ce que vous ayez mis en place le cluster sur lequel vous avez effectué les opérations de maintenance et de rétablissement.

Vous pouvez gérer les opérations suivantes :

- ["Configurer un site IP MetroCluster"](#)
- ["Configuration du peering de MetroCluster IP"](#)
- ["Configurez un site MetroCluster IP"](#)
- ["Réalisez le basculement et le rétablissement IP MetroCluster"](#)
- ["Résolution des problèmes liés aux configurations IP MetroCluster"](#)
- ["Mettre à niveau ONTAP sur des clusters MetroCluster"](#)

## Configurer un site IP MetroCluster

Depuis ONTAP 9.8, vous pouvez utiliser System Manager pour configurer une configuration IP sur un site MetroCluster.

Un site MetroCluster se compose de deux clusters. En règle générale, les clusters se trouvent dans des emplacements géographiques différents.

### Avant de commencer

- Votre système doit déjà être installé et câblé conformément au ["Instructions d'installation et de configuration"](#) fourni avec le système.
- Les interfaces réseau de clusters doivent être configurées sur chaque nœud de chaque cluster pour des communications intra-cluster.

### Attribuez une adresse IP de gestion des nœuds

#### Système Windows

Vous devez connecter votre ordinateur Windows au même sous-réseau que les contrôleurs. L'adresse IP de gestion des nœuds sera automatiquement attribuée à votre système.

#### Étapes

1. À partir du système Windows, ouvrez le lecteur **réseau** pour découvrir les nœuds.
2. Double-cliquez sur le nœud pour lancer l'assistant de configuration du cluster.

#### Autres systèmes

Vous devez configurer l'adresse IP node-management pour l'un des nœuds du cluster. Vous pouvez utiliser cette adresse IP node-management pour lancer l'assistant de configuration des clusters.

Voir ["Création du cluster sur le premier nœud"](#) Pour plus d'informations sur l'attribution d'une adresse IP de

gestion des nœuds.

## Initialiser et configurer le cluster

Vous initialisez le cluster en définissant un mot de passe administratif pour le cluster et en configurant les réseaux de gestion du cluster et de gestion des nœuds. Vous pouvez également configurer des services tels qu'un serveur DNS pour résoudre les noms d'hôtes et un serveur NTP pour synchroniser l'heure.

### Étapes

1. Dans un navigateur Web, saisissez l'adresse IP de gestion des nœuds que vous avez configurée :  
"<https://node-management-IP>"

System Manager détecte automatiquement les nœuds restants dans le cluster.

2. Dans la fenêtre **Initialize Storage System**, effectuez les opérations suivantes :
  - a. Saisissez les données de configuration du réseau de gestion du cluster.
  - b. Entrez les adresses IP de gestion des nœuds pour tous les nœuds.
  - c. Indiquez les détails des serveurs de noms de domaine (DNS).
  - d. Dans la section **autre**, cochez la case **utiliser le service de temps (NTP)** pour ajouter les serveurs de temps.

Lorsque vous cliquez sur **Submit**, attendez que le cluster soit créé et configuré. Ensuite, un processus de validation a lieu.

### Et la suite ?

Une fois les deux clusters configurés, initialisés et configurés, effectuez la procédure suivante :

- "[Configuration du peering de MetroCluster IP](#)"

## Configurez ONTAP sur une nouvelle vidéo de cluster



## Configuration du peering de MetroCluster IP

Depuis ONTAP 9.8, vous pouvez gérer la configuration IP d'une opération MetroCluster avec System Manager. Une fois que deux clusters sont configurés, vous configurez le peering entre eux.

### Avant de commencer

Vous devez avoir terminé la procédure suivante pour configurer deux clusters :

- ["Configurer un site IP MetroCluster"](#)

Différentes étapes sont réalisées par différents administrateurs système sur les sites géographiques de chaque cluster. Pour expliquer ce processus, les clusters sont appelés « grappe de sites A » et « grappe de sites B ».

### Exécution du processus de peering à partir du site A

Ce processus est exécuté par un administrateur système sur le site A.

#### Étapes

1. Connectez-vous au site A cluster.
2. Dans System Manager, sélectionnez **Dashboard** dans la colonne de navigation de gauche pour afficher la vue d'ensemble du cluster.

Le tableau de bord affiche les détails de ce cluster (site A). Dans la section **MetroCluster**, site Un cluster est affiché sur la gauche.

3. Cliquez sur **attacher le cluster partenaire**.
4. Entrez les détails des interfaces réseau permettant aux nœuds du cluster site A de communiquer avec les

nœuds du cluster site B.

5. Cliquez sur **Enregistrer et continuer**.
6. Dans la fenêtre **Attach Partner Cluster**, sélectionnez **Je n'ai pas de phrase de passe**, ce qui vous permet de générer une phrase de passe.
7. Copiez le mot de passe généré et partagez-le avec l'administrateur système du site B.
8. Sélectionnez **Fermer**.

## Exécution du processus de peering depuis le site B

Ce processus est effectué par un administrateur système sur le site B.

### Étapes

1. Connectez-vous au cluster site B.
2. Dans System Manager, sélectionnez **Dashboard** pour afficher la vue d'ensemble du cluster.

Le tableau de bord affiche les détails de ce cluster (site B). Dans la section MetroCluster, le cluster du site B est indiqué sur la gauche.

3. Cliquez sur **Attach Partner Cluster** pour démarrer le processus de peering.
4. Entrez les détails des interfaces réseau permettant aux nœuds du cluster site B de communiquer avec les nœuds du cluster site A.
5. Cliquez sur **Enregistrer et continuer**.
6. Dans la fenêtre **Attach Partner Cluster**, sélectionnez **J'ai une phrase de passe**, qui vous permet de saisir la phrase de passe que vous avez reçue de l'administrateur système sur le site A.
7. Sélectionnez **Peer** pour terminer le processus de peering.

### Et la suite ?

Une fois le processus de peering terminé avec succès, vous configurez les clusters. Voir "[Configurez un site MetroCluster IP](#)".

## Configurez un site MetroCluster IP

Depuis ONTAP 9.8, vous pouvez gérer la configuration IP d'une opération MetroCluster avec System Manager. Après avoir configuré deux clusters et peering, vous configurez chaque cluster.

### Avant de commencer

Vous devez avoir effectué les procédures suivantes :

- "[Configurer un site IP MetroCluster](#)"
- "[Configuration du peering de MetroCluster IP](#)"

## Configurer la connexion entre les clusters

### Étapes

1. Connectez-vous à System Manager sur l'un des sites et sélectionnez **Dashboard**.

Dans la section **MetroCluster**, le graphique montre les deux clusters que vous avez configurés et associés

pour les sites MetroCluster. Le cluster depuis lequel vous travaillez (cluster local) s'affiche sur la gauche.

2. Cliquez sur **configurer MetroCluster**. Dans cette fenêtre, vous pouvez effectuer les tâches suivantes :
  - a. Les nœuds de chaque cluster de la configuration MetroCluster sont affichés. Utilisez les listes déroulantes pour sélectionner les nœuds du cluster local qui seront des partenaires de reprise après sinistre avec lesquels les nœuds du cluster distant seront présents.
  - b. Cochez la case si vous souhaitez configurer un service de médiateur ONTAP. Voir [Configurez le service Mediator ONTAP](#).
  - c. Si les deux clusters disposent d'une licence pour activer le chiffrement, la section **Encryption** s'affiche.  
  
Pour activer le chiffrement, entrez une phrase de passe.
  - d. Cochez la case si vous souhaitez configurer MetroCluster avec un réseau partagé de couche 3.



Les nœuds partenaires haute disponibilité et les commutateurs réseau qui se connectent aux nœuds doivent avoir une configuration correspondante.

3. Cliquez sur **Enregistrer** pour configurer les sites MetroCluster.

Dans la section **MetroCluster** du **Tableau de bord**, le graphique montre une coche sur la liaison entre les deux grappes, indiquant une connexion saine.


## Configurez le service Mediator ONTAP

Le service médiateur ONTAP est généralement installé dans un emplacement géographique distinct de l'un ou l'autre des clusters. Les clusters communiquent régulièrement avec le service pour indiquer qu'ils sont opérationnels. Si l'un des clusters de la configuration MetroCluster détecte que la communication avec son cluster partenaire est en panne, il consulte le médiateur ONTAP pour déterminer si le cluster partenaire est en panne.

### Avant de commencer

Les deux clusters des sites MetroCluster doivent être up et associés.

### Étapes

1. Dans System Manager sous ONTAP 9.8, sélectionnez **Cluster > Paramètres**.
2. Dans la section **Mediator**, cliquez sur .
3. Dans la fenêtre **Configure Mediator**, cliquez sur **Add+**.
4. Entrez les détails de configuration du médiateur ONTAP.

Vous pouvez entrer les détails suivants lors de la configuration d'un médiateur ONTAP avec le Gestionnaire système.

- Adresse IP du Mediator.
- Nom d'utilisateur.
- Le mot de passe.

## Gérer le Mediator avec System Manager

À l'aide de System Manager, vous pouvez effectuer des tâches de gestion du Mediator.






## À propos de ces tâches

À partir de ONTAP 9.8, vous pouvez utiliser System Manager comme interface simplifiée pour gérer une configuration IP à quatre nœuds d'une configuration MetroCluster, qui peut inclure un médiateur ONTAP installé à un troisième emplacement.

Depuis ONTAP 9.14.1, vous pouvez utiliser System Manager pour effectuer ces opérations dans une configuration IP à huit nœuds d'un site MetroCluster. Bien que vous ne puissiez pas configurer ou développer un système à huit nœuds avec System Manager, si vous avez déjà configuré un système IP MetroCluster à huit nœuds, vous pouvez effectuer ces opérations.

Effectuez les tâches suivantes pour gérer le Mediator.

| Pour effectuer cette tâche...                                                  | Prenez ces mesures...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configurez le service Mediator                                                 | Effectuez les étapes de la section " <a href="#">Configurez le service Mediator ONTAP</a> ".                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Activer ou désactiver la commutation automatique assistée par Mediator (MAUSO) | <div><div><div>1. Dans System Manager, cliquez sur <b>Dashboard</b>.</div><div>2. Faites défiler jusqu'à la section MetroCluster.</div><div>3. Cliquez sur  en regard du nom du site MetroCluster.</div><div>4. Sélectionnez <b>Activer</b> ou <b>Désactiver</b>.</div><div>5. Entrez le nom d'utilisateur et le mot de passe de l'administrateur, puis cliquez sur <b>Activer</b> ou <b>Désactiver</b>.</div></div><div><div></div><div><p>Vous pouvez activer ou désactiver le Mediator lorsqu'il est accessible et que les deux sites sont en mode « Normal ». Le médiateur est toujours accessible lorsque MAUSO est activé ou désactivé si le système MetroCluster est en bon état.</p></div></div></div> |
| Retirez le Mediator de la configuration MetroCluster                           | <div><div><div>1. Dans System Manager, cliquez sur <b>Dashboard</b>.</div><div>2. Faites défiler jusqu'à la section MetroCluster.</div><div>3. Cliquez sur  en regard du nom du site MetroCluster.</div><div>4. Sélectionnez <b>Supprimer le médiateur</b>.</div><div>5. Entrez le nom d'utilisateur et le mot de passe de l'administrateur, puis cliquez sur <b>Supprimer</b>.</div></div></div>                                                                                                                                                                                                                                                                                                                                                                                               |
| Vérifiez l'état de santé du Mediator                                           | Effectuez les étapes de la section " <a href="#">Résolution des problèmes liés aux configurations IP MetroCluster</a> ".                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Effectuer un basculement et un rétablissement                                  | Effectuez les étapes de la section " <a href="#">Réalisez le basculement et le rétablissement IP MetroCluster</a> ".                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Réalisez le basculement et le rétablissement IP MetroCluster

Vous pouvez basculer le contrôle d'un site IP MetroCluster à un autre pour effectuer des opérations de maintenance ou de restauration suite à un problème.



Les procédures de basculement et de rétablissement ne sont prises en charge que pour les configurations IP MetroCluster.

## Présentation du basculement et du rétablissement

Un basculement peut se produire dans deux cas :

- **Un basculement planifié**

Le basculement est initié par un administrateur système qui utilise System Manager. Le basculement planifié permet à l'administrateur système d'un cluster local de contrôler par commutation afin que les services de données du cluster distant soient gérés par le cluster local. Ensuite, un administrateur système sur le site distant du cluster peut réaliser des opérations de maintenance sur le cluster distant.

- **Un basculement non planifié**

Dans certains cas, lorsqu'un cluster MetroCluster tombe en panne ou que les connexions entre les clusters sont en panne, ONTAP lance automatiquement une procédure de basculement, de sorte que le cluster toujours en cours d'exécution gère les responsabilités de gestion des données du cluster en panne.

Lorsque ONTAP ne peut pas déterminer l'état de l'un des clusters, l'administrateur système du site qui travaille lance la procédure de basculement pour prendre le contrôle des responsabilités de gestion des données de l'autre site.

Pour tout type de procédure de basculement, la fonctionnalité de service de données est renvoyée au cluster au moyen d'un processus *rétablissement*.

Plusieurs processus de basculement et de rétablissement sont exécutés pour ONTAP 9.7 et 9.8 :

- [Utilisez System Manager dans ONTAP 9.7 pour le basculement et le rétablissement](#)
- [Utilisez System Manager dans ONTAP 9.8 pour le basculement et le rétablissement](#)

## Utilisez System Manager dans ONTAP 9.7 pour le basculement et le rétablissement

### Étapes

1. Connectez-vous à System Manager dans ONTAP 9.7.
2. Cliquez sur \* (revenir à la version classique)\*.
3. Cliquez sur **Configuration > MetroCluster**.

System Manager vérifie si un basculement négocié est possible.

4. Effectuez l'une des opérations suivantes lorsque le processus de validation est terminé :
  - a. Si la validation échoue, mais que le site B est en cours, une erreur s'est produite. Par exemple, il peut y avoir un problème avec un sous-système, ou la mise en miroir NVRAM peut ne pas être synchronisée.
    - i. Corrigez le problème à l'origine de l'erreur, cliquez sur **Fermer**, puis recommencez à l'étape 2.
    - ii. Arrêtez les nœuds du site B, cliquez sur **Fermer**, puis suivez les étapes de la section "[Effectuer un basculement non planifié](#)".
  - b. Si la validation échoue et que le site B est en panne, il est fort probable qu'il y ait un problème de connexion. Vérifiez que le site B est vraiment en panne, puis effectuez les étapes de la section


"Effectuer un basculement non planifié".

5. Cliquez sur **basculer du site B vers le site A** pour lancer le processus de basculement.
6. Cliquez sur **basculer vers la nouvelle expérience**.

## Utilisez System Manager dans ONTAP 9.8 pour le basculement et le rétablissement

### Exécution d'un basculement planifié (ONTAP 9.8)

#### Étapes

1. Connectez-vous au Gestionnaire système dans ONTAP 9.8.
2. Sélectionnez **Tableau de bord**. Dans la section **MetroCluster**, les deux clusters sont affichés avec une connexion.
3. Dans le cluster local (illustré à gauche), cliquez sur , puis sélectionnez **switchover les services de données distants vers le site local**.

Une fois la demande de basculement validée, le contrôle est transféré du site distant vers le site local, qui effectue les demandes de service de données pour les deux clusters.

Le cluster distant redémarre, mais les composants de stockage ne sont pas actifs et le cluster ne répond pas aux demandes de données. Elle est maintenant disponible pour la maintenance planifiée.



Le cluster distant ne doit pas être utilisé pour la maintenance des données tant que vous n'avez pas effectué de rétablissement.


### Exécution d'un basculement non planifié (ONTAP 9.8)

Un basculement non planifié peut être initié automatiquement par ONTAP. Si ONTAP ne peut pas déterminer s'il est nécessaire de procéder au rétablissement, l'administrateur système du site MetroCluster en cours d'exécution lance le basculement. Pour ce faire, procédez comme suit :

#### Étapes

1. Connectez-vous au Gestionnaire système dans ONTAP 9.8.
2. Sélectionnez **Tableau de bord**.

Dans la section **MetroCluster**, la connexion entre les deux clusters est indiquée par un « X », ce qui signifie qu'une connexion ne peut pas être détectée. Les connexions ou le cluster sont arrêtés.

3. Dans le cluster local (illustré à gauche), cliquez sur , puis sélectionnez **switchover les services de données distants vers le site local**.

Si le basculement échoue par erreur, cliquez sur le lien « Afficher les détails » dans le message d'erreur et confirmez le basculement non planifié.

Une fois la demande de basculement validée, le contrôle est transféré du site distant vers le site local, qui effectue les demandes de service de données pour les deux clusters.

Le cluster doit être réparé avant de pouvoir être remis en ligne.



Une fois le cluster distant mis en ligne à nouveau, il ne doit pas être utilisé pour le service des données tant que vous n'avez pas effectué de rétablissement.

## Exécution d'un rétablissement (ONTAP 9.8)

### Avant de commencer

Si le cluster distant était indisponible pour la maintenance planifiée ou en raison d'un incident, il devrait être à présent opérationnel et en attente du rétablissement.

### Étapes

1. Sur le cluster local, connectez-vous à System Manager dans ONTAP 9.8.

2. Sélectionnez **Tableau de bord**.

Dans la section **MetroCluster**, les deux clusters sont affichés.

3. Dans le cluster local (illustré à gauche), cliquez sur , puis sélectionnez **reprendre le contrôle**.

Les données sont *guéri* en premier, pour garantir que les données sont synchronisées et mises en miroir entre les deux clusters.

4. Une fois la correction des données terminée, cliquez sur , puis sélectionnez **lancer le rétablissement**.

Lorsque le rétablissement est terminé, les deux clusters sont actifs et le service des requêtes de données. De plus, les données sont en miroir et synchronisées entre les clusters.

## Modifiez l'adresse, le masque de réseau et la passerelle dans une adresse IP MetroCluster

Depuis ONTAP 9.10.1, vous pouvez modifier les propriétés suivantes d'une interface IP MetroCluster : adresse IP et masque, et passerelle. Vous pouvez utiliser n'importe quelle combinaison de paramètres pour la mise à jour.

Vous devrez peut-être mettre à jour ces propriétés, par exemple si une adresse IP dupliquée est détectée ou si une passerelle doit changer dans le cas d'un réseau de couche 3 en raison de modifications de configuration du routeur. Vous ne pouvez modifier qu'une interface à la fois. Cette interface entraînera une perturbation du trafic jusqu'à ce que les autres interfaces soient mises à jour et que les connexions soient réétablies.



Vous devez effectuer les modifications sur chaque port. De même, les commutateurs réseau doivent également mettre à jour leur configuration. Par exemple, si la passerelle est mise à jour, elle est idéalement modifiée sur les deux nœuds d'une paire haute disponibilité, car ils sont identiques. De plus, le switch connecté à ces nœuds doit également mettre à jour sa passerelle.

### Étape

Mettez à jour l'adresse IP, le masque de réseau et la passerelle pour chaque nœud et interface.

## Résolution des problèmes liés aux configurations IP MetroCluster

Depuis ONTAP 9.8, System Manager surveille l'intégrité des configurations IP MetroCluster et vous aide à identifier et à corriger les problèmes potentiels.

### Présentation de la vérification de l'état du système MetroCluster

System Manager vérifie régulièrement l'état de santé de votre configuration IP MetroCluster. Lorsque vous affichez la section MetroCluster du tableau de bord, le message généralement « les systèmes MetroCluster

sont sains ».

Cependant, lorsqu'un problème se produit, le message indique le nombre d'événements. Vous pouvez cliquer sur ce message et afficher les résultats de la vérification de l'état des composants suivants :

- Nœud
- Interface réseau
- Niveau (stockage)
- Cluster
- Connexion
- Volumétrie
- Réplication de la configuration

La colonne **Status** identifie les composants qui présentent des problèmes et la colonne **Details** indique comment corriger le problème.

## Dépannage de MetroCluster

### Étapes

1. Dans System Manager, sélectionnez **Dashboard**.
2. Dans la section **MetroCluster**, notez le message.
  - a. Si le message indique que la configuration de votre MetroCluster est correcte et que les connexions entre les clusters et le médiateur ONTAP sont en bon état (avec des cases à cocher), alors vous n'avez aucun problème à corriger.
  - b. Si le message indique le nombre d'événements, ou si les connexions ont diminué (indiqué par un « X »), passez à l'étape suivante.
3. Cliquez sur le message indiquant le nombre d'événements.

Le rapport d'intégrité MetroCluster s'affiche.

4. Dépanner les problèmes qui apparaissent dans le rapport en utilisant les suggestions dans la colonne **Détails**.
5. Lorsque tous les problèmes ont été corrigés, cliquez sur **vérifier l'état de santé du MetroCluster**.



La vérification de l'état de santé MetroCluster utilise une quantité importante de ressources. Il est donc recommandé d'effectuer toutes vos tâches de dépannage avant d'exécuter la vérification.

La vérification de l'état de santé de MetroCluster s'exécute en arrière-plan. Vous pouvez travailler sur d'autres tâches pendant que vous attendez la fin.

## Protection des données par sauvegarde sur bandes

### Présentation de la sauvegarde sur bande des volumes FlexVol

ONTAP supporte la sauvegarde sur bande et la restauration via le protocole NDMP (Network Data Management Protocol). NDMP vous permet de sauvegarder directement

les données des systèmes de stockage sur bande, ce qui optimise l'utilisation de la bande passante réseau. ONTAP prend en charge les moteurs dump et SMTape pour la sauvegarde sur bande.

Vous pouvez effectuer une sauvegarde ou une restauration dump ou SMTape à l'aide des applications de sauvegarde conformes à NDMP. Seule la version 4 de NDMP est prise en charge.

### Sauvegarde sur bande à l'aide de dump

Dump est une sauvegarde à base de copies Snapshot dans laquelle les données de votre système de fichiers sont sauvegardées sur bande. Le moteur de vidage ONTAP sauvegarde les fichiers, les répertoires et les informations de la liste de contrôle d'accès (ACL) applicable sur bande. Vous pouvez sauvegarder un volume entier, un qtree entier ou un sous-arbre qui n'est pas un volume entier ou un qtree entier. Le dump prend en charge les sauvegardes de base, différentielles et incrémentielles.

### Sauvegarde sur bande utilisant SMTape

SMTape est une solution de reprise après incident basée sur les copies Snapshot de ONTAP qui sauvegarde des blocs de données sur bande. Vous pouvez utiliser SMTape afin d'effectuer des sauvegardes de volume sur bandes. Toutefois, vous ne pouvez pas effectuer de sauvegarde au niveau qtree ou sous-arbre. SMTape prend en charge les sauvegardes de base, différentielles et incrémentielles.

À partir de ONTAP 9.13.1, la sauvegarde sur bande à l'aide de SMTape est prise en charge par [Synchronisation active SnapMirror](#).

## Sauvegarde sur bande et restauration du flux de travail

Vous pouvez effectuer des opérations de sauvegarde sur bande et de restauration à l'aide d'une application de sauvegarde NDMP.

### Description de la tâche

Le flux de production de sauvegarde et restauration sur bande présente les tâches impliquées dans les opérations de sauvegarde et de restauration sur bande. Pour plus d'informations sur l'exécution d'une opération de sauvegarde et de restauration, reportez-vous à la documentation de l'application de sauvegarde.

### Étapes

1. Définissez une configuration de librairie de bandes en choisissant une topologie de bande prise en charge par NDMP.
2. Activez les services NDMP sur votre système de stockage.

Vous pouvez activer les services NDMP au niveau des nœuds ou au niveau des machines virtuelles de stockage (SVM). Cela dépend du mode NDMP dans lequel vous choisissez d'effectuer l'opération de sauvegarde sur bande et de restauration.

3. Utilisez les options NDMP pour gérer NDMP sur votre système de stockage.

Vous pouvez utiliser les options NDMP au niveau des nœuds ou au niveau de la SVM. Cela dépend du mode NDMP dans lequel vous choisissez d'effectuer l'opération de sauvegarde sur bande et de restauration.

Vous pouvez modifier les options NDMP au niveau du nœud en utilisant la `system services ndmp modify` Commande et au niveau du SVM à l'aide de `vserver services ndmp modify` commande. Pour plus d'informations sur ces commandes, consultez les pages de manuels.

4. Effectuez une opération de sauvegarde sur bande ou de restauration à l'aide d'une application de sauvegarde NDMP.

ONTAP prend en charge les moteurs dump et SMTape pour la sauvegarde sur bande et la restauration.

Pour plus d'informations sur l'utilisation de l'application de sauvegarde (également appelée *Data Management applications* ou *DMA*) pour effectuer des opérations de sauvegarde ou de restauration, consultez la documentation de votre application de sauvegarde.

## Informations associées

[Topologies de sauvegarde sur bande NDMP courantes](#)

[Présentation du moteur de dump pour les volumes FlexVol](#)

## Cas d'utilisation pour choisir un moteur de sauvegarde sur bandes

ONTAP prend en charge deux moteurs de sauvegarde : SMTape et dump. Il est important de connaître les cas d'utilisation des moteurs de sauvegarde SMTape et dump afin de vous aider à choisir le moteur de sauvegarde permettant d'effectuer des opérations de sauvegarde sur bande et de restauration.

Le vidage peut être utilisé dans les cas suivants :

- La récupération d'accès direct des fichiers et des répertoires
- Sauvegarde d'un sous-ensemble de sous-répertoires ou de fichiers dans un chemin spécifique
- Exclusion de fichiers et de répertoires spécifiques pendant les sauvegardes
- Conserver les sauvegardes sur de longues durées

SMTape peut être utilisé dans les cas suivants :

- Solution de reprise après incident
- Préservation des économies de déduplication et des paramètres de déduplication sur les données sauvegardées au cours d'une opération de restauration
- Sauvegarde de volumes volumineux

## Gérer les lecteurs de bandes

### Présentation de la gestion des lecteurs de bandes

Vous pouvez vérifier les connexions de la librairie de bandes et afficher les informations relatives au lecteur de bandes avant d'effectuer une sauvegarde sur bande ou une restauration. Vous pouvez utiliser un lecteur de bande non qualifié en l'émulant sur un lecteur de bande qualifié. Vous pouvez également attribuer et supprimer des alias de bande en plus d'afficher des alias existants.

Lorsque vous sauvegardez des données sur bande, celles-ci sont stockées dans des fichiers sur bande. Les repères de fichier séparent les fichiers de bande et les fichiers n'ont pas de nom. Vous spécifiez un fichier de bande en fonction de sa position sur la bande. Vous écrivez un fichier de bande à l'aide d'un lecteur de bande. Lorsque vous lisez le fichier de bande, vous devez spécifier un périphérique ayant le même type de

compression que celui utilisé pour écrire ce fichier de bande.

## Commandes pour la gestion des lecteurs de bande, des changeurs de supports et des opérations de lecteurs de bande

Il existe des commandes permettant d'afficher des informations sur les lecteurs de bande et les changeurs de support d'un cluster, de mettre un lecteur de bande en ligne et de le mettre hors ligne, de modifier la position de la cartouche du lecteur de bande, de définir et d'effacer le nom d'alias du lecteur de bande, et de réinitialiser un lecteur de bande. Vous pouvez également afficher et réinitialiser les statistiques du lecteur de bande.

| Les fonctions que vous recherchez...                                                           | Utilisez cette commande...                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mettre un lecteur de bande en ligne                                                            | <code>storage tape online</code>                                                                                                                                                                                  |
| Effacez un nom d'alias pour le lecteur de bande ou le changeur de supports                     | <code>storage tape alias clear</code>                                                                                                                                                                             |
| Permet d'activer ou de désactiver une opération de trace de bande pour un lecteur de bande     | <code>storage tape trace</code>                                                                                                                                                                                   |
| Modifiez la position de la cartouche du lecteur de bande                                       | <code>storage tape position</code>                                                                                                                                                                                |
| Réinitialisez un lecteur de bande                                                              | <div><code>storage tape reset</code></div> <div> Cette commande est disponible uniquement au niveau de privilège avancé.</div> |
| Définissez un nom d'alias pour le lecteur de bande ou le changeur de supports                  | <code>storage tape alias set</code>                                                                                                                                                                               |
| Mettez un lecteur de bande hors ligne                                                          | <code>storage tape offline</code>                                                                                                                                                                                 |
| Permet d'afficher des informations sur tous les lecteurs de bande et les changeurs de supports | <code>storage tape show</code>                                                                                                                                                                                    |
| Afficher des informations sur les lecteurs de bande connectés au cluster                       | <ul style="list-style-type: none"><li>• <code>storage tape show-tape-drive</code></li><li>• <code>system node hardware tape drive show</code></li></ul>                                                           |
| Affiche des informations sur les changeurs de supports reliés au cluster                       | <code>storage tape show-media-changer</code>                                                                                                                                                                      |
| Afficher les informations d'erreur relatives aux lecteurs de bande connectés au cluster        | <code>storage tape show-errors</code>                                                                                                                                                                             |



| Les fonctions que vous recherchez...                                                                                            | Utilisez cette commande...                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Affichez tous les lecteurs de bande ONTAP qualifiés et pris en charge reliés à chaque nœud du cluster                           | <code>storage tape show-supported-status</code>                                                                                                                                                                                   |
| Afficher les alias de tous les lecteurs de bande et changeurs de support reliés à chaque nœud du cluster                        | <code>storage tape alias show</code>                                                                                                                                                                                              |
| Réinitialisez la lecture des statistiques d'un lecteur de bande                                                                 | <code>storage stats tape zero tape_name</code><br><br>Vous devez utiliser cette commande au niveau du nodeshell.                                                                                                                  |
| Afficher les lecteurs de bande pris en charge par ONTAP                                                                         | <code>storage show tape supported [-v]</code><br><br>Vous devez utiliser cette commande au niveau du nodeshell. Vous pouvez utiliser le <code>-v</code> option permettant d'afficher plus de détails sur chaque lecteur de bande. |
| Affichez les statistiques des lecteurs de bande pour comprendre les performances des bandes et vérifier le modèle d'utilisation | <code>storage stats tape tape_name</code><br><br>Vous devez utiliser cette commande au niveau du nodeshell.                                                                                                                       |

Pour plus d'informations sur ces commandes, consultez les pages de manuels.

### Utilisez un lecteur de bande non qualifié

Vous pouvez utiliser un lecteur de bande non qualifié sur un système de stockage s'il peut émuler un lecteur de bande qualifié. Il est ensuite traité comme un lecteur de bande qualifié. Pour utiliser un lecteur de bande non qualifié, vous devez d'abord déterminer s'il émule un des lecteurs de bande qualifiés.

#### Description de la tâche

Un lecteur de bande non qualifié est connecté au système de stockage, mais il n'est pas pris en charge ou reconnu par ONTAP.

#### Étapes

1. Affichez les lecteurs de bande non qualifiés connectés à un système de stockage à l'aide du `storage tape show-supported-status` commande.

La commande suivante affiche les lecteurs de bande connectés au système de stockage ainsi que l'état de support et de qualification de chaque lecteur de bande. Les lecteurs de bande non qualifiés sont également répertoriés. `tape_drive_vendor_name` Est un lecteur de bande non qualifié connecté au système de stockage, mais non pris en charge par ONTAP.

```
cluster1::> storage tape show-supported-status -node Node1
```

| Node: Node1               |              |                         |
|---------------------------|--------------|-------------------------|
| Tape Drive                | Is Supported | Support Status          |
| -----                     | -----        | -----                   |
| "tape_drive_vendor_name"  | false        | Nonqualified tape drive |
| Hewlett-Packard C1533A    | true         | Qualified               |
| Hewlett-Packard C1553A    | true         | Qualified               |
| Hewlett-Packard Ultrium 1 | true         | Qualified               |
| Sony SDX-300C             | true         | Qualified               |
| Sony SDX-500C             | true         | Qualified               |
| StorageTek T9840C         | true         | Dynamically Qualified   |
| StorageTek T9840D         | true         | Dynamically Qualified   |
| Tandberg LTO-2 HH         | true         | Dynamically Qualified   |

## 2. Émuler le lecteur de bande qualifié.

["Téléchargements NetApp : fichiers de configuration des lecteurs de bande"](#)

### Informations associées

[Lecteurs de bande qualifiés](#)

### Attribuer des alias de bande

Pour faciliter l'identification du périphérique, vous pouvez attribuer des alias de bande à un lecteur de bande ou à un changeur de support. Les alias fournissent une correspondance entre les noms logiques des périphériques de sauvegarde et un nom attribué de façon permanente au lecteur de bande ou au changeur de support.

### Étapes

1. Attribuez un alias à un lecteur de bande ou à un changeur de support à l'aide de la `storage tape alias set` commande.

Pour plus d'informations sur cette commande, consultez les pages de manuels.

Vous pouvez afficher les informations relatives au numéro de série (SN) sur les lecteurs de bande en utilisant le `system node hardware tape drive show` commande et à propos des bibliothèques de bandes à l'aide du `system node hardware tape library show` commandes.

La commande suivante définit un nom d'alias sur un lecteur de bande dont le numéro de série SN[123456]L4 est rattaché au nœud, cluster1-01 :

```
cluster-01::> storage tape alias set -node cluster-01 -name st3
-mapping SN[123456]L4
```

La commande suivante définit un nom d'alias sur un changeur de supports avec le numéro de série SN[65432] attaché au nœud, cluster1-01 :

```
cluster-01::> storage tape alias set -node cluster-01 -name mc1
-mapping SN[65432]
```

### Informations associées

[Quel est le crénelage de la bande](#)

[Suppression des alias de bande](#)

### Supprimer les alias de bande

Vous pouvez supprimer des alias en utilisant le `storage tape alias clear` commande lorsque les alias persistants ne sont plus nécessaires pour un lecteur de bande ou un chargeur de support.

#### Étapes

1. Retirez un alias d'un lecteur de bande ou d'un changeur de support à l'aide de la `storage tape alias clear` commande.

Pour plus d'informations sur cette commande, consultez les pages de manuels.

La commande suivante supprime les alias de tous les lecteurs de bande en spécifiant l'étendue de l'opération d'effacement d'alias à `tape`:

```
cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
```

### Une fois que vous avez terminé

Si vous effectuez une sauvegarde sur bande ou une opération de restauration à l'aide de NDMP, après avoir supprimé un alias d'un lecteur de bande ou d'un changeur de support, vous devez attribuer un nouveau nom d'alias au lecteur de bande ou au changeur de support pour continuer à accéder au périphérique de bande.

### Informations associées

[Quel est le crénelage de la bande](#)

[Attribution d'alias de bande](#)

### Activation ou désactivation des réservations sur bandes

Vous pouvez contrôler la manière dont ONTAP gère les réservations de périphériques de bandes à l'aide de `tape.reservations` option. Par défaut, la réservation sur bande est désactivée.

#### Description de la tâche

L'activation de l'option de réservation de bandes peut entraîner des problèmes si les lecteurs de bandes, les changeurs de supports, les ponts ou les bibliothèques ne fonctionnent pas correctement. Si les commandes

sur bande signalent que le périphérique est réservé lorsqu’aucun autre système de stockage n’utilise le périphérique, cette option doit être désactivée.

Étapes

- 1. Pour utiliser le mécanisme de réserve/libération SCSI ou la réserve permanente SCSI pour désactiver les réservations sur bande, entrez la commande suivante :

```
options -option-name tape.reservations -option-value {scsi | persistent | off}
```

scsi Sélectionne le mécanisme de réserve/libération SCSI.

persistent Sélectionne les réservations persistantes SCSI.

off désactive les réservations sur bande.

Informations associées

[Quelles sont les réservations sur bandes](#)

Commandes permettant de vérifier les connexions de la bibliothèque de bandes

Vous pouvez afficher des informations sur le chemin de connexion entre un système de stockage et une configuration de bibliothèque de bandes attachée au système de stockage. Vous pouvez utiliser ces informations pour vérifier le chemin de connexion à la configuration de la bibliothèque de bandes ou pour résoudre les problèmes liés aux chemins de connexion.

Vous pouvez afficher les détails de la bibliothèque de bandes suivants pour vérifier les connexions de la bibliothèque de bandes après avoir ajouté ou créé une nouvelle bibliothèque de bandes, ou après avoir restauré un chemin d’accès à un seul chemin ou à un chemin d’accès multichemin vers une bibliothèque de bandes. Vous pouvez également utiliser ces informations pendant le dépannage des erreurs liées au chemin ou en cas d’échec de l’accès à une bibliothèque de bandes.

- Nœud auquel la bibliothèque de bandes est attachée
- ID de périphérique
- Chemin NDMP
- Nom de la bibliothèque de bandes
- ID de port cible et de port initiateur
- Un accès à chemin unique ou multivoie à une bibliothèque de bandes pour chaque port cible ou initiateur FC
- Détails sur l’intégrité des données liées aux chemins, tels que « erreurs de chemin » et « Path Qual »
- Groupes de LUN et nombre de LUN

| Les fonctions que vous recherchez...                                    | Utilisez cette commande...             |
|-------------------------------------------------------------------------|----------------------------------------|
| Affiche des informations sur une bibliothèque de bandes dans un cluster | system node hardware tape library show |

| Les fonctions que vous recherchez...                                                                      | Utilisez cette commande...                               |
|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Afficher les informations sur le chemin d'accès d'une bibliothèque de bandes                              | <code>storage tape library path show</code>              |
| Affiche les informations sur le chemin d'accès d'une bibliothèque de bandes pour chaque port d'initiateur | <code>storage tape library path show-by-initiator</code> |
| Affichez les informations de connectivité entre une librairie de bandes de stockage et un cluster         | <code>storage tape library config show</code>            |

Pour plus d'informations sur ces commandes, consultez les pages de manuels.

## À propos des lecteurs de bande

### Présentation des lecteurs de bande qualifiés

Vous devez utiliser un lecteur de bande qualifié qui a été testé et trouvé pour fonctionner correctement sur un système de stockage. Vous pouvez suivre le repliement des bandes et également activer les réservations de bandes pour vous assurer qu'un seul système de stockage accède à un lecteur de bande à tout moment.

Un lecteur de bande qualifié est un lecteur de bande qui a été testé et qui fonctionne correctement sur les systèmes de stockage. Vous pouvez qualifier les lecteurs de bande pour les versions ONTAP existantes à l'aide du fichier de configuration de bande.

### Format du fichier de configuration de la bande

Le format du fichier de configuration de bande comprend des champs tels que l'ID du fournisseur, l'ID du produit et les détails des types de compression pour un lecteur de bande. Ce fichier se compose également de champs facultatifs pour l'activation de la fonction d'autochargement d'un lecteur de bande et la modification des valeurs de délai de commande d'un lecteur de bande.

Le tableau suivant affiche le format du fichier de configuration de la bande :

| Élément                          | Taille            | Description                                                                    |
|----------------------------------|-------------------|--------------------------------------------------------------------------------|
| <code>vendor_id</code> (chaîne)  | jusqu'à 8 octets  | L'ID du fournisseur tel que signalé par le SCSI <code>Inquiry</code> commande. |
| <code>product_id</code> (chaîne) | jusqu'à 16 octets | L'ID du produit tel qu'indiqué par le SCSI <code>Inquiry</code> commande.      |

| Élément                             | Taille            | Description                                                                                                                                                                                              |
|-------------------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>id_match_size(nombre)</code>  |                   | Nombre d'octets de l'ID produit à utiliser pour la correspondance pour détecter le lecteur de bande à identifier, en commençant par le premier caractère de l'ID produit dans les données de la requête. |
| <code>vendor_pretty (chaîne)</code> | jusqu'à 16 octets | Si ce paramètre est présent, il est spécifié par la chaîne affichée par la commande, <code>storage tape show -device-names</code> ; Sinon, <code>INQ_VENDOR_ID</code> est affiché.                       |
| <code>product_pretty(chaîne)</code> | jusqu'à 16 octets | Si ce paramètre est présent, il est spécifié par la chaîne affichée par la commande, <code>storage tape show -device-names</code> ; Sinon, <code>INQ_PRODUCT_ID</code> s'affiche.                        |




Le `vendor_pretty` et `product_pretty` les champs sont facultatifs, mais si l'un de ces champs a une valeur, l'autre doit également avoir une valeur.

Le tableau suivant explique la description, le code de densité et l'algorithme de compression des différents types de compression, tels que l, m, h, et a:

| Élément                               | Taille            | Description                                                                                                                                       |
|---------------------------------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>`{l</code>                      | m                 | h                                                                                                                                                 |
| <code>a}_description=(string)`</code> | jusqu'à 24 octets | La chaîne à imprimer pour la commande <code>nodeshell, sysconfig -t</code> , qui décrit les caractéristiques du paramètre de densité particulier. |
| <code>`{l</code>                      | m                 | h                                                                                                                                                 |
| <code>a}_density=(hex codes)`</code>  |                   | Le code de densité à définir dans le descripteur de bloc de page en mode SCSI correspondant au code de densité souhaité pour l, m, h ou a.        |
| <code>`{l</code>                      | m                 | h                                                                                                                                                 |

| Élément                   | Taille | Description                                                                                                                                                   |
|---------------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a}_algorithm=(hex codes)` |        | L'algorithme de compression à définir dans la page du mode de compression SCSI correspondant au code de densité et à la caractéristique de densité souhaitée. |

Le tableau suivant décrit les champs facultatifs disponibles dans le fichier de configuration de bande :

| Champ                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| autoload=(Boolean yes/no) | Ce champ est défini sur <code>yes</code> si le lecteur de bande dispose d'une fonction de chargement automatique, c'est-à-dire après l'insertion de la cartouche de bande, le lecteur de bande devient prêt sans avoir à exécuter un <code>SCSI load</code> (unité de démarrage/arrêt). La valeur par défaut de ce champ est <code>no</code> .                                                                                                                                                                                                                                                      |
| cmd_timeout_0x            | Valeur de temporisation individuelle. Vous devez utiliser ce champ uniquement si vous souhaitez spécifier une valeur de temporisation différente de celle utilisée par défaut par le pilote de bande. L'exemple de fichier répertorie les valeurs de délai d'expiration de la commande SCSI par défaut utilisées par le lecteur de bande. La valeur de temporisation peut être exprimée en minutes (m), secondes (s) ou millisecondes (ms).<br><br><div>  <div>Vous ne devez pas modifier ce champ.</div> </div> |

Vous pouvez télécharger et afficher le fichier de configuration de bandes sur le site de support NetApp.

### Exemple de format de fichier de configuration de bande

Le format de fichier de configuration de bande pour le lecteur de bande HP LTO5 ULTRIUM est le suivant :

vendor\_id= « HP »

product\_id= « Ultrium 5-SCSI »

id\_match\_size=9

vendor\_pretty= « Hewlett-Packard »

product\_pretty= « LTO-5 »

l\_description=« LTO-3 (ro)/4 4 Go »

l\_density=0x00

```
l_algorithm=0x00
m_description=« LTO-3(ro)/4 8/1600 go cmp »
m_density=0x00
m_algorithm=0x01
h_description=« LTO-5 1600 GO »
h_density=0x58
h_algorithm=0x00
a_description=« LTO-5 700 Go cmp »
a_density=0x58
a_algorithm=0x01
autoload= « oui »
```

### Informations associées

["Outils NetApp : fichiers de configuration des lecteurs de bandes"](#)

### Comment le système de stockage qualifie de façon dynamique un nouveau lecteur de bande

Le système de stockage qualifie dynamiquement un lecteur de bande en faisant correspondre son ID fournisseur et son ID produit avec les informations contenues dans le tableau de qualification de bande.

Lorsque vous connectez un lecteur de bande au système de stockage, il recherche un ID de fournisseur et un ID de produit correspondant entre les informations obtenues lors de la détection de bande et les informations de la table de qualification de bande interne. Si le système de stockage détecte une correspondance, il marque le lecteur de bande comme étant qualifié et peut accéder au lecteur de bande. Si le système de stockage ne trouve pas de correspondance, le lecteur de bande reste dans l'état non qualifié et n'est pas accessible.

### Présentation des lecteurs de bande

#### Présentation des lecteurs de bande

Un lecteur de bande est une représentation d'un lecteur de bande. Il s'agit d'une combinaison spécifique de type de rembobinage et de capacité de compression d'un lecteur de bande.

Un périphérique de bande est créé pour chaque combinaison de type de rembobinage et de capacité de compression. Par conséquent, un lecteur de bande ou une bibliothèque de bandes peut avoir plusieurs périphériques de bande qui lui sont associés. Vous devez spécifier un périphérique de bande pour déplacer, écrire ou lire des bandes.

Lorsque vous installez un lecteur de bande ou une bibliothèque de bandes sur un système de stockage,



ONTAP crée des unités de bande associées au lecteur de bande ou à la bibliothèque de bandes.

ONTAP détecte les lecteurs de bandes et les bibliothèques de bandes et leur attribue des numéros logiques et des lecteurs de bandes. ONTAP détecte les lecteurs et bibliothèques de bandes Fibre Channel, SAS et SCSI parallèle lorsqu'ils sont connectés aux ports d'interface. ONTAP détecte ces disques lorsque leurs interfaces sont activées.

#### Format du nom du périphérique de bande

Chaque unité de bande possède un nom associé qui apparaît dans un format défini. Le format inclut des informations sur le type de périphérique, le type de rembobinage, l'alias et le type de compression.

Le format d'un nom de périphérique de bande est le suivant :

```
rewind_type st alias_number compression_type
```

`rewind_type` est le type de rembobinage.

La liste suivante décrit les différentes valeurs de type de rembobinage :

- **r**

ONTAP rembobinait la bande après avoir fini d'écrire le fichier de bande.

- **nr**

ONTAP ne rembobinait pas la bande après avoir terminé l'écriture du fichier de bande. Vous devez utiliser ce type de rembobinage pour écrire plusieurs fichiers de bande sur la même bande.

- **ur**

Il s'agit du type de rembobinage de déchargement/rechargement. Lorsque vous utilisez ce type de rembobinage, la bibliothèque de bandes décharge la bande lorsqu'elle atteint la fin d'un fichier de bande, puis charge la bande suivante, s'il en existe une.

Vous devez utiliser ce type de rembobinage uniquement dans les cas suivants :

- Le lecteur de bande associé à ce périphérique se trouve dans une bibliothèque de bandes ou dans un changeur de support en mode bibliothèque.
- Le lecteur de bande associé à ce périphérique est connecté à un système de stockage.
- Le nombre de bandes suffisant pour l'opération que vous effectuez est disponible dans la séquence de bandes de bibliothèque définie pour ce lecteur de bande.



Si vous enregistrez une bande à l'aide d'un périphérique sans rembobinage, vous devez rembobiner la bande avant de la lire.

`st` est la désignation standard pour un lecteur de bande.

`alias_number` Est l'alias attribué par ONTAP au lecteur de bande. Lorsque ONTAP détecte un nouveau lecteur de bande, ONTAP attribue un alias au lecteur de bande.

`compression_type` est un code spécifique au lecteur pour la densité des données sur la bande et le type de

compression.

La liste suivante décrit les différentes valeurs de `compression_type`:

- **a**  
Compression la plus élevée
- **h**  
Compression élevée
- **m**  
Compression moyenne
- **l**  
Compression faible

**Exemples**

`nrst0a` spécifie un périphérique sans rembobinage sur le lecteur de bande 0 en utilisant la compression la plus élevée.

**Exemple de liste des lecteurs de bande**

L'exemple suivant illustre les périphériques de bande associés à HP Ultrium 2-SCSI :

|                     | Tape drive (fc202_6:2.126L1) | HP         | Ultrium 2-SCSI    |
|---------------------|------------------------------|------------|-------------------|
| <code>rst0l</code>  | - rewind device,             | format is: | HP (200GB)        |
| <code>nrst0l</code> | - no rewind device,          | format is: | HP (200GB)        |
| <code>urst0l</code> | - unload/reload device,      | format is: | HP (200GB)        |
| <code>rst0m</code>  | - rewind device,             | format is: | HP (200GB)        |
| <code>nrst0m</code> | - no rewind device,          | format is: | HP (200GB)        |
| <code>urst0m</code> | - unload/reload device,      | format is: | HP (200GB)        |
| <code>rst0h</code>  | - rewind device,             | format is: | HP (200GB)        |
| <code>nrst0h</code> | - no rewind device,          | format is: | HP (200GB)        |
| <code>urst0h</code> | - unload/reload device,      | format is: | HP (200GB)        |
| <code>rst0a</code>  | - rewind device,             | format is: | HP (400GB w/comp) |
| <code>nrst0a</code> | - no rewind device,          | format is: | HP (400GB w/comp) |
| <code>urst0a</code> | - unload/reload device,      | format is: | HP (400GB w/comp) |

La liste suivante décrit les abréviations présentées dans l'exemple précédent :

- Go—gigaoctets ; il s'agit de la capacité de la bande.
- avec compression ; indique la capacité de bande avec compression.

**Nombre de périphériques de bande simultanés pris en charge**

ONTAP prend en charge un maximum de 64 connexions simultanées de lecteurs de

bande, 16 changeurs de taille moyenne et 16 dispositifs de pont ou de routeur pour chaque système de stockage (par nœud) dans n'importe quelle combinaison de connexions Fibre Channel, SCSI ou SAS.

Les lecteurs de bandes ou les changeurs de taille moyenne peuvent être des périphériques dans des bibliothèques de bandes physiques ou virtuelles ou des périphériques autonomes.



Bien qu'un système de stockage puisse détecter 64 connexions de lecteur de bande, le nombre maximal de sessions de sauvegarde et de restauration pouvant être exécutées simultanément dépend des limites d'évolutivité du moteur de sauvegarde.

Informations associées

[Limite d'évolutivité pour les sessions de sauvegarde et de restauration](#)

Crénelage de l'adhésif

Présentation de l'alias de bande

Le crénelage simplifie le processus d'identification du dispositif. Le crénelage lie un nom de chemin physique (PPN) ou un numéro de série (SN) d'une bande ou d'un changeur de support à un nom d'alias persistant mais modifiable.

Le tableau suivant décrit comment le repliement de bande vous permet de vous assurer qu'un lecteur de bande (ou une bibliothèque de bandes ou un changeur de support) est toujours associé à un nom d'alias unique :

| Scénario                                                             | Réaffectation de l'alias                                                                        |
|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Lorsque le système redémarre                                         | Le lecteur de bande est automatiquement réaffecté à son alias précédent.                        |
| Lorsqu'un périphérique de bande se déplace vers un autre port        | L'alias peut être réglé pour pointer vers la nouvelle adresse.                                  |
| Lorsque plusieurs systèmes utilisent un lecteur de bande particulier | L'utilisateur peut définir l'alias de manière à ce qu'il soit identique pour tous les systèmes. |



Lorsque vous effectuez une mise à niveau de Data ONTAP 8.1.x vers Data ONTAP 8.2.x, la fonction d'alias de bande de Data ONTAP 8.2.x modifie les noms d'alias de bande existants. Dans ce cas, vous devrez peut-être mettre à jour les noms d'alias de bande dans l'application de sauvegarde.

L'attribution d'alias de bande fournit une correspondance entre les noms logiques des périphériques de sauvegarde (par exemple st0 ou mc1) et un nom attribué de façon permanente à un port, un lecteur de bande ou un chargeur de support.



st0 et st00 sont des noms logiques différents.



Les noms logiques et les numéros de série sont utilisés uniquement pour accéder à un périphérique. Une fois le périphérique accédé, il renvoie tous les messages d'erreur en utilisant le nom du chemin physique.

Il existe deux types de noms disponibles pour le changement de dénomination : le nom du chemin physique et le numéro de série.

#### Quels sont les noms de chemin physique

Les noms de chemin physique (PPN) sont les séquences d'adresses numériques que ONTAP attribue aux lecteurs de bande et aux bibliothèques de bandes en fonction de l'adaptateur ou du commutateur SCSI-2/3 (emplacement spécifique) qu'ils sont connectés au système de stockage. Les noms PPN sont également appelés noms électriques.

Les PPN des périphériques connectés directement utilisent le format suivant : `host_adapter.device_id_lun`



La valeur LUN s'affiche uniquement pour les unités de bande et de changeur de support dont les valeurs LUN ne sont pas nulles, c'est-à-dire si la valeur LUN est zéro `lun`. Une partie du PPN n'est pas affichée.

Par exemple, le PPN 8.6 indique que le numéro de l'adaptateur hôte est 8, que l'ID du périphérique est 6 et que le numéro de l'unité logique (LUN) est 0.

Les lecteurs de bande SAS sont également des périphériques à connexion directe. Par exemple, le PPN 5c.4 indique que dans un système de stockage, l'adaptateur HBA SAS est connecté à l'emplacement 5, la bande SAS est connectée au port C de l'adaptateur HBA SAS et l'ID du périphérique est 4.

Les PPN des périphériques connectés par commutateur Fibre Channel utilisent le format suivant : `switch:port_id.device_id_lun`

Par exemple, le PPN MY\_SWITCH:5.3L2 indique que le lecteur de bande connecté au port 5 d'un commutateur appelé MY\_SWITCH est défini avec l'ID de périphérique 3 et possède la LUN 2.

La LUN (numéro d'unité logique) est déterminée par le lecteur. Les bibliothèques et lecteurs de bande SCSI, Fibre Channel et les disques possèdent des PPN.

Les PPN des lecteurs de bande et des bibliothèques ne changent pas, sauf si le nom du commutateur change, que le lecteur de bande ou la bibliothèque se déplace ou que le lecteur de bande ou la bibliothèque est reconfiguré. Les PPN restent inchangés après le redémarrage. Par exemple, si un lecteur de bande nommé MY\_SWITCH:5.3L2 est retiré et qu'un nouveau lecteur de bande avec le même ID de périphérique et le même LUN est connecté au port 5 du commutateur MY\_SWITCH, le nouveau lecteur de bande sera accessible à l'aide DE MY\_SWITCH:5.3L2.

#### Quels sont les numéros de série

Un numéro de série (SN) est un identifiant unique pour un lecteur de bande ou un chargeur de support. ONTAP génère des alias basés sur SN à la place du WWN.

Comme le SN est un identifiant unique pour un lecteur de bande ou un chargeur de support, l'alias reste le même quel que soit le chemin de connexion multiple vers le lecteur de bande ou le changeur de support. Les

systèmes de stockage peuvent ainsi suivre le même lecteur de bande ou le même changeur de support dans une configuration de librairie de bandes.

Le numéro de série d'un lecteur de bande ou d'un changeur de support ne change pas même si vous renommez le commutateur Fibre Channel auquel le lecteur de bande ou le changeur de support est connecté. Toutefois, dans une bibliothèque de bandes, si vous remplacez un lecteur de bandes existant par un nouveau, ONTAP génère de nouveaux alias car le numéro de série du lecteur de bande change. De même, si vous déplacez un lecteur de bande existant dans un nouveau slot dans une librairie de bandes ou si vous remappage le LUN du lecteur de bande, ONTAP génère un nouvel alias pour ce lecteur de bande.



Vous devez mettre à jour les applications de sauvegarde avec les alias nouvellement générés.

Le numéro de série d'un périphérique à bande utilise le format suivant : SN [xxxxxxxxxx] L [X]

x Est un caractère alphanumérique et un caractère Lx Est le LUN du périphérique de bande. Si le LUN est 0, le Lx une partie de la chaîne n'est pas affichée.

Chaque numéro de série comprend jusqu'à 32 caractères ; le format du numéro de série n'est pas sensible à la casse.

### **Considérations relatives à la configuration de l'accès aux bandes multivoie**

Vous pouvez configurer deux chemins à partir du système de stockage pour accéder aux lecteurs de bande dans une bibliothèque de bandes. En cas de défaillance d'un chemin, le système de stockage peut utiliser les autres chemins pour accéder aux lecteurs de bande sans avoir à réparer immédiatement le chemin défaillant. Ainsi, les opérations sur bandes peuvent être redémarrées.

Vous devez tenir compte des éléments suivants lors de la configuration de l'accès aux bandes multivoies à partir de votre système de stockage :

- Dans les bibliothèques de bandes prenant en charge le mappage des LUN, pour l'accès multivoie à un groupe de LUN, le mappage des LUN doit être symétrique sur chaque chemin.

Les lecteurs de bande et les changeurs de supports sont affectés à des groupes de LUN (ensemble de LUN partageant le même chemin d'accès d'initiateur) dans une bibliothèque de bandes. Tous les lecteurs de bande d'un groupe de LUN doivent être disponibles pour les opérations de sauvegarde et de restauration sur tous les chemins multiples.

- Il est possible de configurer deux chemins au maximum à partir du système de stockage pour accéder aux lecteurs de bande d'une bibliothèque de bandes.
- L'accès aux bandes multivoie prend en charge l'équilibrage de la charge. L'équilibrage de la charge est désactivé par défaut.

Dans l'exemple suivant, le système de stockage accède au groupe LUN 0 via deux chemins d'initiateur : 0b et 0d. Dans ces deux chemins, le groupe de LUN porte le même numéro de LUN, 0, et le nombre de LUN, 5. Le système de stockage accède à la LUN group 1 via un seul chemin d'initiateur, la 3d.

```
STSW-3070-2_cluster::> storage tape library config show
```

| Node                   | LUN Group | LUN Count | Library Name  | Library |
|------------------------|-----------|-----------|---------------|---------|
| Target Port Initiator  |           |           |               |         |
| STSW-3070-2_cluster-01 | 0         | 5         | IBM 3573-TL_1 |         |
| 510a09800000412d       | 0b        |           |               |         |
| 0d                     |           |           |               |         |
|                        | 1         | 2         | IBM 3573-TL_2 |         |
| 50050763124b4d6f       | 3d        |           |               |         |

3 entries were displayed

Pour plus d'informations, consultez les pages de manuel.

### Comment ajouter des lecteurs de bande et des bibliothèques aux systèmes de stockage

Vous pouvez ajouter des lecteurs de bandes et des bibliothèques au système de stockage de façon dynamique (sans mettre le système de stockage hors ligne).

Lorsque vous ajoutez un nouveau chargeur de support, le système de stockage détecte sa présence et l'ajoute à la configuration. Si le chargeur de support est déjà référencé dans les informations d'alias, aucun nouveau nom logique n'est créé. Si la bibliothèque n'est pas référencée, le système de stockage crée un nouvel alias pour le changeur de support.

Dans une configuration de librairie de bandes, vous devez configurer un lecteur de bande ou un changeur de support sur la LUN 0 d'un port cible pour ONTAP afin de détecter tous les changeurs de support et lecteurs de bande sur ce port cible.

### Quelles sont les réservations sur bandes

Plusieurs systèmes de stockage peuvent partager l'accès aux lecteurs de bande, aux changeurs de taille moyenne, aux ponts ou aux bibliothèques de bandes. Les réservations sur bande garantissent qu'un seul système de stockage accède à un périphérique à un moment donné en activant soit le mécanisme de réserve/libération SCSI, soit les réservations permanentes SCSI pour tous les lecteurs de bande, les changeurs de taille moyenne, les ponts et les bibliothèques de bandes.



Tous les systèmes qui partagent des périphériques dans une bibliothèque, qu'ils soient impliqués ou non, doivent utiliser la même méthode de réservation.

Le mécanisme de réserve/libération SCSI pour la réservation des périphériques fonctionne bien dans des conditions normales. Cependant, durant les procédures de récupération des erreurs de l'interface, les réservations peuvent être perdues. Dans ce cas, les initiateurs autres que le propriétaire réservé peuvent accéder au périphérique.

Les réservations effectuées avec SCSI persistent Reservations ne sont pas affectées par les mécanismes de récupération d’erreurs, tels que la réinitialisation de boucle ou la réinitialisation de la cible ; cependant, tous les périphériques n’implémentent pas correctement les réservations permanentes SCSI.

## Transférer des données à l’aide de ndmcopy

### Transférer des données à l’aide de la vue d’ensemble ndmcopy

Le `ndmcopy` La commande `nodeshell` transfère les données entre les systèmes de stockage qui prennent en charge NDMP v4. Vous pouvez effectuer des transferts de données complets et incrémentiels. Vous pouvez transférer des volumes complets ou partiels, des qtrees, des répertoires ou des fichiers individuels.

#### Description de la tâche

Avec ONTAP 8.x et les versions antérieures, les transferts incrémentiels sont limités à deux niveaux au maximum (une sauvegarde complète et jusqu’à deux sauvegardes incrémentielles).


Depuis la version ONTAP 9.0 et les versions ultérieures, les transferts incrémentiels se limitent à neuf niveaux maximum (une sauvegarde complète et jusqu’à neuf sauvegardes incrémentielles).

Vous pouvez exécuter `ndmcopy` à la ligne de commande `nodeshell` des systèmes de stockage source et de destination, ou d’un système de stockage qui n’est ni la source ni la destination du transfert de données. Vous pouvez également exécuter `ndmcopy` sur un système de stockage unique qui est à la fois la source et la destination du transfert de données.

Vous pouvez utiliser les adresses IPv4 ou IPv6 des systèmes de stockage source et de destination dans `ndmcopy` commande. Le format du chemin d’accès est `/vserver_name/volume_name \[path\]`.

#### Étapes

1. Activer le service NDMP sur les systèmes de stockage source et cible :

|                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Si vous effectuez le transfert des données à la source ou à la destination dans... | Utiliser la commande suivante...                                                                                                                                                                                                                                                                                                                                                                                               |
| Mode SVM-scoped NDMP                                                               | <div><pre>vserver services ndmp on</pre></div> <div><div></div><div>Pour l’authentification NDMP au SVM admin, le compte utilisateur est admin et le rôle de l’utilisateur est admin ou backup. Au sein de la SVM de données, le compte utilisateur est vsadmin et le rôle de l’utilisateur est vsadmin ou vsadmin-backup rôle.</div></div> |
| Mode node-scoped NDMP                                                              | <pre>system services ndmp on</pre>                                                                                                                                                                                                                                                                                                                                                                                             |

2. Transfert de données au sein d’un système de stockage ou entre des systèmes de stockage utilisant le `ndmcopy` commande au `nodeshell` :

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-
mcd {inet|inet6}] [-md {inet|inet6}]
```



Les noms DNS ne sont pas pris en charge dans ndmpcopy. Vous devez fournir l'adresse IP de la source et de la destination. L'adresse de bouclage (127.0.0.1) n'est pas prise en charge pour l'adresse IP source ou l'adresse IP de destination.

- ° Le ndmpcopy commande détermine le mode d'adresse pour les connexions de contrôle comme suit :
  - Le mode d'adresse pour la connexion de contrôle correspond à l'adresse IP fournie.
  - Vous pouvez remplacer ces règles à l'aide du -mcs et -mcd options.
- ° Si la source ou la destination est le système ONTAP, selon le mode NDMP (node-scoped ou SVM-scoped), utiliser une adresse IP permettant d'accéder au volume cible.
- ° source\_path et destination\_path sont les noms de chemin absolus jusqu'au niveau granulaire du volume, qtree, répertoire ou fichier.
- ° -mcs spécifie le mode d'adressage préféré pour la connexion de contrôle au système de stockage source.

inet Indique un mode d'adresse IPv4 et inet6 Indique un mode d'adresse IPv6.

- ° -mcd spécifie le mode d'adressage préféré pour la connexion de contrôle au système de stockage de destination.

inet Indique un mode d'adresse IPv4 et inet6 Indique un mode d'adresse IPv6.

- ° -md spécifie le mode d'adressage préféré pour les transferts de données entre les systèmes de stockage source et de destination.

inet Indique un mode d'adresse IPv4 et inet6 Indique un mode d'adresse IPv6.

Si vous n'utilisez pas le -md dans le ndmpcopy commande, le mode d'adressage de la connexion de données est déterminé comme suit :

- Si l'une des adresses spécifiées pour les connexions de contrôle est une adresse IPv6, le mode d'adresse de la connexion de données est IPv6.
- Si les deux adresses spécifiées pour les connexions de contrôle sont des adresses IPv4, le ndmpcopy La commande tente d'abord de passer en mode d'adresse IPv6 pour la connexion de données.

Si cela échoue, la commande utilise un mode d'adresse IPv4.



Une adresse IPv6, si elle est spécifiée, doit être entre crochets.

Cet exemple de commande migre les données d'un chemin source (source\_path) vers un chemin de destination (destination\_path).



```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
-st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+

Cet exemple de commande définit explicitement les connexions de contrôle et la connexion de données pour utiliser le mode d'adresse IPv6 :


```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdg:7e78]:/<dst_svm>/<dst_vol>
```

## Options de la commande ndmpcopy

Il est important de connaître les options disponibles pour le `ndmpcopy` nodeshell commande pour le transfert des données réussi.

Le tableau suivant répertorie les options disponibles. Pour plus d'informations, reportez-vous à la section `ndmpcopy` pages man disponibles via le nodeshell.

| Option                                                                                                                                                                                                                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-sa username:[password]</code>                                                                                                                                                                                                                     | <p>Cette option définit le nom d'utilisateur et le mot de passe d'authentification source pour la connexion au système de stockage source. Cette option est obligatoire.</p> <p>Pour un utilisateur sans privilège admin, vous devez spécifier le mot de passe spécifique NDMP généré par le système de l'utilisateur. Le mot de passe généré par le système est obligatoire pour les utilisateurs admin et non-admin.</p> |
| <code>-da username:[password]</code>                                                                                                                                                                                                                     | <p>Cette option définit le nom d'utilisateur et le mot de passe d'authentification de destination pour la connexion au système de stockage de destination. Cette option est obligatoire.</p>                                                                                                                                                                                                                               |
| <code>-st {md5</code>                                                                                                                                                                                                                                    | <code>text}</code>                                                                                                                                                                                                                                                                                                                                                                                                         |
| Cette option définit le type d'authentification source à utiliser lors de la connexion au système de stockage source. Il s'agit d'une option obligatoire. L'utilisateur doit donc fournir l'une ou l'autre <code>text</code> ou <code>md5</code> option. | <code>-dt {md5</code>                                                                                                                                                                                                                                                                                                                                                                                                      |

| Option   | Description                                                                                                                                                                                                                                                                                                                                                                                    |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| text}    | Cette option définit le type d'authentification de destination à utiliser lors de la connexion au système de stockage de destination.                                                                                                                                                                                                                                                          |
| -l       | Cette option définit le niveau de vidage utilisé pour le transfert vers la valeur spécifiée de niveau.les valeurs valides sont 0, 1, à 9, où 0 indique un transfert complet et 1 à 9 spécifie un transfert incrémentiel. La valeur par défaut est 0.                                                                                                                                           |
| -d       | Cette option permet de générer des messages de journal de débogage ndmcopy. Les fichiers journaux de débogage ndmcopy se trouvent dans le /mroot/etc/log volume racine. Les noms des fichiers journaux de débogage ndmcopy se trouvent dans le ndmcopy.yyyymmdd format.                                                                                                                        |
| -f       | Cette option active le mode forcé. Ce mode permet d'écraser les fichiers système dans /etc Répertoire à la racine du volume 7-mode.                                                                                                                                                                                                                                                            |
| -h       | Cette option imprime le message d'aide.                                                                                                                                                                                                                                                                                                                                                        |
| -p       | <p>Cette option vous invite à saisir le mot de passe pour l'autorisation source et de destination. Ce mot de passe remplace le mot de passe spécifié pour -sa et -da options.</p> <div>  <p>Vous ne pouvez utiliser cette option que lorsque la commande s'exécute dans une console interactive.</p> </div> |
| -exclude | Cette option exclut les fichiers ou répertoires spécifiés du chemin spécifié pour le transfert de données. Cette valeur peut être une liste séparée par des virgules de noms de répertoire ou de fichier tels que <b>.pst</b> ou <b>.txt</b> .                                                                                                                                                 |

## NDMP pour volumes FlexVol

### À propos de NDMP pour volumes FlexVol

Le protocole Network Data Management Protocol (NDMP) est un protocole standardisé pour contrôler la sauvegarde, la restauration et d'autres types de transfert de données entre les périphériques de stockage primaire et secondaire, tels que les systèmes de stockage et les bibliothèques de bandes.

En activant la prise en charge NDMP sur un système de stockage, vous permettez à ce système de stockage de communiquer avec les applications de sauvegarde NAS compatibles NDMP (également appelées *Data Management applications* ou *DMA*), les serveurs de données et les serveurs de bandes participant aux opérations de sauvegarde ou de restauration. Toutes les communications réseau sont effectuées sur le réseau TCPIP ou TCP/IPv6. NDMP offre également un contrôle bas niveau des lecteurs de bandes et des changeurs de taille moyenne.

Il est possible d'effectuer des opérations de sauvegarde sur bande et de restauration en mode node-scoped NDMP ou SVM (Storage Virtual machine) scoped NDMP.

Vous devez tenir compte des considérations à prendre en compte lors de l'utilisation du protocole NDMP, de la liste des variables d'environnement et des topologies de sauvegarde sur bande NDMP prises en charge. Vous pouvez également activer ou désactiver la fonctionnalité DAR améliorée. Les deux méthodes d'authentification prises en charge par ONTAP pour l'authentification de l'accès NDMP sur un système de stockage sont : texte clair et défi.

#### Informations associées

[Variables d'environnement prises en charge par ONTAP](#)

#### À propos des modes de fonctionnement NDMP

Vous pouvez effectuer des opérations de sauvegarde sur bande et de restauration au niveau du nœud ou du SVM (Storage Virtual machine). Pour réaliser correctement ces opérations au niveau du SVM, le service NDMP doit être activé sur la SVM.

Si vous effectuez une mise à niveau de Data ONTAP 8.2 vers Data ONTAP 8.3, le mode d'opération NDMP utilisé dans 8.2 sera conservé après la mise à niveau de 8.2 à 8.3.

Si vous installez un nouveau cluster avec Data ONTAP 8.2 ou version ultérieure, NDMP est en mode SVM-scoped NDMP par défaut. Pour effectuer des opérations de sauvegarde sur bande et de restauration en mode node-scoped NDMP, vous devez activer de façon explicite le mode node-scoped NDMP.

#### Informations associées

[Commandes permettant de gérer le mode node-scoped NDMP](#)

[Gérer le mode NDMP node-scoped pour les volumes FlexVol](#)

[Gérer le mode SVM-scoped NDMP pour les volumes FlexVol](#)

#### Le mode node-scoped NDMP est

En mode node-scoped NDMP, vous pouvez effectuer des opérations de backup sur bande et restore au niveau du nœud. Le mode d'opération NDMP utilisé dans Data ONTAP 8.2 reste conservé après la mise à niveau de 8.2 à 8.3.

En mode node-scoped NDMP, vous pouvez effectuer des opérations de backup sur bande et restore sur un nœud propriétaire du volume. Pour effectuer ces opérations, vous devez établir des connexions de contrôle NDMP sur une LIF hébergée sur le nœud qui détient le volume ou les lecteurs de bande.



Ce mode est obsolète et sera supprimé dans une prochaine version majeure.

#### Informations associées

### Le mode SVM-scoped NDMP est

Vous pouvez réaliser des opérations de sauvegarde sur bande et de restauration au niveau des SVM (Storage Virtual machine) si le service NDMP est activé sur la SVM. Vous pouvez sauvegarder et restaurer tous les volumes hébergés sur différents nœuds du SVM d'un cluster si l'application de sauvegarde prend en charge l'extension CAB.

Une connexion de contrôle NDMP peut être établie sur différents types de LIF. En mode SVM-scoped NDMP, ces LIFs appartiennent au SVM de données ou au SVM admin. La connexion peut être établie sur une LIF uniquement si le service NDMP est activé sur le SVM qui possède cette LIF.

Une LIF de données appartient au SVM de données et au LIF intercluster, ainsi qu'au LIF node-management et au LIF cluster-management appartient au SVM admin.

En mode SVM-scoped NDMP, la disponibilité des volumes et des dispositifs sur bande pour les opérations de backup et restore dépend du type de LIF sur lequel la connexion NDMP control est établie et de l'état de l'extension CAB. Si votre application de sauvegarde prend en charge l'extension CAB et qu'un volume et le périphérique de bande partagent la même affinité, alors l'application de sauvegarde peut effectuer une opération de sauvegarde ou de restauration locale, au lieu d'une opération de sauvegarde ou de restauration à trois voies.

### Informations associées

[Gérer le mode SVM-scoped NDMP pour les volumes FlexVol](#)

### Considérations relatives à l'utilisation de NDMP

Lorsque vous démarrez le service NDMP sur votre système de stockage, vous devez prendre en compte un certain nombre de considérations.

- Chaque nœud prend en charge jusqu'à 16 sauvegardes, restaurations ou combinaisons de les deux à l'aide de lecteurs de bande connectés.
- Les services NDMP peuvent générer des données d'historique de fichiers à la demande des applications de sauvegarde NDMP.

L'historique des fichiers est utilisé par les applications de sauvegarde pour permettre la restauration optimisée de sous-ensembles de données sélectionnés à partir d'une image de sauvegarde. La génération et le traitement de l'historique des fichiers peuvent s'avérer chronophages et nécessitent beaucoup de ressources CPU pour le système de stockage et l'application de sauvegarde.



SMTape ne prend pas en charge l'historique des fichiers.

Si la protection de vos données est configurée pour la reprise après incident, où l'image de sauvegarde complète sera récupérée, vous pouvez désactiver la génération de l'historique des fichiers pour réduire le temps de sauvegarde. Consultez la documentation de votre application de sauvegarde pour déterminer s'il est possible de désactiver la génération de l'historique du fichier NDMP.

- La politique de pare-feu pour NDMP est activée par défaut sur tous les types LIF.
- En mode node-scoped NDMP, la sauvegarde d'un volume FlexVol nécessite que vous utilisiez l'application de backup pour initier une sauvegarde sur un nœud propriétaire du volume.

Toutefois, vous ne pouvez pas sauvegarder un volume racine de nœud.

- Vous pouvez effectuer une sauvegarde NDMP à partir de n'importe quelle LIF, comme le permettent les politiques de pare-feu.

Si vous utilisez une LIF de données, vous devez sélectionner une LIF qui n'est pas configurée pour le basculement. Si une LIF de données bascule lors d'une opération NDMP, l'opération NDMP échoue et doit être de nouveau exécutée.

- En mode node-scoped NDMP et Storage Virtual machine (SVM) scoped NDMP sans support d'extension CAB, la connexion de données NDMP utilise le même LIF que la connexion NDMP control.
- Au cours de la migration de LIF, les opérations régulières de sauvegarde et de restauration sont interrompues.

Vous devez lancer les opérations de sauvegarde et de restauration après la migration LIF.

- Le chemin de sauvegarde NDMP est du format `/vserver_name/volume_name/path_name`.

*path\_name* Est facultatif et spécifie le chemin d'accès au répertoire, au fichier ou à la copie Snapshot.

- Lorsqu'une destination SnapMirror est sauvegardée sur bande à l'aide du moteur de dump, seules les données du volume sont sauvegardées.

Toutefois, lorsqu'une destination SnapMirror est sauvegardée sur bande à l'aide de SMTape, les métadonnées sont également sauvegardées. Les relations SnapMirror et les métadonnées associées ne sont pas sauvegardées sur bande. Dès lors, pendant la restauration, seules les données de ce volume sont restaurées, mais les relations SnapMirror associées ne sont pas restaurées.

## Informations associées

[Rôle de l'extension Cluster Aware Backup](#)

["Administration du système"](#)

## Variable d'environnement

### Présentation des variables d'environnement

Les variables d'environnement servent à communiquer des informations sur une opération de sauvegarde ou de restauration entre une application de sauvegarde NDMP et un système de stockage.

Par exemple, si un utilisateur indique qu'une application de sauvegarde doit effectuer une sauvegarde `/vserver1/vol1/dir1`, L'application de sauvegarde définit la variable d'environnement DU SYSTÈME DE FICHIERS sur `/vserver1/vol1/dir1`. De même, si un utilisateur spécifie qu'une sauvegarde doit être une sauvegarde de niveau 1, l'application de sauvegarde définit la variable d'environnement DE NIVEAU sur 1 (une).



La définition et l'examen des variables d'environnement sont généralement transparents pour les administrateurs de sauvegarde, c'est-à-dire que l'application de sauvegarde les définit automatiquement.

Un administrateur de sauvegarde spécifie rarement des variables d'environnement. Il est toutefois préférable de modifier la valeur d'une variable d'environnement dans cette variable définie par l'application de

sauvegarde pour caractériser ou contourner un problème de fonctionnement ou de performances. Par exemple, un administrateur peut désactiver temporairement la génération de l'historique des fichiers pour déterminer si le traitement par l'application de sauvegarde des informations de l'historique des fichiers contribue à des problèmes de performances ou à des problèmes fonctionnels.

De nombreuses applications de sauvegarde offrent un moyen de remplacer ou de modifier des variables d'environnement ou de spécifier des variables d'environnement supplémentaires. Pour plus d'informations, consultez la documentation de votre application de sauvegarde.

**Variables d'environnement prises en charge par ONTAP**

Les variables d'environnement servent à communiquer des informations sur une opération de sauvegarde ou de restauration entre une application de sauvegarde NDMP et un système de stockage. ONTAP prend en charge les variables d'environnement qui ont une valeur par défaut associée. Toutefois, vous pouvez modifier manuellement ces valeurs par défaut.

Si vous modifiez manuellement les valeurs définies par l'application de sauvegarde, il se peut que l'application se comporte de façon imprévisible. En effet, les opérations de sauvegarde ou de restauration ne peuvent pas faire ce que l'application de sauvegarde attend d'elles. Mais dans certains cas, une modification judicieuse pourrait aider à identifier ou à gérer des problèmes.

Les tableaux ci-dessous répertorient les variables d'environnement dont le comportement est commun à dump et SMTape, ainsi que les variables prises en charge uniquement pour dump et SMTape. Ces tableaux contiennent également des descriptions du fonctionnement des variables d'environnement prises en charge par ONTAP, le cas échéant :



Dans la plupart des cas, les variables qui ont la valeur, Y accepter également T et N accepter également F.

**Variables d'environnement prises en charge pour dump et SMTape**

| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                |
|--------------------------|-----------------|-------------------|----------------------------------------------------------------------------|
| DÉBOGAGE                 | Y ou N          | N                 | Spécifie que les informations de débogage sont imprimées.                  |
| SYSTÈME DE FICHIERS      | string          | none              | Indique le chemin d'accès de la racine des données en cours de sauvegarde. |

| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|-----------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NDMP_VERSION             | return_only     | none              | <p>Vous ne devez pas modifier la variable NDMP_VERSION. Créée par l'opération de sauvegarde, la variable NDMP_VERSION renvoie la version NDMP.</p> <p>ONTAP définit la variable NDMP_VERSION lors d'une sauvegarde à des fins d'utilisation interne et de la transmission à une application de sauvegarde à titre d'information. La version NDMP d'une session NDMP n'est pas définie avec cette variable.</p> |
| SÉPARATEUR_CHEMIN        | return_value    | none              | <p>Spécifie le caractère séparateur de nom de chemin d'accès.</p> <p>Ce caractère dépend du système de fichiers à sauvegarder. Pour ONTAP, le caractère "/" est attribué à cette variable. Le serveur NDMP définit cette variable avant de démarrer une opération de sauvegarde sur bande.</p>                                                                                                                 |
| TYPE                     | dump ou smtape  | dump              | Indique le type de sauvegarde pris en charge pour effectuer des opérations de sauvegarde et de restauration sur bande.                                                                                                                                                                                                                                                                                         |
| PROLIXE                  | Y ou N          | N                 | Augmente les messages du journal lors de l'exécution d'une opération de sauvegarde sur bande ou de restauration.                                                                                                                                                                                                                                                                                               |

## Variables d'environnement prises en charge pour dump

| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------|-----------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ACL_START                | return_only     | none              | <p>Créée par l'opération de sauvegarde, la variable ACL_START est une valeur de décalage utilisée par une opération de restauration à accès direct ou de sauvegarde NDMP redémarrable.</p> <p>La valeur de décalage est le décalage d'octet dans le fichier de vidage où les données ACL (Pass V) commencent et sont renvoyées à la fin d'une sauvegarde. Pour qu'une opération de restauration d'accès direct restaure correctement les données sauvegardées, la valeur ACL_START doit être transmise à l'opération de restauration lorsqu'elle démarre. Une opération de sauvegarde NDMP redémarrable utilise la valeur ACL_START pour communiquer à l'application de sauvegarde où la partie non redémarrable du flux de sauvegarde commence.</p> |



| Variable d'environnement | Valeurs valides            | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|----------------------------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DATE_DE_BASE             | 0, -1, ou DUMP_DATE valeur | -1                | <p>Spécifie la date de début des sauvegardes incrémentielles.</p> <p>Lorsqu'il est réglé sur -1, LE spécificateur incrémentiel BASE_DATE est désactivé. Lorsqu'il est réglé sur 0 sur une sauvegarde de niveau 0, les sauvegardes incrémentielles sont activées. Après la sauvegarde initiale, la valeur de la variable DUMP_DATE de la sauvegarde incrémentielle précédente est affectée à la variable BASE_DATE.</p> <p>Ces variables constituent une alternative aux sauvegardes incrémentielles BASÉES SUR LE NIVEAU/MISE À JOUR.</p> |
| DIRECTE                  | Y ou N                     | N                 | <p>Indique qu'une restauration doit être envoyée rapidement vers l'emplacement de la bande sur lequel se trouvent les données du fichier au lieu d'analyser la bande entière.</p> <p>Pour que la restauration puisse fonctionner, l'application de sauvegarde doit fournir des informations de positionnement. Si cette variable est définie sur Y, l'application de sauvegarde indique les noms de fichier ou de répertoire et les informations de positionnement.</p>                                                                   |

| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|-----------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NOM_DMP                  | string          | none              | <p>Indique le nom d'une sauvegarde de plusieurs sous-arborescences.</p> <p>Cette variable est obligatoire pour les sauvegardes de plusieurs sous-arborescences.</p>                                                                                                                                                                                                                                                                                                                                                             |
| DUMP_DATE                | return_value    | none              | <p>Vous ne modifiez pas cette variable directement. Elle est créée par la sauvegarde si la variable BASE_DATE est définie sur une valeur autre que -1.</p> <p>La variable DUMP_DATE est dérivée par la préattente de la valeur de niveau 32 bits vers une valeur de temps de 32 bits calculée par le logiciel dump. Le niveau est incrémenté à partir de la valeur du dernier niveau passée dans la variable BASE_DATE. La valeur obtenue est utilisée comme valeur BASE_DATE sur une sauvegarde incrémentielle ultérieure.</p> |


| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|-----------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ENHANCED_DAR_ENABLED     | Y ou N          | N                 | <p>Indique si la fonctionnalité DAR améliorée est activée. La fonctionnalité DAR améliorée prend en charge les fichiers de DAR et DAR avec les flux NT. Elle permet d'améliorer les performances.</p> <p>La DAR améliorée pendant la restauration n'est possible que si les conditions suivantes sont remplies :</p> <ul style="list-style-type: none"> <li>• ONTAP prend en charge les applications de DAR optimisées.</li> <li>• L'historique des fichiers est activé (HIST=y) pendant la sauvegarde.</li> <li>• Le <code>ndmpd.offset_map.enable</code> l'option est définie sur <code>on</code>.</li> <li>• LA variable <code>ENHANCED_DAR_ENABLED</code> est définie sur <code>Y</code> pendant la restauration.</li> </ul> |

| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|-----------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EXCLUDE                  | pattern_string  | none              | <p>Spécifie les fichiers ou les répertoires qui sont exclus lors de la sauvegarde des données.</p> <p>La liste d'exclusion est une liste séparée par des virgules de noms de fichier ou de répertoire. Si le nom d'un fichier ou d'un répertoire correspond à l'un des noms de la liste, il est exclu de la sauvegarde.</p> <p>Les règles suivantes s'appliquent lors de la spécification de noms dans la liste d'exclusion :</p> <ul style="list-style-type: none"> <li>• Le nom exact du fichier ou répertoire doit être utilisé.</li> <li>• L'astérisque (*), caractère générique, doit être le premier ou le dernier caractère de la chaîne.</li> </ul> <p>Chaque chaîne peut comporter jusqu'à deux astérisques.</p> <ul style="list-style-type: none"> <li>• Une virgule dans un fichier ou un nom de répertoire doit être précédée d'une barre oblique inverse.</li> <li>• La liste d'exclusion peut contenir jusqu'à 32 noms.</li> </ul> |
| 3106                     |                 |                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------|-----------------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EXTRAIRE                 | Y, N, ou E      | N                 | <p>Indique que les sous-arborescences d'un ensemble de données sauvegardées doivent être restaurées.</p> <p>L'application de sauvegarde spécifie les noms des sous-arborescences à extraire. Si un fichier spécifié correspond à un répertoire dont le contenu a été sauvegardé, le répertoire est extrait de façon récursive.</p> <p>Pour renommer un fichier, un répertoire ou un qtree pendant la restauration sans utiliser DAR, vous devez définir la variable d'environnement D'EXTRACTION sur E.</p> |
| EXTRAIRE_ACL             | Y ou N          | Y                 | <p>Spécifie que les listes de contrôle d'accès du fichier sauvegardé sont restaurées lors d'une opération de restauration.</p> <p>La valeur par défaut est de restaurer les listes de contrôle d'accès lors de la restauration des données, à l'exception de DDARS (DIRECT=y).</p>                                                                                                                                                                                                                          |

| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------|-----------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DE FORCE                 | Y ou N          | N                 | <p>Détermine si l'opération de restauration doit vérifier l'espace du volume et la disponibilité des inode sur le volume de destination.</p> <p>Réglage de cette variable sur Y provoque l'opération de restauration pour ignorer les vérifications de l'espace volume et de la disponibilité d'inode sur le chemin de destination.</p> <p>Si un espace volume suffisant ou des inodes ne sont pas disponibles sur le volume de destination, l'opération de restauration récupère autant de données que l'espace du volume de destination et la disponibilité d'inodes. L'opération de restauration s'arrête lorsque l'espace de volume ou les inodes ne sont pas disponibles.</p> |

| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------|-----------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HIST                     | Y ou N          | N                 | <p>Indique que les informations de l'historique des fichiers sont envoyées à l'application de sauvegarde.</p> <p>La plupart des applications de sauvegarde commerciales définissent la variable HIST sur Y. Si vous voulez augmenter la vitesse d'une opération de sauvegarde ou si vous voulez résoudre un problème avec la collecte de l'historique de fichiers, vous pouvez définir cette variable sur N.</p> <div>  <p>Vous ne devez pas définir la variable HIST sur Y si l'application de sauvegarde ne prend pas en charge l'historique des fichiers.</p> </div> |

| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|-----------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGNORE_CTIME             | Y ou N          | N                 | <p>Spécifie qu'un fichier n'est pas sauvegardé de façon incrémentielle si seule sa valeur de temps de restauration a changé depuis la sauvegarde incrémentielle précédente.</p> <p>Certaines applications, telles que les logiciels d'analyse antivirus, modifient la valeur de temps de lecture d'un fichier au sein de l'inode, même si le fichier ou ses attributs n'ont pas changé. Par conséquent, une sauvegarde incrémentielle peut sauvegarder des fichiers qui n'ont pas été modifiés. Le IGNORE_CTIME variable ne doit être spécifiée que si les sauvegardes incrémentielles prennent une quantité de temps ou d'espace inacceptable car la valeur de temps de ctime a été modifiée.</p> <div>  <p>Le NDMP dump jeux de commandes IGNORE_CTIME à false par défaut. Réglage sur true peut entraîner la perte de données suivante :</p> <ol style="list-style-type: none"> <li>Si IGNORE_CTIME est défini sur vrai</li> </ol> </div> |
| 3110                     |                 |                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |




| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------|-----------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGNORE_QTREES            | Y ou N          | N                 | Spécifie que l'opération de restauration ne restaure pas les informations qtree à partir de qtrees sauvegardés.                                                                                                                                                                                                                                                                                                                                                                             |
| NIVEAU                   | 0-31            | 0                 | <p>Spécifie le niveau de sauvegarde.</p> <p>Le niveau 0 copie l'ensemble du jeu de données. Les niveaux de sauvegarde incrémentielle, spécifiés par les valeurs supérieures à 0, copient tous les fichiers (nouveaux ou modifiés) depuis la dernière sauvegarde incrémentielle. Par exemple, un niveau 1 sauvegarde les fichiers nouveaux ou modifiés depuis la sauvegarde de niveau 0, un niveau 2 sauvegarde les fichiers nouveaux ou modifiés depuis la sauvegarde de niveau 1, etc.</p> |
| LISTE                    | Y ou N          | N                 | Répertorie les noms de fichiers sauvegardés et les numéros d'inode sans restaurer les données.                                                                                                                                                                                                                                                                                                                                                                                              |
| LISTE_QTREE              | Y ou N          | N                 | Le répertoire les qtrees sauvegardés sans réellement restaurer les données.                                                                                                                                                                                                                                                                                                                                                                                                                 |

qui sont déplacés via des qtrees sur la source lors de la restauration

incrémentielle.

| Variable d'environnement     | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|-----------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NOMS_DE_SOUS-ARBRE_MULTIPLES | string          | none              | <p>Indique que la sauvegarde est une sauvegarde à plusieurs sous-arborescences.</p> <p>Plusieurs sous-arborescences sont spécifiées dans la chaîne, qui est une liste de noms de sous-arborescences séparées par une nouvelle ligne et comportant des valeurs NULL. Les sous-arbres sont spécifiés par des noms de chemin par rapport à leur répertoire racine commun, qui doivent être spécifiés comme dernier élément de la liste.</p> <p>Si vous utilisez cette variable, vous devez également utiliser la variable DMP_NAME.</p> |
| NDMP_UNICODE_FH              | Y ou N          | N                 | <p>Indique qu'un nom Unicode est inclus en plus du nom NFS du fichier dans les informations de l'historique des fichiers.</p> <p>Cette option n'est pas utilisée par la plupart des applications de sauvegarde et ne doit pas être définie sauf si l'application de sauvegarde est conçue pour recevoir ces noms de fichiers supplémentaires. La variable HIST doit également être définie.</p>                                                                                                                                      |

| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------|-----------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NO_ACL                   | Y ou N          | N                 | Spécifie que les listes de contrôle d'accès ne doivent pas être copiées lors de la sauvegarde des données.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| NON_QUOTA_TREE           | Y ou N          | N                 | <p>Spécifie que les fichiers et les répertoires des qtrees doivent être ignorés lors de la sauvegarde des données.</p> <p>Lorsqu'il est réglé sur Y, Les éléments dans les qtrees du jeu de données spécifié par la variable DE SYSTÈME DE FICHIERS ne sont pas sauvegardés. Cette variable n'a un effet que si la variable FILESYSTEM spécifie un volume entier. La variable NON_QUOTA_TREE fonctionne uniquement sur une sauvegarde de niveau 0 et ne fonctionne pas si LA variable MULTI_SUBTREE_NAMES est spécifiée.</p> <div>  <p>Les fichiers ou les répertoires spécifiés à exclure pour la sauvegarde ne sont pas exclus si vous définissez NON_QUOTA_TREE sur Y simultanément.</p> </div> |

| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                       |
|--------------------------|-----------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| NON WRITE                | Y ou N          | N                 | <p>Spécifie que l'opération de restauration ne doit pas écrire de données sur le disque.</p> <p>Cette variable est utilisée pour le débogage.</p> |

| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------|-----------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RÉCURSIF                 | Y ou N          | Y                 | <p>Indique que les entrées de répertoire lors d'une restauration DAR sont développées.</p> <p>Les variables d'environnement DIRECTES et OPTIMISÉES_DAR_ENABLED doivent être activées (définies sur Y) également. Si la variable RÉCURSIVE est désactivée (définie sur N), seules les autorisations et listes de contrôle d'accès de tous les répertoires du chemin source d'origine sont restaurées à partir de la bande, et non du contenu des répertoires. Si la variable RÉCURSIVE est définie sur N Ou LA variable RECOVER_FULL_PATHS est définie sur Y, le chemin de récupération doit se terminer par le chemin d'origine.</p> |
|                          |                 |                   | 3115                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|-----------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RECOVER_FULL_PATHS       | Y ou N          | N                 | Indique que le chemin de récupération complet aura ses autorisations et listes de contrôle d'accès restaurées après le DAR.<br><br>DIRECT et ENHANCED_DAR_ENABLED doivent être activés (défini sur Y) également. Si LE paramètre RECOVER_FULL_PATHS est défini sur Y, le chemin de récupération doit se terminer par le chemin d'origine. Si des répertoires existent déjà sur le volume de destination, leurs autorisations et listes de contrôle d'accès ne seront pas restaurées à partir d'une bande. |
| MISE À JOUR              | Y ou N          | Y                 | Met à jour les informations de métadonnées pour permettre une sauvegarde incrémentielle BASÉE SUR LE NIVEAU.                                                                                                                                                                                                                                                                                                                                                                                              |

#### Variables d'environnement prises en charge par SMTape

trouvent dans  
foo/dir1/deepdir/my  
file:

- /foo
- /foo/dir
- /foo/dir1/deepdir
- /foo/dir1/deepdir/myfile

Les chemins de  
récupération suivants ne  
sont pas valides :

- /foo
- /foo/dir
- /foo/dir1/myfile

- 

- /foo/dir2/myfile

| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|-----------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DATE_DE_BASE             | DUMP_DATE       | -1                | <p>Spécifie la date de début des sauvegardes incrémentielles.</p> <div> <p>`BASE_DATE` Est une représentation de chaîne des identificateurs d'instantané de référence. À l'aide du `BASE_DATE` String, SMTape localise la copie Snapshot de référence.</p> <p>`BASE_DATE` n'est pas requis pour les sauvegardes de base. Pour une sauvegarde incrémentielle, la valeur de `DUMP_DATE` variable de la sauvegarde de base ou incrémentielle précédente est attribuée à `BASE_DATE` variable.</p> <p>L'application de sauvegarde affecte DUMP_DATE Valeur d'une copie de base SMTape précédente ou sauvegarde incrémentielle.</p> </div> |



| Variable d'environnement | Valeurs valides | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------|-----------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DUMP_DATE                | return_value    | none              | <p>À la fin d'une sauvegarde SMTape, DUMP_DATE contient un identifiant de chaîne qui identifie la copie Snapshot utilisée pour cette sauvegarde. Cette copie Snapshot peut être utilisée comme copie Snapshot de référence pour une sauvegarde incrémentielle ultérieure.</p> <p>La valeur résultante de DUMP_DATE est utilisée comme valeur BASE_DATE pour les sauvegardes incrémentielles suivantes.</p> |
| SMTAPE_BACKUP_SET_ID     | string          | none              | <p>Identifie la séquence des sauvegardes incrémentielles associées à la sauvegarde de base.</p> <p>L'ID du jeu de sauvegardes est un ID unique de 128 bits généré au cours d'une sauvegarde de base. L'application de sauvegarde attribue cet ID en tant qu'entrée au SMTAPE_BACKUP_SET_ID variable pendant une sauvegarde incrémentielle.</p>                                                             |

| Variable d'environnement   | Valeurs valides                                       | Valeur par défaut | Description                                                                                                                                                                                                                                                                                                                          |
|----------------------------|-------------------------------------------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SMTAPE_SNAPSHOT_N<br>AME   | Toute copie Snapshot valide disponible dans le volume | Invalid           | <p>Lorsque la variable SMTAPE_SNAPSHOT_N AME est définie sur une copie Snapshot, cette copie Snapshot et ses anciennes copies Snapshot sont sauvegardées sur bande.</p> <p>Pour la sauvegarde incrémentielle, cette variable spécifie la copie Snapshot incrémentielle. LA variable BASE_DATE fournit la copie Snapshot de base.</p> |
| SMTAPE_DELETE_SNA<br>PSHOT | Y ou N                                                | N                 | <p>Pour une copie Snapshot créée automatiquement par SMTape, lorsque la variable SMTAPE_DELETE_SNA PSHOT est définie sur Y, Puis, une fois l'opération de sauvegarde terminée, SMTape supprime cette copie Snapshot.</p> <p>Cependant, une copie Snapshot créée par l'application de sauvegarde ne sera pas supprimée.</p>           |
| SMTAPE_BREAK_MIRR<br>OR    | Y ou N                                                | N                 | <p>Lorsque la variable SMTAPE_BREAK_MIRROR est définie sur Y, le volume de type DP est remplacé par un RW volume après une restauration réussie.</p>                                                                                                                                                                                 |

### Topologies de sauvegarde sur bande NDMP courantes

NDMP prend en charge un certain nombre de topologies et de configurations entre les applications de sauvegarde et les systèmes de stockage ou d'autres serveurs NDMP fournissant des données (systèmes de fichiers) et des services de bande.

## Du système de stockage sur bande locale

Dans la configuration la plus simple, une application de sauvegarde sauvegarde sauvegarde sauvegarde sauvegarde des données d'un système de stockage vers un sous-système de bande connecté au système de stockage. Il existe une connexion de contrôle NDMP sur la limite du réseau. La connexion de données NDMP qui existe dans le système de stockage entre les services de données et de bande est appelée configuration locale NDMP.

## Système de stockage à bande connecté à un autre système de stockage

Une application de sauvegarde peut également sauvegarder les données d'un système de stockage vers une librairie de bandes (un changeur de moyenne taille avec un ou plusieurs lecteurs de bande) connectée à un autre système de stockage. Dans ce cas, la connexion de données NDMP entre les services de données et de bande est fournie par une connexion réseau TCP ou TCP/IPv6. Il s'agit d'une configuration NDMP à trois voies système de stockage vers stockage.

## Bibliothèque de bandes reliée système/réseau de stockage

Les bibliothèques de bandes NDMP fournissent une variante de la configuration à trois voies. Dans ce cas, la bibliothèque de bandes se connecte directement au réseau TCP/IP et communique avec l'application de sauvegarde et le système de stockage par l'intermédiaire d'un serveur NDMP interne.

## Système de stockage à serveur de données sur bande ou serveur de données à système de stockage sur bande

NDMP prend également en charge les configurations trivoies entre système de stockage à serveur de données et serveur de données à stockage, bien que ces variantes soient moins largement déployées. Le système de stockage à serveur permet de sauvegarder les données du système de stockage dans une bibliothèque de bandes reliée à l'hôte de l'application de sauvegarde ou à un autre système de serveur de données. La configuration du système de serveur à stockage permet de sauvegarder les données du serveur dans une bibliothèque de bandes reliée au système de stockage.

## Méthodes d'authentification NDMP prises en charge

Vous pouvez spécifier une méthode d'authentification pour autoriser les requêtes de connexion NDMP. ONTAP prend en charge deux méthodes d'authentification de l'accès NDMP à un système de stockage : le texte brut et les défis.

En mode node-scoped NDMP, challenge et texte sont tous deux activés par défaut. Toutefois, vous ne pouvez pas désactiver le défi. Vous pouvez activer et désactiver le texte en texte brut. Dans la méthode d'authentification en texte clair, le mot de passe de connexion est transmis en texte clair.

En mode SVM (Storage Virtual machine)-scoped NDMP, la méthode d'authentification est par défaut un défi. Contrairement au mode node-scoped NDMP, dans ce mode, vous pouvez activer et désactiver à la fois les méthodes d'authentification en texte clair et les méthodes d'authentification en question.

## Informations associées

[Authentification de l'utilisateur en mode node-scoped NDMP](#)

[Authentification de l'utilisateur en mode SVM-scoped NDMP](#)

## Extensions NDMP prises en charge par ONTAP

NDMP v4 fournit un mécanisme de création d'extensions de protocole NDMP v4 sans modifier le protocole NDMP v4 principal. Vous devez connaître les extensions NDMP v4

prises en charge par ONTAP.

Les extensions NDMP v4 suivantes sont prises en charge par ONTAP :

- Sauvegarde « cluster Aware Backup » (CAB)



Cette extension n'est supportée que en mode SVM-scoped NDMP.

- Extension d'adresse de connexion (CAE) pour la prise en charge d'IPv6
- Classe d'extension 0x2050

Cette extension prend en charge les opérations de sauvegarde redémarrables et les extensions de gestion Snapshot.



Le NDMP\_SNAP\_RECOVER Message, qui fait partie de Snapshot Management Extensions, sert à lancer une opération de restauration et à transférer les données récupérées depuis une copie Snapshot locale vers un emplacement local du système de fichiers. Dans ONTAP, ce message permet de restaurer des volumes et des fichiers standard uniquement.

Le NDMP\_SNAP\_DIR\_LIST Message vous permet de parcourir les copies Snapshot d'un volume. Si une opération sans interruption a lieu pendant une opération de navigation, l'application de sauvegarde doit recommencer l'opération de navigation.

### **Extension de sauvegarde NDMP redémarrable pour un dump pris en charge par ONTAP**

Vous pouvez utiliser la fonctionnalité RBE (NDMP restartable Backup extension) pour redémarrer une sauvegarde à partir d'un point de contrôle connu dans le flux de données avant la panne.

### **Qu'est-ce que la fonctionnalité DAR améliorée**

Vous pouvez utiliser la fonctionnalité de récupération d'accès direct (DAR) améliorée pour les DAR et DAR de fichiers et les flux NT. Par défaut, la fonctionnalité améliorée DAR est activée.

L'activation de la fonctionnalité DAR améliorée peut avoir un impact sur les performances de sauvegarde car une carte de décalage doit être créée et écrite sur bande. Vous pouvez activer ou désactiver Enhanced DAR dans les modes node-scoped et SVM (Storage Virtual machine)-scoped NDMP.

### **Limite d'évolutivité pour les sessions NDMP**

Vous devez connaître le nombre maximal de sessions NDMP qui peuvent être établies simultanément sur les systèmes de stockage de différentes capacités de mémoire système. Ce nombre maximum dépend de la mémoire système d'un système de stockage.

Les limites mentionnées dans le tableau suivant sont destinées au serveur NDMP. Les limites mentionnées dans la section «limites de capacités pour les sessions de sauvegarde et de restauration de vidage» sont pour la session de sauvegarde et de restauration.

| Mémoire système d'un système de stockage         | Nombre maximal de sessions NDMP |
|--------------------------------------------------|---------------------------------|
| Moins de 16 Go                                   | 8                               |
| Supérieur ou égal à 16 Go mais inférieur à 24 Go | 20                              |
| Supérieur ou égal à 24 Go                        | 36                              |

Vous pouvez obtenir la mémoire système de votre système de stockage à l'aide du `sysconfig -a` commande (disponible via le nodeshell). Pour plus d'informations sur l'utilisation de cette commande, consultez les pages de manuels.

## À propos de NDMP pour volumes FlexGroup

Depuis ONTAP 9.7, NDMP est pris en charge sur les volumes FlexGroup.

Depuis ONTAP 9.7, la commande `ndmpcopy` est prise en charge pour le transfert de données entre les volumes FlexVol et FlexGroup.

Si vous restaurez ONTAP 9.7 vers une version antérieure, les informations de transfert incrémentiel des transferts précédents ne sont pas conservées. Par conséquent, vous devez effectuer une copie de base après le rétablissement.

Les fonctionnalités NDMP suivantes sont prises en charge sur les volumes FlexGroup depuis ONTAP 9.8 :

- Le message `NDMP_SNAP_RECOVER` de la classe d'extension `0x2050` peut être utilisé pour récupérer des fichiers individuels dans un volume FlexGroup.
- L'extension de sauvegarde NDMP redémarrable (RBE) est prise en charge pour les volumes FlexGroup.
- Les variables d'environnement `EXCLUDE` et `MULTI_SUBTREE_NAMES` sont prises en charge pour les volumes FlexGroup.

## À propos de NDMP avec les volumes SnapLock

La création de plusieurs copies de données réglementées vous permet de bénéficier de scénarios de restauration redondants. En outre, grâce à ce processus, vous pouvez conserver les caractéristiques WORM (Write Once, Read Many) des fichiers source sur un volume SnapLock.

Les attributs WORM des fichiers du volume SnapLock sont conservés lors de la sauvegarde, de la restauration et de la copie des données. Toutefois, les attributs WORM ne sont appliqués que lors de la restauration vers un volume SnapLock. Si une sauvegarde d'un volume SnapLock est restaurée dans un volume autre qu'un volume SnapLock, les attributs WORM sont conservés, mais ils sont ignorés et ne sont pas appliqués par ONTAP.

## Gérer le mode node-scoped NDMP pour les volumes FlexVol

**Manage node-scoped NDMP mode for FlexVol volumes overview**

Vous pouvez gérer NDMP au niveau nœud à l’aide des options et commandes NDMP. Vous pouvez modifier les options NDMP en utilisant le `options` commande. Vous devez utiliser les identifiants spécifiques à NDMP pour accéder à un système de stockage afin d’effectuer des opérations de sauvegarde sur bande et de restauration.

Pour plus d’informations sur le `options` commandes, consultez les pages de manuels.

**Informations associées**

[Commandes permettant de gérer le mode node-scoped NDMP](#)

[Le mode node-scoped NDMP est](#)

**Commandes permettant de gérer le mode node-scoped NDMP**

Vous pouvez utiliser le `system services ndmp` Commandes permettant de gérer NDMP au niveau des nœuds. Certaines de ces commandes sont obsolètes et seront supprimées dans une prochaine version majeure.

Vous ne pouvez utiliser les commandes NDMP suivantes qu’au niveau de privilège avancé :

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`
- `system services ndmp log start`
- `system services ndmp log stop`

| Les fonctions que vous recherchez...      | Utilisez cette commande...                       |
|-------------------------------------------|--------------------------------------------------|
| Activez le service NDMP                   | <code>system services ndmp on*</code>            |
| Désactiver le service NDMP                | <code>system services ndmp off*</code>           |
| Affiche la configuration NDMP             | <code>system services ndmp show*</code>          |
| Modifier la configuration NDMP            | <code>system services ndmp modify*</code>        |
| Afficher la version NDMP par défaut       | <code>system services ndmp version*</code>       |
| Afficher la configuration du service NDMP | <code>system services ndmp service show</code>   |
| Modifier la configuration du service NDMP | <code>system services ndmp service modify</code> |
| Affiche toutes les sessions NDMP          | <code>system services ndmp status</code>         |

| Les fonctions que vous recherchez...                             | Utilisez cette commande...                                |
|------------------------------------------------------------------|-----------------------------------------------------------|
| Affiche des informations détaillées sur toutes les sessions NDMP | <code>system services ndmp probe</code>                   |
| Mettre fin à la session NDMP spécifiée                           | <code>system services ndmp kill</code>                    |
| Mettre fin à toutes les sessions NDMP                            | <code>system services ndmp kill-all</code>                |
| Modifier le mot de passe NDMP                                    | <code>system services ndmp password*</code>               |
| Activer le mode node-scoped NDMP                                 | <code>system services ndmp node-scope-mode on*</code>     |
| Désactiver le mode node-scoped NDMP                              | <code>system services ndmp node-scope-mode off*</code>    |
| Afficher l'état du mode node-scoped NDMP                         | <code>system services ndmp node-scope-mode status*</code> |
| Arrêtez toutes les sessions NDMP avec force                      | <code>system services ndmp service terminate</code>       |
| Démarrez le démon du service NDMP                                | <code>system services ndmp service start</code>           |
| Arrêtez le démon du service NDMP                                 | <code>system services ndmp service stop</code>            |
| Démarrez la connexion pour la session NDMP spécifiée             | <code>system services ndmp log start*</code>              |
| Arrêter la journalisation de la session NDMP spécifiée           | <code>system services ndmp log stop*</code>               |

- Ces commandes sont obsolètes et seront supprimées dans une prochaine version majeure.

Pour plus d'informations sur ces commandes, consultez les pages de manuels pour le `system services ndmp` commandes.

### Authentification de l'utilisateur en mode node-scoped NDMP

En mode node-scoped NDMP, il faut utiliser des identifiants spécifiques NDMP pour accéder à un système de stockage afin de réaliser des opérations de backup sur bande et restore.

L'ID utilisateur par défaut est « root ». Avant d'utiliser NDMP sur un nœud, veuillez à modifier le mot de passe NDMP par défaut associé à l'utilisateur NDMP. Vous pouvez également modifier l'ID utilisateur NDMP par défaut.

### Informations associées





| Les fonctions que vous recherchez...                             | Utilisez cette commande...                                                                                               |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Désactiver le service NDMP                                       | <code>vserver services ndmp off</code>                                                                                   |
| Affiche la configuration NDMP                                    | <code>vserver services ndmp show</code>                                                                                  |
| Modifier la configuration NDMP                                   | <code>vserver services ndmp modify</code>                                                                                |
| Affiche la version NDMP par défaut                               | <code>vserver services ndmp version</code>                                                                               |
| Affiche toutes les sessions NDMP                                 | <code>vserver services ndmp status</code>                                                                                |
| Affiche des informations détaillées sur toutes les sessions NDMP | <code>vserver services ndmp probe</code>                                                                                 |
| Mettre fin à une session NDMP spécifiée                          | <code>vserver services ndmp kill</code>                                                                                  |
| Mettre fin à toutes les sessions NDMP                            | <code>vserver services ndmp kill-all</code>                                                                              |
| Générer le mot de passe NDMP                                     | <code>vserver services ndmp generate-password</code>                                                                     |
| Affiche l'état de l'extension NDMP                               | <code>vserver services ndmp extensions show</code><br><br>Cette commande est disponible au niveau de privilège avancé.   |
| Modifier (activer ou désactiver) l'état de l'extension NDMP      | <code>vserver services ndmp extensions modify</code><br><br>Cette commande est disponible au niveau de privilège avancé. |
| Démarrez la connexion pour la session NDMP spécifiée             | <code>vserver services ndmp log start</code><br><br>Cette commande est disponible au niveau de privilège avancé.         |
| Arrêter la journalisation de la session NDMP spécifiée           | <code>vserver services ndmp log stop</code><br><br>Cette commande est disponible au niveau de privilège avancé.          |

Pour plus d'informations sur ces commandes, consultez les pages de manuels pour le `vserver services ndmp` commandes.

## Rôle de l'extension Cluster Aware Backup

CAB (Cluster Aware Backup) est une extension de protocole NDMP v4. Cette extension permet au serveur NDMP d'établir une connexion de données sur un nœud qui possède un volume. Cela permet également à l'application de sauvegarde de déterminer si les volumes et les lecteurs de bande sont situés sur le même nœud d'un cluster.

Pour permettre au serveur NDMP d'identifier le nœud qui possède un volume et d'établir une connexion de données sur ce nœud, l'application de backup doit prendre en charge l'extension CAB. L'extension CAB requiert que l'application de backup informe le serveur NDMP au sujet du volume à sauvegarder ou à restaurer avant d'établir la connexion de données. Cela permet au serveur NDMP de déterminer le nœud qui héberge le volume et d'établir de manière appropriée la connexion de données.

Avec l'extension CAB prise en charge par l'application de sauvegarde, le serveur NDMP fournit des informations d'affinité sur les volumes et les lecteurs de bande. Avec ces informations d'affinité, l'application de sauvegarde peut effectuer une sauvegarde locale au lieu d'une sauvegarde à trois voies si un volume et un périphérique de bande se trouvent sur le même nœud d'un cluster.

### Disponibilité de volumes et de bandes pour les sauvegardes et les restaurations sur différents types de LIF

Vous pouvez configurer une application de backup pour établir une connexion de contrôle NDMP sur l'un des types LIF d'un cluster. En mode NDMP (SVM)-scoped, il est possible de déterminer la disponibilité des volumes et des dispositifs à bandes pour les opérations de backup et restore, selon ces types de LIF et le statut de l'extension CAB.

Les tableaux suivants montrent la disponibilité des volumes et des dispositifs à bande pour les types LIF de connexion de contrôle NDMP et le statut de l'extension CAB :

#### Disponibilité des volumes et des dispositifs à bande lorsque l'extension CAB n'est pas prise en charge par l'application de sauvegarde

| Type LIF de connexion de contrôle NDMP | Volumes disponibles pour la sauvegarde ou la restauration                                    | Périphériques à bande disponibles pour la sauvegarde ou la restauration     |
|----------------------------------------|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| LIF node-management                    | Tous volumes hébergés par un nœud                                                            | Dispositifs de bande connectés au nœud hébergeant la LIF de node-management |
| LIF de données                         | Seuls les volumes qui appartiennent au SVM hébergé par un nœud qui héberge la LIF de données | Aucune                                                                      |
| LIF Cluster-management                 | Tous les volumes hébergés par un nœud qui héberge la LIF de cluster-management               | Aucune                                                                      |

| Type LIF de connexion de contrôle NDMP | Volumes disponibles pour la sauvegarde ou la restauration             | Périphériques à bande disponibles pour la sauvegarde ou la restauration |
|----------------------------------------|-----------------------------------------------------------------------|-------------------------------------------------------------------------|
| FRV InterCluster                       | Tous les volumes hébergés par un nœud qui héberge le LIF intercluster | Périphériques de bande connectés au nœud hébergeant le LIF intercluster |

**Disponibilité des volumes et des dispositifs à bande lorsque l'extension CAB est prise en charge par l'application de sauvegarde**

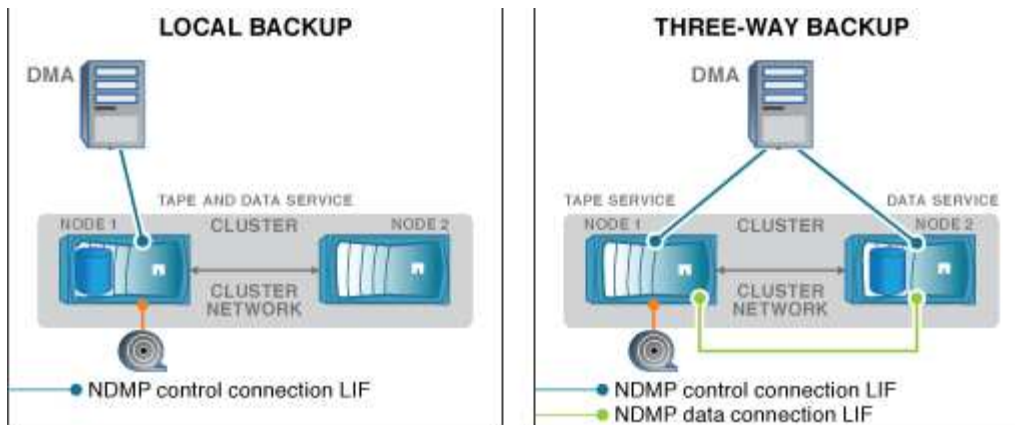
| Type LIF de connexion de contrôle NDMP | Volumes disponibles pour la sauvegarde ou la restauration               | Périphériques à bande disponibles pour la sauvegarde ou la restauration     |
|----------------------------------------|-------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| LIF node-management                    | Tous volumes hébergés par un nœud                                       | Dispositifs de bande connectés au nœud hébergeant la LIF de node-management |
| LIF de données                         | Tous les volumes qui appartiennent au SVM qui héberge la LIF de données | Aucune                                                                      |
| LIF Cluster-management                 | Tous les volumes du cluster                                             | Tous les périphériques de bande du cluster                                  |
| FRV InterCluster                       | Tous les volumes du cluster                                             | Tous les périphériques de bande du cluster                                  |

### Quelles sont les informations d'affinité

Avec l'application de sauvegarde orientée CAB, le serveur NDMP fournit des informations d'emplacement uniques sur les volumes et les lecteurs de bande. Avec ces informations d'affinité, l'application de sauvegarde peut effectuer une sauvegarde locale au lieu d'une sauvegarde à trois voies si un volume et un périphérique de bande partagent la même affinité.

Si la connexion de contrôle NDMP est établie sur une LIF de node-management, LIF de cluster management, Ou d'une LIF intercluster, l'application de sauvegarde peut utiliser les informations d'affinité pour déterminer si un volume et une unité de bande sont situés sur le même nœud, puis effectuer une opération de sauvegarde ou de restauration locale ou à trois voies. Si la connexion de contrôle NDMP est établie sur une LIF de données, l'application de sauvegarde effectue toujours une sauvegarde à trois voies.

### Sauvegarde NDMP locale et sauvegarde NDMP à trois voies



À l'aide des informations d'affinité concernant les volumes et les périphériques de bande, le DMA (application de sauvegarde) effectue une sauvegarde NDMP locale sur le volume et le périphérique de bande situés sur le nœud 1 du cluster. Si le volume passe du nœud 1 au nœud 2, les informations d'affinité concernant le volume et le périphérique de bande changent. Par conséquent, pour une sauvegarde ultérieure, le DMA effectue une opération de sauvegarde NDMP à trois voies. Cela assure la continuité de la stratégie de sauvegarde pour le volume, quel que soit le nœud vers lequel le volume est déplacé.

### Informations associées

[Rôle de l'extension Cluster Aware Backup](#)

### NDMP Server prend en charge les connexions de contrôle sécurisé en mode SVM-scoped

Une connexion de contrôle sécurisée peut être établie entre l'application de gestion des données (DMA) et le serveur NDMP en utilisant des sockets sécurisés (SSL/TLS) comme mécanisme de communication. Cette communication SSL est basée sur les certificats du serveur. Le serveur NDMP écoute sur le port 30000 (attribué par IANA au service « ndmps »).

Une fois la connexion établie à partir du client sur ce port, la liaison SSL standard s'ensuit lorsque le serveur présente le certificat au client. Lorsque le client accepte le certificat, l'établissement de liaison SSL est terminé. Une fois ce processus terminé, toute la communication entre le client et le serveur est cryptée. Le workflow du protocole NDMP reste identique à celui précédent. La connexion NDMP sécurisée ne nécessite qu'une authentification par certificat côté serveur. Un DMA peut choisir d'établir une connexion soit en se connectant au service NDMP sécurisé soit au service NDMP standard.

Par défaut, le service NDMP sécurisé est désactivé pour les machines virtuelles de stockage (SVM). Vous pouvez activer ou désactiver le service NDMP sécurisé sur une SVM donnée en utilisant le `vserver services ndmp modify -vserver vserver -is-secure-control-connection-enabled [true|false]` commande.

### Types de connexions de données NDMP

En mode SVM (Storage Virtual machine)-scoped NDMP, les types de connexions de données NDMP pris en charge dépendent du type LIF de « NDMP control connection » et du statut de l'extension CAB. Ce type de connexion de données NDMP indique si vous pouvez effectuer une opération de sauvegarde ou de restauration NDMP locale ou à trois voies.

Vous pouvez effectuer une sauvegarde ou une restauration NDMP à trois voies sur un réseau TCP ou TCP/IPv6. Les tableaux suivants présentent les types de connexions de données NDMP, basés sur le type LIF de connexion de contrôle NDMP et le statut de l'extension DE CAB.

**Type de connexion de données NDMP lorsque l'extension CAB est prise en charge par l'application de backup**

| Type LIF de connexion de contrôle NDMP | Type de connexion de données NDMP |
|----------------------------------------|-----------------------------------|
| LIF node-management                    | LOCAL, TCP, TCP/IPV6              |
| LIF de données                         | TCP, TCP/IPv6                     |
| LIF Cluster-management                 | LOCAL, TCP, TCP/IPV6              |
| FRV InterCluster                       | LOCAL, TCP, TCP/IPV6              |

**Type de connexion de données NDMP lorsque l'extension CAB n'est pas prise en charge par l'application de backup**

| Type LIF de connexion de contrôle NDMP | Type de connexion de données NDMP |
|----------------------------------------|-----------------------------------|
| LIF node-management                    | LOCAL, TCP, TCP/IPV6              |
| LIF de données                         | TCP, TCP/IPv6                     |
| LIF Cluster-management                 | TCP, TCP/IPv6                     |
| FRV InterCluster                       | LOCAL, TCP, TCP/IPV6              |

**Informations associées**

[Rôle de l'extension Cluster Aware Backup](#)

["Gestion du réseau"](#)

**Authentification de l'utilisateur en mode SVM-scoped NDMP**

En mode SVM (Storage Virtual machine)-scoped NDMP, l'authentification utilisateur NDMP est intégrée au contrôle d'accès basé sur des rôles. Dans le contexte SVM, l'utilisateur NDMP doit avoir le rôle « vsadmin » ou « vsadmin-backup ». Dans un contexte de cluster, l'utilisateur NDMP doit avoir le rôle « admin » ou « backup ».

Outre ces rôles prédéfinis, un compte utilisateur associé à un rôle personnalisé peut également être utilisé pour l'authentification NDMP à condition que le rôle personnalisé ait le dossier « vserver services ndmp » dans son répertoire de commandes et que le niveau d'accès du dossier n'est pas « nul ». Dans ce mode, vous devez générer un mot de passe NDMP pour un compte utilisateur donné, créé par le biais du contrôle d'accès basé sur des rôles. Les utilisateurs de cluster en rôle d'administrateur ou de sauvegarde peuvent accéder à une LIF de node-management, à une LIF de cluster-management ou à un LIF intercluster. Les utilisateurs ayant un rôle vsadmin-backup ou vsadmin peuvent accéder uniquement à la LIF de données pour ce SVM. Par conséquent, selon le rôle d'un utilisateur, la disponibilité des volumes et des périphériques de bande pour les opérations de sauvegarde et de restauration varie.

Ce mode prend également en charge l'authentification des utilisateurs pour les utilisateurs NIS et LDAP. Ainsi, les utilisateurs NIS et LDAP peuvent accéder à plusieurs SVM avec un ID utilisateur et un mot de passe communs. Cependant, l'authentification NDMP ne prend pas en charge les utilisateurs Active Directory.

Dans ce mode, un compte utilisateur doit être associé à l'application SSH et à la méthode d'authentification « Mot de passe utilisateur ».

### Informations associées

[Commandes de gestion du mode SVM-scoped NDMP](#)

["Administration du système"](#)

### Générez un mot de passe spécifique NDMP pour les utilisateurs NDMP

En mode Storage Virtual machine (SVM)-scoped NDMP, vous devez générer un mot de passe pour un ID utilisateur spécifique. Le mot de passe généré est basé sur le mot de passe de connexion réel pour l'utilisateur NDMP. Si le mot de passe de connexion change, vous devez générer à nouveau le mot de passe spécifique au NDMP.

#### Étapes

1. Utilisez le `vserver services ndmp generate-password` Commande permettant de générer un mot de passe spécifique au NDMP.

Vous pouvez utiliser ce mot de passe pour toute opération NDMP actuelle ou future nécessitant la saisie d'un mot de passe.



Depuis le contexte SVM (anciennement appelé Vserver), vous pouvez générer des mots de passe NDMP pour les utilisateurs appartenant uniquement à ce SVM.

L'exemple suivant montre comment générer un mot de passe spécifique au protocole NDMP pour un ID utilisateur utilisateur1 :

```
cluster1::vserver services ndmp> generate-password -vserver vs1 -user
user1

Vserver: vs1
User: user1
Password: jWZiNt57huPOoD8d
```

2. Si vous remplacez le mot de passe par votre compte normal du système de stockage, répétez cette procédure pour obtenir votre nouveau mot de passe spécifique au NDMP.

### L'impact des opérations de sauvegarde sur bande et de restauration sur la reprise après incident en configuration MetroCluster

Vous pouvez effectuer des opérations de sauvegarde sur bande et de restauration simultanément pendant la reprise sur incident dans une configuration MetroCluster. Vous devez comprendre l'impact de ces opérations sur la reprise sur incident.

Si les opérations de sauvegarde et de restauration sur bande sont effectuées sur un volume d'SVM dans une

relation de reprise après incident, vous pouvez continuer à effectuer les opérations de sauvegarde et de restauration sur bande incrémentielles après le basculement et le rétablissement.

## À propos du moteur de dump pour les volumes FlexVol

### À propos du moteur de dump pour les volumes FlexVol

Dump est une solution de sauvegarde et de restauration basée sur des copies Snapshot de ONTAP qui vous permet de sauvegarder des fichiers et des répertoires d'une copie Snapshot sur un périphérique de bande et de restaurer les données sauvegardées sur un système de stockage.

Vous pouvez sauvegarder les données de votre système de fichiers, telles que les répertoires, les fichiers et leurs paramètres de sécurité associés, sur un périphérique de bande à l'aide de la sauvegarde dump. Vous pouvez sauvegarder un volume entier, un qtree entier ou un sous-arbre qui n'est ni un volume entier, ni un qtree entier.

Vous pouvez effectuer une sauvegarde ou une restauration de dump à l'aide d'applications de sauvegarde conformes NDMP.

Lorsque vous effectuez une sauvegarde de dump, vous pouvez spécifier la copie Snapshot à utiliser pour une sauvegarde. Si vous ne spécifiez pas de copie Snapshot pour la sauvegarde, le moteur de dump crée une copie Snapshot pour la sauvegarde. Une fois l'opération de sauvegarde terminée, le moteur de dump supprime cette copie Snapshot.

Vous pouvez effectuer des sauvegardes de niveau 0, incrémentielles ou différentielles sur bande à l'aide du moteur de vidage.



Après avoir revenir à une version antérieure à Data ONTAP 8.3, vous devez effectuer une opération de sauvegarde de base avant d'effectuer une opération de sauvegarde incrémentielle.

### Informations associées

["Mise à niveau, rétablissement ou mise à niveau vers une version antérieure"](#)

### Fonctionnement d'une sauvegarde de vidage

Une sauvegarde de vidage écrit les données du système de fichiers de disque à bande en utilisant un processus prédéfini. Vous pouvez sauvegarder un volume, un qtree ou une sous-arborescence qui n'est ni un volume entier, ni un qtree entier.

Le tableau ci-dessous décrit le processus utilisé par ONTAP pour sauvegarder l'objet indiqué par le chemin de vidage :

| Étape | Action                                                                                                                                                                                                                         |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | Pour les sauvegardes qtree complètes ou à volume complet, ONTAP traverse des répertoires pour identifier les fichiers à sauvegarder. Si vous sauvegardez un volume entier ou un qtree, ONTAP associe cette étape à la phase 2. |
| 2     | Pour une sauvegarde de volume complet ou qtree complet, ONTAP identifie les répertoires des volumes ou des qtrees à sauvegarder.                                                                                               |

| Étape | Action                                                            |
|-------|-------------------------------------------------------------------|
| 3     | ONTAP écrit les répertoires sur bande.                            |
| 4     | ONTAP écrit les fichiers sur bande.                               |
| 5     | ONTAP écrit les informations de l'ACL (le cas échéant) sur bande. |

La sauvegarde de dump utilise une copie Snapshot de vos données à des fins de sauvegarde. Par conséquent, vous n'avez pas besoin de mettre le volume hors ligne avant de lancer la sauvegarde.

La sauvegarde de dump attribue la création de chaque copie Snapshot `snapshot_for_backup.n`, où `n` est un entier commençant à 0. Chaque fois que la sauvegarde de dump crée une copie Snapshot, elle incrémente le nombre entier de 1. L'entier est réinitialisé à 0 après le redémarrage du système de stockage. Une fois l'opération de sauvegarde terminée, le moteur de dump supprime cette copie Snapshot.

Lorsque ONTAP effectue plusieurs sauvegardes de dump simultanément, le moteur de dump crée plusieurs copies Snapshot. Par exemple, si ONTAP exécute simultanément deux sauvegardes de dump, vous trouverez les copies Snapshot suivantes dans les volumes à partir desquels les données sont sauvegardées : `snapshot_for_backup.0` et `snapshot_for_backup.1`.



Lorsque vous effectuez une sauvegarde à partir d'une copie Snapshot, le moteur de dump ne crée pas de copie Snapshot supplémentaire.

### Types de données que le moteur de vidage sauvegarde

Le moteur de dump vous permet de sauvegarder les données sur bande afin d'éviter les incidents ou les perturbations sur les contrôleurs. Outre la sauvegarde d'objets de données tels que des fichiers, des répertoires, des qtrees ou des volumes entiers, le moteur de dump peut sauvegarder de nombreux types d'informations sur chaque fichier. La connaissance des types de données que le moteur de dump peut sauvegarder et des restrictions à prendre en compte peut vous aider à planifier votre approche de la reprise sur incident.

En plus de sauvegarder des données dans des fichiers, le moteur de vidage peut sauvegarder les informations suivantes sur chaque fichier, selon le cas :

- GID UNIX, UID de propriétaire et autorisations de fichier
- Heure d'accès, de création et de modification UNIX
- Type de fichier
- Taille du fichier
- Nom DOS, attributs DOS et heure de création
- Listes de contrôle d'accès (ACL) avec 1,024 entrées de contrôle d'accès (ACE)
- Informations sur les qtrees
- Chemins de liaison

Les chemins de jonction sont sauvegardés en tant que liens symboliques.



- Clones de LUN et de LUN

Vous pouvez sauvegarder un objet LUN entier ; cependant, vous ne pouvez pas sauvegarder un seul fichier dans cet objet. De la même manière, vous pouvez restaurer tout un objet LUN, mais pas un seul fichier au sein de ce dernier.



Le moteur de dump sauvegarde les clones de LUN en tant que LUN indépendantes.

- Fichiers alignés sur les machines virtuelles

La sauvegarde des fichiers alignés sur les machines virtuelles n'est pas prise en charge dans les versions antérieures à Data ONTAP 8.1.2.



Lorsqu'un clone de LUN avec snapshot est passé de Data ONTAP 7-mode à ONTAP, il devient LUN incohérent. Le moteur de vidage ne sauvegarde pas les LUN incohérentes.

Lorsque vous restaurez les données sur un volume, les E/S client sont restreintes sur les LUN en cours de restauration. La restriction de LUN est supprimée uniquement lorsque l'opération de restauration de vidage est terminée. De même, lors de l'opération de restauration de fichiers ou de LUN SnapMirror, les E/S clientes sont limitées sur les fichiers et les LUN en cours de restauration. Cette restriction est supprimée uniquement lorsque l'opération de restauration de fichier ou de LUN est terminée. Lorsqu'une sauvegarde de dump est effectuée sur un volume sur lequel une restauration de dump ou une opération de restauration de fichier unique SnapMirror ou de restauration de LUN est en cours, les fichiers ou les LUN dont les restrictions d'E/S sont présentes sur le client ne sont pas inclus dans la sauvegarde. Ces fichiers ou LUN sont inclus dans une opération de sauvegarde suivante si la restriction d'E/S du client est supprimée.



Une LUN exécutée sur Data ONTAP 8.3 et qui est sauvegardée sur bande ne peut être restaurée qu'à partir des versions 8.3 et ultérieures, et non vers une version antérieure. Si la LUN est restaurée dans une version antérieure, la LUN est restaurée en tant que fichier.

Lorsque vous sauvegardez un volume secondaire SnapVault ou une destination SnapMirror volume sur bande, seules les données du volume sont sauvegardées. Les métadonnées associées ne sont pas sauvegardées. Par conséquent, lorsque vous tentez de restaurer le volume, seules les données de ce volume sont restaurées. Les informations relatives aux relations SnapMirror volume ne sont pas disponibles dans la sauvegarde et n'ont donc pas été restaurées.

Si vous dump un fichier qui ne dispose que d'autorisations Windows NT et le restaurez sur un qtree ou un volume de style UNIX, le fichier obtient les autorisations UNIX par défaut pour ce qtree ou volume.

Si vous dump un fichier qui ne dispose que d'autorisations UNIX et que vous le restaurez sur un qtree ou un volume de style NTFS, le fichier obtient les autorisations Windows par défaut pour ce qtree ou ce volume.

Les autres « dumps » et les restaurations préservent les autorisations.

Vous pouvez sauvegarder des fichiers alignés sur les machines virtuelles et le `vm-align-sector` option. Pour plus d'informations sur les fichiers alignés sur les machines virtuelles, voir "[Gestion du stockage logique](#)".

## Quelles sont les chaînes d'incrémentation

Une chaîne d'incrémentation est une série de sauvegardes incrémentielles du même chemin. Comme vous pouvez spécifier n'importe quel niveau de sauvegarde à tout moment, vous devez comprendre incrémenter les chaînes pour pouvoir effectuer

efficacement les sauvegardes et les restaurations. Vous pouvez effectuer 31 niveaux d'opérations de sauvegarde incrémentielles.

Il existe deux types de chaînes d'incrémentation :

- Une chaîne d'incrémentation consécutive, qui est une séquence de sauvegardes incrémentielles commençant par le niveau 0 et qui est élevée par 1 à chaque sauvegarde suivante.
- Chaîne d'incrémentation non consécutive, où les sauvegardes incrémentielles ignorent des niveaux ou ont des niveaux hors séquence, tels que 0, 2, 3, 1, 4, ou plus fréquemment 0, 1, 1, 1 ou 0, 1, 2, 1, 2.

Les sauvegardes incrémentielles reposent sur la sauvegarde de niveau inférieur la plus récente. Par exemple, la séquence des niveaux de sauvegarde 0, 2, 3, 1, 4 fournit deux chaînes d'incrément : 0, 2, 3 et 0, 1, 4. Le tableau suivant explique les bases de sauvegardes incrémentielles :

| Ordre de sauvegarde | Niveau d'incrémentation | Incrémenter la chaîne | Base                                                                                                         | Fichiers sauvegardés                                                                                                                                                |
|---------------------|-------------------------|-----------------------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1                   | 0                       | Les deux              | Fichiers sur le système de stockage                                                                          | Tous les fichiers du chemin de sauvegarde                                                                                                                           |
| 2                   | 2                       | 0, 2, 3               | Sauvegarde de niveau 0                                                                                       | Fichiers dans le chemin de sauvegarde créé depuis la sauvegarde de niveau 0                                                                                         |
| 3                   | 3                       | 0, 2, 3               | Sauvegarde de niveau 2                                                                                       | Fichiers dans le chemin de sauvegarde créé depuis la sauvegarde de niveau 2                                                                                         |
| 4                   | 1                       | 0, 1, 4               | Sauvegarde de niveau 0, car il s'agit du niveau le plus récent qui est inférieur à la sauvegarde de niveau 1 | Fichiers dans le chemin de sauvegarde créé depuis la sauvegarde de niveau 0, y compris les fichiers qui se trouvent dans les sauvegardes de niveau 2 et de niveau 3 |

| Ordre de sauvegarde | Niveau d'incrémentation | Incrémenter la chaîne | Base                                                                                                                    | Fichiers sauvegardés                            |
|---------------------|-------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| 5                   | 4                       | 0, 1, 4               | La sauvegarde de niveau 1, car elle est un niveau inférieur et est plus récente que les sauvegardes de niveau 0, 2 ou 3 | Fichiers créés depuis la sauvegarde de niveau 1 |

### Quel est le facteur de blocage

Un bloc de bandes est de 1,024 octets de données. Lors d'une sauvegarde ou d'une restauration sur bande, vous pouvez spécifier le nombre de blocs de bandes transférés dans chaque opération de lecture/écriture. Ce nombre est appelé le *facteur de blocage*.

Vous pouvez utiliser un facteur de blocage de 4 à 256. Si vous envisagez de restaurer une sauvegarde sur un système autre que celui qui a effectué la sauvegarde, le système de restauration doit prendre en charge le facteur de blocage que vous avez utilisé pour la sauvegarde. Par exemple, si vous utilisez un facteur de blocage de 128, le système sur lequel vous restaurez cette sauvegarde doit prendre en charge un facteur de blocage de 128.

Lors d'une sauvegarde NDMP, LE MOVER\_RECORD\_SIZE détermine le facteur de blocage. ONTAP autorise une valeur maximale de 256 Ko pour MOVER\_RECORD\_SIZE.

### Quand redémarrer une sauvegarde de vidage

Une sauvegarde de dump ne se termine parfois pas en raison d'erreurs internes ou externes, telles que les erreurs d'écriture sur les bandes, les pannes d'alimentation, les interruptions accidentelles des utilisateurs ou les incohérences internes du système de stockage. Si votre sauvegarde échoue pour l'une de ces raisons, vous pouvez la redémarrer.

Vous pouvez choisir d'interrompre et de redémarrer une sauvegarde pour éviter les pics de trafic sur le système de stockage ou d'éviter la concurrence pour d'autres ressources limitées sur le système de stockage, comme les lecteurs de bandes. Vous pouvez interrompre une sauvegarde longue et la redémarrer ultérieurement si une restauration (ou une sauvegarde) plus urgente nécessite le même lecteur de bande. Les sauvegardes redémarrables sont conservées entre les redémarrages. Vous ne pouvez redémarrer une sauvegarde abandonnée sur bande que si les conditions suivantes sont vraies :

- La sauvegarde abandonnée est en phase IV
- Toutes les copies Snapshot associées qui ont été verrouillées par la commande dump sont disponibles.
- L'historique du fichier doit être activé.

Lorsqu'une telle opération de vidage est abandonnée et reste à l'état redémarrable, les copies Snapshot associées sont verrouillées. Ces copies Snapshot sont libérées une fois ces contextes supprimés. Vous pouvez afficher la liste des contextes de sauvegarde à l'aide du `vserver services ndmp restartable backup show` commande.

```

cluster::> vserver services ndmpd restartable-backup show
Vserver Context Identifier Is Cleanup Pending?

vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

Vserver: vserver1
Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
Volume Name: /vserver1/vol1
Is Cleanup Pending?: false
Backup Engine Type: dump
Is Snapshot Copy Auto-created?: true
Dump Path: /vol/vol1
Incremental Backup Level ID: 0
Dump Name: /vserver1/vol1
Context Last Updated Time: 1460624875
Has Offset Map?: true
Offset Verify: true
Is Context Restartable?: true
Is Context Busy?: false
Restart Pass: 4
Status of Backup: 2
Snapshot Copy Name: snapshot_for_backup.1
State of the Context: 7

cluster::>"

```

## Fonctionnement d'une restauration de vidage

Une restauration de vidage écrit les données du système de fichiers de la bande sur le disque à l'aide d'un processus prédéfini.

Le processus du tableau suivant montre le fonctionnement de la restauration de vidage :

| Étape | Action                                               |
|-------|------------------------------------------------------|
| 1     | ONTAP catalogue les fichiers à extraire de la bande. |
| 2     | ONTAP crée des répertoires et des fichiers vides.    |

| Étape | Action                                                                                                                                                 |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3     | ONTAP lit un fichier à partir de la bande, l'écrit sur le disque et définit les autorisations (y compris les listes de contrôle d'accès) sur celui-ci. |
| 4     | ONTAP répète les étapes 2 et 3 jusqu'à ce que tous les fichiers spécifiés soient copiés à partir de la bande.                                          |

### Types de données que le moteur de vidage restaure

En cas d'incident ou de perturbation du contrôleur, le moteur de dump offre plusieurs méthodes permettant de restaurer l'ensemble des données sauvegardées, depuis des fichiers uniques jusqu'aux attributs de fichiers, vers des répertoires entiers. Connaître les types de données que le moteur de vidage peut restaurer et quand utiliser quelle méthode de récupération peut aider à réduire les temps d'arrêt.

Vous pouvez restaurer les données sur une LUN mappée en ligne. Cependant, les applications hôtes ne peuvent pas accéder à cette LUN tant que l'opération de restauration n'est pas terminée. Une fois l'opération de restauration terminée, le cache hôte des données de la LUN doit être vidé pour assurer la cohérence avec les données restaurées.

Le moteur de vidage peut récupérer les données suivantes :

- Contenu des fichiers et répertoires
- Autorisations relatives aux fichiers UNIX
- ACL

Si vous restaurez un fichier possédant uniquement des autorisations de fichier UNIX sur un qtree ou un volume NTFS, le fichier ne dispose pas de listes de contrôle d'accès Windows NT. Le système de stockage utilise uniquement les autorisations de fichier UNIX sur ce fichier jusqu'à ce que vous y créiez une liste de contrôle d'accès Windows NT.



Si vous restaurez les listes de contrôle d'accès sauvegardées à partir des systèmes de stockage exécutant Data ONTAP 8.2 vers les systèmes de stockage exécutant Data ONTAP 8.1.x et les versions antérieures ayant une limite ACE inférieure à 1,024, une liste de contrôle d'accès par défaut est restaurée.

- Informations sur les qtrees

Les informations relatives à qtree sont utilisées uniquement si un qtree est restauré à la racine d'un volume. Les informations qtree ne sont pas utilisées si un qtree est restauré dans un répertoire inférieur, par exemple `/vs1/vol1/subdir/lowerdir`, et il cesse d'être un qtree.

- Tous les autres attributs de fichier et de répertoire
- Flux Windows NT
- LUN
  - Une LUN doit être restaurée au niveau d'un volume ou d'une qtree pour qu'elle reste une LUN.

S'il est restauré dans un répertoire, il est restauré en tant que fichier car il ne contient aucune

métadonnées valide.

- Une LUN 7-mode est restaurée sous forme de LUN sur un volume ONTAP.
- Un volume 7-mode peut être restauré vers un volume ONTAP.
- Les fichiers alignés sur les machines virtuelles restaurés sur un volume de destination héritent des propriétés d'alignement des machines virtuelles du volume de destination.
- Le volume de destination pour une opération de restauration peut avoir des fichiers avec des verrous obligatoires ou consultatifs.

Lors de l'exécution de l'opération de restauration sur un tel volume de destination, le moteur de vidage ignore ces verrous.

## Considérations avant de restaurer les données

Vous pouvez restaurer les données sauvegardées dans leur chemin d'origine ou vers une destination différente. Si vous restaurez les données sauvegardées vers une autre destination, vous devez préparer la destination pour l'opération de restauration.

Avant de restaurer les données sur son chemin d'origine ou vers une autre destination, vous devez disposer des informations suivantes et satisfaire les exigences suivantes :

- Niveau de la restauration
- Le chemin vers lequel vous restaurez les données
- Facteur de blocage utilisé pendant la sauvegarde
- Si vous effectuez une restauration incrémentielle, toutes les bandes doivent être dans la chaîne de sauvegarde
- Lecteur de bande disponible et compatible avec la bande à restaurer

Avant de restaurer les données vers une autre destination, vous devez effectuer les opérations suivantes :

- Si vous restaurez un volume, vous devez créer un nouveau volume.
- Si vous restaurez un qtree ou un répertoire, vous devez renommer ou déplacer des fichiers susceptibles d'avoir les mêmes noms que les fichiers que vous restaurez.



Dans ONTAP 9, les noms de qtree prennent en charge le format Unicode. Les versions antérieures de ONTAP ne prennent pas en charge ce format. Si un qtree avec des noms Unicode dans ONTAP 9 est copié dans une version antérieure de ONTAP à l'aide de l'`ndmcopy` Commande ou par restauration à partir d'une image de sauvegarde sur bande, le qtree est restauré en tant que répertoire normal et non en tant que qtree au format Unicode.



Si un fichier restauré porte le même nom qu'un fichier existant, le fichier existant est écrasé par le fichier restauré. Toutefois, les répertoires ne sont pas écrasés.

Pour renommer un fichier, un répertoire ou un qtree pendant la restauration sans utiliser DAR, vous devez définir la variable d'environnement D'EXTRACTION sur `E`.

## Espace requis sur le système de stockage de destination

Vous avez besoin d'environ 100 Mo d'espace supplémentaire sur le système de stockage de destination par

rapport à la quantité de données à restaurer.



L'opération de restauration vérifie l'espace volume et la disponibilité d'inode sur le volume de destination au démarrage de l'opération de restauration. Définition de la variable d'environnement `DE FORCE` sur `Y` provoque l'opération de restauration pour ignorer les vérifications de l'espace volume et de la disponibilité d'inode sur le chemin de destination. S'il n'y a pas assez d'espace volume ou d'inodes disponible sur le volume de destination, l'opération de restauration restaure autant de données que l'espace du volume de destination et la disponibilité d'inode. L'opération de restauration s'arrête lorsqu'il ne reste plus d'espace ou d'inodes.

### Limite d'évolutivité pour les sessions de sauvegarde et de restauration

Vous devez connaître le nombre maximal de sessions de sauvegarde et de restauration de vidage que vous pouvez effectuer simultanément sur les systèmes de stockage de différentes capacités de mémoire système. Ce nombre maximum dépend de la mémoire système d'un système de stockage.

Les limites mentionnées dans le tableau suivant concernent le moteur de vidage ou de restauration. Les limites mentionnées dans les limites d'évolutivité des sessions NDMP sont destinées au serveur NDMP, qui sont supérieures aux limites du moteur.

| Mémoire système d'un système de stockage         | Nombre total de sessions de sauvegarde et de restauration de vidage |
|--------------------------------------------------|---------------------------------------------------------------------|
| Moins de 16 Go                                   | 4                                                                   |
| Supérieur ou égal à 16 Go mais inférieur à 24 Go | 16                                                                  |
| Supérieur ou égal à 24 Go                        | 32                                                                  |



Si vous utilisez `ndmpcopy` Commande pour copier les données dans les systèmes de stockage, deux sessions NDMP sont établies, l'une pour dump backup et l'autre pour dump restore.

Vous pouvez obtenir la mémoire système de votre système de stockage à l'aide du `sysconfig -a` commande (disponible via le nodeshell). Pour plus d'informations sur l'utilisation de cette commande, consultez les pages de manuels.

### Informations associées

[Limite d'évolutivité pour les sessions NDMP](#)

### Prise en charge de la sauvegarde sur bande et des restaurations entre Data ONTAP sous 7-mode et ONTAP

Vous pouvez restaurer les données sauvegardées à partir d'un système de stockage sous 7-mode ou exécutant ONTAP vers un système de stockage sous 7-mode ou exécutant ONTAP.

Les opérations suivantes de sauvegarde sur bande et de restauration sont prises en charge entre Data ONTAP en 7-mode et ONTAP :

- Sauvegarde d'un volume 7-mode sur un lecteur de bandes connecté à un système de stockage exécutant ONTAP
- Sauvegarde d'un volume ONTAP sur un lecteur de bandes connecté à un système 7-mode
- Restauration des données sauvegardées d'un volume 7-mode depuis un lecteur de bande connecté à un système de stockage exécutant ONTAP
- Restauration des données sauvegardées d'un volume ONTAP à partir d'un lecteur de bande connecté à un système 7-mode
- Restauration d'un volume 7-mode vers un volume ONTAP



- A 7-Mode LUN is restored as a LUN on an ONTAP volume.
- You should retain the ONTAP LUN identifiers when restoring a 7-Mode LUN to an existing ONTAP LUN.

- Restauration d'un volume ONTAP sur un volume 7-mode



Une LUN ONTAP est restaurée sous forme de fichier standard sur un volume 7-mode.

## Supprimer des contextes réstartables

Si vous souhaitez démarrer une sauvegarde au lieu de redémarrer un contexte, vous pouvez supprimer le contexte.

### Description de la tâche

Vous pouvez supprimer un contexte redémarrable à l'aide de l'`vserver services ndmp restartable-backup delete` Commande utilisant le nom du SVM et l'ID de contexte.

### Étapes

1. Supprimer un contexte redémarrable :

```
vserver services ndmp restartable-backup delete -vserver vserver-name -context -id context_identifieur.
```



```

cluster::> vservice ndmp restartable-backup show
Vserver Context Identifier Is Cleanup Pending?

vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vservice ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vservice ndmp restartable-backup show
Vserver Context Identifier Is Cleanup Pending?

vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"

```

### Fonctionnement de dump sur un volume secondaire SnapVault

Vous pouvez effectuer des opérations de sauvegarde sur bande sur des données mises en miroir sur le volume secondaire SnapVault. Vous pouvez sauvegarder uniquement les données mises en miroir sur le volume secondaire SnapVault sur bande, et non sur les métadonnées liées à la relation SnapVault.

Quand on rompt la relation de miroir de protection des données (`snapmirror break`) Ou lorsqu'une resynchronisation SnapMirror se produit, vous devez toujours effectuer une sauvegarde de base.

### Fonctionnement de dump avec les opérations de basculement de stockage et d'ARL

Avant d'effectuer des opérations de sauvegarde et de restauration de type dump, il est important de comprendre le fonctionnement de ces opérations avec les opérations de basculement du stockage (Takeover et giveback) ou de transfert d'agrégats (ARL). Le `-override-vetoes` Détermine le comportement du moteur de vidage lors d'une opération de basculement du stockage ou d'ARL.

Lorsqu'une opération de sauvegarde ou de restauration est en cours d'exécution et `-override-vetoes` l'option est définie sur `false`, Un basculement de stockage ou une opération ARL initié par l'utilisateur est arrêté. Cependant, si `-override-vetoes` l'option est définie sur `true`, Le basculement du stockage ou l'opération ARL est ensuite poursuivi et l'opération de sauvegarde ou de restauration de vidage est abandonnée. Lorsqu'une opération de basculement ou d'ARL de stockage est automatiquement lancée par le système de stockage, une opération de sauvegarde ou de restauration des données de dump actif est toujours abandonnée. Vous ne pouvez pas redémarrer les opérations de sauvegarde et de restauration de vidage,

même après la fin des opérations de basculement du stockage ou d'ARL.

#### Opérations de vidage lorsque l'extension DE CABINE est prise en charge

Si l'application de sauvegarde prend en charge l'extension CAB, vous pouvez continuer à effectuer les opérations de sauvegarde et de restauration incrémentielles sans reconfigurer les règles de sauvegarde après un basculement de stockage ou un transfert d'agrégats.

#### Les opérations de vidage lorsque l'extension DE CABINE n'est pas prise en charge

Si l'application de sauvegarde ne prend pas en charge l'extension CAB, vous pouvez continuer d'effectuer les opérations de sauvegarde et de restauration du dump incrémentiel si vous migrez la LIF configurée dans la politique de sauvegarde vers le nœud qui héberge l'agrégat de destination. Sinon, après le basculement du stockage et l'ARL, vous devez effectuer une sauvegarde de base avant d'effectuer l'opération de sauvegarde incrémentielle.



Pour les opérations de basculement du stockage, la LIF configurée dans la stratégie de sauvegarde doit être migrée vers le nœud partenaire.

#### Informations associées

"Haute disponibilité"

#### Fonctionnement de dump lors du déplacement de volumes

Les opérations de sauvegarde et de restauration sur bande et de déplacement de volumes peuvent être exécutées en parallèle jusqu'à la phase de mise en service finale du système de stockage. Après cette phase, les nouvelles opérations de sauvegarde et de restauration sur bandes ne sont pas autorisées sur le volume en cours de déplacement. Cependant, les opérations en cours continuent de fonctionner jusqu'à la fin.

Le tableau suivant décrit le comportement des opérations de sauvegarde et de restauration sur bande après le déplacement du volume :

| Si vous effectuez des opérations de sauvegarde sur bande et de restauration dans...                                             | Alors...                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Storage Virtual machine (SVM) a scoped NDMP (mode NDMP) lorsque l'extension CAB est prise en charge par l'application de backup | Vous pouvez continuer à effectuer des sauvegardes incrémentielles sur bande et restaurer des volumes en lecture/écriture et en lecture seule sans reconfigurer les règles de sauvegarde.                                                                                                                                                                                                                                              |
| Mode SVM-scoped NDMP lorsque l'extension CAB n'est pas prise en charge par l'application de backup                              | Vous pouvez continuer à effectuer des opérations de sauvegarde incrémentielle sur bande et de restauration sur des volumes en lecture/écriture et en lecture seule si vous migrez la LIF configurée dans la stratégie de sauvegarde vers le nœud qui héberge l'agrégat de destination. Sinon, après le déplacement du volume, vous devez effectuer une sauvegarde de base avant d'effectuer l'opération de sauvegarde incrémentielle. |



Lorsqu'un déplacement de volumes se produit, si le volume appartenant à un autre SVM sur le nœud de destination porte le même nom que celui du volume déplacé, vous ne pouvez pas effectuer d'opérations de sauvegarde incrémentielle du volume déplacé.

### **Fonctionnement de dump lorsqu'un volume FlexVol est plein**

Avant d'effectuer une opération de sauvegarde incrémentielle de dump, vous devez vérifier que l'espace disponible est suffisant dans le volume FlexVol.

En cas d'échec de l'opération, vous devez augmenter l'espace libre du volume Flex vol, soit en augmentant sa taille, soit en supprimant les copies Snapshot. Effectuez ensuite à nouveau l'opération de sauvegarde incrémentielle.

### **Fonctionnement de dump lorsque le type d'accès de volume change**

Lorsqu'un volume de destination SnapMirror ou un volume secondaire SnapVault passe de l'état lecture/écriture à lecture seule ou de la lecture seule à la lecture/écriture, vous devez effectuer une opération de sauvegarde ou de restauration de base sur bande.

La destination SnapMirror et les volumes secondaires SnapVault sont des volumes en lecture seule. Si vous effectuez des opérations de sauvegarde sur bande et de restauration sur de tels volumes, vous devez effectuer une opération de sauvegarde ou de restauration de base chaque fois que le volume passe de l'état lecture seule à lecture/écriture ou de la lecture/écriture à la lecture seule.

### **Fonctionnement de dump avec la restauration de fichiers ou de LUN SnapMirror**

Avant d'effectuer des sauvegardes de dump ou des opérations de restauration sur un volume sur lequel un fichier ou une LUN unique est restauré à l'aide de la technologie SnapMirror, vous devez comprendre le fonctionnement des opérations de dump avec une seule opération de restauration de fichiers ou de LUN.

Lors de l'opération de restauration d'un seul fichier ou de LUN SnapMirror, le nombre d'E/S client est limité sur le fichier ou la LUN en cours de restauration. Une fois l'opération de restauration de fichier ou de LUN terminée, la restriction d'E/S sur le fichier ou la LUN est supprimée. Si une sauvegarde de dump est effectuée sur un volume sur lequel un seul fichier ou LUN est restauré, alors le fichier ou la LUN qui a une restriction d'E/S client n'est pas inclus dans la sauvegarde dump. Lors d'une opération de sauvegarde ultérieure, ce fichier ou ce LUN est sauvegardé sur bande après suppression de la restriction d'E/S.

Vous ne pouvez pas effectuer simultanément une restauration de dump et une opération de restauration SnapMirror ou de LUN sur le même volume.

### **Le rôle des opérations de vidage et de restauration dans les configurations MetroCluster est affecté**

Avant d'effectuer les opérations de sauvegarde et de restauration de dump dans une configuration MetroCluster, vous devez en déterminer l'impact des opérations de dump en cas d'opération de basculement ou de rétablissement.

#### **Vidage de l'opération de sauvegarde ou de restauration suivi du basculement**

Envisager deux clusters : cluster 1 et cluster 2. Lors d'une opération de sauvegarde ou de restauration sur le cluster 1, si un basculement est initié du cluster 1 au cluster 2, ce qui suit se produit :

- Si la valeur de `override-vetoes` l'option est `false`, le basculement est alors interrompu et l'opération de sauvegarde ou de restauration se poursuit.
- Si la valeur de l'option est `true`, l'opération de sauvegarde ou de restauration du vidage est alors abandonnée et le basculement se poursuit.

#### Vidage de l'opération de sauvegarde ou de restauration, suivi du rétablissement

Un basculement est effectué du cluster 1 vers le cluster 2 et une opération de sauvegarde ou de restauration de « dump » est lancée sur le cluster 2. L'opération de dump sauvegarde ou restaure un volume situé sur le cluster 2. À ce stade, si un rétablissement est initié du cluster 2 au cluster 1, ce qui suit se produit :

- Si la valeur de `override-vetoes` l'option est `false`, le rétablissement est alors annulé et l'opération de sauvegarde ou de restauration se poursuit.
- Si la valeur de l'option est `true`, l'opération de sauvegarde ou de restauration est alors abandonnée et le rétablissement se poursuit.

#### Vidage de l'opération de sauvegarde ou de restauration initié lors d'un basculement ou d'un rétablissement

Lors du basculement d'un cluster 1 vers un cluster 2, si une opération de sauvegarde ou de restauration de dump est initiée sur le cluster 1, l'opération de sauvegarde ou de restauration échoue et le basculement se poursuit.

Lors du rétablissement d'un cluster 2 vers le cluster 1, si une opération de sauvegarde ou de restauration de vidage est lancée depuis le cluster 2, l'opération de sauvegarde ou de restauration échoue et le rétablissement se poursuit.

## À propos du moteur SMTape pour les volumes FlexVol

### À propos du moteur SMTape pour les volumes FlexVol

SMTape est une solution de reprise après incident de ONTAP qui sauvegarde des blocs de données sur bande. Vous pouvez utiliser SMTape afin d'effectuer des sauvegardes de volume sur bandes. Toutefois, vous ne pouvez pas effectuer de sauvegarde au niveau qtrees ou sous-arbre. SMTape prend en charge les sauvegardes de base, différentielles et incrémentielles. SMTape ne nécessite pas de licence.

Vous pouvez effectuer une opération de sauvegarde et de restauration SMTape à l'aide d'une application de sauvegarde conforme au protocole NDMP. Vous pouvez choisir SMTape afin d'effectuer des opérations de sauvegarde et de restauration uniquement en mode NDMP étendue de la machine virtuelle de stockage (SVM).



Le processus de réversion n'est pas pris en charge lorsqu'une session de sauvegarde ou de restauration SMTape est en cours. Vous devez attendre la fin de la session ou abandonner la session NDMP.

SMTape permet de sauvegarder 255 copies Snapshot. Pour les sauvegardes de base, incrémentielles ou différentielles suivantes, vous devez supprimer les anciennes copies Snapshot sauvegardées.

Avant d'effectuer la restauration de base, le volume sur lequel les données sont restaurées doit être de type `DP` et ce volume doit être à l'état restreint. Une fois la restauration effectuée, ce volume est automatiquement en ligne. Vous pouvez effectuer ensuite des restaurations incrémentielles ou différentielles sur ce volume dans l'ordre dans lequel les sauvegardes ont été effectuées.

## Utilisation des copies Snapshot pendant la sauvegarde SMTape

Il est important de comprendre comment les copies Snapshot sont utilisées lors d'une sauvegarde de base SMTape et d'une sauvegarde incrémentielle. Vous devez également tenir compte des considérations d'ordre à prendre en compte lors de la sauvegarde sur SMTape.

### Sauvegarde de base

Lors de l'exécution d'une sauvegarde de base, vous pouvez indiquer le nom de la copie Snapshot à sauvegarder sur bande. Si aucune copie Snapshot n'est spécifiée, selon le type d'accès du volume (lecture/écriture ou lecture seule), une copie Snapshot est créée automatiquement ou des copies Snapshot existantes sont utilisées. Lorsque vous spécifiez une copie Snapshot pour la sauvegarde, toutes les copies Snapshot antérieures à la copie Snapshot spécifiée sont également sauvegardées sur bande.

Si vous ne spécifiez pas de copie Snapshot pour la sauvegarde, les événements suivants se produisent :

- Pour un volume en lecture/écriture, une copie Snapshot est créée automatiquement.

La nouvelle copie Snapshot et toutes les anciennes copies Snapshot sont sauvegardées sur bande.

- Pour un volume en lecture seule, toutes les copies Snapshot, y compris la dernière copie Snapshot, sont sauvegardées sur bande.

Aucune sauvegarde n'est effectuée après le démarrage de la sauvegarde.

### Sauvegarde incrémentielle

Pour les opérations de sauvegarde incrémentielle ou différentielle SMTape, les applications de sauvegarde conformes au protocole NDMP créent et gèrent les copies Snapshot.

Vous devez toujours spécifier une copie Snapshot lors de l'opération de sauvegarde incrémentielle. Pour que la sauvegarde incrémentielle soit couronnée de succès, la copie Snapshot sauvegardée lors de l'opération de sauvegarde précédente (copie de base ou incrémentielle) doit se trouver sur le volume à partir duquel la sauvegarde est effectuée. Pour vous assurer que vous utilisez cette copie Snapshot sauvegardée, vous devez tenir compte de la règle Snapshot attribuée à ce volume lors de la configuration de la règle de sauvegarde.

### Considérations relatives aux sauvegardes SMTape sur les destinations SnapMirror

- Une relation de miroir de protection des données crée des copies Snapshot temporaires sur le volume de destination pour la réplication.

Il est interdit d'utiliser ces copies Snapshot pour la sauvegarde SMTape.

- Lorsqu'une mise à jour SnapMirror se produit sur un volume de destination dans une relation de miroir de protection des données lors d'une opération de sauvegarde SMTape sur le même volume, la copie Snapshot sauvegardée par SMTape ne doit pas être supprimée du volume source.

Lors de la sauvegarde, SMTape verrouille la copie Snapshot sur le volume de destination. Si la copie Snapshot correspondante est supprimée sur le volume source, l'opération de mise à jour SnapMirror suivante échoue.

- Vous ne devez pas utiliser ces copies Snapshot pendant la sauvegarde incrémentielle.


Fonctionnalités SMTape

Les fonctionnalités SMTape, telles que la sauvegarde des copies Snapshot, les sauvegardes incrémentielles et différentielles, la préservation des fonctions de déduplication et de compression des volumes restaurés et la « Tape seeding » des bandes, vous permettent d’optimiser vos opérations de sauvegarde et de restauration sur bande.

SMTape offre les fonctionnalités suivantes :

- Offre une solution de reprise après incident
- Permet des sauvegardes incrémentielles et différentielles
- Sauvegarde des copies Snapshot
- Permet la sauvegarde et la restauration des volumes dédupliqués et préserve la déduplication sur les volumes restaurés
- Sauvegarde les volumes compressés et préserve la compression sur les volumes restaurés
- Permet l’ensemencement des bandes

SMTape prend en charge le facteur de blocage en multiples de 4 Ko, dans une plage de 4 Ko à 256 Ko.




Vous pouvez restaurer les données sur des volumes créés pour deux versions ONTAP consécutives majeures uniquement.

Fonctionnalités non prises en charge par SMTape

SMTape ne prend pas en charge les sauvegardes redémarrables et la vérification des fichiers sauvegardés.

Limites d’évolutivité pour les sessions de sauvegarde et de restauration SMTape

Lors de la réalisation des opérations de sauvegarde et de restauration SMTape via NDMP ou CLI (Tape seeding), vous devez connaître le nombre maximal de sessions de sauvegarde et de restauration SMTape qui peuvent être effectuées simultanément sur les systèmes de stockage dotés de différentes capacités de mémoire système. Ce nombre maximum dépend de la mémoire système d’un système de stockage.



Les limites d’évolutivité des sessions de sauvegarde et de restauration SMTape sont différentes des limites des sessions NDMP et des sessions de vidage.

| Mémoire système du système de stockage           | Nombre total de sessions de sauvegarde et de restauration SMTape |
|--------------------------------------------------|------------------------------------------------------------------|
| Moins de 16 Go                                   | 6                                                                |
| Supérieur ou égal à 16 Go mais inférieur à 24 Go | 16                                                               |
| Supérieur ou égal à 24 Go                        | 32                                                               |

Vous pouvez obtenir la mémoire système de votre système de stockage à l'aide du `sysconfig -a` commande (disponible via le nodeshell). Pour plus d'informations sur l'utilisation de cette commande, consultez les pages de manuels.

#### Informations associées

[Limite d'évolutivité pour les sessions NDMP](#)

[Limite d'évolutivité pour les sessions de sauvegarde et de restauration](#)

#### En quoi consiste l'amorçage des bandes

La fonction SMTape permet d'initialiser un volume FlexVol de destination dans une relation de miroir de protection des données.

Le « Tape seeding » permet d'établir une relation de miroir de protection des données entre le système source et le système de destination via une connexion à faible bande passante.

La mise en miroir incrémentielle des copies Snapshot de la source vers la destination est possible via une connexion à faible bande passante. Cependant, une mise en miroir initiale de la copie Snapshot de base prend beaucoup de temps sur une connexion à faible bande passante. Il est ainsi possible d'effectuer une sauvegarde SMTape du volume source sur bande, puis d'utiliser la bande pour transférer la copie Snapshot de la base initiale vers la destination. Vous pouvez ensuite configurer des mises à jour SnapMirror incrémentielles sur le système de destination à l'aide de la connexion à faible bande passante.

#### Fonctionnement de SMTape avec basculement du stockage et opérations d'ARL

Avant d'effectuer des opérations de sauvegarde ou de restauration SMTape, vous devez comprendre le fonctionnement de ces opérations grâce au basculement du stockage (basculement et rétablissement) ou au transfert d'agrégats (ARL). Le `-override -vetoes` Détermine le comportement du moteur SMTape lors du basculement du stockage ou du transfert d'agrégats.

Lorsqu'une opération de sauvegarde ou de restauration SMTape est en cours d'exécution sur `-override -vetoes` l'option est définie sur `false`, Un basculement de stockage initié par l'utilisateur ou une opération ARL est arrêté et l'opération de sauvegarde ou de restauration est terminée. Si l'application de sauvegarde prend en charge l'extension CAB, vous pouvez continuer à effectuer les opérations de sauvegarde et de restauration incrémentielles SMTape sans reconfigurer les règles de sauvegarde. Cependant, si `-override -vetoes` l'option est définie sur `true`, Le basculement du stockage ou l'opération ARL est ensuite poursuivi et l'opération de sauvegarde ou de restauration SMTape est abandonnée.

#### Informations associées

["Gestion du réseau"](#)

["Haute disponibilité"](#)

#### Fonctionnement de SMTape avec le déplacement de volumes

Les opérations de sauvegarde SMTape et de déplacement de volumes peuvent fonctionner en parallèle jusqu'à la fin de la phase de mise en service finale du système de stockage. Après cette phase, les nouvelles opérations de sauvegarde SMTape ne peuvent pas s'exécuter sur le volume en cours de déplacement. Cependant, les

opérations en cours continuent de fonctionner jusqu'à la fin.

Avant le démarrage de la phase de mise en service d'un volume, l'opération de déplacement de volume vérifie si les opérations de sauvegarde SMTape actives sur le même volume. En cas d'opérations de sauvegarde SMTape actives, l'opération de déplacement des volumes passe en mode « différé » de mise en service et permet le processus de sauvegarde SMTape. Une fois ces opérations de sauvegarde terminées, vous devez redémarrer manuellement l'opération de déplacement de volume.

Si l'application de sauvegarde prend en charge l'extension CAB, vous pouvez continuer à effectuer les sauvegardes incrémentielles sur bande et à les restaurer sur les volumes en lecture/écriture et en lecture seule sans reconfigurer les règles de sauvegarde.

Les opérations de restauration de base et de déplacement des volumes ne peuvent pas être exécutées simultanément. Toutefois, la restauration incrémentielle peut être exécutée en parallèle avec les opérations de déplacement de volumes, avec un comportement similaire à celui des opérations de sauvegarde SMTape lors des opérations de déplacement de volumes.

### **Fonctionnement de SMTape avec les opérations de réhébergement de volumes**

Les opérations SMTape ne peuvent pas commencer lorsqu'une opération de réhébergement de volume est en cours sur un volume. Lorsqu'un volume est impliqué dans une opération de réhébergement de volumes, les sessions SMTape ne doivent pas être lancées sur ce volume.

Lorsque des opérations de réhébergement de volumes sont en cours, la sauvegarde ou la restauration SMTape échoue. Lorsqu'une sauvegarde ou une restauration SMTape est en cours, les opérations de réhébergement de volume rencontrent un message d'erreur approprié. Cette condition s'applique aux opérations de sauvegarde ou de restauration basées sur NDMP et sur l'interface de ligne de commande.

### **Comment la politique de sauvegarde NDMP est-elle affectée pendant ADB**

Lorsque l'équilibreur de données automatique (ADB) est activé, l'équilibreur analyse les statistiques d'utilisation des agrégats afin d'identifier l'agrégat qui a dépassé le pourcentage d'utilisation à seuil élevé configuré.

Après avoir identifié l'agrégat qui a dépassé le seuil, l'équilibreur identifie un volume pouvant être déplacé vers des agrégats résidant dans un autre nœud du cluster et tente de déplacer ce volume. Cette situation affecte la stratégie de sauvegarde configurée pour ce volume car si l'application de gestion des données (DMA) n'est pas compatible AVEC CAB, l'utilisateur doit reconfigurer la stratégie de sauvegarde et exécuter l'opération de sauvegarde de base.



Si le DMA est conscient DE CAB et que la politique de sauvegarde a été configurée à l'aide d'une interface spécifique, alors l'ADB n'est pas affecté.

### **Comment les opérations de sauvegarde et de restauration SMTape sont affectées dans les configurations MetroCluster**

Avant d'effectuer les opérations de sauvegarde et de restauration SMTape sur une configuration MetroCluster, vous devez d'abord comprendre comment les opérations SMTape sont affectées lors d'une opération de basculement ou de rétablissement.



### Opération de sauvegarde ou de restauration SMTape, suivie du basculement

Envisager deux clusters : cluster 1 et cluster 2. Lors d'une opération de sauvegarde ou de restauration SMTape sur le cluster 1, si un basculement est initié du cluster 1 au cluster 2, ce qui suit se produit :

- Si la valeur de `-override-vetoes` l'option est `false`, le processus de basculement est alors interrompu et l'opération de sauvegarde ou de restauration se poursuit.
- Si la valeur de l'option est `true`, Puis l'opération de sauvegarde ou de restauration SMTape est abandonnée et le processus de basculement se poursuit.

### Opération de sauvegarde ou de restauration SMTape, suivie du rétablissement

Un basculement est effectué du cluster 1 vers le cluster 2. Une opération de sauvegarde ou de restauration SMTape est lancée sur le cluster 2. L'opération SMTape permet de sauvegarder ou de restaurer un volume situé sur le cluster 2. À ce stade, si un rétablissement est initié du cluster 2 au cluster 1, ce qui suit se produit :

- Si la valeur de `-override-vetoes` l'option est `false`, le processus de rétablissement est alors interrompu et l'opération de sauvegarde ou de restauration se poursuit.
- Si la valeur de l'option est `true`, l'opération de sauvegarde ou de restauration est alors abandonnée et le processus de rétablissement se poursuit.

### Opération de sauvegarde ou de restauration SMTape initiée lors du basculement ou du rétablissement

Lors d'un processus de basculement du cluster 1 vers le cluster 2, si une opération de sauvegarde ou de restauration SMTape est lancée sur le cluster 1, alors l'opération de sauvegarde ou de restauration échoue et le basculement se poursuit.

Lors du processus de rétablissement du cluster 2 vers le cluster 1, si une opération de sauvegarde ou de restauration SMTape est lancée depuis le cluster 2, l'opération de sauvegarde ou de restauration échoue et le rétablissement se poursuit.

## Surveillance des opérations de sauvegarde sur bande et de restauration des volumes FlexVol

### Surveiller les opérations de sauvegarde sur bande et de restauration des volumes FlexVol

Vous pouvez afficher les fichiers journaux des événements pour surveiller les opérations de sauvegarde et de restauration sur bande. ONTAP consigne automatiquement des événements significatifs relatifs aux sauvegardes et aux restaurations, ainsi que l'heure à laquelle ils se produisent dans un fichier journal nommé `backup` dans les contrôleurs `/etc/log/` répertoire. Par défaut, la journalisation des événements est définie sur `on`.

Vous pouvez vouloir afficher les fichiers journaux des événements pour les raisons suivantes :

- Vérification de la réussite d'une sauvegarde nocturne
- Collecte de statistiques sur les opérations de sauvegarde
- Pour utiliser les informations contenues dans les fichiers journaux d'événements précédents afin de faciliter le diagnostic des problèmes liés aux opérations de sauvegarde et de restauration

Une fois par semaine, les fichiers journaux d'événements sont pivotés. Le `/etc/log/backup` le fichier est renommé `/etc/log/backup.0`, le `/etc/log/backup.0` le fichier est renommé `/etc/log/backup.1`,

etc. Le système enregistre les fichiers journaux pendant six semaines maximum ; vous pouvez donc avoir jusqu'à sept fichiers de messages (/etc/log/backup.[0-5] et le courant /etc/log/backup fichier).

**Accéder aux fichiers journaux des événements**

Vous pouvez accéder aux fichiers journaux des événements pour les opérations de sauvegarde sur bande et de restauration dans /etc/log/ répertoire à l'aide du `rdfile` commande au nodeshell. Vous pouvez afficher ces fichiers journaux d'événements pour surveiller les opérations de sauvegarde sur bande et de restauration.

**Description de la tâche**

Avec des configurations supplémentaires, telles qu'un rôle de contrôle d'accès avec accès à l' `spi` service web ou compte d'utilisateur configuré avec le `http` méthode d'accès, vous pouvez également utiliser un navigateur web pour accéder à ces fichiers journaux.

**Étapes**

- 1. Pour accéder au nodeshell, entrez la commande suivante :

```
node run -node node_name
```

`node_name` est le nom du nœud.

- 2. Pour accéder aux fichiers journaux des événements pour les opérations de sauvegarde et de restauration sur bande, entrez la commande suivante :

```
rdfile /etc/log/backup
```

**Informations associées**

["Administration du système"](#)

**Format du message du journal des événements de vidage et de restauration**

**Présentation du format de message du journal des événements de vidage et de restauration**

Pour chaque événement de vidage et de restauration, un message est écrit dans le fichier journal de sauvegarde.

Le format du message du journal des événements de vidage et de restauration est le suivant :

```
type timestamp identifier event (event_info)
```

La liste suivante décrit les champs au format des messages du journal des événements :

- Chaque message du journal commence par l'un des indicateurs de type décrits dans le tableau suivant :

| Type    | Description                   |
|---------|-------------------------------|
| journal | Journalisation de l'événement |
| dmp     | Événement de vidage           |

| Type | Description               |
|------|---------------------------|
| rst  | Événement de restauration |

- `timestamp` affiche la date et l'heure de l'événement.
- **Le `identifier`** Le champ d'un événement de vidage inclut le chemin de vidage et l'ID unique du dump. Le `identifier` le champ d'un événement de restauration utilise uniquement le nom du chemin de destination de restauration comme identifiant unique. Les messages d'événement liés à la journalisation n'incluent pas de `identifier` légale.

#### En quoi sont les événements d'enregistrement

Le champ d'événement d'un message qui commence par un journal indique le début d'une consignation ou la fin d'une consignation.

Il contient l'un des événements présentés dans le tableau suivant :

| Événement        | Description                                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------|
| Démarrer_Logging | Indique le début de la consignation ou que la consignation a été remise sous tension après la désactivation. |
| Stop_Logging     | Indique que la consignation a été désactivée.                                                                |

#### Quels sont les événements de vidage

Le champ événement d'un événement de vidage contient un type d'événement suivi d'informations spécifiques à un événement entre parenthèses.

Le tableau suivant décrit les événements, leurs descriptions et les informations d'événement associées qui peuvent être enregistrées pour une opération de vidage :

| Événement  | Description                              | Informations sur l'événement                                              |
|------------|------------------------------------------|---------------------------------------------------------------------------|
| Démarrer   | Le dump NDMP est démarré                 | Niveau de vidage et type de vidage                                        |
| Fin        | Vidage terminé avec succès               | Quantité de données traitées                                              |
| Abandonner | L'opération est annulée                  | Quantité de données traitées                                              |
| Options    | Les options spécifiées sont répertoriées | Toutes les options et leurs valeurs associées, y compris les options NDMP |
| Tape_open  | La bande est ouverte en lecture/écriture | Nom du nouveau périphérique de bande                                      |

| Événement           | Description                                                              | Informations sur l'événement                                                           |
|---------------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Tape_close          | La bande est fermée pour lecture/écriture                                | Nom du lecteur de bande                                                                |
| Changement de phase | Un vidage entre dans une nouvelle phase de traitement                    | Nom de la nouvelle phase                                                               |
| Erreur              | Un vidage a rencontré un événement inattendu                             | Message d'erreur                                                                       |
| Snapshot            | Une copie Snapshot est créée ou située                                   | Nom et heure de la copie Snapshot                                                      |
| Base_dump           | Une entrée de vidage de base dans le métafichier interne a été localisée | Le niveau et le temps du vidage de la base (pour les vidages incrémentiels uniquement) |

#### Que sont les événements de restauration

Le champ événement d'un événement de restauration contient un type d'événement suivi d'informations spécifiques à un événement entre parenthèses.

Le tableau suivant fournit des informations sur les événements, leurs descriptions et les informations sur l'événement associé qui peuvent être enregistrées pour une opération de restauration :

| Événement  | Description                               | Informations sur l'événement                                              |
|------------|-------------------------------------------|---------------------------------------------------------------------------|
| Démarrer   | La restauration NDMP est démarrée         | Niveau de restauration et type de restauration                            |
| Fin        | Restaurations effectuées avec succès      | Nombre de fichiers et quantité de données traitées                        |
| Abandonner | L'opération est annulée                   | Nombre de fichiers et quantité de données traitées                        |
| Options    | Les options spécifiées sont répertoriées  | Toutes les options et leurs valeurs associées, y compris les options NDMP |
| Tape_open  | La bande est ouverte en lecture/écriture  | Nom du nouveau périphérique de bande                                      |
| Tape_close | La bande est fermée pour lecture/écriture | Nom du lecteur de bande                                                   |

| Événement           | Description                                                 | Informations sur l'événement |
|---------------------|-------------------------------------------------------------|------------------------------|
| Changement de phase | La restauration entre dans une nouvelle phase de traitement | Nom de la nouvelle phase     |
| Erreur              | La restauration rencontre un événement inattendu            | Message d'erreur             |

## Activation ou désactivation de la journalisation des événements

Vous pouvez activer ou désactiver la journalisation des événements.

### Étapes

1. Pour activer ou désactiver la journalisation des événements, entrez la commande suivante au niveau du clustershell :

```
options -option_name backup.log.enable -option-value {on | off}
```

`on` active la journalisation des événements.

`off` désactive la journalisation des événements.



Le journal des événements est activé par défaut.

## Messages d'erreur relatifs à la sauvegarde sur bande et à la restauration des volumes FlexVol

### Messages d'erreur de sauvegarde et de restauration

Limitation des ressources : pas de thread disponible

- **Message**

```
Resource limitation: no available thread
```

- **Cause**

Le nombre maximal de threads d'E/S de bande locale actifs est actuellement utilisé. Vous pouvez avoir un maximum de 16 lecteurs de bande locaux actifs.

- **\* Action corrective\***

Attendez la fin de certaines tâches de bande avant de lancer une nouvelle tâche de sauvegarde ou de restauration.

### Réservation de bandes préemptée

- **Message**

```
Tape reservation preempted
```

- **Cause**

Le lecteur de bande est utilisé par une autre opération ou la bande a été fermée prématurément.

- \* Action corrective\*

Assurez-vous que le lecteur de bande n'est pas utilisé par une autre opération et que l'application DMA n'a pas interrompu le travail, puis réessayez.

#### Impossible d'initialiser le support

- **Message**

`Could not initialize media`

- **Cause**

Cette erreur peut s'afficher pour l'une des raisons suivantes :

- Le lecteur de bande utilisé pour la sauvegarde est corrompu ou endommagé.
- La bande ne contient pas la sauvegarde complète ou est corrompue.
- Le nombre maximal de threads d'E/S de bande locale actifs est actuellement utilisé.

Vous pouvez avoir un maximum de 16 lecteurs de bande locaux actifs.

- \* Action corrective\*

- Si le lecteur de bande est endommagé ou corrompu, relancez l'opération avec un lecteur de bande valide.
- Si la bande ne contient pas la sauvegarde complète ou est corrompue, vous ne pouvez pas effectuer l'opération de restauration.
- Si les ressources sur bande ne sont pas disponibles, attendez la fin de certaines tâches de sauvegarde ou de restauration, puis relancez l'opération.

#### Nombre maximal de sauvegardes ou de restaurations autorisées (limite maximale de session) en cours

- **Message**

`Maximum number of allowed dumps or restores (maximum session limit) in progress`

- **Cause**

Le nombre maximal de tâches de sauvegarde ou de restauration est déjà en cours d'exécution.

- \* Action corrective\*

Réessayez l'opération une fois que certains travaux en cours d'exécution ont terminé.

#### Erreur de support lors de l'écriture sur bande

- **Message**

Media error on tape write

- **Cause**

La bande utilisée pour la sauvegarde est endommagée.

- \* Action corrective\*

Remplacez la bande et relancez la procédure de sauvegarde.

#### **Échec de l'écriture sur bande**

- **Message**

Tape write failed

- **Cause**

La bande utilisée pour la sauvegarde est endommagée.

- \* Action corrective\*

Remplacez la bande et relancez la procédure de sauvegarde.

#### **Échec de l'écriture sur la bande - une nouvelle bande a rencontré une erreur de support**

- **Message**

Tape write failed - new tape encountered media error

- **Cause**

La bande utilisée pour la sauvegarde est endommagée.

- \* Action corrective\*

Remplacez la bande et réessayez la sauvegarde.

#### **Échec de l'écriture de la bande : la nouvelle bande est cassée ou protégée en écriture**

- **Message**

Tape write failed - new tape is broken or write protected

- **Cause**

La bande utilisée pour la sauvegarde est corrompue ou protégée en écriture.

- \* Action corrective\*

Remplacez la bande et réessayez la sauvegarde.

### Échec de l'écriture sur bande : la nouvelle bande est déjà à la fin du support

- **Message**

Tape write failed - new tape is already at the end of media

- **Cause**

L'espace disponible sur la bande est insuffisant pour terminer la sauvegarde.

- **\* Action corrective\***

Remplacez la bande et réessayez la sauvegarde.

### Erreur d'écriture de bande

- **Message**

Tape write error - The previous tape had less than the required minimum capacity, size MB, for this tape operation, The operation should be restarted from the beginning

- **Cause**

La capacité de la bande est insuffisante pour contenir les données de sauvegarde.

- **\* Action corrective\***

Utilisez des bandes d'une capacité supérieure et relancez la tâche de sauvegarde.

### Erreur de support lors de la lecture de la bande

- **Message**

Media error on tape read

- **Cause**

La bande à partir de laquelle les données sont restaurées est corrompue et peut ne pas contenir toutes les données de sauvegarde.

- **\* Action corrective\***

Si vous êtes sûr que la bande a la sauvegarde complète, réessayez l'opération de restauration. Si la bande ne contient pas la sauvegarde complète, vous ne pouvez pas effectuer l'opération de restauration.

### Erreur de lecture de bande

- **Message**

Tape read error

- **Cause**



Le lecteur de bande est endommagé ou la bande ne contient pas la sauvegarde complète.

- \* Action corrective\*

Si le lecteur de bande est endommagé, utilisez un autre lecteur de bande. Si la bande ne contient pas la sauvegarde complète, vous ne pouvez pas restaurer les données.

#### Déjà à la fin de la bande

- **Message**

Already at the end of tape

- **Cause**

La bande ne contient pas de données ou doit être rembobinée.

- \* Action corrective\*

Si la bande ne contient pas de données, utilisez la bande contenant la sauvegarde et relancez la procédure de restauration. Sinon, rembobinez la bande et relancez la tâche de restauration.

#### La taille de l'enregistrement sur bande est trop petite. Essayez une taille plus grande.

- **Message**

Tape record size is too small. Try a larger size.

- **Cause**

Le facteur de blocage spécifié pour l'opération de restauration est plus petit que le facteur de blocage utilisé pendant la sauvegarde.

- \* Action corrective\*

Utilisez le même facteur de blocage que celui spécifié lors de la sauvegarde.

#### La taille de l'enregistrement sur bande doit être Block\_size1 et non block\_size2

- **Message**

Tape record size should be block\_size1 and not block\_size2

- **Cause**

Le facteur de blocage spécifié pour la restauration locale est incorrect.

- \* Action corrective\*

Relancez la tâche de restauration avec block\_size1 comme facteur de blocage.

**La taille d'enregistrement de la bande doit être comprise entre 4 Ko et 256 Ko**

- **Message**

Tape record size must be in the range between 4KB and 256KB

- **Cause**

Le facteur de blocage spécifié pour l'opération de sauvegarde ou de restauration n'est pas dans la plage autorisée.

- **\* Action corrective\***

Spécifiez un facteur de blocage compris entre 4 Ko et 256 Ko.

## **Messages d'erreur NDMP**

### **Erreur de communication réseau**

- **Message**

Network communication error

- **Cause**

La communication avec une bande distante dans une connexion NDMP à trois voies a échoué.

- **\* Action corrective\***

Vérifiez la connexion réseau au dispositif de déplacement distant.

### **Message de Read Socket : error\_string**

- **Message**

Message from Read Socket: error\_string

- **Cause**

La restauration de la communication à partir de la bande distante dans la connexion NDMP à 3 voies comporte des erreurs.

- **\* Action corrective\***

Vérifiez la connexion réseau au dispositif de déplacement distant.

### **Message de Write Dirnet : chaîne\_d'erreur**

- **Message**

Message from Write Dirnet: error\_string

- **Cause**

Une erreur est survenue lors de la sauvegarde de la communication sur une bande distante au niveau d'une connexion NDMP à trois voies.

- \* Action corrective\*

Vérifiez la connexion réseau au dispositif de déplacement distant.

#### Prise de lecture reçue EOF

- **Message**

```
Read Socket received EOF
```

- **Cause**

Tentative de communication avec une bande distante dans une connexion à trois voies NDMP a atteint la fin du repère de fichier. Vous tentez peut-être d'effectuer une restauration à trois voies à partir d'une image de sauvegarde d'une taille de bloc supérieure.

- \* Action corrective\*

Spécifiez la taille de bloc correcte et relancez l'opération de restauration.

#### ndmpd numéro de version non valide : numéro\_version ``

- **Message**

```
ndmpd invalid version number: version_number
```

- **Cause**

La version NDMP spécifiée n'est pas prise en charge par le système de stockage.

- \* Action corrective\*

Spécifiez NDMP version 4.

#### Session ndmpd session session\_ID non active

- **Message**

```
ndmpd session session_ID not active
```

- **Cause**

Il se peut que la session NDMP n'existe pas.

- \* Action corrective\*

Utilisez le `ndmpd status` Commande pour afficher les sessions NDMP actives.

#### Impossible d'obtenir la référence vol pour Volume nom\_volume

- **Message**

Could not obtain vol ref for Volume vol\_name

- **Cause**

La référence de volume n'a pas pu être obtenue car le volume peut être utilisé par d'autres opérations.

- **\* Action corrective\***

Réessayez ultérieurement.

#### Type de connexion de données ["NDMP4\_ADDR\_TCP"|"NDMP4\_ADDR\_TCP\_IPv6"] non pris en charge pour les connexions de contrôle ["IPv6"|"IPv4"]

- **Message**

Data connection type ["NDMP4\_ADDR\_TCP"|"NDMP4\_ADDR\_TCP\_IPv6"] not supported for ["IPv6"|"IPv4"] control connections

- **Cause**

En mode node-scoped NDMP, la connexion de données NDMP établie doit être du même type d'adresse réseau (IPv4 ou IPv6) que la connexion de contrôle NDMP.

- **\* Action corrective\***

Contactez le fournisseur de votre application de sauvegarde.

#### ÉCOUTE DES DONNÉES : erreur de préparation de la connexion des données DE LA CABINE

- **Message**

DATA LISTEN: CAB data connection prepare precondition error

- **Cause**

L'écoute des données NDMP échoue lorsque l'application de sauvegarde a négocié l'extension CAB avec le serveur NDMP et il existe une discordance dans le type d'adresse de connexion de données NDMP spécifié entre le message NDMP\_CAB\_DATA\_CONN\_READY et NDMP\_DATA\_LISTEN.

- **\* Action corrective\***

Contactez le fournisseur de votre application de sauvegarde.

#### CONNEXION DES DONNÉES : erreur de préparation de la connexion des données DE LA CABINE

- **Message**

DATA CONNECT: CAB data connection prepare precondition error

- **Cause**

La connexion des données NDMP échoue lorsque l'application de sauvegarde a négocié l'extension CAB avec le serveur NDMP et qu'il existe une discordance dans le type d'adresse de connexion de données NDMP spécifié entre le message NDMP\_CAB\_DATA\_CONN\_READY et le message NDMP\_DATA\_CONNECT.

- \* Action corrective\*

Contactez le fournisseur de votre application de sauvegarde.

**Erreur:échec de l'affichage : impossible d'obtenir le mot de passe de l'utilisateur '<nom d'utilisateur>'**

- **Message**

Error: show failed: Cannot get password for user '<username>'

- **Cause**

Configuration de compte utilisateur incomplète pour NDMP

- \* Action corrective\*

Assurez-vous que le compte utilisateur est associé à la méthode d'accès SSH et que la méthode d'authentification est un mot de passe utilisateur.

## **Vidage des messages d'erreur**

**Le volume de destination est en lecture seule**

- **Message**

Destination volume is read-only

- **Cause**

Le chemin vers lequel l'opération de restauration est tentée est en lecture seule.

- \* Action corrective\*

Essayez de restaurer les données à un autre emplacement.

**Le qtrees de destination est en lecture seule**

- **Message**

Destination qtree is read-only

- **Cause**

Le qtrees vers laquelle la restauration est tentée de lire uniquement.

- \* Action corrective\*

Essayez de restaurer les données à un autre emplacement.

## Vidages temporairement désactivés sur le volume, réessayez

- **Message**

`Dumps temporarily disabled on volume, try again`

- **Cause**

La tentative de sauvegarde du dump NDMP est effectuée sur un volume de destination SnapMirror faisant partie d'un ou plusieurs `snapmirror break` ou un `snapmirror resync` fonctionnement.

- **\* Action corrective\***

Attendez le `snapmirror break` ou `snapmirror resync` opération pour terminer puis effectuer l'opération de vidage.



Chaque fois que l'état d'un volume de destination SnapMirror passe de la lecture/écriture à la lecture seule ou de la lecture seule à la lecture/écriture, vous devez effectuer une sauvegarde de base.

## Étiquettes NFS non reconnues

- **Message**

`Error: Aborting: dump encountered NFS security labels in the file system`

- **Cause**

Les étiquettes de sécurité NFS sont prises en charge à partir de ONTAP 9.9.1 lorsque NFSv4.2 est activé. Toutefois, les étiquettes de sécurité NFS ne sont actuellement pas reconnues par le moteur de vidage. S'il rencontre des étiquettes de sécurité NFS sur les fichiers, les répertoires ou tout fichier spécial dans un format quelconque de dump, le dump échoue.

- **\* Action corrective\***

Vérifiez qu'aucun fichier ni répertoire ne possède d'étiquettes de sécurité NFS.

## Aucun fichier n'a été créé

- **Message**

`No files were created`

- **Cause**

Une tentative de DAR d'annuaire a été effectuée sans activer la fonctionnalité DAR améliorée.

- **\* Action corrective\***

Activez la fonctionnalité DAR améliorée et réessayez le DAR.

#### Échec de la restauration du fichier <nom du fichier>

- **Message**

Restore of the file file name failed

- **Cause**

Lorsqu'un fichier DAR (Direct Access Recovery) d'un fichier dont le nom de fichier est le même que celui d'un LUN sur le volume de destination est exécuté, le DAR échoue.

- **\* Action corrective\***

Essayez de nouveau DAR du fichier.

#### La troncature a échoué pour src inode <numéro inode>...

- **Message**

Truncation failed for src inode <inode number>. Error <error number>. Skipping inode.

- **Cause**

L'inode d'un fichier est supprimé lors de la restauration du fichier.

- **\* Action corrective\***

Attendez la fin de l'opération de restauration sur un volume avant d'utiliser ce volume.

#### Impossible de verrouiller un snapshot requis par le dump

- **Message**

Unable to lock a snapshot needed by dump

- **Cause**

La copie Snapshot spécifiée pour la sauvegarde n'est pas disponible.

- **\* Action corrective\***

Réessayez la sauvegarde avec une autre copie Snapshot.

Utilisez le `snap list` Commande pour afficher la liste des copies Snapshot disponibles.

#### Impossible de localiser les fichiers bitmap

- **Message**

Unable to locate bitmap files

- **Cause**

Les fichiers bitmap requis pour l'opération de sauvegarde ont peut-être été supprimés. Dans ce cas, la sauvegarde ne peut pas être redémarrée.

- \* Action corrective\*

Effectuez à nouveau la sauvegarde.

#### **Le volume est temporairement dans un état transitoire**

- **Message**

Volume is temporarily in a transitional state

- **Cause**

Le volume en cours de sauvegarde est temporairement démonté.

- \* Action corrective\*

Attendez un certain temps avant d'effectuer à nouveau la sauvegarde.

#### **Messages d'erreur SMTape**

##### **Blocs hors service**

- **Message**

Chunks out of order

- **Cause**

Les bandes de sauvegarde ne sont pas restaurées dans l'ordre correct.

- \* Action corrective\*

Relancez l'opération de restauration et chargez les bandes dans l'ordre correct.

##### **Le format de bloc n'est pas pris en charge**

- **Message**

Chunk format not supported

- **Cause**

L'image de sauvegarde n'est pas SMTape.

- \* Action corrective\*

Si l'image de sauvegarde n'est pas SMTape, essayez de procéder à nouveau à l'opération avec une bande dotée de la sauvegarde SMTape.



### Impossible d'allouer de la mémoire

- **Message**

Failed to allocate memory

- **Cause**

La mémoire du système est insuffisante.

- \* Action corrective\*

Réessayez ultérieurement lorsque le système n'est pas trop occupé.

### Impossible d'obtenir le tampon de données

- **Message**

Failed to get data buffer

- **Cause**

Le système de stockage est à court de mémoire tampon.

- \* Action corrective\*

Attendez la fin de certaines opérations du système de stockage, puis relancez la tâche.

### Impossible de trouver le snapshot

- **Message**

Failed to find snapshot

- **Cause**

La copie Snapshot spécifiée pour la sauvegarde est indisponible.

- \* Action corrective\*

Vérifiez si la copie Snapshot spécifiée est disponible. Si ce n'est pas le cas, réessayez avec la copie Snapshot appropriée.

### Impossible de créer un snapshot

- **Message**

Failed to create snapshot

- **Cause**

Le volume contient déjà le nombre maximal de copies Snapshot.

- \* Action corrective\*

Supprimez certaines copies Snapshot, puis réessayez l'opération de sauvegarde.

#### Impossible de verrouiller le snapshot

- **Message**

Failed to lock snapshot

- **Cause**

La copie Snapshot est utilisée ou a été supprimée.

- \* Action corrective\*

Si la copie Snapshot est utilisée par une autre opération, attendez la fin de cette opération, puis réessayez la sauvegarde. Si la copie Snapshot a été supprimée, vous ne pouvez pas effectuer la sauvegarde.

#### Impossible de supprimer le snapshot

- **Message**

Failed to delete snapshot

- **Cause**

Impossible de supprimer la copie Snapshot automatique, car elle est en cours d'utilisation par d'autres opérations.

- \* Action corrective\*

Utilisez le `snap` Commande permettant de déterminer l'état de la copie Snapshot. Si aucune copie Snapshot n'est requise, supprimez-la manuellement.

#### Impossible d'obtenir le dernier snapshot

- **Message**

Failed to get latest snapshot

- **Cause**

Il se peut que la dernière copie Snapshot n'existe pas, car le volume est en cours d'initialisation par SnapMirror.

- \* Action corrective\*

Réessayez une fois l'initialisation terminée.

#### Impossible de charger une nouvelle bande

- **Message**

Failed to load new tape

- **Cause**

Erreur dans le lecteur de bande ou le support.

- **\* Action corrective\***

Remplacez la bande et réessayez l'opération.

#### Impossible d'initialiser la bande

- **Message**

`Failed to initialize tape`

- **Cause**

Ce message d'erreur peut s'afficher pour l'une des raisons suivantes :

- L'image de sauvegarde n'est pas SMTape.
- Le facteur de blocage de la bande spécifié est incorrect.
- La bande est corrompue ou endommagée.
- La mauvaise bande est chargée pour la restauration.

- **\* Action corrective\***

- Si l'image de sauvegarde n'est pas SMTape, essayez de procéder à nouveau à l'opération avec une bande dotée d'une sauvegarde SMTape.
- Si le facteur de blocage est incorrect, spécifiez le facteur de blocage correct et relancez l'opération.
- Si la bande est corrompue, vous ne pouvez pas effectuer l'opération de restauration.
- Si la mauvaise bande est chargée, recommencez l'opération avec la bonne bande.

#### Impossible d'initialiser le flux de restauration

- **Message**

`Failed to initialize restore stream`

- **Cause**

Ce message d'erreur peut s'afficher pour l'une des raisons suivantes :

- L'image de sauvegarde n'est pas SMTape.
- Le facteur de blocage de la bande spécifié est incorrect.
- La bande est corrompue ou endommagée.
- La mauvaise bande est chargée pour la restauration.

- **\* Action corrective\***

- Si l'image de sauvegarde n'est pas SMTape, essayez de procéder à nouveau à l'opération avec une bande dotée de la sauvegarde SMTape.
- Si le facteur de blocage est incorrect, spécifiez le facteur de blocage correct et relancez l'opération.

- Si la bande est corrompue, vous ne pouvez pas effectuer l'opération de restauration.
- Si la mauvaise bande est chargée, recommencez l'opération avec la bonne bande.

#### Impossible de lire l'image de sauvegarde

- **Message**

Failed to read backup image

- **Cause**

La bande est corrompue

- **\* Action corrective\***

Si la bande est corrompue, vous ne pouvez pas effectuer l'opération de restauration.

#### En-tête d'image manquant ou corrompu

- **Message**

Image header missing or corrupted

- **Cause**

La bande ne contient pas de sauvegarde SMTape valide.

- **\* Action corrective\***

Réessayez avec une bande contenant une sauvegarde valide.

#### Assertion interne

- **Message**

Internal assertion

- **Cause**

Il y a une erreur SMTape interne.

- **\* Action corrective\***

Signalez l'erreur et envoyez le `etc/log/backup` dossier au support technique.

#### Numéro magique d'image de sauvegarde non valide

- **Message**

Invalid backup image magic number

- **Cause**

L'image de sauvegarde n'est pas SMTape.

- \* Action corrective\*

Si l'image de sauvegarde n'est pas SMTape, essayez de procéder à nouveau à l'opération avec une bande dotée de la sauvegarde SMTape.

#### Checksum d'image de sauvegarde non valide

- **Message**

Invalid backup image checksum

- **Cause**

La bande est corrompue

- \* Action corrective\*

Si la bande est corrompue, vous ne pouvez pas effectuer l'opération de restauration.

#### Bande d'entrée non valide

- **Message**

Invalid input tape

- **Cause**

La signature de l'image de sauvegarde n'est pas valide dans l'en-tête de bande. Les données de la bande sont corrompues ou ne contiennent pas d'image de sauvegarde valide.

- \* Action corrective\*

Relancez la procédure de restauration avec une image de sauvegarde valide.

#### Chemin de volume non valide

- **Message**

Invalid volume path

- **Cause**

Le volume spécifié pour l'opération de sauvegarde ou de restauration est introuvable.

- \* Action corrective\*

Relancez le travail avec un chemin de volume et un nom de volume valides.

#### Non-concordance de l'ID du jeu de sauvegarde

- **Message**

Mismatch in backup set ID

- **Cause**

La bande chargée pendant un changement de bande ne fait pas partie du jeu de sauvegarde.

- \* Action corrective\*

Chargez la bonne bande et relancez le travail.

#### Incompatibilité dans l'horodatage de sauvegarde

- **Message**

Mismatch in backup time stamp

- **Cause**

La bande chargée pendant un changement de bande ne fait pas partie du jeu de sauvegarde.

- \* Action corrective\*

Utilisez le `smtape restore -h` commande pour vérifier les informations d'en-tête d'une bande.

#### Travail interrompu en raison de l'arrêt

- **Message**

Job aborted due to shutdown

- **Cause**

Le système de stockage est en cours de redémarrage.

- \* Action corrective\*

Relancez le travail après le redémarrage du système de stockage.

#### Travail interrompu en raison de la suppression automatique de l'instantané

- **Message**

Job aborted due to Snapshot autodelete

- **Cause**

L'espace disponible sur le volume est insuffisant et a déclenché la suppression automatique des copies Snapshot.

- \* Action corrective\*

Libérez de l'espace dans le volume et relancez le travail.

#### La bande est actuellement utilisée par d'autres opérations

- **Message**

Tape is currently in use by other operations

- **Cause**

Le lecteur de bande est utilisé par un autre travail.

- \* Action corrective\*

Réessayez la sauvegarde une fois la tâche active terminée.

#### Bandes hors service

- **Message**

Tapes out of order

- **Cause**

La première bande de la séquence de restauration pour l'opération de restauration n'a pas d'en-tête d'image.

- \* Action corrective\*

Chargez la bande avec l'en-tête de l'image et relancez le travail.

#### Échec du transfert (abandon en raison de l'opération MetroCluster)

- **Message**

Transfer failed (Aborted due to MetroCluster operation)

- **Cause**

L'opération SMTape est abandonnée en raison d'une opération de basculement ou de rétablissement.

- \* Action corrective\*

Effectuez l'opération SMTape une fois le basculement ou le rétablissement terminé.

#### Échec du transfert (annulation initiée par l'ARL)

- **Message**

Transfer failed (ARL initiated abort)

- **Cause**

Lorsqu'une opération SMTape est en cours lorsqu'un transfert d'agrégats est lancé, l'opération SMTape est abandonnée.

- \* Action corrective\*

Effectuez l'opération SMTape une fois l'opération de transfert d'agrégats terminée.

#### **Echec du transfert (annulation initiée par le CFO)**

- **Message**

`Transfer failed (CFO initiated abort)`

- **Cause**

L'opération SMTape est abandonnée en raison d'une opération de basculement du stockage (basculement et rétablissement) d'un agrégat CFO.

- \* Action corrective\*

Effectuez l'opération SMTape après le basculement du stockage vers la fin de l'agrégat CFO.

#### **Echec du transfert (annulation initiée SFO)**

- **Message**

`Transfer failed (SFO initiated abort)`

- **Cause**

L'opération SMTape est abandonnée en raison d'une opération de basculement du stockage (basculement et rétablissement).

- \* Action corrective\*

Effectue l'opération SMTape après la fin de l'opération de basculement (basculement et rétablissement) du stockage.

#### **Agrégat sous-jacent en cours de migration**

- **Message**

`Underlying aggregate under migration`

- **Cause**

Lorsqu'une opération SMTape est lancée sur un agrégat en cours de migration (basculement du stockage ou transfert d'agrégats), l'opération SMTape échoue.

- \* Action corrective\*

Effectuez l'opération SMTape une fois la migration de l'agrégat terminée.

#### **Le volume est en cours de migration**

- **Message**



Volume is currently under migration

- **Cause**

La migration de volumes et la sauvegarde SMTape ne peuvent pas s'exécuter simultanément.

- \* Action corrective\*

Relancez la procédure de sauvegarde une fois la migration du volume terminée.

#### Volume hors ligne

- **Message**

Volume offline

- **Cause**

Le volume sauvegardé est hors ligne.

- \* Action corrective\*

Mettez le volume en ligne et réessayez la sauvegarde.

#### Volume non restreint

- **Message**

Volume not restricted

- **Cause**

Le volume de destination vers lequel les données sont restaurées n'est pas restreint.

- \* Action corrective\*

Limitez le volume et relancez l'opération de restauration.

## Configuration NDMP

### Présentation de la configuration NDMP

Vous pouvez rapidement configurer un cluster ONTAP 9 de sorte qu'il utilise le protocole NDMP (Network Data Management Protocol) pour sauvegarder les données directement sur bande à l'aide d'une application de sauvegarde tierce.

Si l'application de backup supporte Cluster Aware Backup (CAB), vous pouvez configurer NDMP sous la forme *SVM-scoped* ou *node-scoped* :

- SVM-scoped au niveau du cluster (admin SVM) permet de sauvegarder tous les volumes hébergés sur différents nœuds du cluster. SVM-scoped NDMP est recommandé si possible.
- Node-scoped NDMP vous permet de sauvegarder tous les volumes hébergés sur ce nœud.

Si l'application de backup ne prend pas en charge CAB, il faut utiliser node-scoped NDMP.

SVM-scoped et node-scoped NDMP sont mutuellement exclusifs ; ils ne peuvent pas être configurés sur le même cluster.



Le protocole NDMP avec étendue du nœud est obsolète dans ONTAP 9.

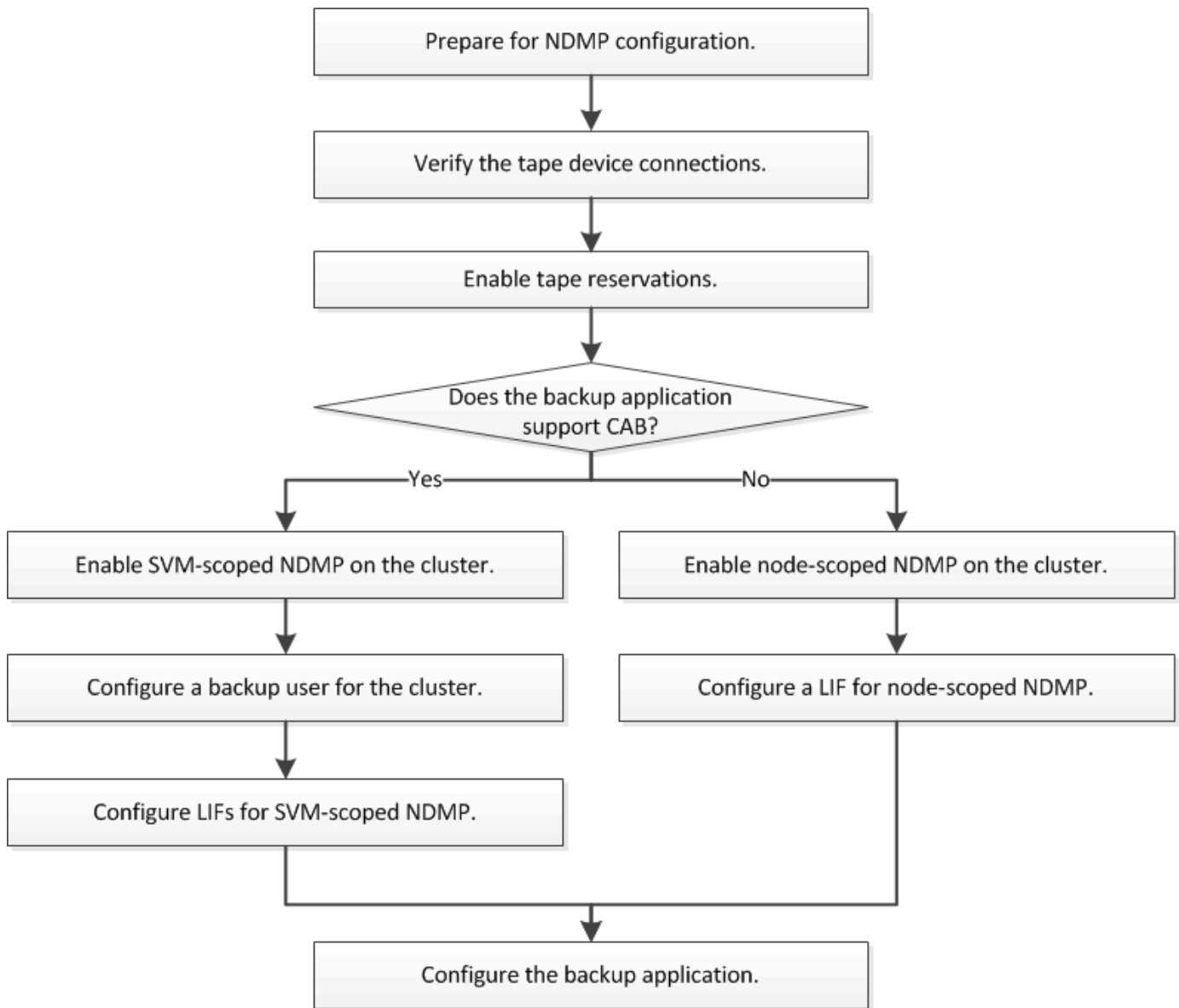
En savoir plus sur "[Sauvegarde « cluster Aware Backup » \(CAB\)](#)".

Avant de configurer NDMP, vérifiez les points suivants :

- Vous disposez d'une application de sauvegarde tierce (également appelée Data Management application ou DMA).
- Vous êtes un administrateur de cluster.
- Les périphériques de bande et un serveur multimédia en option sont installés.
- Les périphériques de bande sont connectés au cluster via un commutateur Fibre Channel (FC) et ne sont pas directement connectés.
- Au moins une unité de bande a un numéro d'unité logique (LUN) de 0.

## Workflow de configuration NDMP

La configuration de la sauvegarde sur bande sur NDMP implique la préparation de la configuration NDMP, la vérification des connexions du périphérique de bande, l'activation des réservations sur bande, la configuration de NDMP au niveau SVM ou node, l'activation de NDMP sur le cluster, la configuration d'un utilisateur de sauvegarde, la configuration des LIFs et la configuration de l'application de sauvegarde.



## Préparation à la configuration NDMP

Avant de configurer l'accès de sauvegarde sur bande via le protocole NDMP (Network Data Management Protocol), vous devez vérifier que la configuration planifiée est prise en charge. Vérifier que vos lecteurs de bande sont répertoriés comme disques qualifiés sur chaque nœud, vérifier que tous les nœuds disposent des LIF intercluster, Et déterminer si l'application de sauvegarde prend en charge l'extension CLUSTER Aware Backup (CAB).

### Étapes

1. Consultez le tableau de compatibilité de votre fournisseur d'applications de sauvegarde pour la prise en charge du protocole ONTAP (NetApp ne qualifie pas les applications de sauvegarde tierces avec ONTAP ou NDMP).

Vérifiez que les composants NetApp suivants sont compatibles :

- Version de ONTAP 9 qui s'exécute sur le cluster.

- Le fournisseur et la version de l'application de sauvegarde, par exemple Veritas NetBackup 8.2 ou CommVault.
- Les lecteurs de bande décrivent en détail le fabricant, le modèle et l'interface des lecteurs de bande, par exemple IBM Ultrium 8 ou HPE StoreEver Ultrium 30750 LTO-8.
- Plateformes des nœuds du cluster : par exemple, FAS8700 ou A400



Vous trouverez des matrices de support de compatibilité ONTAP existantes pour les applications de sauvegarde dans le "[Matrice d'interopérabilité NetApp](#)".

2. Vérifiez que vos lecteurs de bande sont répertoriés comme lecteurs qualifiés dans le fichier de configuration de bande intégré de chaque nœud :

- a. Sur l'interface de ligne de commande, affichez le fichier de configuration de bande intégré à l'aide du `storage tape show-supported-status` commande.

```
cluster1::> storage tape show-supported-status

Node: cluster1-1

Tape Drives Is
----- -
Certance Ultrium 2 true Dynamically Qualified
Certance Ultrium 3 true Dynamically Qualified
Digital DLT2000 true Qualified
```

- b. Comparez vos lecteurs de bande à la liste des lecteurs qualifiés dans la sortie.



Les noms des périphériques de bande dans la sortie peuvent varier légèrement par rapport aux noms figurant sur l'étiquette du périphérique ou dans la matrice d'interopérabilité. Par exemple, le DLT2000 numérique peut également être appelé DL2k. Vous pouvez ignorer ces différences mineures de dénomination.

- c. Si un périphérique ne figure pas dans la liste comme indiqué dans le résultat, même si celui-ci est qualifié conformément à la matrice d'interopérabilité, téléchargez et installez un fichier de configuration mis à jour pour le périphérique, en suivant les instructions du site du support NetApp.

["Téléchargements NetApp : fichiers de configuration des lecteurs de bande"](#)

Il se peut qu'un périphérique qualifié ne figure pas dans le fichier de configuration de bande intégré si le périphérique de bande a été qualifié après l'expédition du nœud.

3. Vérifier que chaque nœud du cluster dispose d'un LIF intercluster :

- a. Afficher les LIFs intercluster sur les nœuds en utilisant le `network interface show -role intercluster` commande.

```
cluster1::> network interface show -role intercluster
```

|            | Logical   | Status     | Network       | Current    |
|------------|-----------|------------|---------------|------------|
| Current Is |           |            |               |            |
| Vserver    | Interface | Admin/Oper | Address/Mask  | Node       |
| Port       | Home      |            |               |            |
| -----      | -----     | -----      | -----         | -----      |
| -----      | -----     | -----      | -----         | -----      |
| cluster1   | IC1       | up/up      | 192.0.2.65/24 | cluster1-1 |
| e0a        | true      |            |               |            |

- b. Si aucune LIF intercluster n'existe sur un nœud, créer une LIF intercluster en utilisant le `network interface create` commande.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster
```

```
cluster1::> network interface show -role intercluster
```

|            | Logical   | Status     | Network       | Current    |
|------------|-----------|------------|---------------|------------|
| Current Is |           |            |               |            |
| Vserver    | Interface | Admin/Oper | Address/Mask  | Node       |
| Port       | Home      |            |               |            |
| -----      | -----     | -----      | -----         | -----      |
| -----      | -----     | -----      | -----         | -----      |
| cluster1   | IC1       | up/up      | 192.0.2.65/24 | cluster1-1 |
| e0a        | true      |            |               |            |
| cluster1   | IC2       | up/up      | 192.0.2.68/24 | cluster1-2 |
| e0b        | true      |            |               |            |

### "Gestion du réseau"

- Déterminez si l'application de sauvegarde prend en charge Cluster Aware Backup (CAB) à l'aide de la documentation fournie avec l'application de sauvegarde.

Le support CAB est un facteur clé pour déterminer le type de sauvegarde que vous pouvez effectuer.

## Vérifiez les connexions du lecteur de bande

Vous devez vous assurer que tous les lecteurs et changeurs de supports sont visibles dans ONTAP en tant que périphériques.

## Étapes

1. Affichez des informations sur tous les lecteurs et changeurs de supports à l'aide du `storage tape show` commande.

```
cluster1::> storage tape show
```

```
Node: cluster1-01
```

| Device ID | Device Type   | Description       |
|-----------|---------------|-------------------|
| sw4:10.11 | tape drive    | HP LTO-3          |
| 0b.125L1  | media changer | HP MSL G3 Series  |
| 0d.4      | tape drive    | IBM LTO 5 ULT3580 |
| 0d.4L1    | media changer | IBM 3573-TL       |
| ...       |               |                   |

2. Si aucun lecteur de bande n'est affiché, résolvez le problème.
3. Si un changeur de supports n'est pas affiché, affichez les informations relatives aux changeurs de supports à l'aide du `storage tape show-media-changer` commande, puis résolution du problème.

```
cluster1::> storage tape show-media-changer
```

```
Media Changer: sw4:10.11L1
```

```
Description: PX70-TL
```

```
WWNN: 2:00a:000e11:10b919
```

```
WWPN: 2:00b:000e11:10b919
```

```
Serial Number: 00FRU7800000_LL1
```

```
Errors: -
```

```
Paths:
```

| Node        | Initiator | Alias | Device State |
|-------------|-----------|-------|--------------|
| cluster1-01 | 2b        | mc0   | in-use       |
| normal      |           |       |              |
| ...         |           |       |              |

## Activer les réservations sur bande

Vous devez vous assurer que les lecteurs de bande sont réservés à l'utilisation par les applications de sauvegarde pour les opérations de sauvegarde NDMP.

### Description de la tâche

Les paramètres de réservation varient selon les applications de sauvegarde et ces paramètres doivent correspondre à l'application de sauvegarde et aux nœuds ou serveurs utilisant les mêmes lecteurs. Consultez la documentation fournisseur de l'application de sauvegarde pour connaître les paramètres de réservation corrects.

### Étapes

1. Activer les réservations à l'aide de options `-option-name tape.reservations -option-value persistent` commande.

La commande suivante active les réservations avec le `persistent` valeur :

```
cluster1::> options -option-name tape.reservations -option-value
persistent
2 entries were modified.
```

2. Vérifiez que les réservations sont activées sur tous les nœuds à l'aide de l' options `tape.reservations` commande, puis vérifiez la sortie.

```
cluster1::> options tape.reservations

cluster1-1
 tape.reservations persistent

cluster1-2
 tape.reservations persistent
2 entries were displayed.
```

## Configurer SVM-scoped NDMP

### Activer SVM-scoped NDMP sur le cluster

Si le DMA prend en charge l'extension Cluster Aware Backup (CAB), vous pouvez sauvegarder tous les volumes hébergés sur différents nœuds d'un cluster en activant SVM-scoped NDMP, en activant le service NDMP sur le cluster (admin SVM) et en configurant les LIF de données et de contrôle.

### Ce dont vous avez besoin

L'extension CAB doit être prise en charge par le DMA.

### Description de la tâche

La désactivation du mode node-scoped NDMP permet d'activer le mode SVM-scoped NDMP sur le cluster.

Étapes

- 1. Activer le mode NDMP SVM-scoped :

```
cluster1::> system services ndmp node-scope-mode off
```

Le mode NDMP SVM-scoped est activé.

- 2. Activer le service NDMP sur le SVM d'admin:

```
cluster1::> vservice services ndmp on -vservice cluster1
```

Le type d'authentification est défini sur challenge par défaut, l'authentification en texte brut est désactivée.



Pour des communications sécurisées, vous devez maintenir l'authentification en texte brut désactivée.

- 3. Vérifier que le service NDMP est activé :

```
cluster1::> vservice services ndmp show
```

| Vservice | Enabled | Authentication type |
|----------|---------|---------------------|
| -----    | -----   | -----               |
| cluster1 | true    | challenge           |
| vs1      | false   | challenge           |

Activez un utilisateur de sauvegarde pour l'authentification NDMP

Pour authentifier SVM-scoped NDMP depuis l'application de backup, un utilisateur administratif doit disposer des privilèges suffisants et d'un mot de passe NDMP.

Description de la tâche

Vous devez générer un mot de passe NDMP pour les utilisateurs admin de sauvegarde. Vous pouvez activer les utilisateurs admin de sauvegarde au niveau du cluster ou de la SVM et, si nécessaire, vous pouvez créer un nouvel utilisateur. Par défaut, les utilisateurs disposant des rôles suivants peuvent s'authentifier pour la sauvegarde NDMP :

- Au niveau du cluster : admin ou backup
- SVM individuels : vsadmin ou vsadmin-backup

Si vous utilisez un utilisateur NIS ou LDAP, l'utilisateur doit exister sur le serveur respectif. Vous ne pouvez pas utiliser un utilisateur Active Directory.



## Étapes

1. Afficher les utilisateurs et autorisations admin actuels :

```
security login show
```

2. Si nécessaire, créez un nouvel utilisateur de sauvegarde NDMP avec le `security login create` Commande et le rôle approprié pour les privilèges des SVM au niveau du cluster ou individuels.

Vous pouvez spécifier un nom d'utilisateur de sauvegarde locale ou un nom d'utilisateur NIS ou LDAP pour l' `-user-or-group-name` paramètre.

La commande suivante crée l'utilisateur de sauvegarde `backup_admin1` avec le `backup` rôle pour l'ensemble du cluster :

```
cluster1::> security login create -user-or-group-name backup_admin1
-application ssh -authmethod password -role backup
```

La commande suivante crée l'utilisateur de sauvegarde `vsbackup_admin1` avec le `vsadmin-backup` Rôle d'un SVM individuel :

```
cluster1::> security login create -user-or-group-name vsbackup_admin1
-application ssh -authmethod password -role vsadmin-backup
```

Entrez un mot de passe pour le nouvel utilisateur et confirmez.

3. Générer un mot de passe pour la SVM d'admin via le `vserver services ndmp generate password` commande.

Le mot de passe généré doit être utilisé pour authentifier la connexion NDMP par l'application de sauvegarde.

```
cluster1::> vserver services ndmp generate-password -vserver cluster1
-user backup_admin1

Vserver: cluster1
User: backup_admin1
Password: qG5CqQHYxw7tE57g
```

## Configurez les LIF

Vous devez identifier les LIF qui seront utilisées pour établir une connexion de données entre les données et les ressources sur bande, et pour contrôler la connexion entre la SVM d'administration et l'application de sauvegarde. Une fois les LIF définies, vous devez vérifier que les politiques de pare-feu et de basculement sont définies pour les LIF et spécifier le rôle d'interface privilégié.

Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir ["LIF et politiques de services dans ONTAP 9.6 et versions ultérieures"](#).

Étapes

- 1. Identifier les LIF intercluster, cluster-management et node-management en utilisant le network interface show commande avec -role paramètre.

La commande suivante affiche les LIFs intercluster :

```
cluster1::> network interface show -role intercluster
```

| Current  | Is    | Logical   | Status     | Network       | Current    |
|----------|-------|-----------|------------|---------------|------------|
| Vserver  |       | Interface | Admin/Oper | Address/Mask  | Node       |
| Port     | Home  |           |            |               |            |
| -----    | ----- | -----     | -----      | -----         |            |
| cluster1 |       | IC1       | up/up      | 192.0.2.65/24 | cluster1-1 |
| e0a      | true  |           |            |               |            |
| cluster1 |       | IC2       | up/up      | 192.0.2.68/24 | cluster1-2 |
| e0b      | true  |           |            |               |            |

La commande suivante affiche la LIF cluster-management :

```
cluster1::> network interface show -role cluster-mgmt
```

| Current  | Is    | Logical      | Status     | Network       | Current    |
|----------|-------|--------------|------------|---------------|------------|
| Vserver  |       | Interface    | Admin/Oper | Address/Mask  | Node       |
| Port     | Home  |              |            |               |            |
| -----    | ----- | -----        | -----      | -----         |            |
| cluster1 |       | cluster_mgmt | up/up      | 192.0.2.60/24 | cluster1-2 |
| e0M      | true  |              |            |               |            |

La commande suivante affiche les LIFs de node-management :

```
cluster1::> network interface show -role node-mgmt
```

|            | Logical          | Status     | Network       | Current    |
|------------|------------------|------------|---------------|------------|
| Current Is |                  |            |               |            |
| Vserver    | Interface        | Admin/Oper | Address/Mask  | Node       |
| Port       | Home             |            |               |            |
| -----      | -----            | -----      | -----         | -----      |
| -----      | -----            |            |               |            |
| cluster1   | cluster1-1_mgmt1 | up/up      | 192.0.2.69/24 | cluster1-1 |
| e0M        | true             |            |               |            |
|            | cluster1-2_mgmt1 | up/up      | 192.0.2.70/24 | cluster1-2 |
| e0M        | true             |            |               |            |

2. S'assurer que la politique de pare-feu est activée pour NDMP sur les LIF intercluster, cluster-management (cluster-mgmt) et node-management (node-mgmt) :

- Vérifiez que la politique de pare-feu est activée pour NDMP à l'aide de `system services firewall policy show` commande.

La commande suivante affiche la politique de pare-feu pour la LIF cluster-management :

```
cluster1::> system services firewall policy show -policy cluster
```

| Vserver | Policy  | Service | Allowed     |
|---------|---------|---------|-------------|
| -----   | -----   | -----   | -----       |
| cluster | cluster | dns     | 0.0.0.0/0   |
|         |         | http    | 0.0.0.0/0   |
|         |         | https   | 0.0.0.0/0   |
|         |         | ** ndmp | 0.0.0.0/0** |
|         |         | ndmps   | 0.0.0.0/0   |
|         |         | ntp     | 0.0.0.0/0   |
|         |         | rsh     | 0.0.0.0/0   |
|         |         | snmp    | 0.0.0.0/0   |
|         |         | ssh     | 0.0.0.0/0   |
|         |         | telnet  | 0.0.0.0/0   |

10 entries were displayed.

La commande suivante affiche la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy show -policy intercluster
```

| Vserver  | Policy       | Service | Allowed           |
|----------|--------------|---------|-------------------|
| cluster1 | intercluster | dns     | -                 |
|          |              | http    | -                 |
|          |              | https   | -                 |
|          |              | **ndmp  | 0.0.0.0/0, ::/0** |
|          |              | ndmps   | -                 |
|          |              | ntp     | -                 |
|          |              | rsh     | -                 |
|          |              | ssh     | -                 |
|          |              | telnet  | -                 |

9 entries were displayed.

La commande suivante affiche la politique de pare-feu pour la LIF node-management :

```
cluster1::> system services firewall policy show -policy mgmt
```

| Vserver    | Policy | Service | Allowed           |
|------------|--------|---------|-------------------|
| cluster1-1 | mgmt   | dns     | 0.0.0.0/0, ::/0   |
|            |        | http    | 0.0.0.0/0, ::/0   |
|            |        | https   | 0.0.0.0/0, ::/0   |
|            |        | **ndmp  | 0.0.0.0/0, ::/0** |
|            |        | ndmps   | 0.0.0.0/0, ::/0   |
|            |        | ntp     | 0.0.0.0/0, ::/0   |
|            |        | rsh     | -                 |
|            |        | snmp    | 0.0.0.0/0, ::/0   |
|            |        | ssh     | 0.0.0.0/0, ::/0   |
|            |        | telnet  | -                 |

10 entries were displayed.

- b. Si la politique de pare-feu n'est pas activée, activez la politique de pare-feu à l'aide du `system services firewall policy modify` commande avec `-service` paramètre.

La commande suivante active la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. S'assurer que la règle de basculement est correctement définie pour l'ensemble des LIFs :

- a. Vérifier que la policy de basculement pour la LIF de cluster-management est définie sur `broadcast-`

domain-wide, Et la policy pour les LIFs intercluster et node-management est définie sur local-only à l'aide du network interface show -failover commande.

La commande suivante affiche la politique de basculement pour les LIFs cluster-management, intercluster et node-management :

```
cluster1::> network interface show -failover
```

| Failover Vserver Group | Logical Interface | Home Node:Port | Failover Policy            |
|------------------------|-------------------|----------------|----------------------------|
| cluster cluster        | cluster1_clus1    | cluster1-1:e0a | local-only                 |
|                        |                   |                | Failover Targets:<br>..... |
| **cluster1 Default**   | cluster_mgmt      | cluster1-1:e0m | broadcast-domain-wide      |
|                        |                   |                | Failover Targets:<br>..... |
| **IC1 Default**        | **IC1             | cluster1-1:e0a | local-only                 |
|                        |                   |                | Failover Targets:<br>..... |
| **IC2 Default**        | **IC2             | cluster1-1:e0b | local-only                 |
|                        |                   |                | Failover Targets:<br>..... |
| **cluster1-1 Default** | cluster1-1_mgmt1  | cluster1-1:e0m | local-only                 |
|                        |                   |                | Failover Targets:<br>..... |
| **cluster1-2 Default** | cluster1-2_mgmt1  | cluster1-2:e0m | local-only                 |
|                        |                   |                | Failover Targets:<br>..... |

- Si les stratégies de basculement ne sont pas définies de manière appropriée, modifiez la stratégie de basculement en utilisant le network interface modify commande avec -failover-policy paramètre.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

4. Spécifier les LIFs requises pour la connexion de données à l'aide de `vserver services ndmp modify` commande avec `preferred-interface-role` paramètre.

```
cluster1::> vserver services ndmp modify -vserver cluster1 -preferred
-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Vérifiez que le rôle d'interface préféré est défini pour le cluster à l'aide de `vserver services ndmp show` commande.

```
cluster1::> vserver services ndmp show -vserver cluster1

Vserver: cluster1
NDMP Version: 4
.....
.....
Preferred Interface Role: intercluster, cluster-mgmt, node-
mgmt
```

## Configurer node-scoped NDMP

### Activez NDMP node-scoped sur le cluster

Vous pouvez sauvegarder des volumes hébergés sur un seul nœud en activant NDMP node-scoped, en activant le service NDMP et en configurant une LIF pour la connexion data et contrôle. Cela peut être effectué pour tous les nœuds du cluster.



Le protocole NDMP avec étendue du nœud est obsolète dans ONTAP 9.

### Description de la tâche

Si vous utilisez NDMP en mode node-scope, l'authentification doit être configurée sur la base de chaque nœud. Pour plus d'informations, voir "[L'article de la base de connaissances "Comment configurer l'authentification NDMP en mode 'node-scope'"](#)".

### Étapes

1. Activer le mode NDMP node-scoped :

```
cluster1::> system services ndmp node-scope-mode on
```

NDMP node-scope-mode est activé.

2. Activer le service NDMP sur tous les nœuds du cluster :

L'utilisation du caractère générique "\*" permet le service NDMP sur tous les nœuds en même temps.

Vous devez spécifier un mot de passe pour l'authentification de la connexion NDMP par l'application de

backup.

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

### 3. Désactivez le `-clear-text` Option pour la communication sécurisée du mot de passe NDMP :

Utilisation du caractère générique "\*" disables the `-clear-text` option sur tous les nœuds simultanément.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

### 4. Vérifiez que le service NDMP est activé et que `-clear-text` l'option est désactivée :

```
cluster1::> system services ndmp show
```

| Node       | Enabled | Clear text | User Id |
|------------|---------|------------|---------|
| cluster1-1 | true    | false      | root    |
| cluster1-2 | true    | false      | root    |

2 entries were displayed.

## Configurer une LIF

Vous devez identifier une LIF qui sera utilisée pour établir une connexion de données et une connexion de contrôle entre le nœud et l'application de sauvegarde. Après avoir identifié le LIF, vous devez vérifier que les politiques de pare-feu et de basculement sont définies pour le LIF.



Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir ["Configuration des politiques de pare-feu pour les LIF"](#).

## Étapes

1. Identifier le LIF intercluster hébergé sur les nœuds en utilisant le `network interface show` commande avec `-role` paramètre.

```
cluster1::> network interface show -role intercluster
```

| Current Is | Logical   | Status     | Network       | Current    |      |
|------------|-----------|------------|---------------|------------|------|
| Vserver    | Interface | Admin/Oper | Address/Mask  | Node       | Port |
| Home       |           |            |               |            |      |
| -----      | -----     | -----      | -----         | -----      |      |
| cluster1   | IC1       | up/up      | 192.0.2.65/24 | cluster1-1 | e0a  |
| true       |           |            |               |            |      |
| cluster1   | IC2       | up/up      | 192.0.2.68/24 | cluster1-2 | e0b  |
| true       |           |            |               |            |      |

2. S'assurer que la politique de pare-feu est activée pour NDMP sur les LIFs intercluster :

- Vérifiez que la politique de pare-feu est activée pour NDMP à l'aide de `system services firewall policy show` commande.

La commande suivante affiche la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy show -policy intercluster
```

| Vserver  | Policy       | Service | Allowed           |
|----------|--------------|---------|-------------------|
| cluster1 | intercluster | dns     | -                 |
|          |              | http    | -                 |
|          |              | https   | -                 |
|          |              | **ndmp  | 0.0.0.0/0, ::/0** |
|          |              | ndmps   | -                 |
|          |              | ntp     | -                 |
|          |              | rsh     | -                 |
|          |              | ssh     | -                 |
|          |              | telnet  | -                 |

9 entries were displayed.

- Si la politique de pare-feu n'est pas activée, activez la politique de pare-feu à l'aide du `system services firewall policy modify` commande avec `-service` paramètre.

La commande suivante active la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. S'assurer que la politique de basculement est correctement définie pour les LIFs intercluster :



- a. Vérifier que la policy de basculement pour les LIFs intercluster est définie sur `local-only` à l'aide du `network interface show -failover` commande.

```
cluster1::> network interface show -failover
```

| Vserver    | Logical Interface | Home Node:Port | Failover Policy   | Failover Group |
|------------|-------------------|----------------|-------------------|----------------|
| cluster1   | **IC1             | cluster1-1:e0a | local-only        |                |
| Default**  |                   |                |                   |                |
|            |                   |                | Failover Targets: |                |
|            |                   |                | .....             |                |
|            | **IC2             | cluster1-2:e0b | local-only        |                |
| Default**  |                   |                |                   |                |
|            |                   |                | Failover Targets: |                |
|            |                   |                | .....             |                |
| cluster1-1 | cluster1-1_mgmt1  | cluster1-1:e0m | local-only        | Default        |
|            |                   |                | Failover Targets: |                |
|            |                   |                | .....             |                |

- b. Si la stratégie de basculement n'est pas définie de manière appropriée, modifiez la stratégie de basculement en utilisant le `network interface modify` commande avec `-failover-policy` paramètre.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

## Configurez l'application de sauvegarde

Une fois le cluster configuré pour l'accès NDMP, vous devez collecter les informations de la configuration du cluster, puis configurer le reste du processus de sauvegarde dans l'application de sauvegarde.

### Étapes

- Collectez les informations suivantes que vous avez configurées précédemment dans ONTAP :
  - Nom d'utilisateur et mot de passe requis par l'application de sauvegarde pour créer la connexion NDMP
  - Les adresses IP des LIFs intercluster que l'application de sauvegarde nécessite pour se connecter au cluster
- Dans ONTAP, affichez les alias attribués par ONTAP à chaque périphérique en utilisant le `storage tape alias show` commande.

Les alias sont souvent utiles pour configurer l'application de sauvegarde.

```
cluster1::> storage tape show -alias
```

```
Device ID: 2a.0
```

```
Device Type: tape drive
```

```
Description: Hewlett-Packard LTO-5
```

| Node               | Alias | Mapping        |
|--------------------|-------|----------------|
| -----              | ----- | -----          |
| stsw-3220-4a-4b-02 | st2   | SN[HU19497WVR] |
| ...                |       |                |

3. Dans l'application de sauvegarde, configurez le reste du processus de sauvegarde à l'aide de la documentation de l'application de sauvegarde.

### Une fois que vous avez terminé

En cas de mobilité des données, comme un déplacement de volume ou une migration LIF, vous devez être prêt à réinitialiser les opérations de sauvegarde interrompues.

## Réplication entre le logiciel NetApp Element et ONTAP

### Réplication entre le logiciel NetApp Element et ONTAP en vue d'ensemble

Pour assurer la continuité de l'activité sur les systèmes Element, utilisez SnapMirror pour répliquer les copies Snapshot d'un volume Element vers une destination ONTAP. En cas d'incident au niveau du système Element, vous pouvez délivrer les données aux clients via le système ONTAP, puis réactiver ce système une fois que le service est restauré.

Depuis ONTAP 9.4, vous pouvez répliquer les copies Snapshot d'une LUN créée sur un nœud ONTAP et les renvoyer dans un système Element. Vous pouvez avoir créé une LUN en cas de panne sur le site Element ou utiliser un LUN pour migrer les données d'un système ONTAP vers le logiciel Element.

Vous devez travailler avec Element pour la sauvegarde ONTAP si les conditions suivantes s'appliquent :

- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.
- Vous souhaitez utiliser l'interface de ligne de commandes ONTAP et non System Manager, ni un outil de création de scripts automatisé.
- Vous utilisez le protocole iSCSI pour transmettre des données aux clients.

Si vous avez besoin d'informations supplémentaires sur la configuration ou les concepts, consultez les documents suivants :

- Configuration d'élément

["Documentation du logiciel NetApp Element"](#)

- Concepts et configuration de SnapMirror

["Présentation de la protection des données"](#)

## À propos de la réplication entre Element et ONTAP

Depuis ONTAP 9.3, vous pouvez utiliser SnapMirror pour répliquer les copies Snapshot d'un volume Element vers une destination ONTAP. En cas d'incident au niveau du système Element, vous pouvez délivrer les données aux clients via le système ONTAP, puis réactiver le volume source Element une fois que le service est restauré.

Depuis ONTAP 9.4, vous pouvez répliquer les copies Snapshot d'une LUN créée sur un nœud ONTAP et les renvoyer dans un système Element. Vous pouvez avoir créé une LUN en cas de panne sur le site Element ou utiliser un LUN pour migrer les données d'un système ONTAP vers le logiciel Element.

### Types de relation de protection des données

SnapMirror propose deux types de relation de protection des données. Pour chaque type, SnapMirror crée une copie Snapshot du volume source Element avant d'initialiser ou de mettre à jour la relation :

- Dans une relation *Disaster Recovery* protection de données, le volume de destination ne contient que la copie Snapshot créée par SnapMirror, à partir de laquelle vous pouvez continuer à transmettre des données en cas de catastrophe sur le site primaire.
- Dans une relation *conservation* protection des données à long terme, le volume de destination contient des copies Snapshot ponctuelles créées par le logiciel Element, ainsi que la copie Snapshot créée par SnapMirror. Par exemple, vous pouvez conserver les copies Snapshot mensuelles créées sur 20 ans.

### Règles par défaut

La première fois que vous appelez SnapMirror, il effectue un *transfert de base* du volume source vers le volume de destination. La *SnapMirror policy* définit le contenu de la base et ses mises à jour.

Vous pouvez utiliser une règle par défaut ou personnalisée lors de la création d'une relation de protection des données. Le *type de stratégie* détermine les copies Snapshot à inclure et le nombre de copies à conserver.

Le tableau ci-dessous présente les politiques par défaut. Utilisez le `MirrorLatest` Règle permettant de créer une relation classique de reprise sur incident. Utilisez le `MirrorAndVault` ou `Unified7year` Règle permettant de créer une relation de réplication unifiée dans laquelle la reprise sur incident et la conservation à long terme sont configurées sur le même volume de destination.

| Politique      | Type de stratégie         | Comportement de mise à jour                                                                                                                                                                                                                        |
|----------------|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MirrorLatest   | mise en miroir asynchrone | Transférez la copie Snapshot créée par SnapMirror.                                                                                                                                                                                                 |
| MirrorAndVault | coffre-fort               | Transférer la copie Snapshot créée par SnapMirror et toutes les copies Snapshot moins récentes effectuées depuis la dernière mise à jour, à condition qu'elles aient des étiquettes SnapMirror « diotidienne » ou « hebdomadaires ».               |
| Unifié 7ans    | coffre-fort               | Transférer la copie Snapshot créée par SnapMirror et toutes les copies Snapshot moins récentes effectuées depuis la dernière mise à jour, à condition qu'elles aient des étiquettes SnapMirror « diotidienne », « hebdomadaire » ou « mensuelle ». |



Pour obtenir des informations complètes sur les règles de SnapMirror, notamment des instructions sur la règle à utiliser, reportez-vous à "[La protection des données](#)".

### Présentation des étiquettes SnapMirror

Chaque règle avec le type de règle « iroir-vault » doit disposer d'une règle qui spécifie les copies Snapshot à répliquer. La règle « diotidienne », par exemple, indique que seules les copies Snapshot affectées à l'étiquette SnapMirror « q uotidienne » doivent être répliquées. Vous attribuez l'étiquette SnapMirror lors de la configuration des copies Snapshot Element.

### La réplication s'effectue depuis un cluster source Element vers un cluster cible ONTAP

Vous pouvez utiliser SnapMirror pour répliquer les copies Snapshot d'un volume Element sur un système de destination ONTAP. En cas d'incident au niveau du système Element, vous pouvez délivrer les données aux clients via le système ONTAP, puis réactiver le volume source Element une fois que le service est restauré.

Un volume Element équivaut à peu près à un LUN ONTAP. SnapMirror crée un LUN avec le nom du volume Element lorsqu'une relation de protection des données entre le logiciel Element et ONTAP est initialisée. SnapMirror réplique les données vers un LUN existant si le LUN répond aux besoins de réplication d'Element vers ONTAP.

Les règles de réplication sont les suivantes :

- Un volume ONTAP peut contenir uniquement des données d'un volume Element.
- Vous ne pouvez pas répliquer les données depuis un volume ONTAP vers plusieurs volumes Element.

### Effectuer une réplication depuis un cluster source ONTAP vers un cluster cible Element

Depuis ONTAP 9.4, vous pouvez répliquer les copies Snapshot d'un LUN créé sur un système ONTAP et les renvoyer dans un volume Element :

- Si une relation SnapMirror existe déjà entre une source Element et une destination ONTAP, une LUN créée pendant l'accès aux données de la destination est automatiquement répliquée lorsque la source est réactivée.
- Sinon, vous devez créer et initialiser une relation SnapMirror entre le cluster source ONTAP et le cluster destination Element.

Les règles de réplication sont les suivantes :

- La relation de réplication doit avoir une règle de type « async-mirror ».

Les règles de type "iroir-vault" ne sont pas prises en charge.

- Seules les LUN iSCSI sont prises en charge.
- Vous ne pouvez pas répliquer plusieurs LUN depuis un volume ONTAP vers un volume Element.
- Vous ne pouvez pas répliquer un LUN depuis un volume ONTAP vers plusieurs volumes Element.

### Prérequis

Vous devez avoir effectué les tâches suivantes avant de configurer une relation de protection des données entre Element et ONTAP :

- Le cluster Element doit exécuter NetApp Element version 10.1 ou ultérieure.

- Le cluster ONTAP doit exécuter ONTAP 9.3 ou version ultérieure.
- SnapMirror doit avoir été sous licence sur le cluster ONTAP.
- Vous devez disposer de volumes configurés sur les clusters Element et ONTAP suffisamment grands pour gérer les transferts de données anticipés.
- Si vous utilisez le type de règle « miroir-coffre-fort », une étiquette SnapMirror doit avoir été configurée pour que les copies Snapshot Element soient répliquées.



Vous pouvez effectuer cette tâche uniquement dans l'interface utilisateur Web du logiciel Element. Pour plus d'informations, reportez-vous à la section "[Documentation du logiciel NetApp Element](#)"

- Vous devez vous assurer que le port 5010 est disponible.
- Si vous pensez avoir besoin de déplacer un volume de destination, vous devez vous assurer que la connectivité full-mesh existe entre la source et la destination. Chaque nœud du cluster source Element doit pouvoir communiquer avec chaque nœud du cluster cible ONTAP.

### Détails du support

Le tableau suivant présente les informations de support pour la sauvegarde Element vers ONTAP.

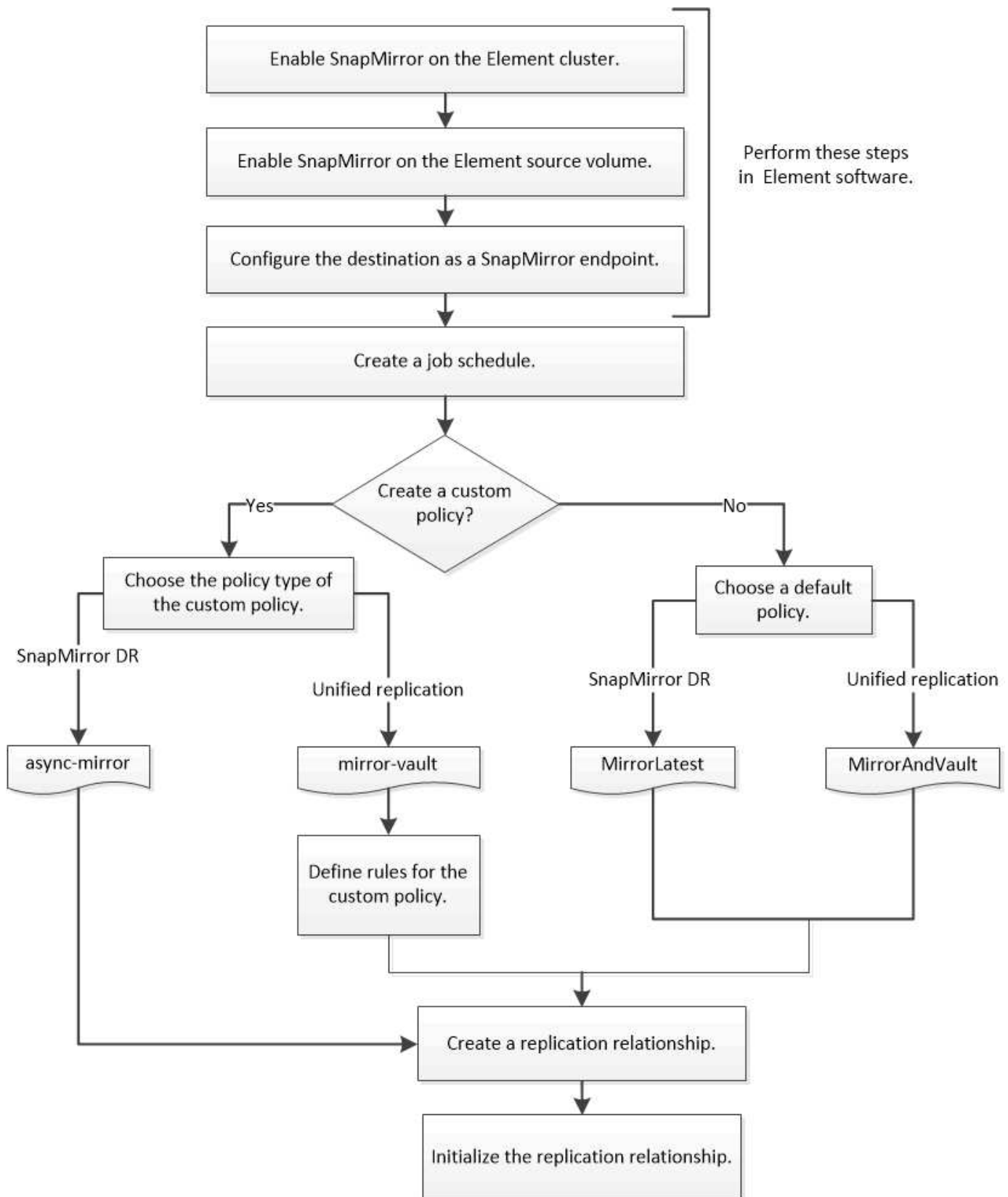
| Ressource ou fonctionnalité | Détails du support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SnapMirror                  | <ul style="list-style-type: none"> <li>• La fonctionnalité de restauration SnapMirror n'est pas prise en charge.</li> <li>• Le <code>MirrorAllSnapshots</code> et <code>XDPDefault</code> les règles ne sont pas prises en charge.</li> <li>• Le type de politique « coffre-fort » n'est pas pris en charge.</li> <li>• La règle définie par le système « <code>tous_source_snapshots</code> » n'est pas prise en charge.</li> <li>• Le type de règle « miroir-coffre-fort » n'est pris en charge que pour la réplication à partir du logiciel Element vers ONTAP. Utilisez le mot « asynchrone-miroir » pour la réplication du logiciel ONTAP vers le logiciel Element.</li> <li>• Le <code>-schedule</code> et <code>-prefix</code> options pour <code>snapmirror policy add-rule</code> ne sont pas pris en charge.</li> <li>• Le <code>-preserve</code> et <code>-quick-resync</code> options pour <code>snapmirror resync</code> ne sont pas pris en charge.</li> <li>• L'efficacité du stockage n'est pas préservée.</li> <li>• Les déploiements de protection des données « Fan-Out » et « cascade » ne sont pas pris en charge.</li> </ul> |
| ONTAP                       | <ul style="list-style-type: none"> <li>• ONTAP Select est pris en charge à partir de ONTAP 9.4 et Element 10.3.</li> <li>• Cloud Volumes ONTAP est pris en charge à partir de ONTAP 9.5 et Element 11.0.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Elément                        | <ul style="list-style-type: none"> <li>• La taille maximale du volume est de 8 Tio.</li> <li>• La taille de bloc du volume doit être de 512 octets. Une taille de bloc de 4 Ko n'est pas prise en charge.</li> <li>• La taille du volume doit être un multiple de 1 MIB.</li> <li>• Les attributs de volume ne sont pas conservés.</li> <li>• Le nombre maximal de copies Snapshot à répliquer est de 30.</li> </ul> |
| Le réseau                      | <ul style="list-style-type: none"> <li>• Une connexion TCP unique est autorisée par transfert.</li> <li>• Le nœud élément doit être spécifié en tant qu'adresse IP. La recherche de nom d'hôte DNS n'est pas prise en charge.</li> <li>• Les IPspaces ne sont pas prises en charge.</li> </ul>                                                                                                                       |
| SnapLock                       | Les volumes SnapLock ne sont pas pris en charge.                                                                                                                                                                                                                                                                                                                                                                     |
| FlexGroup                      | Les volumes FlexGroup ne sont pas pris en charge.                                                                                                                                                                                                                                                                                                                                                                    |
| REPRISE APRÈS INCIDENT DES SVM | Les volumes ONTAP d'une configuration SVM de reprise après incident ne sont pas pris en charge.                                                                                                                                                                                                                                                                                                                      |
| MetroCluster                   | Les volumes ONTAP avec une configuration MetroCluster ne sont pas pris en charge.                                                                                                                                                                                                                                                                                                                                    |

## Workflow de réplication entre Element et ONTAP

Que vous répliquant des données d'Element vers ONTAP ou de ONTAP vers Element, vous devez configurer une planification de tâche, spécifier une règle et créer et initialiser la relation. Vous pouvez utiliser une stratégie par défaut ou personnalisée.

Le flux de travail suppose que vous avez terminé les tâches préalables répertoriées dans [Prérequis](#). Pour obtenir des informations complètes sur les règles de SnapMirror, notamment des instructions sur la règle à utiliser, reportez-vous à "[Protection des données](#)".



## Activez SnapMirror dans Element

### Activez SnapMirror sur le cluster Element

Vous devez activer SnapMirror sur le cluster Element avant de créer une relation de

réplication. Vous pouvez effectuer cette tâche uniquement dans l'interface utilisateur Web du logiciel Element.

#### Avant de commencer

- Le cluster Element doit exécuter NetApp Element version 10.1 ou ultérieure.
- SnapMirror ne peut être activé que pour les clusters Element utilisés avec les volumes NetApp ONTAP.

#### Description de la tâche

Le système Element est fourni avec SnapMirror désactivé par défaut. SnapMirror n'est pas automatiquement activé dans le cadre d'une nouvelle installation ou mise à niveau.



Une fois activé, SnapMirror ne peut pas être désactivé. Vous pouvez uniquement désactiver la fonctionnalité SnapMirror et restaurer les paramètres par défaut en retournant le cluster à l'image d'usine.

#### Étapes

1. Cliquez sur **clusters > Paramètres**.
2. Recherchez les paramètres cluster pour SnapMirror.
3. Cliquez sur **Activer SnapMirror**.

#### Activez SnapMirror sur le volume source Element

Vous devez activer SnapMirror sur le volume source Element avant de créer une relation de réplication. Vous pouvez effectuer cette tâche uniquement dans l'interface utilisateur Web du logiciel Element.


#### Avant de commencer

- Vous devez avoir activé SnapMirror sur le cluster Element.
- La taille de bloc du volume doit être de 512 octets.
- Le volume ne doit pas participer à la réplication à distance d'Element.
- Le type d'accès au volume ne doit pas être « cible de réplication ».

#### Description de la tâche

La procédure ci-dessous suppose que le volume existe déjà. Vous pouvez également activer SnapMirror lorsque vous créez ou clonez un volume.

#### Étapes

1. Sélectionnez **Management > volumes**.
2. Sélectionnez le  bouton du volume.
3. Dans le menu déroulant, sélectionnez **Modifier**.
4. Dans la boîte de dialogue **Modifier le volume**, sélectionnez **Activer SnapMirror**.
5. Sélectionnez **Enregistrer les modifications**.

#### Créer un terminal SnapMirror

Vous devez créer un terminal SnapMirror avant de pouvoir créer une relation de réplication. Vous pouvez effectuer cette tâche uniquement dans l'interface utilisateur Web



du logiciel Element.

### Avant de commencer

Vous devez avoir activé SnapMirror sur le cluster Element.

### Étapes

1. Cliquez sur **Data protection > SnapMirror Endpoints**.
2. Cliquez sur **Créer un point final**.
3. Dans la boîte de dialogue **Créer un nouveau point final**, entrez l'adresse IP de gestion du cluster ONTAP.
4. Entrez l'ID utilisateur et le mot de passe de l'administrateur du cluster ONTAP.
5. Cliquez sur **Créer un point final**.

## Configurer une relation de réplication

### Créer une planification de tâche de réplication

Que vous répliquant des données d'Element vers ONTAP ou de ONTAP vers Element, vous devez configurer une planification de tâche, spécifier une règle et créer et initialiser la relation. Vous pouvez utiliser une stratégie par défaut ou personnalisée.

Vous pouvez utiliser le `job schedule cron create` commande pour créer une planification de tâche de réplication. La planification des tâches détermine lorsque SnapMirror met automatiquement à jour la relation de protection des données à laquelle la planification est attribuée.

### Description de la tâche

Vous affectez un planning de travail lorsque vous créez une relation de protection des données. Si vous n'attribuez pas de programme de travail, vous devez mettre à jour la relation manuellement.

### Étape

1. Création d'un programme de travail :

```
job schedule cron create -name job_name -month month -dayofweek day_of_week
-day day_of_month -hour hour -minute minute
```

Pour `-month`, `-dayofweek`, et `-hour`, vous pouvez spécifier `all` pour exécuter le travail chaque mois, jour de la semaine et heure, respectivement.

Depuis ONTAP 9.10.1, vous pouvez inclure le vServer dans votre calendrier des tâches :

```
job schedule cron create -name job_name -vserver Vserver_name -month month
-dayofweek day_of_week -day day_of_month -hour hour -minute minute
```

L'exemple suivant crée un programme de travail nommé `my_weekly` Le samedi à 3:00 :

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

## Personnaliser une règle de réplication

### Création d'une règle de réplication personnalisée

Vous pouvez utiliser une règle par défaut ou personnalisée lorsque vous créez une relation de réplication. Pour une règle de réplication unifiée personnalisée, vous devez définir une ou plusieurs *règles* qui déterminent quelles copies Snapshot sont transférées lors de l'initialisation et de la mise à jour.

Vous pouvez créer une stratégie de réplication personnalisée si la stratégie par défaut d'une relation n'est pas appropriée. Vous pouvez compresser les données d'un transfert réseau, par exemple, ou modifier le nombre de tentatives de transfert de copies Snapshot par SnapMirror.

### Description de la tâche

Le *policy type* de la règle de réplication détermine le type de relation qu'elle prend en charge. Le tableau ci-dessous présente les types de stratégies disponibles.

| Type de règle             | Type de relation                |
|---------------------------|---------------------------------|
| mise en miroir asynchrone | Reprise sur incident SnapMirror |
| coffre-fort               | Réplication unifiée             |

### Étape

1. Création d'une règle de réplication personnalisée :

```
snapmirror policy create -vserver SVM -policy policy -type async-
mirror|mirror-vault -comment comment -tries transfer_tries -transfer-priority
low|normal -is-network-compression-enabled true|false
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Depuis la version ONTAP 9.5, vous pouvez spécifier la planification de la création d'une planification commune des copies Snapshot pour les relations SnapMirror synchrones à l'aide du `-common-snapshot-schedule` paramètre. Par défaut, la planification commune des copies Snapshot pour les relations SnapMirror synchrones est d'une heure. Vous pouvez définir une valeur comprise entre 30 minutes et deux heures pour la planification des copies Snapshot des relations SnapMirror synchrones.

L'exemple suivant crée une règle de réplication personnalisée pour SnapMirror DR qui permet la compression réseau pour les transferts de données :

```
cluster_dst::> snapmirror policy create -vserver svml -policy
DR_compressed -type async-mirror -comment "DR with network compression
enabled" -is-network-compression-enabled true
```

L'exemple suivant crée une règle de réplication personnalisée pour la réplication unifiée :

```
cluster_dst::> snapmirror policy create -vserver svml -policy my_unified
-type mirror-vault
```

### Une fois que vous avez terminé

Pour les types de règles « miroir-coffre-fort », vous devez définir des règles qui déterminent les copies Snapshot qui sont transférées lors de l'initialisation et de la mise à jour.

Utilisez le `snapmirror policy show` Commande pour vérifier que la règle SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).

### Définir une règle pour une règle

Pour les règles personnalisées avec le type de règle « miroir-coffre-fort », vous devez définir au moins une règle qui détermine les copies Snapshot transférées lors de l'initialisation et de la mise à jour. Vous pouvez également définir des règles pour les stratégies par défaut avec le type de stratégie "miroir-coffre-fort".

### Description de la tâche

Chaque règle avec le type de règle « iroir-vault » doit disposer d'une règle qui spécifie les copies Snapshot à répliquer. La règle « bimensuelle », par exemple, indique que seules les copies Snapshot affectées au label SnapMirror « bimensuel » doivent être répliquées. Vous attribuez l'étiquette SnapMirror lors de la configuration des copies Snapshot Element.

Chaque type de stratégie est associé à une ou plusieurs règles définies par le système. Ces règles sont automatiquement attribuées à une règle lorsque vous spécifiez son type de stratégie. Le tableau ci-dessous présente les règles définies par le système.

| Règle définie par le système | Utilisé dans les types de stratégie | Résultat                                                                                                                                                   |
|------------------------------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sm_créé                      | asynchrone-mirror, mirror-vault     | Une copie Snapshot créée par SnapMirror est transférée lors de l'initialisation et de la mise à jour.                                                      |
| tous les jours               | coffre-fort                         | Les nouvelles copies Snapshot de la source portant le label SnapMirror « `diotidienne » sont transférées lors de l'initialisation et de la mise à jour.    |
| hebdomadaire                 | coffre-fort                         | Les nouvelles copies Snapshot de la source portant l'étiquette SnapMirror « hebdomadaire » sont transférées lors de l'initialisation et de la mise à jour. |

|               |             |                                                                                                                                                     |
|---------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| tous les mois | coffre-fort | Les nouvelles copies Snapshot de la source avec le libellé SnapMirror « `mensuel` » sont transférées lors de l'initialisation et de la mise à jour. |
|---------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|

Vous pouvez indiquer des règles supplémentaires selon vos besoins pour les règles par défaut ou personnalisées. Par exemple :

- Pour la valeur par défaut `MirrorAndVault` Politique, vous pouvez créer une règle appelée « deux mois » pour faire correspondre les copies Snapshot de la source avec l'étiquette SnapMirror « deux mois ».
- Dans le cas d'une règle personnalisée avec le type de règle « miroir-coffre-fort », vous pouvez créer une règle appelée « deux semaines » pour faire correspondre les copies Snapshot de la source avec l'étiquette SnapMirror « deux semaines ».

## Étape

1. Définir une règle pour une règle :

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
-label snapmirror-label -keep retention_count
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).

L'exemple suivant ajoute une règle avec l'étiquette SnapMirror `bi-monthly` par défaut `MirrorAndVault` règle :

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

L'exemple suivant ajoute une règle avec l'étiquette SnapMirror `bi-weekly` au personnalisé `my_snapvault` règle :

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

L'exemple suivant ajoute une règle avec l'étiquette SnapMirror `app_consistent` au personnalisé `Sync` règle :

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy Sync
-snapmirror-label app_consistent -keep 1
```

Vous pouvez ensuite répliquer les copies Snapshot à partir du cluster source correspondant à l'étiquette SnapMirror :

```
cluster_src::> snapshot create -vserver vs1 -volume voll -snapshot
snapshot1 -snapmirror-label app_consistent
```

## Créer une relation de réplication

### Création d'une relation entre une source d'élément et une destination ONTAP

La relation entre le volume source du stockage primaire et le volume de destination du stockage secondaire est appelée « relation de protection des données ». Vous pouvez utiliser le `snapmirror create` Commande permettant de créer une relation de protection des données à partir d'une source Element vers une destination ONTAP, ou d'une source ONTAP vers une destination Element.

Vous pouvez utiliser SnapMirror pour répliquer les copies Snapshot d'un volume Element sur un système de destination ONTAP. En cas d'incident au niveau du système Element, vous pouvez délivrer les données aux clients via le système ONTAP, puis réactiver le volume source Element une fois que le service est restauré.

### Avant de commencer

- Le nœud Element contenant le volume à répliquer doit avoir été accessible à ONTAP.
- Le volume Element doit avoir été activé pour la réplication SnapMirror.
- Si vous utilisez le type de règle « miroir-coffre-fort », une étiquette SnapMirror doit avoir été configurée pour que les copies Snapshot Element soient répliquées.



Vous pouvez effectuer cette tâche uniquement dans l'interface utilisateur Web du logiciel Element. Pour plus d'informations, reportez-vous à la section "[Documentation sur les éléments](#)".

### Description de la tâche

Vous devez spécifier le chemin source de l'élément sous la forme `<hostip:>/lun/<name>`, où « lun » est la chaîne réelle « lun » et `name` le nom du volume d'élément.

Un volume Element équivaut à peu près à un LUN ONTAP. SnapMirror crée un LUN avec le nom du volume Element lorsqu'une relation de protection des données entre le logiciel Element et ONTAP est initialisée. SnapMirror réplique les données vers une LUN existante si la LUN répond aux exigences en matière de réplication depuis le logiciel Element vers ONTAP.

Les règles de réplication sont les suivantes :

- Un volume ONTAP peut contenir uniquement des données d'un volume Element.
- Vous ne pouvez pas répliquer les données depuis un volume ONTAP vers plusieurs volumes Element.

Dans ONTAP 9.3 et version antérieure, un volume de destination peut contenir jusqu'à 251 copies Snapshot. Dans ONTAP 9.4 et versions ultérieures, un volume de destination peut contenir jusqu'à 1019 copies Snapshot.

### Étape

1. Depuis le cluster destination, créer une relation de réplication depuis une source Element vers une destination ONTAP :

```
snapmirror create -source-path <hostip:>/lun/<name> -destination-path
<SVM:volume>|<cluster://SVM/volume> -type XDP -schedule schedule -policy
<policy>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création d'une relation SnapMirror DR à l'aide de la valeur par défaut MirrorLatest règle :

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorLatest
```

L'exemple suivant illustre la création d'une relation de réplication unifiée à l'aide de la valeur par défaut MirrorAndVault règle :

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorAndVault
```

L'exemple suivant illustre la création d'une relation de réplication unifiée à l'aide de Unified7year règle :

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy Unified7year
```

L'exemple suivant illustre la création d'une relation de réplication unifiée à l'aide de la commande personnalisée my\_unified règle :

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy my_unified
```

## Une fois que vous avez terminé

Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

## Création d'une relation entre une source ONTAP et une destination Element

Depuis ONTAP 9.4, vous pouvez utiliser SnapMirror pour répliquer les copies Snapshot d'un LUN créé sur une source ONTAP et les renvoyer vers une destination Element. Il est possible d'utiliser le LUN pour migrer les données d'ONTAP vers le logiciel Element.

## Avant de commencer

- Le nœud de destination de l'élément doit avoir été accessible à ONTAP.
- Le volume Element doit avoir été activé pour la réplication SnapMirror.

### Description de la tâche

Vous devez spécifier le chemin de destination de l'élément sous la forme <hostip:>/lun/<name>, où « lun » est la chaîne réelle « lun » et name le nom du volume d'élément.

Les règles de réplication sont les suivantes :

- La relation de réplication doit avoir une règle de type « async-mirror ».

Vous pouvez utiliser une stratégie par défaut ou personnalisée.

- Seules les LUN iSCSI sont prises en charge.
- Vous ne pouvez pas répliquer plusieurs LUN depuis un volume ONTAP vers un volume Element.
- Vous ne pouvez pas répliquer un LUN depuis un volume ONTAP vers plusieurs volumes Element.

### Étape

1. Créer une relation de réplication depuis une source ONTAP vers une destination Element :

```
snapmirror create -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <hostip:>/lun/<name> -type XDP -schedule schedule -policy
<policy>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création d'une relation SnapMirror DR à l'aide de la valeur par défaut MirrorLatest règle :

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy MirrorLatest
```

L'exemple suivant illustre la création d'une relation SnapMirror DR à l'aide de la commande personnalisée my\_mirror règle :

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy my_mirror
```

### Une fois que vous avez terminé

Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

### Initialiser une relation de réplication

Pour tous les types de relations, l'initialisation effectue un *transfert de base* : il effectue

une copie Snapshot du volume source, puis transfère cette copie et tous les blocs de données qu'elle référence au volume de destination.

#### Avant de commencer

- Le nœud Element contenant le volume à répliquer doit avoir été accessible à ONTAP.
- Le volume Element doit avoir été activé pour la réplication SnapMirror.
- Si vous utilisez le type de règle « miroir-coffre-fort », une étiquette SnapMirror doit avoir été configurée pour que les copies Snapshot Element soient répliquées.

#### Description de la tâche

Vous devez spécifier le chemin source de l'élément sous la forme <hostip:>/lun/<name>, où « lun » est la chaîne réelle « lun » et *name* le nom du volume d'élément.

L'initialisation peut prendre beaucoup de temps. Vous pouvez exécuter le transfert de base en dehors des heures creuses.

Si l'initialisation d'une relation entre une source ONTAP et une destination d'élément échoue pour une raison quelconque, elle continuera à échouer même après avoir corrigé le problème (un nom de LUN non valide, par exemple). La solution est la suivante :



1. Supprimer la relation.
2. Supprimez le volume de destination Element.
3. Créer un nouveau volume de destination Element.
4. Créez et initialisez une nouvelle relation entre la source ONTAP et le volume cible Element.

#### Étape

1. Initialiser une relation de réplication :

```
snapmirror initialize -source-path <hostip:>/lun/<name> -destination-path
<SVM:volume|cluster://SVM/volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).

L'exemple suivant initialise la relation entre le volume source 0005 à l'adresse IP 10.0.0.11 et au volume de destination volA\_dst marche svm\_backup:

```
cluster_dst::> snapmirror initialize -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

## Activation des données à partir d'un volume de destination de reprise après incident SnapMirror

#### Rendre le volume de destination inscriptible

Lorsque l'incident désactive le site principal pour une relation SnapMirror DR, vous pouvez transmettre les données à partir du volume de destination sans interruption minimale. Vous pouvez réactiver le volume source une fois que le service est restauré au



niveau du site principal.

Vous devez rendre le volume de destination inscriptible avant de pouvoir transmettre les données du volume à des clients. Vous pouvez utiliser le `snapmirror quiesce` commande pour arrêter les transferts programmés vers la destination, le `snapmirror abort` pour arrêter les transferts en cours, et le `snapmirror break` commande permettant de rendre la destination inscriptible.

### Description de la tâche

Vous devez spécifier le chemin source de l'élément sous la forme `<hostip:>/lun/<name>`, où « lun » est la chaîne réelle « lun » et `name` le nom du volume d'élément.

### Étapes

1. Arrêter les transferts programmés vers la destination :

```
snapmirror quiesce -source-path <hostip:>/lun/<name> -destination-path
<SVM:volume>|<cluster://SVM/volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).

L'exemple suivant arrête les transferts programmés entre le volume source `0005` À l'adresse IP `10.0.0.11` et au volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror quiesce -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

2. Arrêter les transferts en cours vers la destination :

```
snapmirror abort -source-path <hostip:>/lun/<name> -destination-path
<SVM:volume>|<cluster://SVM/volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).

L'exemple suivant arrête les transferts en cours entre le volume source `0005` À l'adresse IP `10.0.0.11` et au volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

3. Interrompre la relation SnapMirror DR :

```
snapmirror break -source-path <hostip:>/lun/<name> -destination-path
<SVM:volume>|<cluster://SVM/volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).

L'exemple suivant rompt la relation entre le volume source `0005` À l'adresse IP `10.0.0.11` et au volume de destination `volA_dst` marche `svm_backup` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

## Configurer le volume de destination pour l'accès aux données

Une fois le volume de destination inscriptible, vous devez configurer le volume pour l'accès aux données. LES hôtes SAN peuvent accéder aux données à partir du volume de destination jusqu'à ce que le volume source soit réactivé.

1. Mappez la LUN Element sur le groupe initiateur approprié.
2. Créer des sessions iSCSI entre les initiateurs d'hôte SAN et les LIFs SAN.
3. Sur le client SAN, effectuez une nouvelle analyse de stockage pour détecter la LUN connectée.

## Réactiver le volume source d'origine

Vous pouvez rétablir la relation initiale de protection des données entre les volumes source et destination lorsque vous n'avez plus besoin de transmettre des données depuis la destination.

### Description de la tâche

La procédure ci-dessous suppose que la ligne de base du volume source d'origine est intacte. Si la base n'est pas intacte, vous devez créer et initialiser la relation entre le volume dont vous accédez aux données et le volume source d'origine avant d'effectuer la procédure.

Vous devez spécifier le chemin source de l'élément sous la forme <hostip:>/lun/<name>, où « lun » est la chaîne réelle « lun » et name le nom du volume d'élément.

Depuis ONTAP 9.4, les copies Snapshot d'une LUN créée pendant l'accès aux données depuis la destination ONTAP sont automatiquement répliquées à la réactivation de la source Element.

Les règles de réplication sont les suivantes :

- Seules les LUN iSCSI sont prises en charge.
- Vous ne pouvez pas répliquer plusieurs LUN depuis un volume ONTAP vers un volume Element.
- Vous ne pouvez pas répliquer un LUN depuis un volume ONTAP vers plusieurs volumes Element.

## Étapes

1. Supprimez la relation de protection des données d'origine :

```
snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <hostip:>/lun/<name> -policy <policy>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant supprime la relation entre le volume source d'origine, 0005 À l'adresse IP 10.0.0.11, et le volume que vous servant des données, volA\_dst marche svm\_backup:

```
cluster_dst:> snapmirror delete -source-path 10.0.0.11:/lun/0005
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

## 2. Inverser la relation de protection des données d'origine :

```
snapmirror resync -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <hostip:>/lun/<name> -policy <policy>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.

L'exemple suivant inverse la relation entre le volume source d'origine, 0005 À l'adresse IP 10.0.0.11, et le volume que vous servant des données, volA\_dst marche svm\_backup:

```
cluster_dst:> snapmirror resync -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

## 3. Mettre à jour la relation inversée :

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <hostip:>/lun/<name>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Échec de la commande si une copie Snapshot commune n'existe pas sur la source et la destination. Utiliser `snapmirror initialize` pour réinitialiser la relation.

L'exemple suivant met à jour la relation entre le volume que vous servant des données, volA\_dst marche svm\_backup, et le volume source d'origine, 0005 À l'adresse IP 10.0.0.11 :

```
cluster_dst:> snapmirror update -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

## 4. Arrêter les transferts programmés pour la relation inversée :

```
snapmirror quiesce -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <hostip:>/lun/<name>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant arrête les transferts programmés entre le volume à partir de où vous accédez les données, volA\_dst marche svm\_backup, et le volume source d'origine, 0005 À l'adresse IP 10.0.0.11 :

```
cluster_dst:> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

#### 5. Arrêter les transferts en cours pour la relation inversée :

```
snapmirror abort -source-path <SVM:volume>|<cluster://SVM/volume> -destination
-path <hostip:>/lun/<name>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant arrête les transferts en cours entre le volume dont vous accédez à des données, volA\_dst marche svm\_backup, et le volume source d'origine, 0005 À l'adresse IP 10.0.0.11 :

```
cluster_dst:> snapmirror abort -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

#### 6. Rompez la relation inversée :

```
snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume> -destination
-path <hostip:>/lun/<name>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant rompt la relation entre le volume dont vous servant des données, volA\_dst marche svm\_backup, et le volume source d'origine, 0005 À l'adresse IP 10.0.0.11 :

```
cluster_dst:> snapmirror break -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

#### 7. Supprimez la relation de protection des données inversée :

```
snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <hostip:>/lun/<name> -policy <policy>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant supprime la relation inversée entre le volume source d'origine, 0005 À l'adresse IP 10.0.0.11, et le volume que vous servant des données, volA\_dst marche svm\_backup:

```
cluster_src:> snapmirror delete -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

#### 8. Rétablir la relation initiale de protection des données :

```
snapmirror resync -source-path <hostip:>/lun/<name> -destination-path
<SVM:volume>|<cluster://SVM/volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant rétablit la relation entre le volume source d'origine, 0005 À l'adresse IP 10.0.0.11, et au volume de destination d'origine, volA\_dst marche svm\_backup:

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

### Une fois que vous avez terminé

Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

## Mettre à jour une relation de réplication manuellement

Vous devrez peut-être mettre à jour une relation de réplication manuellement si une mise à jour échoue en raison d'une erreur réseau.

### Description de la tâche

Vous devez spécifier le chemin source de l'élément sous la forme <hostip:>/lun/<name>, où « lun » est la chaîne réelle « lun » et name le nom du volume d'élément.

### Étapes

1. Mettre à jour une relation de réplication manuellement :

```
snapmirror update -source-path <hostip:>/lun/<name> -destination-path
<SVM:volume>|<cluster://SVM/volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Échec de la commande si une copie Snapshot commune n'existe pas sur la source et la destination. Utiliser `snapmirror initialize` pour réinitialiser la relation.

L'exemple suivant met à jour la relation entre le volume source 0005 À l'adresse IP 10.0.0.11 et au volume de destination volA\_dst marche svm\_backup:

```
cluster_src::> snapmirror update -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

## Resynchroniser une relation de réplication

Vous devez resynchroniser une relation de réplication après avoir créé un volume de destination inscriptible, après une mise à jour échoue, car une copie Snapshot commune n'existe pas sur les volumes source et de destination, ou si vous souhaitez modifier la règle de réplication pour la relation.

### Description de la tâche

Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.

Vous devez spécifier le chemin source de l'élément sous la forme <hostip:>/lun/<name>, où « lun » est la chaîne réelle « lun » et name le nom du volume d'élément.

### Étape

#### 1. Resynchronisation des volumes source et de destination :

```
snapmirror resync -source-path <hostip:>/lun/<name> -destination-path
<SVM:volume>|<cluster://SVM/volume> -type XDP -policy <policy>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant resynchronise la relation entre le volume source 0005 à l'adresse IP 10.0.0.11 et au volume de destination volA\_dst marche svm\_backup:

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

# Surveillance des événements, des performances et de l'état du système

## Contrôle des performances du cluster avec System Manager


### Contrôle des performances du cluster à l'aide de System Manager

Les sections de cette section permettent de gérer l'état et les performances des clusters à l'aide de System Manager dans ONTAP 9.7 et versions ultérieures.

Vous pouvez contrôler les performances du cluster en affichant les informations sur votre système dans le tableau de bord de System Manager. Le tableau de bord affiche des informations sur les alertes et notifications importantes, l'efficacité et la capacité des tiers et des volumes de stockage, les nœuds disponibles dans un cluster, l'état des nœuds d'une paire HA, les applications et objets les plus actifs, et les metrics de performance d'un cluster ou d'un nœud.

Le tableau de bord vous permet de déterminer les informations suivantes :

- **Santé**: La grappe est-elle saine?
- **Capacité** : quelle est la capacité disponible sur le cluster ?
- **Performance** : quel est le niveau de performances du cluster, en fonction de la latence, des IOPS et du débit ?
- **Network** : comment le réseau est-il configuré avec des hôtes et des objets de stockage, tels que des ports, des interfaces et des machines virtuelles de stockage ?

Dans les aperçus Santé et capacité, vous pouvez cliquer sur  pour afficher des informations supplémentaires et effectuer des tâches.

Dans la vue d'ensemble des performances, vous pouvez afficher des mesures basées sur l'heure, le jour, la semaine, le mois ou l'année.

Dans la présentation réseau, le nombre de chaque objet du réseau est affiché (par exemple, « 8 ports NVMe/FC »). Vous pouvez cliquer sur les numéros pour afficher les détails de chaque objet réseau.

### Affichez la présentation des clusters sur le tableau de bord de System Manager

Le tableau de bord de System Manager offre une vue rapide et complète de votre cluster ONTAP à partir d'un emplacement unique.

Le tableau de bord de System Manager vous permet d'afficher des informations d'un coup d'œil sur les alertes et notifications importantes, l'efficacité et la capacité des tiers et des volumes de stockage, les nœuds disponibles dans un cluster, l'état des nœuds d'une paire haute disponibilité, les applications et objets les plus actifs, et les metrics de performance d'un cluster ou d'un nœud.

Le tableau de bord comprend quatre panneaux décrits comme suit :

## Santé

La vue Santé affiche des informations sur l'état de santé global de tous les nœuds détectables dans le cluster.

La vue Santé affiche également les erreurs et les avertissements au niveau du cluster, tels que les détails d'un nœud non configuré, indiquant les caractéristiques qui peuvent être modifiées pour améliorer les performances du cluster.

Cliquez → sur pour développer la vue Santé afin d'obtenir une vue d'ensemble du cluster, par exemple le nom du cluster, la version, la date et l'heure de création du cluster, etc. Vous pouvez également contrôler les statistiques relatives à l'état de santé des nœuds associés à un cluster. Vous pouvez gérer les balises qui vous permettent de regrouper et d'identifier les ressources de votre environnement. La section Insights vous aide à optimiser la capacité, la conformité en matière de sécurité et la configuration de votre système.

## Puissance

La vue capacité affiche l'espace de stockage d'un cluster. Vous pouvez afficher l'espace logique total utilisé, l'espace physique total utilisé et l'espace disque disponible.

Vous pouvez choisir de vous enregistrer avec ActiveIQ pour afficher l'historique des données de cluster. Cliquez → pour développer la vue capacité et afficher un aperçu des niveaux associés à un cluster. Vous pouvez afficher des informations de capacité sur chacun des niveaux : l'espace total, l'espace utilisé et l'espace disponible. Des informations détaillées concernant le débit, les IOPS et la latence sont affichées. ["Pour en savoir plus sur ces mesures de capacité, consultez System Manager"](#).

Vous pouvez choisir d'ajouter un Tier local ou un Tier cloud à l'aide de la vue capacité. Pour plus d'informations sur la vue capacité, reportez-vous à la section ["Afficher la capacité d'un cluster"](#).

## Le réseau

La vue réseau affiche les ports physiques, les interfaces réseau et les machines virtuelles de stockage faisant partie du réseau.

La vue réseau affiche le type de clients connectés au réseau. Chacun de ces clients connectés au réseau est représenté par un chiffre, par exemple « NVMe/FC 16 ». Sélectionnez le numéro pour afficher des détails spécifiques sur chacun de ces éléments réseau.

Cliquez → pour afficher une vue complète du réseau qui englobe les ports, les interfaces réseau, les machines virtuelles de stockage et les hôtes sur le réseau.

## Performance

La vue performances affiche les statistiques de performances pour vous aider à contrôler l'état et l'efficacité de votre cluster ONTAP. Les statistiques incluent des indicateurs clés de performance du cluster, tels que la latence, le débit et les IOPS, représentés sous forme de graphiques.

La vue performances affiche les statistiques de performances à différents intervalles de temps par jour, heure, semaine ou année. Vous pouvez rapidement analyser les performances du cluster à l'aide des différents graphiques et identifier les caractéristiques susceptibles de nécessiter une optimisation. Cette analyse rapide vous aide à décider comment ajouter ou déplacer des charges de travail. Vous pouvez également examiner les heures de pointe pour planifier les changements potentiels.


La vue des performances affiche les mesures de performances totales liées à la latence, au débit et aux IOPS.

Depuis la version 9.15.1, l'affichage des performances est amélioré et affiche des graphiques pour les



mesures de performance en lecture, écriture, autre et totale liées à la latence, au débit et aux IOPS. Les autres indicateurs incluent les opérations qui ne sont pas lues ou écrites.

Les valeurs de performance sont renouvelées toutes les 3 secondes et le graphique de performances est actualisé toutes les 15 secondes. Un graphique ne s'affiche pas si les informations relatives aux performances du cluster ne sont pas disponibles.

Cliquez  pour afficher un aperçu complet des mesures de performances par heure, jour, semaine, mois et année. Vous pouvez également télécharger un rapport des mesures de performances de votre système local.

## Identification des volumes fortement sollicités et des autres objets

Accélérez les performances du cluster en identifiant les volumes (volumes fortement sollicités) et les données (objets fortement sollicités).



À partir de ONTAP 9.10.1, vous pouvez utiliser la fonction de suivi des activités de l'analyse du système de fichiers pour surveiller les objets actifs d'un volume.


### Étapes

1. Cliquez sur **Storage > volumes**.
2. Filtrez les colonnes IOPS, latence et débit pour afficher les volumes et données fréquemment utilisés.

## Modifier la QoS

À partir de ONTAP 9.8, lorsque vous provisionnez du stockage, **Qualité de service (QoS)** est activé par défaut. Vous pouvez désactiver QoS ou choisir une règle de qualité de services personnalisée lors du processus de provisionnement. Vous pouvez également modifier la QoS une fois le stockage provisionné.

### Étapes

1. Dans System Manager, sélectionnez **Storage** puis **volumes**.
2. En regard du volume pour lequel vous souhaitez modifier la QoS, sélectionnez , puis **Edit**.

## Surveiller les risques

Depuis ONTAP 9.10.0, System Manager permet de surveiller les risques signalés par le conseiller digital Active IQ. Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour prendre en compte les risques.

Le conseiller digital NetApp Active IQ crée des opportunités de réduction des risques et d'amélioration des performances et de l'efficacité de votre environnement de stockage. Avec System Manager, vous découvrez les risques signalés par Active IQ et bénéficiez d'informations exploitables pour la gestion du stockage, une disponibilité accrue, une sécurité renforcée et des performances de stockage supérieures.

### Lien vers votre compte Active IQ

Pour recevoir des informations sur les risques Active IQ, vous devez d'abord créer un lien vers votre compte Active IQ de System Manager.

## Étapes

1. Dans System Manager, cliquez sur **Cluster > Paramètres**.
2. Sous **Active IQ Registration**, cliquez sur **Register**.
3. Saisissez vos identifiants pour Active IQ.
4. Une fois vos informations d'identification authentifiées, cliquez sur **confirmer pour lier Active IQ à System Manager**.

## Afficher le nombre de risques

Depuis ONTAP 9.10.0, vous pouvez consulter le tableau de bord dans System Manager le nombre de risques signalé par Active IQ.

### Avant de commencer

Vous devez établir une connexion depuis System Manager vers votre compte Active IQ. Reportez-vous à la section [Lien vers votre compte Active IQ](#).

## Étapes

1. Dans System Manager, cliquez sur **Dashboard**.
2. Dans la section **Santé**, consultez le nombre de risques signalés.



Vous pouvez afficher des informations plus détaillées sur chaque risque en cliquant sur le message indiquant le nombre de risques. Voir [Afficher les détails des risques](#).

## Afficher les détails des risques

Depuis ONTAP 9.10.0, vous pouvez visualiser dans System Manager la façon dont les risques signalés par Active IQ sont classés par zone d'impact. Vous pouvez également consulter des informations détaillées sur chaque risque signalé, son impact potentiel sur votre système et les actions correctives que vous pouvez prendre.

### Avant de commencer

Vous devez établir une connexion depuis System Manager vers votre compte Active IQ. Reportez-vous à la section [Lien vers votre compte Active IQ](#).

## Étapes

1. Cliquez sur **Événements > tous les événements**.
2. Dans la section **Aperçu**, sous **suggestions de Active IQ**, consultez le nombre de risques dans chaque catégorie de zone d'impact. Les catégories de risque sont les suivantes :
  - Performances et efficacité
  - Disponibilité et protection des données
  - Puissance
  - Configuration
  - Sécurité
3. Cliquez sur l'onglet **suggestions** de Active IQ pour afficher des informations sur chaque risque, notamment :
  - Niveau d'impact sur votre système

- Catégorie du risque
- Nœuds affectés
- Type d'atténuation nécessaire
- Actions correctives possibles

## Reconnaître les risques

À partir de ONTAP 9.10.1, vous pouvez utiliser System Manager pour prendre en compte les risques ouverts.

### Étapes

1. Dans System Manager, affichez la liste des risques en exécutant la procédure dans [Afficher les détails des risques](#).
2. Cliquez sur le nom du risque d'un risque ouvert que vous souhaitez reconnaître.
3. Entrez les informations dans les champs suivants :
  - Rappel (date)
  - Justification
  - Commentaires
4. Cliquez sur **Acknowledge**.



Une fois que vous avez reconnu un risque, ce changement ne prend que quelques minutes et se reflète dans la liste des suggestions de Active IQ.

## Prendre en compte les risques

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour annuler le risque reconnu précédemment.

### Étapes

1. Dans System Manager, affichez la liste des risques en exécutant la procédure dans [Afficher les détails des risques](#).
2. Cliquez sur le nom du risque d'un risque reconnu que vous souhaitez annuler.
3. Entrez les informations dans les champs suivants :
  - Justification
  - Commentaires
4. Cliquez sur **UnAcknowledge**.



Une fois que vous reconnaissez un risque, ce changement prend quelques minutes. Il faut que ce changement soit reflété dans la liste des suggestions de Active IQ.

## Informations sur System Manager

Depuis ONTAP 9.11.1, System Manager affiche *Insights* qui vous aide à optimiser les performances et la sécurité de votre système.



Pour afficher, personnaliser et répondre aux informations, reportez-vous à la section "[Obtenez des informations exploitables pour optimiser votre système](#)"

## Informations sur la capacité

System Manager peut afficher les informations suivantes en fonction des conditions de capacité de votre système :

| Visibilité                                        | Gravité              | Condition                                                                                                                                                                                                                                                                | Correctifs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Les tiers locaux manquent d'espace                | Remédier aux risques | Un ou plusieurs niveaux locaux sont pleins à plus de 95 % et connaissent une croissance rapide. Il se peut que les workloads existants ne puissent pas croître ou, dans des cas extrêmes, que l'espace disponible des workloads existants soit insuffisant pour échouer. | <b>Correctif recommandé</b> : effectuez l'une des options suivantes. <ul style="list-style-type: none"><li>• Effacez la file d'attente de restauration du volume.</li><li>• Activez le provisionnement fin sur des volumes à provisionnement lourd pour libérer du stockage piégé.</li><li>• Déplacez les volumes vers un autre niveau local.</li><li>• Supprimer les copies Snapshot inutiles</li><li>• Supprimez les répertoires ou fichiers inutiles des volumes.</li><li>• Activez FabricPool pour hiérarchiser les données dans le cloud.</li></ul> |
| Et l'espace est insuffisant pour les applications | A besoin d'attention | Un ou plusieurs volumes sont remplis à plus de 95 %, mais leur croissance automatique n'est pas activée.                                                                                                                                                                 | <b>Recommandé</b> : activez la croissance automatique jusqu'à 150 % de la capacité actuelle.<br><b>Autres options</b> : <ul style="list-style-type: none"><li>• Pour gagner de l'espace, supprimez les copies Snapshot.</li><li>• Redimensionner les volumes.</li><li>• Supprimez des répertoires ou des fichiers.</li></ul>                                                                                                                                                                                                                             |

|                                                              |                       |                                                                                                                                                                                                                                                                             |                                                                                                                |
|--------------------------------------------------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| La capacité du volume FlexGroup est déséquilibrée            | Optimisez le stockage | La taille des volumes constitutifs d'un ou plusieurs volumes FlexGroup a augmenté de façon inégale au fil du temps, entraînant un déséquilibre dans l'utilisation de la capacité. Si les volumes constitutifs sont pleins, des défaillances d'écriture peuvent se produire. | <b>Recommandé</b> : rééquilibrer les volumes FlexGroup.                                                        |
| Les machines virtuelles de stockage sont à court de capacité | Optimisez le stockage | Une ou plusieurs machines virtuelles de stockage sont proches de leur capacité maximale. Vous ne pourrez pas provisionner davantage d'espace pour les volumes nouveaux ou existants si les VM de stockage atteignent leur capacité maximale.                                | <b>Recommandé</b> : si possible, augmentez la limite de capacité maximale de la machine virtuelle de stockage. |

## Informations de sécurité

System Manager peut afficher les informations suivantes en réponse à des conditions susceptibles de compromettre la sécurité de vos données ou de votre système.

| Visibilité                                                                 | Gravité              | Condition                                                                          | Correctifs                                                                                                                                                                                     |
|----------------------------------------------------------------------------|----------------------|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Les volumes sont toujours en mode de formation anti-ransomware             | A besoin d'attention | Un ou plusieurs volumes sont en mode de formation anti-ransomware depuis 90 jours. | <b>Recommandé</b> : activez le mode actif anti-ransomware pour ces volumes.                                                                                                                    |
| La suppression automatique des copies Snapshot est activée sur les volumes | A besoin d'attention | La suppression automatique des snapshots est activée sur un ou plusieurs volumes.  | <b>Recommandé</b> : désactivez la suppression automatique des copies Snapshot. Sinon, en cas d'attaque par ransomware, il n'est pas toujours possible de restaurer les données de ces volumes. |

|                                               |                             |                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Les volumes n'ont pas de règles Snapshot      | A besoin d'attention        | Une règle Snapshot adéquate n'est pas associée à un ou plusieurs volumes.                                                        | <b>Recommandé</b> : rattachez une règle Snapshot à des volumes qui n'en ont pas. Sinon, en cas d'attaque par ransomware, il n'est pas toujours possible de restaurer les données de ces volumes.                                                                                                                                                                                                                                                                                                                                                                            |
| FPolicy natif n'est pas configuré             | Et des meilleures pratiques | Le système natif FPolicy n'est pas configuré sur une ou plusieurs machines virtuelles de stockage NAS.                           | <b>Recommandé: IMPORTANT:</b> Le blocage des extensions peut entraîner des résultats inattendus. À partir de la version 9.11.1, vous pouvez activer la fonctionnalité FPolicy native pour les machines virtuelles de stockage, qui bloque plus de 3000 extensions de fichier connues pour être utilisées dans le cadre d'attaques par ransomware. <a href="#">"Configuration de FPolicy natif"</a> Dans les machines virtuelles de stockage NAS pour contrôler les extensions de fichiers qui sont autorisées ou non à être écrites sur des volumes de votre environnement. |
| Telnet est activé                             | Et des meilleures pratiques | Secure Shell (SSH) doit être utilisé pour sécuriser l'accès à distance.                                                          | <b>Recommandé</b> : désactivez Telnet et utilisez SSH pour un accès distant sécurisé.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Trop peu de serveurs NTP sont configurés      | Et des meilleures pratiques | Le nombre de serveurs configurés pour NTP est inférieur à 3.                                                                     | <b>Recommandé</b> : associez au moins trois serveurs NTP au cluster. Sinon, des problèmes peuvent se produire lors de la synchronisation de l'heure du cluster.                                                                                                                                                                                                                                                                                                                                                                                                             |
| Le shell distant (RSH) est activé             | Et des meilleures pratiques | Secure Shell (SSH) doit être utilisé pour sécuriser l'accès à distance.                                                          | <b>Recommandé</b> : désactivez RSH et utilisez SSH pour un accès distant sécurisé.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| La bannière de connexion n'est pas configurée | Et des meilleures pratiques | Les messages de connexion ne sont pas configurés ni pour le cluster, ni pour la machine virtuelle de stockage, ni pour les deux. | <b>Recommandé</b> : configurez les bannières de connexion pour le cluster et la machine virtuelle de stockage et activez leur utilisation.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| AutoSupport utilise un protocole non sécurisé | Et des meilleures pratiques | AutoSupport n'est pas configuré pour communiquer via HTTPS.                                                                      | <b>Recommandé</b> : il est fortement recommandé d'utiliser HTTPS comme protocole de transport par défaut pour envoyer des messages AutoSupport au support technique.                                                                                                                                                                                                                                                                                                                                                                                                        |

|                                                                                               |                             |                                                                                                                                          |                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L'utilisateur admin par défaut n'est pas verrouillé                                           | Et des meilleures pratiques | Personne n'a ouvert de session à l'aide d'un compte d'administration par défaut (admin ou diag), et ces comptes ne sont pas verrouillés. | <b>Recommandé:</b> Verrouiller les comptes d'administration par défaut lorsqu'ils ne sont pas utilisés.                                                                                                                                                                                         |
| Secure Shell (SSH) utilise des chiffrements non sécurisés                                     | Et des meilleures pratiques | La configuration actuelle utilise des chiffrements CBC non sécurisés.                                                                    | <b>Recommandé:</b> Vous devez autoriser uniquement les chiffrements sécurisés sur votre serveur Web pour protéger les communications sécurisées avec vos visiteurs. Supprimer les chiffriers qui ont des noms contenant "cbc", tels que "ais128-cbc", "aes192-cbc", "aes256-cbc" et "3des-cbc". |
| La conformité à la norme FIPS 140-2 globale est désactivée                                    | Et des meilleures pratiques | La conformité à la norme FIPS 140-2 est désactivée sur le cluster.                                                                       | <b>Recommandé :</b> pour des raisons de sécurité, vous devez activer la cryptographie conforme à la norme FIPS 140-2 pour garantir que ONTAP peut communiquer en toute sécurité avec des clients externes ou des clients serveur.                                                               |
| Les attaques par ransomware ne font pas l'objet d'une surveillance des volumes                | A besoin d'attention        | La protection contre les ransomware est désactivée sur un ou plusieurs volumes.                                                          | <b>Recommandé :</b> activez la protection contre les ransomware sur les volumes. Sinon, vous ne remarquerez peut-être pas si des volumes sont menacés ou en cours d'attaque.                                                                                                                    |
| Les machines virtuelles de stockage ne sont pas configurées pour lutter contre les ransomware | Et des meilleures pratiques | Une ou plusieurs machines virtuelles de stockage ne sont pas configurées pour la protection contre les ransomware.                       | <b>Recommandé :</b> activez la protection contre les ransomware sur les machines virtuelles de stockage. Sinon, vous ne remarquerez peut-être pas la menace ou l'attaque des machines virtuelles de stockage.                                                                                   |

## Informations de configuration

System Manager peut afficher les informations suivantes en réponse à des problèmes de configuration de votre système.

|            |         |           |            |
|------------|---------|-----------|------------|
| Visibilité | Gravité | Condition | Correctifs |
|------------|---------|-----------|------------|

|                                                                    |                             |                                                                                                                                                                                                                                              |                                                                   |
|--------------------------------------------------------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Le cluster n'est pas configuré pour les notifications              | Et des meilleures pratiques | Les e-mails, les webhooks ou les trapshot SNMP ne sont pas configurés pour vous permettre de recevoir des notifications sur les problèmes rencontrés avec le cluster.                                                                        | <b>Recommandé</b> : configurer les notifications pour le cluster. |
| Le cluster n'est pas configuré pour les mises à jour automatiques. | Et des meilleures pratiques | Le cluster n'a pas été configuré pour recevoir les mises à jour automatiques des derniers fichiers de qualification de disque, de firmware de disque, de firmware de tiroir et de firmware SP/BMC lorsqu'ils sont disponibles.               | <b>Recommandé</b> : activez cette fonction.                       |
| Le firmware du cluster n'est pas à jour                            | Et des meilleures pratiques | Votre système ne dispose pas de la dernière mise à jour du micrologiciel qui pourrait avoir des améliorations, des correctifs de sécurité ou de nouvelles fonctionnalités qui aident à sécuriser le cluster pour de meilleures performances. | <b>Recommandé</b> : mettre à jour le micrologiciel ONTAP.         |

## Obtenez des informations exploitables pour optimiser votre système

Avec System Manager, vous pouvez afficher des informations exploitables qui vous aident à optimiser votre système.

### Description de la tâche

Depuis ONTAP 9.11.0, vous pouvez voir une vue d'ensemble de System Manager qui vous aide à optimiser la capacité et la conformité de sécurité de votre système.

Depuis ONTAP 9.11.1, vous pouvez afficher des informations supplémentaires pour optimiser la capacité, la conformité de sécurité et la configuration de votre système.



**Le blocage des extensions peut entraîner des résultats inattendus.** à partir de ONTAP 9.11.1, vous pouvez activer FPolicy natif pour les machines virtuelles de stockage à l'aide de System Manager. Il se peut que vous receviez un message System Manager Insight vous recommandant "[Configuration de FPolicy natif](#)" Pour une VM de stockage.



Avec le mode natif FPolicy, vous pouvez autoriser ou interdire des extensions de fichiers spécifiques. System Manager recommande plus de 3000 extensions de fichiers interdites utilisées dans les attaques par ransomware précédentes. Certaines de ces extensions peuvent être utilisées par des fichiers légitimes dans votre environnement et leur blocage peut entraîner des problèmes inattendus.

Par conséquent, il est fortement conseillé de modifier la liste des extensions pour répondre aux besoins de votre environnement. Reportez-vous à la section "[Comment supprimer une extension de fichier d'une configuration FPolicy native créée par System Manager à l'aide de System Manager pour recréer la règle](#)".

Pour en savoir plus sur FPolicy natif, consultez "[Types de configuration FPolicy](#)" la section .

En fonction des meilleures pratiques, ces informations sont affichées sur une page à partir de laquelle vous pouvez lancer des actions immédiates pour optimiser votre système. Pour plus de détails sur chaque information, reportez-vous à la section "[Informations sur System Manager](#)".

## Affichez les informations exploitables concernant l'optimisation





### Étapes

1. Dans System Manager, cliquez sur **Insights** dans la colonne de navigation de gauche.

La page **Insights** affiche des groupes de vues. Chaque groupe d'informations peut contenir une ou plusieurs informations. Les groupes suivants sont affichés :

- A votre attention
- Remédier aux risques
- Optimisez le stockage

2. (Facultatif) filtrez les informations affichées en cliquant sur ces boutons dans le coin supérieur droit de la page :

-  Affiche les informations relatives à la sécurité.
-  Affiche les informations relatives à la capacité.
-  Affiche les informations relatives à la configuration.
-  Affiche toutes les informations.

## Répondez aux informations exploitables pour optimiser votre système

Dans System Manager, vous pouvez répondre à des analyses en les rejetant, en explorant différentes façons de résoudre les problèmes ou en initiant le processus pour les résoudre.

### Étapes

1. Dans System Manager, cliquez sur **Insights** dans la colonne de navigation de gauche.
2. Passez le curseur sur un aperçu pour afficher les boutons permettant d'effectuer les opérations suivantes :
  - **Rejeter** : supprimez l'aperçu de la vue. Pour « rejeter » les avis, reportez-vous à [\[customize-settings-insights\]](#).
  - **Explorer** : Découvrez différentes façons de résoudre le problème mentionné dans la perspicacité. Ce bouton apparaît uniquement si plusieurs méthodes de correction sont possibles.
  - **Fix** : lancer le processus de résolution du problème mentionné dans l'InSight. Il vous sera demandé de confirmer si vous souhaitez prendre les mesures nécessaires pour appliquer le correctif.



Certaines de ces actions peuvent être lancées à partir d'autres pages de System Manager, mais la page **Insights** vous aide à rationaliser vos tâches quotidiennes en vous permettant de lancer ces actions à partir de cette page.

## Personnalisez les paramètres pour obtenir des informations exploitables

Vous pouvez personnaliser les informations dont vous recevrez des notifications dans System Manager.

### Étapes

1. Dans System Manager, cliquez sur **Insights** dans la colonne de navigation de gauche.
2. Dans le coin supérieur droit de la page, cliquez sur , puis sélectionnez **Paramètres**.
3. Sur la page **Paramètres**, assurez-vous que les cases à cocher situées en regard des informations que vous souhaitez en être averti. Si vous avez précédemment rejeté une idée, vous pouvez la « rejeter » en vous assurant qu'une case à cocher est cochée.
4. Cliquez sur **Enregistrer**.

## Exportez les informations sous forme de fichier PDF

Vous pouvez exporter toutes les informations applicables sous forme de fichier PDF.

### Étapes

1. Dans System Manager, cliquez sur **Insights** dans la colonne de navigation de gauche.
2. Dans le coin supérieur droit de la page, cliquez sur , puis sélectionnez **Exporter**.

## Configuration de FPolicy natif

Depuis ONTAP 9.11.1, lorsque vous recevez une vue System Manager qui suggère d'implémenter FPolicy natif, vous pouvez la configurer sur vos machines virtuelles et volumes de stockage.

### Avant de commencer

Lorsque vous accédez à System Manager Insights, sous **appliquer les meilleures pratiques**, vous pouvez recevoir un message indiquant que FPolicy natif n'est pas configuré.

Pour en savoir plus sur les types de configuration FPolicy, consultez "[Types de configuration FPolicy](#)" la section .

### Étapes

1. Dans System Manager, cliquez sur **Insights** dans la colonne de navigation de gauche.

2. Sous **appliquer les meilleures pratiques**, localisez **le système natif FPolicy n'est pas configuré**.
3. Lisez le message suivant avant de prendre des mesures :



**Le blocage des extensions peut entraîner des résultats inattendus.** à partir de ONTAP 9.11.1, vous pouvez activer FPolicy natif pour les machines virtuelles de stockage à l'aide de System Manager.

Avec le mode natif FPolicy, vous pouvez autoriser ou interdire des extensions de fichiers spécifiques. System Manager recommande plus de 3000 extensions de fichiers interdites utilisées dans les attaques par ransomware précédentes. Certaines de ces extensions peuvent être utilisées par des fichiers légitimes dans votre environnement et leur blocage peut entraîner des problèmes inattendus.

Par conséquent, il est fortement conseillé de modifier la liste des extensions pour répondre aux besoins de votre environnement. Reportez-vous à la section ["Comment supprimer une extension de fichier d'une configuration FPolicy native créée par System Manager à l'aide de System Manager pour recréer la règle"](#).

4. Cliquez sur **fixer**.
5. Sélectionnez les machines virtuelles de stockage auxquelles vous souhaitez appliquer la fonctionnalité FPolicy native.
6. Pour chaque VM de stockage, sélectionnez les volumes qui recevront la FPolicy native.
7. Cliquez sur **configurer**.

## Contrôlez et gérez les performances du cluster à l'aide de l'interface de ligne de commandes

### Contrôle des performances et présentation de la gestion

Vous pouvez également définir des tâches de base de contrôle et de gestion des performances, et identifier et résoudre des problèmes courants de performance.

Vous pouvez utiliser ces procédures pour contrôler et gérer les performances du cluster si les hypothèses suivantes s'appliquent à votre situation :

- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.
- Vous pouvez afficher l'état du système et les alertes, surveiller les performances du cluster et effectuer une analyse de la source des problèmes à l'aide de Active IQ Unified Manager (anciennement OnCommand Unified Manager) en plus de l'interface de ligne de commandes de ONTAP.
- Vous utilisez l'interface de ligne de commandes ONTAP pour configurer la qualité de service (QoS) du stockage. La QoS est également disponible via ce qui suit :
  - System Manager
  - L'API REST DE ONTAP
  - Les outils ONTAP pour VMware vSphere
  - Gestionnaire de niveau de service NetApp
  - OnCommand Workflow Automation (WFA)
- Vous souhaitez installer Unified Manager à l'aide d'une appliance virtuelle au lieu d'une installation Linux ou Windows.

- Vous êtes prêt à utiliser une configuration statique plutôt que DHCP pour installer le logiciel.
- Vous pouvez accéder aux commandes ONTAP au niveau de privilège avancé.
- Vous êtes un administrateur de cluster ayant le rôle « admin ».

### Informations associées

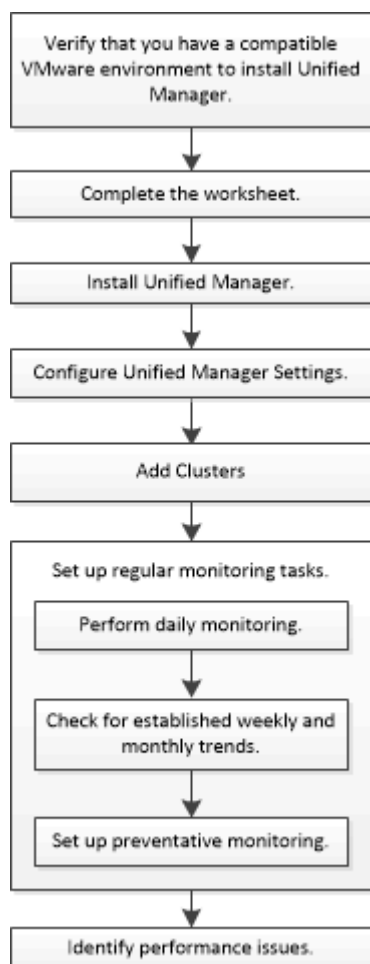
Si ces hypothèses ne sont pas correctes pour votre situation, vous devez consulter les ressources suivantes :

- ["Installation de Active IQ Unified Manager 9.8"](#)
- ["Administration du système"](#)

## Contrôle des performances

### Présentation du workflow de surveillance des performances et de maintenance

Le contrôle et la maintenance des performances du cluster impliquent l'installation du logiciel Active IQ Unified Manager, la configuration des tâches de surveillance de base, l'identification des problèmes de performances et les ajustements nécessaires.



### Vérifiez que votre environnement VMware est pris en charge

Pour installer correctement Active IQ Unified Manager, vous devez vérifier que votre environnement VMware répond aux exigences requises.

## Étapes

1. Vérifiez que votre infrastructure VMware répond aux exigences de dimensionnement pour l'installation de Unified Manager.
2. Accédez au "[Matrice d'interopérabilité](#)" pour vérifier que vous disposez d'une combinaison prise en charge des composants suivants :
  - Version ONTAP
  - Version du système d'exploitation ESXi
  - Version de VMware vCenter Server
  - Version des outils VMware
  - Type et version du navigateur



Le "[Matrice d'interopérabilité](#)" répertorie les configurations prises en charge pour Unified Manager.

3. Cliquez sur le nom de la configuration sélectionnée.

Les détails de cette configuration s'affichent dans la fenêtre Détails de la configuration.

4. Vérifiez les informations dans les onglets suivants :

- Remarques

Le répertoire les alertes et informations importantes spécifiques à votre configuration.

- Politiques et lignes directrices

Présente des recommandations d'ordre général pour toutes les configurations.

## Fiche technique Active IQ Unified Manager

Avant d'installer, de configurer et de connecter Active IQ Unified Manager, vous devez disposer facilement d'informations spécifiques sur votre environnement. Vous pouvez enregistrer les informations dans la fiche.

### Informations sur l'installation de Unified Manager

| Machine virtuelle sur laquelle le logiciel est déployé | Votre valeur |
|--------------------------------------------------------|--------------|
| Adresse IP du serveur ESXi                             |              |
| Nom de domaine complet de l'hôte                       |              |
| Adresse IP de l'hôte                                   |              |
| Masque de réseau                                       |              |
| Adresse IP de la passerelle                            |              |


|                                         |  |
|-----------------------------------------|--|
| Adresse DNS principale                  |  |
| Adresse DNS secondaire                  |  |
| Domaines de recherche                   |  |
| Nom d'utilisateur de maintenance        |  |
| Mot de passe utilisateur de maintenance |  |

#### Informations sur la configuration de Unified Manager

| Réglage                                                         | Votre valeur           |
|-----------------------------------------------------------------|------------------------|
| Adresse e-mail de l'utilisateur de maintenance                  |                        |
| Serveur NTP                                                     |                        |
| Nom d'hôte ou adresse IP du serveur SMTP                        |                        |
| Nom d'utilisateur SMTP                                          |                        |
| Mot de passe SMTP                                               |                        |
| Port SMTP par défaut                                            | 25 (valeur par défaut) |
| E-mail à partir duquel les notifications d'alerte sont envoyées |                        |
| Nom distinctif de la liaison LDAP                               |                        |
| Mot de passe de liaison LDAP                                    |                        |
| Nom d'administrateur Active Directory                           |                        |
| Mot de passe Active Directory                                   |                        |
| Nom distinctif de la base du serveur d'authentification         |                        |
| Nom d'hôte ou adresse IP du serveur d'authentification          |                        |

#### Informations sur le cluster

Capturer les informations suivantes pour chaque cluster sur Unified Manager.

| Cluster 1 de N                                                                                                                                                           | Votre valeur |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Nom d'hôte ou adresse IP de gestion du cluster                                                                                                                           |              |
| <div> <div></div> <div>L'administrateur doit avoir reçu le rôle « admin ».</div> </div> |              |
| Mot de passe administrateur ONTAP                                                                                                                                        |              |
| Protocole (HTTP ou HTTPS)                                                                                                                                                |              |

### Informations associées

"Authentification de l'administrateur et RBAC"

## Installez Active IQ Unified Manager

### Téléchargez et déployez Active IQ Unified Manager

Pour installer le logiciel, vous devez télécharger le fichier d'installation de l'appliance virtuelle (va), puis utiliser un client VMware vSphere pour déployer le fichier sur un serveur VMware ESXi. Le va est disponible dans un fichier OVA.

### Étapes

1. Accédez à la page **NetApp support site Software Download** (Téléchargement de logiciels) et recherchez Active IQ Unified Manager.

<https://mysupport.netapp.com/products/index.html>

2. Sélectionnez **VMware vSphere** dans le menu déroulant **Select Platform** et cliquez sur **Go!**
3. Enregistrez le fichier « OVA » dans un emplacement local ou réseau accessible à votre client VMware vSphere.
4. Dans VMware vSphere client, cliquez sur **fichier > déployer le modèle OVF**.
5. Localisez le fichier « OVA » et utilisez l'assistant pour déployer l'appliance virtuelle sur le serveur ESXi.

Vous pouvez utiliser l'onglet **Propriétés** de l'assistant pour saisir vos informations de configuration statique.

6. Mise sous tension de la machine virtuelle
7. Cliquez sur l'onglet **Console** pour afficher le processus de démarrage initial.
8. Suivez l'invite pour installer VMware Tools sur la machine virtuelle.
9. Configurer le fuseau horaire.
10. Entrez un nom d'utilisateur et un mot de passe de maintenance.
11. Accédez à l'URL affichée par la console de la machine virtuelle.

## Configurez les paramètres Active IQ Unified Manager initiaux

La boîte de dialogue Configuration initiale du Active IQ Unified Manager s’affiche lorsque vous accédez pour la première fois à l’interface utilisateur Web, qui vous permet de configurer certains paramètres initiaux et d’ajouter des clusters.

### Étapes

1. Acceptez le paramètre AutoSupport activé par défaut.
2. Entrez les détails du serveur NTP, l’adresse e-mail de l’utilisateur de maintenance, le nom d’hôte du serveur SMTP et les options SMTP supplémentaires, puis cliquez sur **Enregistrer**.

### Une fois que vous avez terminé

Une fois la configuration initiale terminée, la page sources de données du cluster s’affiche, dans laquelle vous pouvez ajouter les détails du cluster.

### Spécifiez les clusters à surveiller

Vous devez ajouter un cluster à un serveur Active IQ Unified Manager pour surveiller le cluster, afficher l’état de détection du cluster et contrôler ses performances.

### Ce dont vous avez besoin

- Vous devez disposer des informations suivantes :
  - Nom d’hôte ou adresse IP de gestion du cluster

Le nom d’hôte est le nom de domaine complet (FQDN) ou le nom court que Unified Manager utilise pour se connecter au cluster. Ce nom d’hôte doit être résolu sur l’adresse IP de gestion du cluster.

L’adresse IP de gestion du cluster doit être la LIF de gestion du cluster du serveur virtuel de stockage administratif (SVM). Si vous utilisez une LIF node-management, l’opération échoue.
  - Nom d’utilisateur et mot de passe de l’administrateur ONTAP
  - Type de protocole (HTTP ou HTTPS) pouvant être configuré sur le cluster et le numéro de port du cluster
- Vous devez avoir le rôle Administrateur d’applications ou Administrateur de stockage.
- L’administrateur ONTAP doit disposer des rôles d’administrateur ONTAPI et SSH.
- Le FQDN de Unified Manager doit pouvoir exécuter ONTAP.

Vous pouvez le vérifier à l’aide de la commande ONTAP `ping -node node_name -destination Unified_Manager_FQDN`.

### Description de la tâche

Dans le cas d’une configuration MetroCluster, vous devez ajouter les clusters locaux et distants, et les clusters doivent être configurés correctement.

### Étapes

1. Cliquez sur **Configuration > sources de données de cluster**.
2. Sur la page clusters, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un cluster**, spécifiez les valeurs requises, telles que le nom d’hôte ou



l'adresse IP (IPv4 ou IPv6) du cluster, le nom d'utilisateur, le mot de passe, le protocole de communication et le numéro de port.

Par défaut, le protocole HTTPS est sélectionné.

Vous pouvez modifier l'adresse IP de gestion du cluster d'IPv6 au format IPv4 ou d'IPv4 à IPv6. La nouvelle adresse IP est reflétée dans la grille du cluster et la page de configuration du cluster, une fois le cycle de surveillance suivant terminé.

4. Cliquez sur **Ajouter**.

5. Si HTTPS est sélectionné, effectuez les opérations suivantes :

- a. Dans la boîte de dialogue **Authorise Host** , cliquez sur **View Certificate** pour afficher les informations de certificat relatives au cluster.
- b. Cliquez sur **Oui**.

Unified Manager vérifie le certificat uniquement lors de l'ajout initial du cluster, mais ne le vérifie pas pour chaque appel d'API à ONTAP.

Si le certificat a expiré, vous ne pouvez pas ajouter le cluster. Vous devez renouveler le certificat SSL, puis ajouter le cluster.

6. **Facultatif** : affichez l'état de la détection du cluster :

- a. Vérifiez l'état de la détection du cluster à partir de la page **Configuration du cluster**.

Le cluster est ajouté à la base de données Unified Manager après l'intervalle de contrôle par défaut d'environ 15 minutes.

## Configurer les tâches de surveillance de base

### Effectuer un contrôle quotidien

Vous pouvez effectuer une surveillance quotidienne afin de vous assurer que vous n'avez aucun problème de performance immédiat à laquelle vous devez vous préoccuper.

#### Étapes

1. Dans l'interface utilisateur Active IQ Unified Manager, accédez à la page **Inventaire des événements** pour afficher tous les événements actuels et obsolètes.
2. Dans l'option **View**, sélectionnez **Active Performance Events** et déterminer quelle action est nécessaire.

### Utilisez les tendances de performances hebdomadaires et mensuelles pour identifier les problèmes de performances

L'identification des tendances de performances permet de déterminer si le cluster est sur-utilisé ou sous-utilisé en analysant la latence du volume. Vous pouvez utiliser des étapes similaires pour identifier les goulots d'étranglement du processeur, du réseau ou d'autres systèmes.

#### Étapes

1. Identifiez le volume que vous pensez être sous-utilisé ou sur-utilisé.

2. Dans l'onglet **Détails du volume**, cliquez sur **30 d** pour afficher les données historiques.
3. Dans le menu déroulant « données de pause par », sélectionnez **latence**, puis cliquez sur **Envoyer**.
4. Désélectionnez **agrégat** dans le tableau comparatif des composants du cluster, puis comparez la latence du cluster avec celle du tableau de latence du volume.
5. Sélectionnez **agrégat** et désélectionnez tous les autres composants dans le tableau comparatif des composants du cluster, puis comparez la latence globale avec celle du graphique de latence du volume.
6. Comparez le graphique de latence de lecture/écriture sur le tableau de latence du volume.
7. Identifiez si les charges d'application client ont provoqué des conflits au niveau de la charge de travail et rééquilibrez les charges de travail en fonction des besoins.
8. Déterminez si l'agrégat est sur-utilisé et source de conflits, et rééquilibrez les charges de travail si nécessaire.

#### Utilisez des seuils de performances pour générer des notifications d'événements

Les événements sont des notifications que la Active IQ Unified Manager génère automatiquement lorsqu'une condition prédéfinie se produit ou lorsqu'une valeur de compteur de performances franchit un seuil. Les événements vous aident à identifier les problèmes de performance dans les clusters que vous surveillez. Vous pouvez configurer des alertes pour envoyer automatiquement une notification par e-mail lorsque des événements de certains types de gravité se produisent.

#### Définissez des seuils de performances

Vous pouvez définir des seuils de performance pour contrôler les problèmes de performance stratégiques. Des seuils définis par l'utilisateur déclenchent une notification d'avertissement ou d'événement critique lorsque le système approche ou dépasse le seuil défini.

#### Étapes

1. Créez les seuils d'avertissement et d'événement critique :
  - a. Sélectionnez **Configuration > seuils de performances**.
  - b. Cliquez sur **Créer**.
  - c. Sélectionnez le type d'objet et spécifiez un nom et une description de la règle.
  - d. Sélectionnez la condition de compteur d'objets et spécifiez les valeurs limites qui définissent les événements Avertissement et critique.
  - e. Sélectionnez la durée pendant laquelle les valeurs limites doivent être enfreintes pour un événement à envoyer, puis cliquez sur **Enregistrer**.
2. Attribuez la politique de seuil à l'objet de stockage.
  - a. Accédez à la page Inventaire pour le même type d'objet de cluster que vous avez précédemment sélectionné et choisissez **Performance** dans l'option Afficher.
  - b. Sélectionnez l'objet auquel vous souhaitez affecter la stratégie de seuil, puis cliquez sur **affecter stratégie de seuil**.
  - c. Sélectionnez la stratégie que vous avez créée précédemment, puis cliquez sur **affecter stratégie**.

#### Exemple

Vous pouvez définir des seuils définis par l'utilisateur pour en savoir plus sur les problèmes de performance stratégiques. Par exemple, si vous disposez d'un serveur Microsoft Exchange et que vous savez qu'il tombe en panne si la latence du volume dépasse 20 millisecondes, vous pouvez définir un seuil d'avertissement à 12 millisecondes et un seuil critique à 15 millisecondes. Avec ce paramètre de seuil, vous pouvez recevoir des notifications lorsque la latence du volume dépasse la limite.

|                           | Warning               |    | Critical |    |
|---------------------------|-----------------------|----|----------|----|
| Object Counter Condition* | Average Latency ms/op | 12 | ms/op    | 15 |

### Ajouter des alertes

Vous pouvez configurer des alertes pour vous avertir lorsqu'un événement particulier est généré. Vous pouvez configurer les alertes pour une seule ressource, pour un groupe de ressources ou pour les événements d'un type de sévérité particulier. Vous pouvez spécifier la fréquence à laquelle vous souhaitez être averti et associer un script à l'alerte.

### Ce dont vous avez besoin

- Vous devez avoir configuré des paramètres de notification tels que l'adresse e-mail de l'utilisateur, le serveur SMTP et l'hôte d'interruption SNMP pour permettre au serveur Active IQ Unified Manager d'utiliser ces paramètres pour envoyer des notifications aux utilisateurs lorsqu'un événement est généré.
- Vous devez connaître les ressources et les événements pour lesquels vous souhaitez déclencher l'alerte, ainsi que les noms d'utilisateur ou adresses e-mail des utilisateurs que vous souhaitez notifier.
- Si vous souhaitez que le script soit exécuté en fonction de l'événement, vous devez l'avoir ajouté à Unified Manager à l'aide de la page scripts.
- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

### Description de la tâche

Vous pouvez créer une alerte directement à partir de la page Détails de l'événement après avoir reçu un événement en plus de créer une alerte à partir de la page Configuration de l'alerte, comme décrit ici.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management > Alert Setup**.
2. Dans la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom**, puis entrez un nom et une description pour l'alerte.
4. Cliquez sur **Ressources**, puis sélectionnez les ressources à inclure ou à exclure de l'alerte.

Vous pouvez définir un filtre en spécifiant une chaîne de texte dans le champ **Nom contient** pour sélectionner un groupe de ressources. En fonction de la chaîne de texte que vous spécifiez, la liste des ressources disponibles n'affiche que les ressources qui correspondent à la règle de filtre. La chaîne de texte que vous spécifiez est sensible à la casse.

Si une ressource est conforme à la fois aux règles inclure et exclure que vous avez spécifiées, la règle d'exclusion est prioritaire sur la règle inclure et l'alerte n'est pas générée pour les événements liés à la ressource exclue.

5. Cliquez sur **Événements**, puis sélectionnez les événements en fonction du nom de l'événement ou du type de gravité de l'événement pour lequel vous souhaitez déclencher une alerte.



Pour sélectionner plusieurs événements, appuyez sur la touche Ctrl pendant que vous effectuez vos sélections.

6. Cliquez sur **actions** et sélectionnez les utilisateurs que vous souhaitez notifier, choisissez la fréquence de notification, choisissez si une interruption SNMP sera envoyée au récepteur d'interruption et affectez un script à exécuter lorsqu'une alerte est générée.



Si vous modifiez l'adresse e-mail spécifiée pour l'utilisateur et rouvrez l'alerte pour modification, le champ Nom apparaît vide car l'adresse e-mail modifiée n'est plus mappée à l'utilisateur qui a été précédemment sélectionné. En outre, si vous avez modifié l'adresse e-mail de l'utilisateur sélectionné à partir de la page utilisateurs, l'adresse e-mail modifiée n'est pas mise à jour pour l'utilisateur sélectionné.

Vous pouvez également choisir de notifier les utilisateurs via les interruptions SNMP.

7. Cliquez sur **Enregistrer**.

### Exemple d'ajout d'une alerte

Dans cet exemple, vous apprendrez à créer une alerte conforme aux exigences suivantes :

- Nom de l'alerte : HealthTest
- Ressources : inclut tous les volumes dont le nom contient « abc » et exclut tous les volumes dont le nom contient « xyz »
- Événements : inclut tous les événements de santé critiques
- Actions : inclut « [sample@domain.com](mailto:sample@domain.com) », un script « Test » et l'utilisateur doit être averti toutes les 15 minutes

Effectuez les opérations suivantes dans la boîte de dialogue Ajouter une alerte :

1. Cliquez sur **Nom** et saisissez HealthTest Dans le champ **Nom d'alerte**.
2. Cliquez sur **Ressources** et, dans l'onglet inclure, sélectionnez **volumes** dans la liste déroulante.
  - a. Entrez abc Dans le champ **Name contient** pour afficher les volumes dont le nom contient "abc".
  - b. Sélectionnez **<<All Volumes whose name contains 'abc'>>** dans la zone Ressources disponibles, et déplacez-la dans la zone Ressources sélectionnées.
  - c. Cliquez sur **exclude**, puis saisissez xyz Dans le champ **Name contient**, puis cliquez sur **Add**.
3. Cliquez sur **Événements**, puis sélectionnez **critique** dans le champ gravité de l'événement.
4. Sélectionnez **tous les événements critiques** dans la zone événements de correspondance et déplacez-le dans la zone événements sélectionnés.
5. Cliquez sur **actions**, puis saisissez [sample@domain.com](mailto:sample@domain.com) Dans le champ Alert ces utilisateurs.
6. Sélectionnez **rappeler toutes les 15 minutes** pour avertir l'utilisateur toutes les 15 minutes.

Vous pouvez configurer une alerte pour qu'elle envoie régulièrement des notifications aux destinataires pendant une heure donnée. Vous devez déterminer l'heure à laquelle la notification d'événement est active pour l'alerte.

7. Dans le menu Select script to Execute, sélectionnez **Test** script.
8. Cliquez sur **Enregistrer**.

Configurez les paramètres d'alerte

Vous pouvez spécifier les événements provenant de Active IQ Unified Manager qui déclenchent des alertes, les destinataires de ces alertes et la fréquence des alertes.

Ce dont vous avez besoin


Vous devez avoir le rôle Administrateur d'applications.

Description de la tâche

Vous pouvez configurer des paramètres d'alerte uniques pour les types d'événements de performance suivants :

- Événements critiques déclenchés par des violations des seuils définis par l'utilisateur
- Événements d'avertissement déclenchés par des violations des seuils définis par l'utilisateur, des seuils définis par le système ou des seuils dynamiques

Par défaut, des alertes par e-mail sont envoyées aux utilisateurs d'administration de Unified Manager pour tous les nouveaux événements. Vous pouvez envoyer des alertes par e-mail à d'autres utilisateurs en ajoutant les adresses e-mail de ces utilisateurs.



Pour désactiver l'envoi d'alertes pour certains types d'événements, vous devez décocher toutes les cases d'une catégorie d'événement. Cette action n'arrête pas l'apparition des événements dans l'interface utilisateur.

Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Storage Management > Alert Setup**.  
  
La page Configuration des alertes s'affiche.
2. Cliquez sur **Ajouter** et configurez les paramètres appropriés pour chaque type d'événement.  
  
Pour envoyer des alertes par e-mail à plusieurs utilisateurs, entrez une virgule entre chaque adresse e-mail.
3. Cliquez sur **Enregistrer**.

Identification des problèmes de performances dans Active IQ Unified Manager

Si un événement de performance se produit, vous pouvez localiser la source du problème dans Active IQ Unified Manager et utiliser d'autres outils pour le résoudre. Vous recevrez peut-être une notification par e-mail d'un événement ou une notification de cet événement pendant le suivi quotidien.

Étapes

1. Cliquez sur le lien de la notification par e-mail, qui vous mène directement à l'objet de stockage ayant un événement de performances.

| Si...                                               | Alors...                                                                           |
|-----------------------------------------------------|------------------------------------------------------------------------------------|
| Recevoir une notification par e-mail d'un événement | Cliquez sur le lien pour accéder directement à la page des détails de l'événement. |

Remarquez l'événement lors de l'analyse de la page Inventaire des événements

Sélectionnez l'événement pour accéder directement à la page des détails de l'événement.

2. Si l'événement a franchi un seuil défini par le système, suivez les actions suggérées dans l'interface utilisateur pour résoudre le problème.
3. Si l'événement a franchi un seuil défini par l'utilisateur, analysez l'événement pour déterminer si vous devez agir.
4. Si le problème persiste, vérifiez les paramètres suivants :
  - Paramètres de protocole sur le système de stockage
  - Paramètres réseau sur n'importe quel commutateur Ethernet ou Fabric
  - Paramètres réseau sur le système de stockage
  - Disposition des disques et metrics des agrégats sur le système de stockage
5. Si le problème persiste, contactez le support technique pour obtenir de l'aide.

## Utilisez le conseiller numérique Active IQ pour consulter les performances du système

Pour tous les systèmes ONTAP qui envoient la télémétrie AutoSupport à NetApp, vous pouvez afficher des données étendues de performances et de capacité. Active IQ affiche les performances du système sur une période plus longue que ce que vous pouvez voir dans System Manager.

Vous pouvez afficher les graphiques de l'utilisation du CPU, de la latence, des opérations d'entrée/sortie par seconde, des opérations d'entrée/sortie par protocole et du débit du réseau. Vous pouvez également télécharger ces données au format .csv pour les analyser avec d'autres outils.

Outre ces données de performances, Active IQ affiche l'efficacité du stockage par charge de travail et compare cette efficacité à celle attendue pour ce type de charge de travail. Vous pouvez consulter les tendances en matière de capacité et obtenir une estimation de la quantité de stockage supplémentaire à ajouter dans une période donnée.



- L'efficacité du stockage est disponible au niveau du client, du cluster et des nœuds, à gauche du tableau de bord principal.
- La performance est disponible au niveau du cluster et du nœud sur la gauche du tableau de bord principal.

### Informations associées

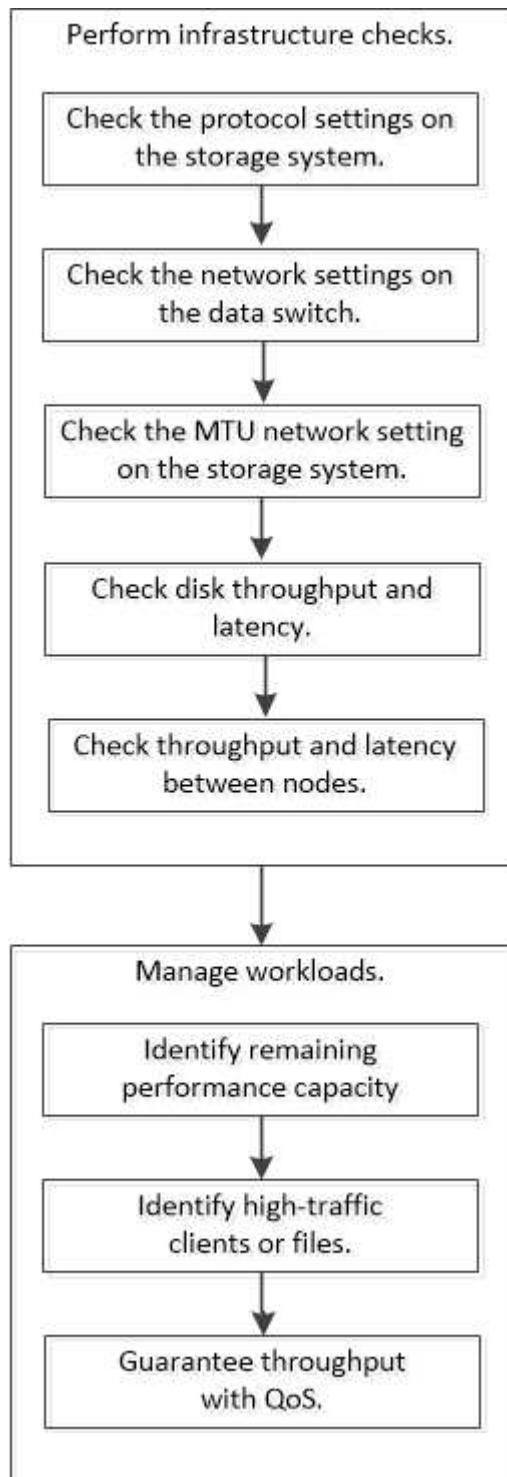
- ["Documentation du conseiller digital Active IQ"](#)
- ["Liste de lecture vidéo conseiller numérique Active IQ"](#)
- ["Portail Web Active IQ"](#)

## Gérez les problèmes de performance

### Workflow de gestion des performances

Une fois que vous avez identifié un problème de performance, vous pouvez procéder à

quelques vérifications de diagnostic de base de votre infrastructure pour éliminer les erreurs de configuration évidentes. Si ceux qui ne identifient pas le problème, vous pouvez commencer par examiner les problèmes liés à la gestion des charges de travail.



## Effectuer des vérifications de base de l'infrastructure

Vérifiez les paramètres de protocole sur le système de stockage

## Vérifiez la taille maximale du transfert TCP NFS

Pour NFS, vous pouvez vérifier si la taille maximale du transfert TCP pour les lectures et les écritures peut provoquer un problème de performances. Si vous pensez que la taille ralentit les performances, vous pouvez l'augmenter.

### Ce dont vous avez besoin

- Pour effectuer cette tâche, vous devez disposer des privilèges d'administrateur de cluster.
- Vous devez utiliser des commandes de niveau de privilège avancé pour cette tâche.

### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Vérifiez la taille maximale du transfert TCP :

```
vserver nfs show -vserver vserver_name -instance
```

3. Si la taille maximale du transfert TCP est trop faible, augmentez la taille :

```
vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
```

4. Revenir au niveau de privilège administratif :

```
set -privilege admin
```

### Exemple

L'exemple suivant modifie la taille maximale de transfert TCP de SVM1 à 1048576 :

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

## Vérifiez la taille de lecture/écriture TCP iSCSI

Pour iSCSI, vous pouvez vérifier la taille de lecture/écriture TCP pour déterminer si le paramètre de taille crée un problème de performances. Si la taille est la source d'un problème, vous pouvez le corriger.

### Ce dont vous avez besoin

Des commandes de niveau de privilège avancé sont requises pour cette tâche.

### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Vérifiez le paramètre de taille de la fenêtre TCP :

```
vserver iscsi show -vserver vserver_name -instance
```



3. Modifiez le paramètre de taille de la fenêtre TCP :

```
vserver iscsi modify -vserver vserver_name -tcp-window-size integer
```

4. Revenir au privilège administratif :

```
set -privilege admin
```

### Exemple

L'exemple suivant modifie la taille de la fenêtre TCP de SVM1 à 131,400 octets :

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

### Contrôler les réglages multiplexés CIFS

Si des performances réseau CIFS lentes sont à l'origine d'un problème de performances, vous pouvez modifier les paramètres multiplexés pour les améliorer et les corriger.

#### Étapes

1. Contrôler le réglage multiplexé CIFS :

```
vserver cifs options show -vserver -vserver_name -instance
```

2. Modifier le paramètre multiplexé CIFS :

```
vserver cifs options modify -vserver -vserver_name -max-mpx integer
```

### Exemple

L'exemple suivant modifie le nombre maximal de multiplexage activé SVM1 à 255 :

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

### Vérifiez la vitesse du port de l'adaptateur FC

La vitesse du port cible de l'adaptateur doit correspondre à la vitesse du périphérique auquel il se connecte, afin d'optimiser les performances. Si le port est défini sur négociation automatique, il peut prendre plus de temps pour vous reconnecter après un basculement et un rétablissement ou une autre interruption.

#### Ce dont vous avez besoin

Toutes les LIFs qui utilisent cet adaptateur comme port de home port doivent être hors ligne.

#### Étapes

1. Mettez l'adaptateur hors ligne :

```
network fcp adapter modify -node nodename -adapter adapter -state down
```

2. Vérifiez la vitesse maximale de l'adaptateur de port :

```
fcg adapter show -instance
```

3. Modifiez la vitesse du port, si nécessaire :

```
network fcg adapter modify -node nodename -adapter adapter -speed
{1|2|4|8|10|16|auto}
```

4. Mettez la carte en ligne :

```
network fcg adapter modify -node nodename -adapter adapter -state up
```

5. Mettre en ligne toutes les LIFs sur l'adaptateur :

```
network interface modify -vserver * -lif * { -home-node node1 -home-port e0c }
-status-admin up
```

### Exemple

L'exemple suivant modifie la vitesse du port de l'adaptateur 0d marche *node1* Jusqu'à 2 Gbits/s :

```
cluster1::> network fcg adapter modify -node node1 -adapter 0d -speed 2
```

### Vérifiez les paramètres réseau sur les commutateurs de données

Bien que vous deviez conserver les mêmes paramètres MTU sur vos clients, serveurs et systèmes de stockage (c'est-à-dire les points de terminaison réseau), les périphériques réseau intermédiaires tels que les cartes réseau et les commutateurs doivent être définis sur leurs valeurs MTU maximales pour garantir que les performances ne sont pas affectées.

Pour des performances optimales, tous les composants du réseau doivent être en mesure de transférer des trames Jumbo (IP de 9000 octets, 9022 octets y compris Ethernet). Les commutateurs de données doivent être réglés sur au moins 9022 octets, mais une valeur typique de 9216 est possible avec la plupart des commutateurs.

### Procédure

Pour les commutateurs de données, vérifiez que la taille de MTU est définie sur 9022 ou plus.

Pour plus d'informations, consultez la documentation du fournisseur du commutateur.

### Vérifiez le paramètre réseau MTU sur le système de stockage

Vous pouvez modifier les paramètres réseau sur le système de stockage s'ils ne sont pas identiques à ceux du client ou d'autres terminaux réseau. Alors que le paramètre MTU du réseau de gestion est défini sur 1500, la taille MTU du réseau de données doit être de 9000.

## Description de la tâche

Tous les ports d'un broadcast-domain ont la même taille de MTU, à l'exception du trafic de gestion du port e0M. Si le port fait partie d'un domaine de diffusion, utilisez le `broadcast-domain modify` Commande permettant de modifier la MTU de tous les ports du broadcast-domain modifié.

Notez que les périphériques réseau intermédiaires tels que les cartes réseau et les commutateurs de données peuvent être configurés sur des MTU plus élevés que les noeuds finaux réseau. Pour plus d'informations, voir ["Vérifiez les paramètres réseau sur les commutateurs de données"](#).

### Étapes

1. Vérifiez le paramètre du port MTU sur le système de stockage :

```
network port show -instance
```

2. Modifier la MTU sur le domaine de diffusion utilisé par les ports :

```
network port broadcast-domain modify -ipspace ipspace -broadcast-domain
broadcast_domain -mtu new_mtu
```

### Exemple

L'exemple suivant modifie le paramètre du port MTU sur 9000 :

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain
Cluster -mtu 9000
```

## Vérifiez le débit et la latence des disques

Vous pouvez vérifier les mesures de débit et de latence des disques pour les nœuds de cluster afin de vous aider à effectuer le dépannage.

## Description de la tâche

Des commandes de niveau de privilège avancé sont requises pour cette tâche.

### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Vérifiez le débit du disque et les mesures de latence :

```
statistics disk show -sort-key latency
```

### Exemple

L'exemple suivant affiche les totaux de chaque opération de lecture ou d'écriture de l'utilisateur pour `node2` marche `cluster1`:

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
```

| Disk    | Node  | Busy (%) | Total Ops | Read Ops | Write Ops | Read (Bps) | Write (Bps) | *Latency (us) |
|---------|-------|----------|-----------|----------|-----------|------------|-------------|---------------|
| 1.10.20 | node2 | 4        | 5         | 3        | 2         | 95232      | 367616      | 23806         |
| 1.10.8  | node2 | 4        | 5         | 3        | 2         | 138240     | 386048      | 22113         |
| 1.10.6  | node2 | 3        | 4         | 2        | 2         | 48128      | 371712      | 19113         |
| 1.10.19 | node2 | 4        | 6         | 3        | 2         | 102400     | 443392      | 19106         |
| 1.10.11 | node2 | 4        | 4         | 2        | 2         | 122880     | 408576      | 17713         |

### Vérifiez le débit et la latence entre les nœuds

Vous pouvez utiliser le `network test-path` commande permettant d'identifier les goulets d'étranglement réseau ou de présélectionner les chemins réseau entre les nœuds. Vous pouvez exécuter la commande entre les nœuds intercluster ou intracluster.

### Ce dont vous avez besoin

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des commandes de niveau de privilège avancé sont requises pour cette tâche.
- Pour un chemin intercluster, les clusters source et destination doivent être associés.

### Description de la tâche

Il arrive que les performances du réseau entre les nœuds ne répondent pas aux attentes de votre configuration de chemin. Un taux de transmission de 1 Gbit/s pour le type de transferts de données volumineux vus dans les opérations de réplication SnapMirror, par exemple, ne serait pas cohérent avec une liaison 10 GbE entre les clusters source et destination.

Vous pouvez utiliser le `network test-path` commande pour mesurer le débit et la latence entre les nœuds. Vous pouvez exécuter la commande entre les nœuds intercluster ou intracluster.



Le test sature le chemin du réseau avec des données, vous devez donc exécuter la commande lorsque le système n'est pas occupé, et lorsque le trafic réseau entre les nœuds n'est pas excessif. Le test s'est terminé après dix secondes. La commande ne peut être exécutée qu'entre des nœuds ONTAP 9.

Le `session-type` Option identifie le type d'opération que vous exécutez sur le chemin réseau, par exemple « AsyncMirrorRemote » pour la réplication SnapMirror vers une destination distante. Le type détermine la quantité de données utilisées dans le test. Le tableau suivant définit les types de session :

| Type de session  | Description                                                        |
|------------------|--------------------------------------------------------------------|
| AsyncMirrorlocal | Paramètres utilisés par SnapMirror entre les nœuds du même cluster |

|                                 |                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AsyncMirrorRemote               | Paramètres utilisés par SnapMirror entre les nœuds dans différents clusters (type par défaut)                                                                                                        |
| Transfert de données à distance | Paramètres utilisés par ONTAP pour l'accès distant aux données entre les nœuds d'un même cluster (par exemple, une requête NFS vers un nœud pour un fichier stocké dans un volume sur un autre nœud) |

## Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Mesure du débit et de la latence entre les nœuds :

```
network test-path -source-node source_nodename |local -destination-cluster
destination_clustername -destination-node destination_nodename -session-type
Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer
```

Le nœud source doit se trouver dans le cluster local. Le nœud de destination peut être situé sur le cluster local ou dans un cluster en clusters à peering. Une valeur de "local" pour `-source-node` spécifie le nœud sur lequel vous exécutez la commande.

La commande suivante mesure le débit et la latence des opérations de réplication de type SnapMirror entre `node1` sur le cluster local et `node3` marche `cluster2`:

```
cluster1::> network test-path -source-node node1 -destination-cluster
cluster2 -destination-node node3 -session-type AsyncMirrorRemote
Test Duration: 10.88 secs
Send Throughput: 18.23 MB/sec
Receive Throughput: 18.23 MB/sec
MB sent: 198.31
MB received: 198.31
Avg latency in ms: 2301.47
Min latency in ms: 61.14
Max latency in ms: 3056.86
```

3. Revenir au privilège administratif :

```
set -privilege admin
```

## Une fois que vous avez terminé

Si les performances ne répondent pas aux attentes en matière de configuration du chemin, vérifiez les statistiques de performances du nœud, utilisez les outils disponibles pour isoler le problème sur le réseau, vérifiez les paramètres du commutateur, etc.

## Gérer les charges de travail

### Identifiez les performances de capacité restante

La capacité de performance, ou *headroom*, mesure le volume de travail que vous pouvez placer sur un nœud ou un agrégat avant que les performances des charges de travail sur la ressource ne commencent à être affectées par la latence. Connaître la capacité en termes de performances disponible sur le cluster vous aide à provisionner et à équilibrer les charges de travail.

### Ce dont vous avez besoin

Des commandes de niveau de privilège avancé sont requises pour cette tâche.

### Description de la tâche

Vous pouvez utiliser les valeurs suivantes pour l' `-object` option pour collecter et afficher les statistiques de marge :

- Pour les CPU, `resource_headroom_cpu`.
- Pour les agrégats, `resource_headroom_aggr`.

Vous pouvez également effectuer cette tâche à l'aide de System Manager et de Active IQ Unified Manager.

### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Démarrer la collecte de statistiques de marge en temps réel :

```
statistics start -object resource_headroom_cpu|aggr
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

3. Afficher les informations statistiques relatives à la marge en temps réel :

```
statistics show -object resource_headroom_cpu|aggr
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

4. Revenir au privilège administratif :

```
set -privilege admin
```

### Exemple

L'exemple suivant affiche les statistiques moyennes sur la marge horaire des nœuds du cluster.

Vous pouvez calculer la capacité de performances disponible d'un nœud en soustrayant la `current_utilization` compteur du `optimal_point_utilization` compteur. Dans cet exemple, la capacité d'utilisation pour CPU\_sti2520-213 Est de -14% (72%-86%), ce qui suggère que le CPU a été surexploité en moyenne au cours de la dernière heure.

Vous avez peut-être spécifié `ewma_daily`, `ewma_weekly`, ou `ewma_monthly` pour obtenir la moyenne des mêmes informations sur des périodes plus longues.

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
(statistics show)
```

```
Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213
```

| Counter                         | Value |
|---------------------------------|-------|
| ewma_hourly                     | -     |
| current_ops                     | 4376  |
| current_latency                 | 37719 |
| current_utilization             | 86    |
| optimal_point_ops               | 2573  |
| optimal_point_latency           | 3589  |
| optimal_point_utilization       | 72    |
| optimal_point_confidence_factor | 1     |

```
Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214
```

| Counter                         | Value |
|---------------------------------|-------|
| ewma_hourly                     | -     |
| current_ops                     | 0     |
| current_latency                 | 0     |
| current_utilization             | 0     |
| optimal_point_ops               | 0     |
| optimal_point_latency           | 0     |
| optimal_point_utilization       | 71    |
| optimal_point_confidence_factor | 1     |

2 entries were displayed.

#### Identifiez les clients ou les fichiers à fort trafic

Vous pouvez utiliser la technologie Active Objects de ONTAP pour identifier les clients ou les fichiers responsables d'une quantité disproportionnée de trafic de grappe. Une fois

que vous avez identifié ces « principaux » clients ou fichiers, vous pouvez rééquilibrer les charges de travail du cluster ou prendre d'autres mesures pour résoudre le problème.

### Ce dont vous avez besoin

Vous devez être un administrateur de cluster pour effectuer cette tâche.

### Étapes

1. Afficher les principaux clients accédant au cluster :

```
statistics top client show -node node_name -sort-key sort_column -interval
seconds_between_updates -iterations iterations -max number_of_instances
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

La commande suivante affiche les principaux clients accédant à cluster1:

```
cluster1::> statistics top client show

cluster1 : 3/23/2016 17:59:10

 *Total
 Client Vserver Node Protocol Ops

```

|                |     |              |     |     |
|----------------|-----|--------------|-----|-----|
| 172.17.180.170 | vs4 | siderop1-vs4 | nfs | 668 |
| 172.17.180.169 | vs3 | siderop1-vs3 | nfs | 337 |
| 172.17.180.171 | vs3 | siderop1-vs3 | nfs | 142 |
| 172.17.180.170 | vs3 | siderop1-vs3 | nfs | 137 |
| 172.17.180.123 | vs3 | siderop1-vs3 | nfs | 137 |
| 172.17.180.171 | vs4 | siderop1-vs4 | nfs | 95  |
| 172.17.180.169 | vs4 | siderop1-vs4 | nfs | 92  |
| 172.17.180.123 | vs4 | siderop1-vs4 | nfs | 92  |
| 172.17.180.153 | vs3 | siderop1-vs3 | nfs | 0   |

2. Afficher les principaux fichiers auxquels a accédé sur le cluster :

```
statistics top file show -node node_name -sort-key sort_column -interval
seconds_between_updates -iterations iterations -max number_of_instances
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

La commande suivante affiche les principaux fichiers auxquels vous accédez cluster1:



```
cluster1::> statistics top file show
```

```
cluster1 : 3/23/2016 17:59:10
```

|                          |       |        | *Total       |       |       |
|--------------------------|-------|--------|--------------|-------|-------|
|                          | File  | Volume | Vserver      | Node  | Ops   |
| -----                    | ----- | -----  | -----        | ----- | ----- |
| /vol/vol1/vm170-read.dat | vol1  | vs4    | siderop1-vs4 | 22    |       |
| /vol/vol1/vm69-write.dat | vol1  | vs3    | siderop1-vs3 | 6     |       |
| /vol/vol2/vm171.dat      | vol2  | vs3    | siderop1-vs3 | 2     |       |
| /vol/vol2/vm169.dat      | vol2  | vs3    | siderop1-vs3 | 2     |       |
| /vol/vol2/p123.dat       | vol2  | vs4    | siderop1-vs4 | 2     |       |
| /vol/vol2/p123.dat       | vol2  | vs3    | siderop1-vs3 | 2     |       |
| /vol/vol1/vm171.dat      | vol1  | vs4    | siderop1-vs4 | 2     |       |
| /vol/vol1/vm169.dat      | vol1  | vs4    | siderop1-vs4 | 2     |       |
| /vol/vol1/vm169.dat      | vol1  | vs4    | siderop1-vs3 | 2     |       |
| /vol/vol1/p123.dat       | vol1  | vs4    | siderop1-vs4 | 2     |       |

## Débit garanti avec la QoS

### Débit garanti avec les QoS

Grâce à la qualité de service (QoS) du stockage, vous pouvez garantir que les performances des workloads stratégiques ne sont pas dégradées par des charges de travail concurrentes. Vous pouvez fixer un plafond de débit sur une charge de travail concurrente pour limiter son impact sur les ressources système, ou définir un débit *sol* pour une charge de travail critique, afin de garantir qu'il répond aux objectifs de débit minimum, indépendamment de la demande des charges de travail concurrentes. Vous pouvez même fixer un plafond et un sol pour la même charge de travail.

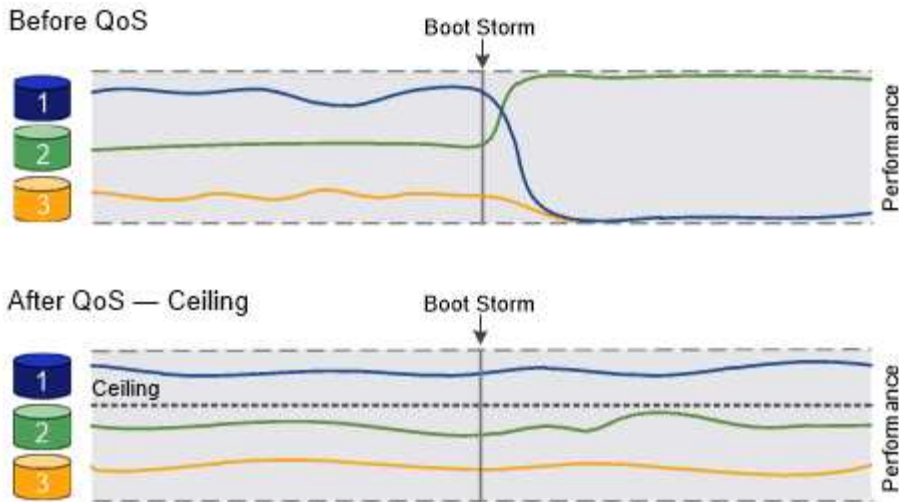
### À propos des plafonds de débit (QoS Max)

Le débit limite le débit pour une charge de travail jusqu'à un nombre maximal d'IOPS ou de Mbit/s, ainsi que les IOPS et les Mbit/s. Dans la figure ci-dessous, le plafond de débit pour la charge de travail 2 garantit qu'il ne « traite » pas les charges de travail 1 et 3.

Un *policy group* définit le plafond de débit pour une ou plusieurs charges de travail. Une charge de travail représente les opérations d'E/S d'un objet *stockage* : un volume, un fichier, qtree ou une LUN, ou l'ensemble des volumes, fichiers, qtrees ou LUN d'un SVM. Vous pouvez spécifier le plafond lorsque vous créez le groupe de règles ou attendre jusqu'à ce que vous contrôliez les charges de travail pour les spécifier.



Le débit des charges de travail peut dépasser jusqu'à 10 % le plafond défini, en particulier si le débit d'une charge de travail change rapidement. Le plafond peut être dépassé de 50 % pour gérer les rafales. Les rafales se produisent sur des nœuds uniques lorsque les jetons s'accumulent jusqu'à 150 %



### À propos du débit au sol (QoS min)

Un plancher de débit garantit que le débit d'une charge de travail ne passe pas en dessous d'un nombre minimal d'IOPS ou de Mo/sec, ou d'IOPS et de Mo/sec. Dans la figure ci-dessous, les niveaux de débit pour la charge de travail 1 et la charge de travail 3 s'assurent qu'ils répondent aux objectifs de débit minimum, indépendamment de la demande par charge de travail 2.



Comme le suggèrent les exemples, un plafond de débit accélère directement le débit. Un plancher de débit accélère indirectement le débit en donnant la priorité aux charges de travail pour lesquelles le sol a été défini.

Vous pouvez spécifier l'étage lors de la création du groupe de règles ou attendre jusqu'à ce que vous surveilliez les charges de travail pour le spécifier.

À partir de la version ONTAP 9.13.1, vous pouvez définir des étages de débit au niveau de l'étendue du SVM avec [\[adaptive-qos-templates\]](#). Dans les versions ONTAP antérieures à 9.13.1, un groupe de règles qui définit un plancher de débit ne peut pas être appliqué à une SVM.



Dans les versions antérieures à ONTAP 9.7, le débit est garanti lorsque la capacité de performance est suffisante.

Dans la ONTAP 9.7 et versions ultérieures, le débit au sol peut être garanti même en cas de capacité de performance insuffisante. Ce nouveau comportement de plancher s'appelle planchers v2. Pour respecter les garanties, au sol v2, peut offrir une plus grande latence sur les charges de travail sans débit ni travail dépassant les paramètres au sol. Au sol v2 s'applique à la QoS et à la qualité de service adaptative.

L'option d'activation/désactivation du nouveau comportement des étages v2 est disponible dans ONTAP 9.7P6 et versions ultérieures. Une charge de travail peut tomber sous le plancher spécifié pendant des opérations critiques comme `volume move trigger-cutover`. Même lorsque vous disposez d'une capacité suffisante et que vos opérations stratégiques n'ont pas lieu, le débit d'une charge de travail peut tomber en dessous du seuil spécifié de 5 %. Si les étages sont surprovisionnés et que la capacité de performance n'est pas disponible, certaines charges de travail peuvent tomber en dessous de l'étage spécifié.



## À propos des groupes de règles de qualité de service partagés et non partagés

À partir de ONTAP 9.4, vous pouvez utiliser un groupe de règles QoS *non-partagé* pour spécifier que le plafond ou le sol de débit défini s'applique à chaque charge de travail membre individuellement. Le comportement des groupes de règles *shared* dépend du type de stratégie :

- Pour les plafonds de débit, le débit total des charges de travail affectées au groupe de règles partagées ne peut dépasser le plafond spécifié.
- Pour les étages de débit, le groupe de règles partagées ne peut être appliqué qu'à une seule charge de travail.

## À propos de la QoS adaptative

En principe, la valeur du groupe de règles que vous attribuez à un objet de stockage est fixe. Vous devez modifier la valeur manuellement lorsque la taille de l'objet de stockage change. Une augmentation de l'espace utilisé sur un volume, par exemple, nécessite généralement une augmentation correspondante du plafond de débit spécifié pour le volume.

*Adaptive* QoS ajuste automatiquement la valeur du groupe de règles en fonction de la taille de la charge de travail, en maintenant le rapport IOPS/To|Go en fonction de la taille des modifications de la charge de travail. C'est un avantage significatif pour la gestion de centaines, voire de milliers de charges de travail dans un déploiement à grande échelle.

Généralement, vous utilisez la QoS adaptative pour ajuster les plafonds de débit, mais vous pouvez également l'utiliser pour gérer le débit (en cas d'augmentation de la taille des charges de travail). La taille du workload est exprimée en espace alloué à l'objet de stockage ou en espace utilisé par l'objet de stockage.



L'espace utilisé est disponible pour les étages de débit dans ONTAP 9.5 et versions ultérieures. Elle n'est pas prise en charge pour les étages de débit dans ONTAP 9.4 et les versions antérieures.

- Une politique *Allocated space* maintient le ratio IOPS/To|Go en fonction de la taille nominale de l'objet de stockage. Si le rapport est de 100 IOPS/Go, un volume de 150 Go plafonné à 15,000 IOPS, tant que la taille du volume reste celle-ci. Si le volume a été redimensionné de façon à 300 Go, la QoS adaptative ajuste le débit au plafond à 30,000 000 IOPS.
- Une règle *Used space* (par défaut) maintient le ratio IOPS/To|Go en fonction de la quantité de données réelles stockées avant le stockage efficace. Si le rapport est de 100 IOPS/Go, un volume de 150 Go contenant 100 Go de données stockées aurait un débit plafond de 10,000 000 IOPS. À mesure que la

quantité d'espace utilisée change, la QoS adaptative ajuste le plafond de débit en fonction du rapport.

Depuis ONTAP 9.5, vous pouvez spécifier une taille de bloc d'E/S pour votre application afin d'indiquer une limite de débit en IOPS et en Mbit/s. La limite de Mbit/s est calculée à partir de la taille de bloc multipliée par la limite d'IOPS. Par exemple, une taille de bloc d'E/S de 32 Ko pour une limite d'IOPS de 6144 IOPS/To permet d'obtenir une limite de 192 Mbit/s en Mbit/s.

Vous pouvez vous attendre à ce que le comportement suivant soit à la fois pour les plafonds de rendement et pour les planchers :

- Lorsqu'une charge de travail est affectée à un groupe de règles QoS adaptative, le plafond ou le sol est immédiatement mis à jour.
- Lorsqu'une charge de travail d'un groupe de règles de QoS adaptative est redimensionnée, la limite ou le sol est mis à jour en cinq minutes environ.

Le débit doit augmenter d'au moins 10 000 IOPS avant la mise à jour.

Les groupes de règles de QoS adaptative sont toujours non partagés : le plafond ou l'étage de débit défini s'applique à chaque charge de travail membre individuellement.

À partir de la version ONTAP 9.6, les niveaux de débit sont pris en charge par ONTAP Select Premium avec SSD.

### Modèle de groupe de règles adaptatif

À partir de la version ONTAP 9.13.1, vous pouvez définir un modèle de QoS adaptative sur une SVM. Les modèles de groupes de règles adaptatifs vous permettent de définir des seuils et des plafonds de débit pour tous les volumes d'une SVM.

Les modèles de groupes de règles adaptatives ne peuvent être définis qu'après la création du SVM. Utilisez le `vserver modify` commande avec `-qos-adaptive-policy-group-template` paramètre permettant de définir la règle.

Lorsque vous définissez un modèle de groupe de règles adaptatives, les volumes créés ou migrés après avoir défini la règle héritent automatiquement de la règle. L'affectation du modèle de règle n'a aucun impact sur les volumes existants du SVM. Si vous désactivez la policy sur le SVM, tout volume ultérieurement migré vers ou créé sur le SVM ne recevra pas la policy. La désactivation du modèle de groupe de règles adaptatives n'a pas d'impact sur les volumes qui ont hérité du modèle de règles car ils conservent le modèle de règles.

Pour plus d'informations, voir [Définissez un modèle de groupe de règles adaptatives](#).

### Assistance générale

Le tableau ci-dessous présente les différences en matière de prise en charge des plafonds de débit, des étages de débit et de la QoS adaptative.

| Ressource ou fonctionnalité | Plafond de débit | Plancher de débit           | Débit au sol v2             | La QoS adaptative           |
|-----------------------------|------------------|-----------------------------|-----------------------------|-----------------------------|
| Version ONTAP 9             | Tout             | 9.2 et versions ultérieures | 9.7 et versions ultérieures | 9.3 et versions ultérieures |

| Ressource ou fonctionnalité | Plafond de débit | Plancher de débit                                                                                                    | Débit au sol v2                                                                                                  | La QoS adaptative |
|-----------------------------|------------------|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|-------------------|
| Plateformes                 | Tout             | <ul style="list-style-type: none"> <li>• AFF</li> <li>• C190 *</li> <li>• ONTAP Select Premium avec SSD *</li> </ul> | <ul style="list-style-type: none"> <li>• AFF</li> <li>• C190</li> <li>• ONTAP Select Premium avec SSD</li> </ul> | Tout              |
| Protocoles                  | Tout             | Tout                                                                                                                 | Tout                                                                                                             | Tout              |
| FabricPool                  | Oui.             | Oui, si la règle de Tiering est définie sur « none » et si aucun bloc n'est dans le cloud.                           | Oui, si la règle de Tiering est définie sur « none » et si aucun bloc n'est dans le cloud.                       | Non               |
| SnapMirror synchrone        | Oui.             | Non                                                                                                                  | Non                                                                                                              | Oui.              |

La prise en charge des baies ONTAP Select et C190 a débuté avec la version ONTAP 9.6.

### Charges de travail prises en charge pour les plafonds de débit

Le tableau ci-dessous présente la prise en charge des charges de travail pour les plafonds de débit dans la version ONTAP 9. Les volumes root, les miroirs de partage de charge et les miroirs de protection des données ne sont pas pris en charge.

| Support de charge de travail - plafond | ONTAP 9.0 | ONTAP 9.1 | ONTAP 9.2 | ONTAP 9.3 | ONTAP 9.4 - 9.7 | ONTAP 9.8 et versions ultérieures |
|----------------------------------------|-----------|-----------|-----------|-----------|-----------------|-----------------------------------|
| Volumétrie                             | oui       | oui       | oui       | oui       | oui             | oui                               |
| Fichier                                | oui       | oui       | oui       | oui       | oui             | oui                               |
| LUN                                    | oui       | oui       | oui       | oui       | oui             | oui                               |
| SVM                                    | oui       | oui       | oui       | oui       | oui             | oui                               |
| Volume FlexGroup                       | non       | non       | non       | oui       | oui             | oui                               |
| qtrees*                                | non       | non       | non       | non       | non             | oui                               |

| <b>Support de charge de travail - plafond</b>     | <b>ONTAP 9.0</b> | <b>ONTAP 9.1</b> | <b>ONTAP 9.2</b> | <b>ONTAP 9.3</b> | <b>ONTAP 9.4 - 9.7</b> | <b>ONTAP 9.8 et versions ultérieures</b> |
|---------------------------------------------------|------------------|------------------|------------------|------------------|------------------------|------------------------------------------|
| Plusieurs charges de travail par groupe de règles | oui              | oui              | oui              | oui              | oui                    | oui                                      |
| Groupes de stratégies non partagés                | non              | non              | non              | non              | oui                    | oui                                      |

Depuis la version ONTAP 9.8, l'accès NFS est pris en charge dans les qtrees des volumes FlexVol et FlexGroup sur lesquels NFS est activé. Depuis la version ONTAP 9.9.1, l'accès SMB est également pris en charge dans les qtrees des volumes FlexVol et FlexGroup sur lesquels SMB est activé.

### Charges de travail prises en charge pour le débit au sol

Le tableau ci-dessous présente la prise en charge des charges de travail pour les débits par la version ONTAP 9. Les volumes root, les miroirs de partage de charge et les miroirs de protection des données ne sont pas pris en charge.

| <b>Soutien de la charge de travail - plancher</b> | <b>ONTAP 9.2</b> | <b>ONTAP 9.3</b> | <b>ONTAP 9.4 - 9.7</b> | <b>ONTAP 9.8 - 9.13.0</b> | <b>ONTAP 9.13.1 et versions ultérieures</b> |
|---------------------------------------------------|------------------|------------------|------------------------|---------------------------|---------------------------------------------|
| Volumétrie                                        | oui              | oui              | oui                    | oui                       | oui                                         |
| Fichier                                           | non              | oui              | oui                    | oui                       | oui                                         |
| LUN                                               | oui              | oui              | oui                    | oui                       | oui                                         |
| SVM                                               | non              | non              | non                    | non                       | oui                                         |
| Volume FlexGroup                                  | non              | non              | oui                    | oui                       | oui                                         |
| qtrees *                                          | non              | non              | non                    | oui                       | oui                                         |
| Plusieurs charges de travail par groupe de règles | non              | non              | oui                    | oui                       | oui                                         |
| Groupes de stratégies non partagés                | non              | non              | oui                    | oui                       | oui                                         |

\*à partir de ONTAP 9.8, l'accès NFS est pris en charge dans les qtrees des volumes FlexVol et FlexGroup sur lesquels NFS est activé. Depuis la version ONTAP 9.9.1, l'accès SMB est également pris en charge dans les qtrees des volumes FlexVol et FlexGroup sur lesquels SMB est activé.

## Prise en charge de workloads pour la QoS adaptative

Le tableau ci-dessous présente la prise en charge des workloads pour la QoS adaptative par la version ONTAP 9. Les volumes root, les miroirs de partage de charge et les miroirs de protection des données ne sont pas pris en charge.

| Prise en charge des workloads : QoS adaptative    | ONTAP 9.3 | ONTAP 9.4 - 9.13.0 | ONTAP 9.13.1 et versions ultérieures |
|---------------------------------------------------|-----------|--------------------|--------------------------------------|
| Volumétrie                                        | oui       | oui                | oui                                  |
| Fichier                                           | non       | oui                | oui                                  |
| LUN                                               | non       | oui                | oui                                  |
| SVM                                               | non       | non                | oui                                  |
| Volume FlexGroup                                  | non       | oui                | oui                                  |
| Plusieurs charges de travail par groupe de règles | oui       | oui                | oui                                  |
| Groupes de stratégies non partagés                | oui       | oui                | oui                                  |

## Nombre maximal de charges de travail et de groupes de règles

Le tableau ci-dessous indique le nombre maximal de charges de travail et de groupes de règles par la version ONTAP 9.

| Prise en charge des workloads            | ONTAP 9.3 et versions antérieures | ONTAP 9.4 et versions ultérieures |
|------------------------------------------|-----------------------------------|-----------------------------------|
| Charges de travail maximales par cluster | 12,000                            | 40,000                            |
| Nombre maximal de workloads par nœud     | 12,000                            | 40,000                            |
| Nombre maximal de stratégies groupes     | 12,000                            | 12,000                            |

## Activer ou désactiver le débit planchers v2

Vous pouvez activer ou désactiver le débit planchers v2 sur AFF. La valeur par défaut est activée. Lorsque la technologie planchers v2 est activée, le débit au sol peut être atteint lorsque les contrôleurs sont utilisés de façon intensive, au détriment d'une latence plus élevée sur d'autres charges de travail. Au niveau de la QoS et de la QoS adaptative.

### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Entrez l'une des commandes suivantes :

| Les fonctions que vous recherchez... | Utilisez cette commande :                                    |
|--------------------------------------|--------------------------------------------------------------|
| Désactiver les étages v2             | <code>qos settings throughput-floors-v2 -enable false</code> |
| Activation de la version 2           | <code>qos settings throughput-floors-v2 -enable true</code>  |



Pour désactiver le débit planchers v2 dans un cluster MetroCluster, vous devez exécuter le

```
qos settings throughput-floors-v2 -enable false
```

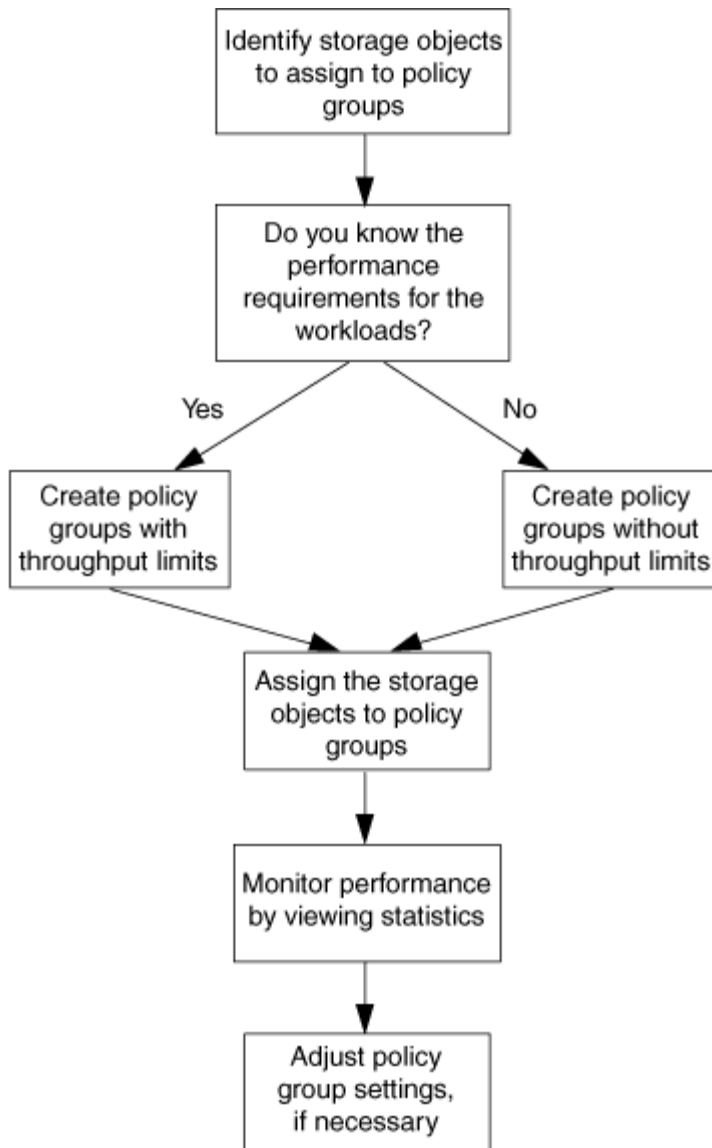
contrôlez à la fois les clusters source et de destination.

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

### Flux de travail de QoS du stockage

Si vous connaissez déjà les exigences de performance des workloads que vous souhaitez gérer avec QoS, vous pouvez définir la limite de débit lors de la création du groupe de règles. Sinon, vous pouvez attendre jusqu'à ce que vous contrôlons les charges de travail pour spécifier la limite.





### Fixer un plafond de débit avec la QoS

Vous pouvez utiliser le `max-throughput` Champ permettant à un groupe de règles de définir une limite de débit pour les workloads d'objets de stockage (QoS max). Vous pouvez appliquer le groupe de règles lors de la création ou de la modification de l'objet de stockage.

#### Ce dont vous avez besoin

- Pour créer une « policy group » il faut être un administrateur de cluster.
- Vous devez être un administrateur de cluster pour appliquer une « policy group » à un SVM.

#### Description de la tâche

- Depuis ONTAP 9.4, vous pouvez utiliser un groupe de règles QoS *non-partagé* pour spécifier que le plafond de débit défini s'applique à chaque charge de travail membre individuellement. Sinon, le groupe de règles est *Shared*: le débit total des charges de travail affectées au groupe de règles ne peut pas dépasser le plafond spécifié.

Réglez `-is-shared=false` pour le `qos policy-group create` commande permettant de spécifier

un groupe de polices non partagé.

- Vous pouvez spécifier la limite de débit pour le plafond en IOPS, Mo/s ou IOPS, Mo/s. Si vous spécifiez les IOPS et Mo/s, la première limite atteinte est appliquée.



Si vous définissez une limite et un sol pour la même charge de travail, vous pouvez spécifier la limite de débit pour le plafond des IOPS uniquement.

- Un objet de stockage faisant l'objet d'une limite QoS doit être contenu par le SVM auquel appartient le groupe de règles. Plusieurs « policy group » peuvent appartenir à la même SVM.
- Vous ne pouvez pas affecter un objet de stockage à un groupe de règles si son objet contenant ou ses objets enfants appartiennent à ce groupe.
- Il s'agit d'une meilleure pratique de QoS pour appliquer un groupe de règles au même type d'objets de stockage.

## Étapes

### 1. Création d'une « policy group » :

```
qos policy-group create -policy-group policy_group -vserver SVM -max
-throughput number_of_iops|Mb/S|iops,Mb/S -is-shared true|false
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man. Vous pouvez utiliser le `qos policy-group modify` commande permettant d'ajuster les plafonds de débit.

La commande suivante crée la « policy group » partagée `pg-vs1` Avec un débit maximum de 5,000 000 IOPS :

```
cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1
-max-throughput 5000iops -is-shared true
```

La commande suivante crée le « policy group » non partagé `pg-vs3` Avec un débit maximum de 100 400 IOPS et 80 Ko/S :

```
cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
-max-throughput 100iops,400KB/s -is-shared false
```

La commande suivante crée le « policy group » non partagé `pg-vs4` sans limite de débit :

```
cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4
-is-shared false
```

### 2. Appliquer une « policy group » à un SVM, fichier, volume ou LUN :

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels. Vous pouvez utiliser le `storage_object modify` commande pour appliquer un autre groupe de règles à l'objet de

stockage.

La commande suivante applique la « policy group » pg-vs1 À la SVM vs1:

```
cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
```

Les commandes suivantes appliquent la « policy group » pg-app aux volumes app1 et app2:

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app
```

### 3. Surveillance des performances des groupes de règles :

```
qos statistics performance show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Contrôle des performances depuis le cluster. N'utilisez pas d'outil sur l'hôte pour surveiller les performances.

La commande suivante affiche les performances de « policy group » :

```
cluster1::> qos statistics performance show
```

| Policy Group        | IOPS  | Throughput | Latency   |
|---------------------|-------|------------|-----------|
| -total-             | 12316 | 47.76MB/s  | 1264.00us |
| pg_vs1              | 5008  | 19.56MB/s  | 2.45ms    |
| _System-Best-Effort | 62    | 13.36KB/s  | 4.13ms    |
| _System-Background  | 30    | 0KB/s      | 0ms       |

### 4. Contrôle de la performance des charges de travail :

```
qos statistics workload performance show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Contrôle des performances depuis le cluster. N'utilisez pas d'outil sur l'hôte pour surveiller les performances.

La commande suivante indique les performances des workloads :

```
cluster1::> qos statistics workload performance show
```

| Workload        | ID    | IOPS  | Throughput | Latency   |
|-----------------|-------|-------|------------|-----------|
| -total-         | -     | 12320 | 47.84MB/s  | 1215.00us |
| app1-wid7967    | 7967  | 7219  | 28.20MB/s  | 319.00us  |
| vs1-wid12279    | 12279 | 5026  | 19.63MB/s  | 2.52ms    |
| _USERSPACE_APPS | 14    | 55    | 10.92KB/s  | 236.00us  |
| _Scan_Backgro.. | 5688  | 20    | 0KB/s      | 0ms       |



Vous pouvez utiliser le `qos statistics workload latency show` Commande pour afficher les statistiques de latence détaillées pour les workloads de QoS.

## Définissez un seuil de débit avec la QoS

Vous pouvez utiliser le `min-throughput` Champ permettant à un groupe de règles de définir un étage de débit pour les workloads d'objets de stockage (QoS min). Vous pouvez appliquer le groupe de règles lors de la création ou de la modification de l'objet de stockage. Depuis la version ONTAP 9.8, vous pouvez spécifier le seuil de débit en IOPS ou Mbit/s, ou IOPS et Mbit/s.

### Avant de commencer

- Vous devez exécuter ONTAP 9.2 ou version ultérieure. Les étages de débit sont disponibles à partir de ONTAP 9.2.
- Pour créer une « policy group » il faut être un administrateur de cluster.
- À partir de la version ONTAP 9.13.1, vous pouvez appliquer des planchers de débit au niveau de la SVM en utilisant une [modèle de groupe de règles adaptatif](#). Vous ne pouvez pas définir de modèle de « policy group » adaptatif sur une SVM disposant d'une « policy group » QoS.

### Description de la tâche

- Depuis ONTAP 9.4, vous pouvez utiliser un groupe de règles QoS *non-partagé* pour spécifier que le niveau de débit défini soit appliqué individuellement à chaque charge de travail membre. C'est la seule condition dans laquelle un groupe de règles pour un étage de débit peut être appliqué à plusieurs charges de travail.

Réglez `-is-shared=false` pour le `qos policy-group create` commande permettant de spécifier une « policy group » non partagée.

- Le débit d'une charge de travail peut tomber en dessous du seuil spécifié si la capacité de performance est insuffisante (marge) sur le nœud ou l'agrégat.
- Un objet de stockage faisant l'objet d'une limite QoS doit être contenu par le SVM auquel appartient le groupe de règles. Plusieurs « policy group » peuvent appartenir à la même SVM.
- Il s'agit d'une meilleure pratique de QoS pour appliquer un groupe de règles au même type d'objets de stockage.
- Un groupe de règles qui définit un étage de débit ne peut pas être appliqué à un SVM.

### Étapes

1. Vérifier que la capacité de performance sur le nœud ou l'agrégat est appropriée, comme décrit dans

"Identification de la capacité de performance restante".

## 2. Création d'une « policy group » :

```
qos policy-group create -policy group policy_group -vserver SVM -min
-throughput qos_target -is-shared true|false
```

Pour connaître la syntaxe complète de la commande, consultez la page man de votre version de ONTAP. Vous pouvez utiliser le `qos policy-group modify` commande permettant de régler les étages de débit.

La commande suivante crée la « policy group » partagée `pg-vs2` Avec un débit minimal de 1,000 000 IOPS :

```
cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2
-min-throughput 1000iops -is-shared true
```

La commande suivante crée le « policy group » non partagé `pg-vs4` sans limite de débit :

```
cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4
-is-shared false
```

## 3. Appliquer une « policy group » à un volume ou une LUN :

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels. Vous pouvez utiliser le `_storage_object_modify` commande pour appliquer un autre groupe de règles à l'objet de stockage.

La commande suivante applique la « policy group » `pg-app2` au volume `app2`:

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app2
```

## 4. Surveillance des performances des groupes de règles :

```
qos statistics performance show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



Contrôle des performances depuis le cluster. N'utilisez pas d'outil sur l'hôte pour surveiller les performances.

La commande suivante affiche les performances de « policy group » :

```
cluster1::> qos statistics performance show
```

| Policy Group        | IOPS  | Throughput | Latency   |
|---------------------|-------|------------|-----------|
| -total-             | 12316 | 47.76MB/s  | 1264.00us |
| pg_app2             | 7216  | 28.19MB/s  | 420.00us  |
| _System-Best-Effort | 62    | 13.36KB/s  | 4.13ms    |
| _System-Background  | 30    | 0KB/s      | 0ms       |

## 5. Contrôle de la performance des charges de travail :

```
qos statistics workload performance show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page [man](#).



Contrôle des performances depuis le cluster. N'utilisez pas d'outil sur l'hôte pour surveiller les performances.

La commande suivante indique les performances des workloads :

```
cluster1::> qos statistics workload performance show
```

| Workload        | ID    | IOPS  | Throughput | Latency   |
|-----------------|-------|-------|------------|-----------|
| -total-         | -     | 12320 | 47.84MB/s  | 1215.00us |
| app2-wid7967    | 7967  | 7219  | 28.20MB/s  | 319.00us  |
| vs1-wid12279    | 12279 | 5026  | 19.63MB/s  | 2.52ms    |
| _USERSPACE_APPS | 14    | 55    | 10.92KB/s  | 236.00us  |
| _Scan_Backgro.. | 5688  | 20    | 0KB/s      | 0ms       |



Vous pouvez utiliser le `qos statistics workload latency show` Commande pour afficher les statistiques de latence détaillées pour les workloads de QoS.

## Utilisez les groupes de règles de QoS adaptatifs

Vous pouvez utiliser un groupe de règles *Adaptive QoS* pour dimensionner automatiquement un plafond de débit ou une taille de sol en fonction du volume, tout en maintenant le rapport IOPS/To|GBs lorsque la taille du volume change. C'est un avantage significatif pour la gestion de centaines, voire de milliers de charges de travail dans un déploiement à grande échelle.

### Avant de commencer

- Vous devez exécuter ONTAP 9.3 ou une version ultérieure. Les groupes de règles de QoS adaptative sont disponibles à partir de la version ONTAP 9.3.
- Pour créer une « policy group » il faut être un administrateur de cluster.

### Description de la tâche

Un objet de stockage peut être membre d'un groupe de règles adaptative ou d'un groupe de règles non adaptatif, mais pas des deux à la fois. Le SVM de l'objet de stockage et la politique doivent être identiques. L'objet de stockage doit être en ligne.

Les groupes de règles de QoS adaptative sont toujours non partagés : le plafond ou l'étage de débit défini s'applique à chaque charge de travail membre individuellement.

Le rapport entre les limites de débit et la taille de l'objet de stockage est déterminé par l'interaction des champs suivants :

- `expected-iops` Correspond au nombre minimal d'IOPS prévu par To|Go alloué.



``expected-iops`` Est garanti uniquement sur les plateformes AFF. ``expected-iops`` La garantie FabricPool s'applique uniquement si la règle de Tiering est définie sur « aucun » et qu'aucun bloc n'est dans le cloud. ``expected-iops`` Est garanti pour les volumes qui ne font pas partie d'une relation synchrone SnapMirror.

- `peak-iops` Est le nombre maximal d'IOPS possible par To alloué ou utilisé|Go.
- `expected-iops-allocation` indique si l'espace alloué (par défaut) ou utilisé est utilisé pour les iops attendues.



`expected-iops-allocation` Est disponible dans ONTAP 9.5 et versions ultérieures. Elle n'est pas prise en charge par ONTAP 9.4 et les versions antérieures.

- `peak-iops-allocation` indique si l'espace alloué ou l'espace utilisé (par défaut) est utilisé pour `peak-iops`.
- `absolute-min-iops` Correspond au nombre minimal d'IOPS absolu. Vous pouvez utiliser ce champ avec de très petits objets de stockage. Elle remplace les deux `peak-iops` et/ou `expected-iops` quand `absolute-min-iops` est supérieur au calcul `expected-iops`.

Par exemple, si vous définissez `expected-iops` À 1,000 000 IOPS/To et la taille du volume est inférieure à 1 Go, le calcul est effectué `expected-iops` Il s'agit d'une IOP fractionnaires. Le calculé `peak-iops` sera une fraction encore plus petite. Vous pouvez éviter cela en définissant le paramètre `absolute-min-iops` à une valeur réaliste.

- `block-size` Spécifie la taille du bloc d'E/S de l'application. La valeur par défaut est 32 Ko. Les valeurs valides sont de 8 Ko, 16 Ko, 32 K, 64 Ko, N'IMPORTE QUEL. TOUTE signifie que la taille de bloc n'est pas appliquée.

Trois groupes de règles de QoS adaptative par défaut sont disponibles, comme illustré dans le tableau ci-dessous. Vous pouvez appliquer ces « policy group » directement à un volume.

| Groupe de règles par défaut | IOPS/To attendu | Pic d'IOPS/To | IOPS min. Absolu |
|-----------------------------|-----------------|---------------|------------------|
| extreme                     | 6,144           | 12,288        | 1000             |

|             |       |       |     |
|-------------|-------|-------|-----|
| performance | 2,048 | 4,096 | 500 |
| value       | 128   | 512   | 75  |

Vous ne pouvez pas affecter un objet de stockage à un groupe de règles si son objet contenant ou ses objets enfants appartiennent à un groupe de règles. Le tableau suivant répertorie les restrictions.

| Si vous attribuez...              | Vous ne pouvez alors pas affecter...                                    |
|-----------------------------------|-------------------------------------------------------------------------|
| SVM vers une « policy group »     | Tout objet de stockage contenu par la SVM vers une « policy group »     |
| Volume vers une « policy group »  | Le volume contenant un SVM ou toute LUN enfant vers un « policy group » |
| LUN vers une « policy group »     | La LUN contenant le volume ou le SVM à une « policy group »             |
| Fichier dans une « policy group » | Fichier contenant le volume ou SVM vers une « policy group »            |

## Étapes

### 1. Création d'une « policy group » QoS adaptative :

```
qos adaptive-policy-group create -policy group policy_group -vserver SVM
-expected-iops number_of_iops/TB|GB -peak-iops number_of_iops/TB|GB -expected
-iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-
space -absolute-min-iops number_of_iops -block-size 8K|16K|32K|64K|ANY
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.



-expected-iops-allocation et -block-size Est disponible dans ONTAP 9.5 et versions ultérieures. Ces options ne sont pas prises en charge par ONTAP 9.4 et les versions antérieures.

La commande suivante crée une « policy group » QoS adaptative *adpg-appl* avec -expected-iops Défini sur 300 IOPS/To, -peak-iops Définis sur 1,000 IOPS/To, -peak-iops-allocation réglez sur used-space, et -absolute-min-iops Définissez sur 50 IOPS :

```
cluster1::> qos adaptive-policy-group create -policy group adpg-appl
-vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
-allocation used-space -absolute-min-iops 50iops
```

### 2. Appliquer une « policy group » QoS adaptative à un volume :

```
volume create -vserver SVM -volume volume -aggregate aggregate -size number_of
TB|GB -qos-adaptive-policy-group policy_group
```



Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

La commande suivante applique la « policy group » de QoS adaptative `adpg-app1` au volume `app1`:

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

Les commandes suivantes appliquent le groupe de règles de QoS adaptative par défaut `extreme` au nouveau volume `app4` et au volume existant `app5`. Le plafond de débit défini pour le groupe de règles s'applique aux volumes `app4` et `app5` chaque participant :

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

## Définissez un modèle de groupe de règles adaptatives

À partir de la ONTAP 9.13.1, vous pouvez appliquer des seuils et des plafonds de débit au niveau des SVM en utilisant un modèle de groupe de règles adaptatif.

### Description de la tâche

- Le modèle de groupe de règles adaptatives est une règle par défaut `apg1`. La règle peut être modifiée à tout moment. Elle peut uniquement être définie avec l'interface de ligne de commandes ou l'API REST de ONTAP et s'applique uniquement aux SVM existants.
- Le modèle de groupe de règles adaptatives n'a d'impact que sur les volumes créés sur le SVM ou migrés vers celui-ci une fois la règle définie. Les volumes existants de la SVM conservent leur état existant.

Si vous désactivez le modèle de « Adaptive policy group », les volumes de la SVM conservent leurs règles existantes. Seuls les volumes créés ou migrés vers le SVM seront affectés par l'interruption.

- Vous ne pouvez pas définir de modèle de « policy group » adaptatif sur une SVM disposant d'une « policy group » QoS.
- Les modèles de groupes de règles adaptatifs sont conçus pour les plateformes AFF. Un modèle de groupe de règles adaptatives peut être défini sur d'autres plates-formes, mais la stratégie peut ne pas imposer un débit minimal. De la même manière, vous pouvez ajouter un modèle de groupe de règles adaptatives à un SVM dans un agrégat FabricPool ou dans un agrégat ne prenant pas en charge un débit minimal ; cependant, le seuil de débit ne sera pas appliqué.
- Si le SVM se trouve dans une configuration MetroCluster ou une relation SnapMirror, le modèle de groupe de règles adaptatives sera appliqué sur le SVM en miroir.

### Étapes

1. Modifier le SVM pour appliquer le modèle Adaptive policy group :  
`vserver modify -qos-adaptive-policy-group-template apg1`

2. Vérifiez que la règle a été définie :

```
vserver show -fields qos-adaptive-policy-group
```

## Surveillez les performances des clusters avec Unified Manager

Avec Active IQ Unified Manager, vous optimisez la disponibilité et gardez le contrôle de votre infrastructure de stockage NetApp AFF et FAS pour améliorer l'évolutivité, la prise en charge, les performances et la sécurité.

Active IQ Unified Manager surveille en permanence l'état du système et envoie des alertes pour permettre à votre entreprise de libérer des ressources IT. Vous pouvez consulter les informations sur l'état du stockage à partir d'un seul tableau de bord et résoudre rapidement les problèmes à l'aide d'actions recommandées.

La gestion des données est simplifiée grâce aux fonctionnalités de détection, de contrôle et de notification vous permettant de gérer le stockage de manière proactive et de résoudre rapidement les problèmes. L'administration est plus efficace, car elle permet de surveiller plusieurs pétaoctets de données à partir d'un même tableau de bord et de gérer vos données à grande échelle.

Grâce à Active IQ Unified Manager, vous pouvez vous adapter à l'évolution des besoins de votre business tout en optimisant les performances à l'aide des données de performance et des fonctionnalités d'analytique avancée. Les fonctionnalités de création de rapports vous permettent d'accéder à des rapports standard ou de créer des rapports opérationnels personnalisés afin de répondre aux besoins spécifiques de votre entreprise.

Liens connexes :

- ["En savoir plus sur Active IQ Unified Manager"](#)
- ["Lancez-vous avec Active IQ Unified Manager"](#)
- ["Découvrez Active IQ Unified Manager pour Linux"](#)
- ["Lancez-vous avec Active IQ Unified Manager pour Windows"](#)

## Contrôle des performances du cluster avec Cloud Insights

NetApp Cloud Insights est un outil de surveillance qui permet d'avoir une grande visibilité sur l'ensemble de l'infrastructure. Avec Cloud Insights, vous pouvez surveiller toutes les ressources, les optimiser et résoudre les problèmes, y compris dans les clouds publics et dans vos data centers privés.

### Cloud Insights est disponible en deux éditions

La version de base de Cloud Insights a été spécialement conçue pour contrôler et optimiser les ressources NetApp Data Fabric. Ce logiciel assure une analytique avancée pour établir des connexions entre toutes les ressources NetApp, y compris les systèmes FAS AFF et HCI dans l'environnement.

L'édition Standard de Cloud Insights est axée non seulement sur les composants d'infrastructure NetApp Data Fabric, mais aussi sur les environnements multifournisseurs et multicloud. Grâce à ses fonctionnalités enrichies, vous pouvez accéder à plus de 100 services et ressources.

Dans le monde actuel, avec des ressources en jeu entre vos data centers sur site et plusieurs clouds publics, il est essentiel d'avoir une vue d'ensemble de l'application elle-même et du disque interne de la baie de

stockage. La prise en charge supplémentaire de la surveillance des applications (comme Kafka, MongoDB et Nginx) vous fournit les informations et les connaissances nécessaires pour fonctionner au niveau optimal d'utilisation ainsi qu'avec le tampon à risques idéal.

Ces deux éditions (de base et standard) peuvent s'intégrer avec NetApp Active IQ Unified Manager. Les clients qui utilisent Active IQ Unified Manager peuvent voir les informations de jointure dans l'interface utilisateur de Cloud Insights. Les notifications publiées sur Active IQ Unified Manager ne sont pas négligées et peuvent être corrélées aux événements dans Cloud Insights. En d'autres termes, vous bénéficiez du meilleur des deux mondes.

## **Surveillance, dépannage et optimisation de toutes vos ressources**

Cloud Insights vous aide à réduire considérablement le délai de résolution des problèmes et à éviter qu'ils n'impactent les utilisateurs finaux. Mais les coûts de l'infrastructure cloud sont également réduits. L'exposition aux menaces internes est réduite en protégeant les données à l'aide d'informations exploitables.

Avec Cloud Insights, vous disposez d'une visibilité complète sur l'ensemble de votre infrastructure hybride à un seul emplacement, du cloud public à votre data Center. Vous pouvez créer instantanément des tableaux de bord pertinents qui peuvent être personnalisés en fonction de vos besoins spécifiques. Vous pouvez également créer des alertes ciblées et conditionnelles spécifiques aux besoins de votre entreprise.

La détection avancée des anomalies vous aide à résoudre les problèmes de manière préventive et proactive. Vous pouvez visualiser automatiquement les conflits et la dégradation des ressources pour restaurer rapidement les workloads impactés. La résolution des problèmes est plus rapide grâce à la hiérarchisation automatique des relations entre les différents composants de votre pile.

Vous pouvez identifier les ressources inutilisées ou orphelines dans votre environnement. Elles vous indiquent comment dimensionner correctement votre infrastructure et optimiser toutes vos dépenses.

Cloud Insights visualise votre topologie système pour mieux comprendre l'architecture Kubernetes. Vous pouvez contrôler l'état des clusters Kubernetes, y compris les nœuds susceptibles de rencontrer des problèmes, puis zoomer en cas de problème.

Cloud Insights vous aide à protéger les données de l'entreprise contre les activités abusives ou les usurpations d'identité à l'aide de fonctionnalités avancées de machine learning et de détection des anomalies qui vous fournissent des informations exploitables sur les menaces internes.

Cloud Insights vous aide à visualiser les metrics Kubernetes de façon à comprendre pleinement les relations entre vos pods, vos nœuds et vos clusters. Vous pouvez évaluer l'état d'un cluster ou d'un module de travail, ainsi que la charge en cours de traitement, ce qui vous permet de prendre le contrôle de votre cluster K8S et de contrôler à la fois l'état de santé et le coût de votre déploiement.

### **Liens connexes**

- ["En savoir plus sur Cloud Insights"](#)
- ["Lancez-vous avec Cloud Insights"](#)

## **Consignation des audits**

### **Mise en œuvre de la journalisation des audits par ONTAP**

Les activités de gestion enregistrées dans le journal d'audit sont incluses dans les rapports AutoSupport standard et certaines activités de consignation sont incluses dans

les messages EMS. Vous pouvez également transférer le journal d'audit aux destinations que vous spécifiez et afficher les fichiers journaux d'audit à l'aide de l'interface de ligne de commande ou d'un navigateur Web.

Depuis ONTAP 9.11.1, vous pouvez afficher le contenu des journaux d'audit à l'aide de System Manager.

Depuis ONTAP 9.12.1, ONTAP fournit des alertes de falsification pour les journaux d'audit. ONTAP exécute une tâche d'arrière-plan quotidienne pour vérifier l'altération des fichiers `audit.log` et envoie une alerte EMS s'il trouve des fichiers journaux qui ont été modifiés ou falsifiés.

ONTAP consigne les activités de gestion qui sont effectuées sur le cluster, par exemple la requête émise, l'utilisateur qui a déclenché la demande, la méthode d'accès de l'utilisateur et l'heure de la demande.

Les activités de gestion peuvent être de l'un des types suivants :

- DÉFINIR LES demandes, qui s'appliquent généralement aux commandes ou opérations non affichées :
  - Ces demandes sont émises lorsque vous exécutez un `create`, `modify`, ou `delete` commande, par exemple.
  - Les demandes de série sont consignées par défaut.
- OBTENEZ des demandes, qui récupèrent les informations et les affichent dans l'interface de gestion :
  - Ces demandes sont émises lorsque vous exécutez un `show` commande, par exemple.
  - Les demandes GET ne sont pas consignées par défaut, mais vous pouvez contrôler si LES demandes GET sont envoyées depuis l'interface de ligne de commande ONTAP (`-cliget`), à partir de l'API ONTAP (`-ontapiget`), ou à partir de l'API REST (`-httpget`) sont consignés dans le fichier.

ONTAP enregistre les activités de gestion dans `/mroot/etc/log/mlog/audit.log` fichier d'un nœud. Les commandes des trois shells pour les commandes CLI—le clustershell, le nodeshell et le systemshell non-interactif (les commandes du systemshell interactives ne sont pas consignées)--ainsi que les commandes d'API sont consignées ici. Les journaux d'audit incluent des horodatages pour indiquer si tous les nœuds d'un cluster sont synchronisés.

Le `audit.log` Le fichier est envoyé par l'outil AutoSupport aux destinataires spécifiés. Vous pouvez également transférer le contenu en toute sécurité vers des destinations externes que vous spécifiez (par exemple, un serveur Splunk ou syslog).

Le `audit.log` le fichier fait l'objet d'une rotation quotidienne. La rotation se produit également lorsqu'elle atteint 100 Mo et que les 48 copies précédentes sont conservées (avec un total maximum de 49 fichiers). Lorsque le fichier d'audit effectue sa rotation quotidienne, aucun message EMS n'est généré. Si le fichier d'audit tourne parce que sa taille limite de fichier est dépassée, un message EMS est généré.

## Modifications de la journalisation des audits dans ONTAP 9

À partir de ONTAP 9, le `command-history.log` le fichier est remplacé par `audit.log`, et le `mgwd.log` le fichier ne contient plus d'informations d'audit. Si vous effectuez une mise à niveau vers ONTAP 9, il est recommandé de consulter les scripts ou les outils qui font référence aux fichiers hérités et à leur contenu.

Après la mise à niveau vers ONTAP 9, existant `command-history.log` les fichiers sont conservés. Ils sont tournés vers l'extérieur (supprimés) comme nouveaux `audit.log` les fichiers sont pivotés dans (créés).

Outils et scripts qui vérifient le `command-history.log` le fichier peut continuer à fonctionner, car un lien logiciel de `command-history.log` à `audit.log` est créée lors de la mise à niveau. Cependant, les outils et les scripts qui vérifient le `mgwd.log` le fichier échoue, car ce fichier ne contient plus d'informations d'audit.

Les journaux d'audit dans ONTAP 9 et les versions ultérieures n'incluent plus les entrées suivantes, car elles ne sont pas considérées comme utiles et n'entraînent pas d'activité de journalisation inutile :

- Commandes internes exécutées par ONTAP (c'est-à-dire où `username=root`)
- Alias de commande (séparément de la commande à laquelle ils pointent)

Depuis ONTAP 9, vous pouvez transmettre les journaux d'audit de manière sécurisée vers des destinations externes à l'aide des protocoles TCP et TLS.

## Afficher le contenu du journal d'audit

Vous pouvez afficher le contenu du cluster `/mroot/etc/log/mlog/audit.log` Fichiers via l'interface de ligne de commandes de ONTAP, System Manager ou un navigateur Web.

Les entrées du fichier journal du cluster sont les suivantes :

### Temps

Horodatage de l'entrée du journal.

### Client supplémentaire

Application utilisée pour se connecter au cluster. Voici des exemples de valeurs possibles `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, et `service-processor`.

### Utilisateur

Nom d'utilisateur de l'utilisateur distant.

### État

État actuel de la demande d'audit, qui pourrait être `success`, `pending`, ou `error`.

### Messagerie

Champ facultatif qui peut contenir une erreur ou des informations supplémentaires sur l'état d'une commande.

### ID de session

ID de session sur lequel la demande est reçue. Un ID de session est attribué à chaque session SSH *session*, tandis que chaque HTTP, ONTAPI ou SNMP *request* se voit attribuer un ID de session unique.

### VM de stockage

SVM via lequel l'utilisateur a connecté.

### Portée

S'affiche `svm` Lorsque la demande se trouve sur une machine virtuelle de stockage de données ; dans le cas contraire, s'affiche `cluster`.

## ID de commande

ID de chaque commande reçue lors d'une session CLI. Cela vous permet de mettre en corrélation une demande et une réponse. Les requêtes ZAPI, HTTP et SNMP ne possèdent pas d'ID de commande.

Vous pouvez afficher les entrées des journaux du cluster depuis l'interface de ligne de commandes de ONTAP, depuis un navigateur Web et depuis ONTAP 9.11.1, depuis System Manager.

### System Manager

- Pour afficher l'inventaire, sélectionnez **Événements et travaux > journaux d'audit**. Chaque colonne dispose de commandes pour filtrer, trier, rechercher, afficher et inventorier les catégories. Les détails de l'inventaire peuvent être téléchargés sous forme de classeur Excel.
- Pour définir des filtres, cliquez sur le bouton **Filter** en haut à droite, puis sélectionnez les champs souhaités. Vous pouvez également afficher toutes les commandes exécutées dans la session au cours de laquelle un échec s'est produit en cliquant sur le lien ID de session.

### CLI

Pour afficher les entrées d'audit fusionnées à partir de plusieurs nœuds du cluster, entrez :

```
security audit log show [parameters]
```

Vous pouvez utiliser le `security audit log show` commande permettant d'afficher les entrées d'audit de nœuds individuels ou fusionnées à partir de plusieurs nœuds du cluster. Vous pouvez également afficher le contenu du `/mroot/etc/log/mlog` répertoire sur un seul nœud à l'aide d'un navigateur web.

Voir la page man pour plus de détails.

### Navigateur Web


Vous pouvez afficher le contenu du `/mroot/etc/log/mlog` répertoire sur un seul nœud à l'aide d'un navigateur web. "[Découvrez comment accéder aux fichiers log, core dump et MIB d'un nœud à l'aide d'un navigateur Web](#)".

## Gérer les paramètres de demande GET d'audit

Lorsque LES demandes DÉFINIES sont consignées par défaut, les demandes GET ne le sont pas. Cependant, vous pouvez contrôler si LES requêtes GET sont envoyées depuis ONTAP HTML (`-httpget`), l'interface de ligne de commande ONTAP (`-cliget`), ou à partir des API ONTAP (`-ontapiget`) sont consignés dans le fichier.

Vous pouvez modifier les paramètres de la journalisation des audits depuis l'interface de ligne de commandes de ONTAP et depuis ONTAP 9.11.1 depuis System Manager.

### System Manager

1. Sélectionnez **événements et travaux > journaux d'audit**.
2. Cliquez  dans le coin supérieur droit, puis choisissez les demandes à ajouter ou à supprimer.

### CLI

- Pour spécifier que les demandes GET depuis l'interface de ligne de commande ou les API ONTAP doivent être enregistrées dans le journal d'audit (fichier audit.log), en plus des demandes SET par défaut, entrez :

```
security audit modify [-cliget {on|off}][--httpget {on|off}][--ontapiget {on|off}]
```

- Pour afficher les paramètres actuels, entrez :

```
security audit show
```

Consultez les pages de manuel pour plus de détails.

## Gérer les destinations du journal d'audit

Vous pouvez transférer le journal d'audit vers un maximum de 10 destinations. Par exemple, vous pouvez transférer le journal vers un serveur Splunk ou syslog à des fins de surveillance, d'analyse ou de sauvegarde.

### Description de la tâche

Pour configurer le transfert, vous devez fournir l'adresse IP de l'hôte syslog ou Splunk, son numéro de port, un protocole de transmission et la fonction syslog à utiliser pour les journaux transférés. ["En savoir plus sur les installations de syslog"](#).

Vous pouvez sélectionner l'une des valeurs de transmission suivantes :

#### UDP non crypté

Protocole de datagramme utilisateur sans sécurité (par défaut)

#### TCP non chiffré

Protocole de contrôle de transmission sans sécurité




#### TCP chiffré

Protocole de contrôle de transmission avec TLS (transport Layer Security)

Une option **Verify Server** est disponible lorsque le protocole TCP chiffré est sélectionné.

Vous pouvez transférer les journaux d'audit depuis l'interface de ligne de commandes de ONTAP et depuis ONTAP 9.11.1 depuis System Manager.

## System Manager

- Pour afficher les destinations du journal d'audit, sélectionnez **Cluster > Paramètres**. + Un nombre de destinations de journaux est affiché dans la vignette **gestion des notifications**. Cliquez  pour afficher les détails.
- Pour ajouter, modifier ou supprimer des destinations du journal d'audit, sélectionnez **Événements et travaux > journaux d'audit**, puis cliquez sur **gérer destinations d'audit** dans le coin supérieur droit de l'écran. + cliquez sur  **Add**, ou cliquez  dans la colonne **adresse hôte** pour modifier ou supprimer des entrées.

## CLI

1. Pour chaque destination vers laquelle vous souhaitez transférer le journal d'audit, spécifiez l'adresse IP ou le nom d'hôte de destination et les options de sécurité.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

- Si le `cluster log-forwarding create` la commande ne peut pas envoyer de requête ping à l'hôte de destination pour vérifier la connectivité, la commande échoue avec une erreur. Bien qu'il ne soit pas recommandé, utiliser le `-force` le paramètre utilisé avec la commande ignore la vérification de connectivité.
  - Lorsque vous définissez le `-verify-server` paramètre à `true`, l'identité de la destination de transfert de journal est vérifiée en validant son certificat. Vous pouvez définir la valeur sur `true` uniquement lorsque vous sélectionnez `tcp-encrypted` valeur dans le `-protocol` légale.
2. Vérifiez que les enregistrements de destination sont corrects à l'aide du `cluster log-forwarding show` commande.

```
cluster1::> cluster log-forwarding show
```

| Destination Host | Port | Protocol        | Verify Server | Syslog Facility |
|------------------|------|-----------------|---------------|-----------------|
| 192.168.123.96   | 514  | udp-unencrypted | false         | user            |
| 192.168.123.98   | 514  | tcp-encrypted   | true          | user            |

2 entries were displayed.

Consultez les pages de manuel pour plus de détails.



# AutoSupport

## Découvrez AutoSupport

### À propos de AutoSupport

AutoSupport est un mécanisme qui surveille de manière proactive l'état de votre système et envoie automatiquement des messages au support technique NetApp, à votre organisation de support interne et à un partenaire de support. Bien que les messages AutoSupport au support technique soient activés par défaut, vous devez définir les options correctes et disposer d'un hôte de messagerie valide pour que les messages soient envoyés à votre service de support interne.

Seul l'administrateur du cluster peut effectuer la gestion AutoSupport. L'administrateur du SVM (Storage Virtual machine) n'a pas accès à AutoSupport.

L'option AutoSupport est activée par défaut lorsque vous configurez votre système de stockage pour la première fois. L'AutoSupport envoie des messages au support technique sous 24 heures après l'activation de AutoSupport. Vous pouvez réduire cette période de 24 heures en mettant à niveau ou en restaurer le système, en modifiant la configuration AutoSupport ou en modifiant l'heure du système pour une période différente de 24 heures.



Vous pouvez désactiver AutoSupport à tout moment, mais vous devez l'activer. L'activation d'AutoSupport peut considérablement accélérer l'identification et la résolution des problèmes sur votre système de stockage. Par défaut, le système collecte les informations AutoSupport et les stocke localement, même si vous désactivez AutoSupport.

Pour en savoir plus sur AutoSupport, consultez le site de support NetApp.

### Informations associées

- ["Support NetApp"](#)
- ["Référence de commande ONTAP"](#)

### À propos de Active IQ Digital Advisor et de AutoSupport

Le composant AutoSupport de ONTAP collecte les données de télémétrie et les envoie pour analyse. Le conseiller digital Active IQ analyse les données d'AutoSupport et fournit un support proactif et une optimisation. Avec l'intelligence artificielle, Active IQ peut identifier les problèmes potentiels et vous aider à les résoudre avant qu'ils n'affectent votre activité.

Active IQ vous permet d'optimiser votre infrastructure de données dans l'ensemble de votre cloud hybride grâce à un portail cloud et à une application mobile qui offrent des analyses prédictives et un support proactif. Les informations et les recommandations basées sur les données de Active IQ sont accessibles à tous les clients NetApp qui possèdent un contrat SupportEdge actif (les fonctionnalités varient selon le produit et le niveau de support).

Voici quelques avantages que vous pouvez faire avec Active IQ :

- Planification des mises à niveau. Active IQ identifie les problèmes qui peuvent être résolus dans votre

environnement en effectuant une mise à niveau vers la plus récente version d'ONTAP et le composant Upgrade Advisor vous aide à planifier une mise à niveau réussie.

- Voir le bien-être du système. Votre tableau de bord Active IQ signale tout problème éventuel et vous aide à le corriger. Surveillez la capacité du système pour vous assurer que votre espace de stockage est insuffisant. Consultez les dossiers de demande de support de votre système.
- Gestion des performances. Active IQ affiche les performances du système sur une période plus longue que ce que vous pouvez voir dans System Manager. Identifiez les problèmes de configuration et de système qui ont un impact sur les performances.
- Optimisez l'efficacité. Affichez les mesures de l'efficacité du stockage et identifiez des moyens de stocker plus de données dans moins d'espace.
- Voir l'inventaire et la configuration. Active IQ affiche des informations complètes sur l'inventaire et la configuration logicielle et matérielle. Voyez quand les contrats de service arrivent à expiration et renouvelez-les pour vous assurer que vous restez pris en charge.

### Informations associées

["Documentation NetApp : conseiller digital Active IQ"](#)

["Lancez Active IQ"](#)

["Services SupportEdge"](#)

### Quand et où les messages AutoSupport sont envoyés

AutoSupport envoie des messages à différents destinataires, en fonction du type de message. Savoir où et quand envoyer des messages AutoSupport peut vous aider à comprendre les messages que vous recevez par e-mail ou consultez le site Web Active IQ (anciennement My AutoSupport).

Sauf indication contraire, les paramètres dans les tableaux suivants sont des paramètres de l'`system node autosupport modify` commande.

#### Messages déclenchés par des événements

Lorsque des événements se produisent sur le système qui nécessitent une action corrective, AutoSupport envoie automatiquement un message déclenché par un événement.

| Lorsque le message est envoyé                                 | Où le message est envoyé                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AutoSupport répond à un événement de déclenchement dans l'EMS | Adresses spécifiées dans <code>-to</code> et <code>-noteto</code> . (Seuls les événements critiques affectant le service sont envoyés.)<br><br>Adresses spécifiées dans <code>-partner-address</code><br><br>Support technique, si <code>-support</code> est défini sur <code>enable</code> |

#### Messages programmés

AutoSupport envoie automatiquement plusieurs messages selon un calendrier normal.

| Lorsque le message est envoyé                                                                                                                                  | Où le message est envoyé                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Quotidien (par défaut, envoyé entre 12 h 00 et 1 h 00 en tant que message de journal)                                                                          | Adresses spécifiées dans <code>-partner-address</code><br><br>Support technique, si <code>-support</code> est défini sur <code>enable</code>     |
| Quotidien (par défaut, envoyé entre 12 h 00 et 1 h 00 comme un message de performance), si le <code>-perf</code> le paramètre est défini sur <code>true</code> | Adresses spécifiées dans <code>-adresse-partenaire»</code><br><br>Support technique, si <code>-support</code> est défini sur <code>enable</code> |
| Hebdomadaire (par défaut, envoyé le dimanche entre 12 h 00 et 1 h 00)                                                                                          | Adresses spécifiées dans <code>-partner-address</code><br><br>Support technique, si <code>-support</code> est défini sur <code>enable</code>     |

### Messages déclenchés manuellement

Vous pouvez lancer ou renvoyer manuellement un message AutoSupport.

| Lorsque le message est envoyé                                                                        | Où le message est envoyé                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Vous lancez manuellement un message à l'aide de <code>system node autosupport invoke commande</code> | Si un URI est spécifié à l'aide de <code>-uri</code> paramètre dans le <code>system node autosupport invoke Commande</code> , le message est envoyé à cet URI.<br><br>Si <code>-uri</code> est omis, le message est envoyé aux adresses spécifiées dans <code>-to</code> et <code>-partner-address</code> . Le message est également envoyé au support technique si <code>-support</code> est défini sur <code>enable</code> . |

| Lorsque le message est envoyé                                                                                                       | Où le message est envoyé                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Vous lancez manuellement un message à l'aide de <code>system node autosupport invoke-core-upload</code> commande</p>             | <p>Si un URI est spécifié à l'aide de <code>-uri</code> paramètre dans le <code>system node autosupport invoke-core-upload</code> Commande, le message est envoyé à cet URI, et le fichier core dump est chargé sur l'URI.</p> <p>Si <code>-uri</code> est omis dans le <code>system node autosupport invoke-core-upload</code> commande, le message est envoyé au support technique et le fichier « core dump » est chargé sur le site du support technique.</p> <p>Cela est nécessaire dans les deux cas <code>-support</code> est défini sur <code>enable</code> et <code>-transport</code> est défini sur <code>https</code> ou <code>http</code>.</p> <p>En raison de la grande taille des fichiers core dump, le message n'est pas envoyé aux adresses spécifiées dans l' <code>-to</code> et <code>-partner-addresses</code> paramètres.</p>                                                           |
| <p>Vous lancez manuellement un message à l'aide de <code>system node autosupport invoke-performance-archive</code> commande</p>     | <p>Si un URI est spécifié à l'aide de <code>-uri</code> paramètre dans le <code>system node autosupport invoke-performance-archive</code> Commande, le message est envoyé à cet URI, et le fichier d'archive de performances est chargé dans l'URI.</p> <p>Si <code>-uri</code> est omis dans le <code>system node autosupport invoke-performance-archive</code>, le message est envoyé au support technique et le fichier d'archive de performances est chargé sur le site de support technique.</p> <p>Cela est nécessaire dans les deux cas <code>-support</code> est défini sur <code>enable</code> et <code>-transport</code> est défini sur <code>https</code> ou <code>http</code>.</p> <p>En raison de la taille importante des fichiers d'archivage de performances, le message n'est pas envoyé aux adresses spécifiées dans l' <code>-to</code> et <code>-partner-addresses</code> paramètres.</p> |
| <p>Vous renvoyez manuellement un message précédent à l'aide de <code>system node autosupport history retransmit</code> commande</p> | <p>Uniquement à l'URI que vous spécifiez dans le <code>-uri</code> paramètre du <code>system node autosupport history retransmit</code> commande</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

### Messages déclenchés par le support technique

Le support technique peut demander des messages à AutoSupport avec la fonction AutoSupport OnDemand.

| Lorsque le message est envoyé                                                                                                                                                          | Où le message est envoyé                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Quand AutoSupport obtient les instructions de livraison pour générer de nouveaux messages AutoSupport                                                                                  | Adresses spécifiées dans <code>-partner-address</code><br><br>Support technique, si <code>-support</code> est défini sur <code>enable</code> et <code>-transport</code> est défini sur <code>https</code>                                                            |
| Quand AutoSupport obtient des instructions de livraison pour renvoyer les messages AutoSupport précédents                                                                              | Support technique, si <code>-support</code> est défini sur <code>enable</code> et <code>-transport</code> est défini sur <code>https</code>                                                                                                                          |
| Quand AutoSupport obtient des instructions de livraison pour générer de nouveaux messages AutoSupport qui chargent des fichiers <code>core dump</code> ou d'archivage des performances | Support technique, si <code>-support</code> est défini sur <code>enable</code> et <code>-transport</code> est défini sur <code>https</code> . Le fichier « <code>core dump</code> » ou d'archivage des performances est téléchargé sur le site du support technique. |

### Comment AutoSupport crée et envoie des messages déclenchés par des événements

AutoSupport crée des messages AutoSupport déclenchés par les événements lorsque le système EMS traite un événement déclencheur. Un message AutoSupport déclenché par un événement alerte les destinataires des problèmes qui requièrent une action corrective et ne contient que des informations pertinentes pour le problème. Vous pouvez personnaliser le contenu à inclure et qui reçoit les messages.

AutoSupport utilise le processus suivant pour créer et envoyer des messages AutoSupport déclenchés par les événements :

1. Lorsque l'EMS traite un événement déclencheur, EMS envoie une requête à AutoSupport.

Un événement déclencheur est un événement EMS avec une destination AutoSupport et un nom commençant par un `callhome.` préfixe.

2. AutoSupport crée un message AutoSupport déclenché par un événement.

AutoSupport collecte des informations de base et de dépannage des sous-systèmes associés au déclencheur afin de créer un message contenant uniquement les informations pertinentes pour l'événement de déclenchement.

Un ensemble de sous-systèmes par défaut est associé à chaque déclencheur. Cependant, vous pouvez choisir d'associer des sous-systèmes supplémentaires à un déclencheur en utilisant le `system node autosupport trigger modify` commande.

3. AutoSupport envoie le message AutoSupport déclenché par l'événement aux destinataires définis par le `system node autosupport modify` commande avec `-to`, `-noteto`, `-partner-address`, et `-support` paramètres.

Vous pouvez activer et désactiver la transmission de messages AutoSupport pour des déclencheurs spécifiques à l'aide de la `system node autosupport trigger modify` commande avec `-to` et `-noteto` paramètres.

**Exemple de données envoyées pour un événement spécifique**

Le `storage shelf PSU failed` L'événement EMS déclenche un message contenant des données de base provenant des fichiers obligatoires, journaux, stockage, RAID, HA, Sous-systèmes de plate-forme et de mise en réseau et données de dépannage des sous-systèmes obligatoire, fichiers journaux et stockage.

Vous souhaitez inclure des données à propos de NFS dans tout message AutoSupport envoyé en réponse à une future `storage shelf PSU failed` événement. Vous entrez la commande suivante pour activer les données de dépannage de NFS pour le `callhome.shlf.ps.fault` événement :

```
cluster1::\>
system node autosupport trigger modify -node node1 -autosupport
-messsage shlf.ps.fault -troubleshooting-additional nfs
```

Notez que le `callhome.` le préfixe est supprimé du `callhome.shlf.ps.fault` événement lorsque vous utilisez le `system node autosupport trigger` Commandes ou lorsqu'elles sont référencées par des événements AutoSupport et EMS dans l'interface de ligne de commande.

**Types de messages AutoSupport et leur contenu**

Les messages AutoSupport contiennent des informations d'état sur les sous-systèmes pris en charge. Découvrez ce que contiennent les messages AutoSupport pour vous aider à interpréter les messages que vous recevez par e-mail ou à consulter sur le site Web Active IQ (anciennement My AutoSupport).

| Type de message     | Type de données que le message contient                                                                  |
|---------------------|----------------------------------------------------------------------------------------------------------|
| Événement déclenché | Fichiers contenant des données contextuelles sur le sous-système spécifique où l'événement s'est produit |
| Tous les jours      | Fichiers journaux                                                                                        |
| Performance         | Données de performance échantillonnées au cours des 24 heures précédentes                                |
| Hebdomadaire        | Données de configuration et d'état                                                                       |

| Type de message                                                                           | Type de données que le message contient                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Déclenché par le <code>system node autosupport invoke commande</code>                     | <p>Dépend de la valeur spécifiée dans <code>-type</code> paramètre :</p> <ul style="list-style-type: none"> <li>• <code>test</code> envoie un message déclenché par l'utilisateur avec certaines données de base.</li> </ul> <p>Ce message déclenche également une réponse automatique par e-mail du support technique à toutes les adresses e-mail spécifiées, à l'aide du <code>-to</code> Pour confirmer la réception des messages AutoSupport.</p> <ul style="list-style-type: none"> <li>• <code>performance</code> envoie des données de performance.</li> <li>• <code>all</code> envoie un message déclenché par l'utilisateur avec un ensemble complet de données similaires au message hebdomadaire, y compris les données de dépannage de chaque sous-système.</li> </ul> <p>L'assistance technique demande généralement ce message.</p> |
| Déclenché par le <code>system node autosupport invoke-core-upload commande</code>         | Fichiers core dump d'un nœud                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Déclenché par le <code>system node autosupport invoke-performance-archive commande</code> | Fichiers d'archivage des performances pendant une période donnée                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Déclenché par AutoSupport OnDemand                                                        | <p>AutoSupport OnDemand peut demander de nouveaux messages ou des messages antérieurs :</p> <ul style="list-style-type: none"> <li>• Les nouveaux messages, selon le type de collection AutoSupport, peuvent être <code>test</code>, <code>all</code>, ou <code>performance</code>.</li> <li>• Les messages antérieurs dépendent du type de message renvoyé.</li> </ul> <p>AutoSupport OnDemand peut demander de nouveaux messages qui téléchargent les fichiers suivants sur le site de support NetApp à l'adresse <a href="https://mysupport.netapp.com">"mysupport.netapp.com"</a>:</p> <ul style="list-style-type: none"> <li>• « Core dump »</li> <li>• Archivage des performances</li> </ul>                                                                                                                                                 |

## Afficher les sous-systèmes AutoSupport

Chaque sous-système fournit des informations de base et de dépannage utilisées par AutoSupport pour ses messages. Chaque sous-système est également associé aux événements de déclenchement qui permettent à AutoSupport de collecter uniquement à partir des informations pertinentes pour l'événement de déclenchement.

AutoSupport collecte du contenu sensible au contexte.

### Étapes

1. Afficher des informations sur les sous-systèmes et les événements de déclenchement :

```
system node autosupport trigger show
```

## Taille et budgets de temps des AutoSupport

AutoSupport collecte des informations, organisées par sous-système, et applique une taille et un budget consacré au contenu pour chaque sous-système. Face à la croissance des systèmes de stockage, les budgets AutoSupport assurent un contrôle de la charge utile AutoSupport, ce qui assure une livraison évolutive des données AutoSupport.

AutoSupport cesse de collecter des informations et de tronquer AutoSupport le contenu du sous-système si sa taille ou son budget. Si le contenu ne peut pas être facilement tronqué (par exemple, les fichiers binaires), AutoSupport omet le contenu.

Vous devez modifier la taille et les budgets par défaut uniquement si le support NetApp vous y invite. Vous pouvez également consulter la taille et les budgets de temps par défaut des sous-systèmes en utilisant le `autosupport manifest show` commande.

## Fichiers envoyés dans des messages AutoSupport déclenchés par un événement

Les messages AutoSupport déclenchés par des événements contiennent uniquement des informations de base et de dépannage des sous-systèmes associés à l'événement qui a généré AutoSupport le message. Ses données spécifiques aident les partenaires de support et les équipes de support NetApp à résoudre le problème.

AutoSupport utilise les critères suivants pour contrôler le contenu des messages AutoSupport déclenchés par les événements :

- Quels sous-systèmes sont inclus

Les données sont regroupées en sous-systèmes, y compris les sous-systèmes communs, tels que les fichiers journaux et certains sous-systèmes, tels que RAID. Chaque événement déclenche un message contenant uniquement les données des sous-systèmes spécifiques.

- Niveau de détail de chaque sous-système inclus

Les données de chaque sous-système inclus sont fournies au niveau de base ou de dépannage.



Vous pouvez afficher tous les événements possibles et déterminer quels sous-systèmes sont inclus dans les messages relatifs à chaque événement à l'aide du `system node autosupport trigger show` commande avec `-instance` paramètre.

En plus des sous-systèmes inclus par défaut pour chaque événement, vous pouvez ajouter des sous-systèmes supplémentaires à un niveau de base ou de dépannage à l'aide de l' `system node autosupport trigger modify` commande.

**Fichiers journaux envoyés dans les messages AutoSupport**

Les messages AutoSupport peuvent contenir plusieurs fichiers journaux clés qui permettent au personnel du support technique de revoir l'activité récente du système.

Tous les types de messages AutoSupport peuvent inclure les fichiers journaux suivants lorsque le sous-système fichiers journaux est activé :

| Fichier journal                                                                                                                                                                                                                                              | Quantité de données incluses dans le fichier                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>Fichiers journaux à partir du /mroot/etc/log/mlog/ répertoire</li><li>Le fichier journal DES MESSAGES</li></ul>                                                                                                        | <p>Seules les nouvelles lignes ajoutées aux journaux depuis le dernier message AutoSupport jusqu'à un maximum spécifié. Cela permet de s'assurer que les messages AutoSupport disposent de données uniques et pertinentes, sans chevauchement.</p> <p>(Les fichiers journaux des partenaires font exception. Pour les partenaires, le nombre maximal de données autorisé est inclus.)</p> |
| <ul style="list-style-type: none"><li>Fichiers journaux à partir du /mroot/etc/log/shelflog/ répertoire</li><li>Fichiers journaux à partir du /mroot/etc/log/acp/ répertoire</li><li>Données de journal du système de gestion des événements (EMS)</li></ul> | <p>Les lignes de données les plus récentes jusqu'à un maximum spécifié.</p>                                                                                                                                                                                                                                                                                                               |

Le contenu des messages AutoSupport peut changer de version d'ONTAP.

**Fichiers envoyés dans des messages AutoSupport hebdomadaires**

Les messages hebdomadaires AutoSupport contiennent des données supplémentaires sur la configuration et l'état, ce qui est utile pour suivre les modifications apportées à votre système au fil du temps.

Les informations suivantes sont envoyées dans des messages AutoSupport hebdomadaires :

- Informations de base sur chaque sous-système
- Contenu de sélectionné /mroot/etc fichiers de répertoire
- Fichiers journaux
- Résultat des commandes fournissant les informations système

- Informations supplémentaires, notamment les informations des bases de données répliquées – RDB –, les statistiques des services et bien plus encore

## **Comment AutoSupport OnDemand obtient des instructions de livraison auprès du support technique**

AutoSupport OnDemand communique régulièrement avec le support technique pour obtenir des instructions de livraison pour envoyer, renvoyer et refuser des messages AutoSupport, et pour télécharger des fichiers volumineux vers le site du support NetApp. AutoSupport OnDemand permet d'envoyer des messages AutoSupport à la demande au lieu d'attendre l'exécution de la tâche AutoSupport hebdomadaire.

AutoSupport OnDemand comprend les composants suivants :

- Client AutoSupport OnDemand qui s'exécute sur chaque nœud
- Service AutoSupport OnDemand qui réside dans le support technique

Le client AutoSupport OnDemand interroge régulièrement le service AutoSupport OnDemand afin d'obtenir des instructions de livraison du support technique. Par exemple, le support technique peut utiliser le service AutoSupport OnDemand pour demander la génération d'un nouveau message AutoSupport. Lorsque le client AutoSupport OnDemand interroge le service AutoSupport OnDemand, le client obtient les instructions de livraison et envoie le nouveau message AutoSupport à la demande.

AutoSupport OnDemand est activé par défaut. Cependant, AutoSupport OnDemand dépend de certains paramètres AutoSupport pour continuer à communiquer avec le support technique. AutoSupport OnDemand communique automatiquement avec le support technique lorsque les exigences suivantes sont respectées :

- AutoSupport est activé.
- AutoSupport est configuré pour envoyer des messages au support technique.
- AutoSupport est configuré pour utiliser le protocole de transport HTTPS.

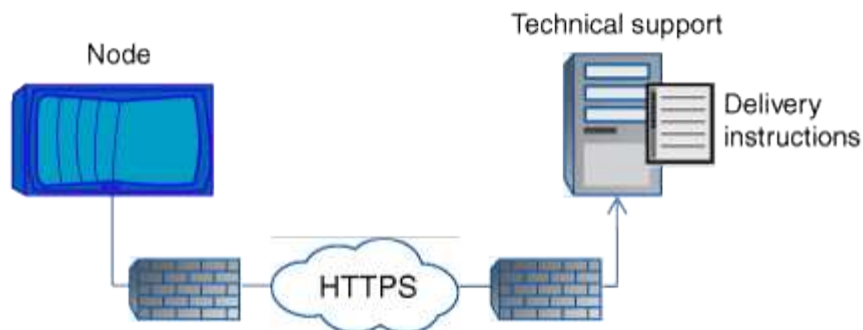
Le client AutoSupport OnDemand envoie des demandes HTTPS au même emplacement de support technique auquel les messages AutoSupport sont envoyés. Le client AutoSupport OnDemand n'accepte pas les connexions entrantes.



AutoSupport OnDemand utilise le compte utilisateur « AutoSupport » pour communiquer avec le support technique. ONTAP vous empêche de supprimer ce compte.

Si vous souhaitez désactiver AutoSupport OnDemand, mais que AutoSupport reste activé, utilisez la commande : `LINK:https://docs.netapp.com/us-en/ontap-cli/system-node-autosupport-modify.html#parameters[system node autosupport modify -ondemand-state disable]`.

L'illustration suivante montre comment AutoSupport OnDemand envoie des demandes HTTPS au support technique pour obtenir des instructions de livraison.



Les instructions de livraison peuvent inclure des demandes pour que AutoSupport puisse faire ce qui suit :

- Générer de nouveaux messages AutoSupport.

Le support technique peut demander de nouveaux messages AutoSupport pour vous aider à trier les problèmes.

- Générer de nouveaux messages AutoSupport qui chargent les fichiers « core dump » ou les fichiers d'archivage des performances sur le site de support NetApp.

Le support technique peut demander des fichiers « core dump » ou d'archivage des performances afin de gérer les problèmes urgents.

- Retransmettre les messages AutoSupport générés précédemment.

Cette demande se produit automatiquement si aucun message n'a été reçu en raison d'un échec de livraison.

- Désactiver la distribution des messages AutoSupport pour des événements déclencheurs spécifiques.

Le support technique peut désactiver la livraison de données non utilisées.

### Structure des messages AutoSupport envoyés par e-mail

Lorsqu'un message AutoSupport est envoyé par e-mail, le message a un objet standard, un corps bref et une pièce jointe de grande taille au format de fichier 7z qui contient les données.



Si AutoSupport est configuré pour masquer les données privées, certaines informations, telles que le nom d'hôte, sont omises ou masquées dans l'en-tête, le sujet, le corps et les pièces jointes.

#### Objet

La ligne d'objet des messages envoyés par le mécanisme AutoSupport contient une chaîne de texte qui identifie la raison de la notification. Le format de la ligne d'objet est le suivant :

Notification de groupe HA de *System\_Name (message) Severity*

- *System\_Name* est le nom d'hôte ou l'ID système, selon la configuration AutoSupport

## Corps

Le corps du message AutoSupport contient les informations suivantes :

- Date et heure du message
- Version de ONTAP sur le nœud qui a généré le message
- L'ID du système, le numéro de série et le nom d'hôte du nœud qui a généré le message
- Numéro de séquence AutoSupport
- Localisation et nom du contact SNMP, si spécifiés
- ID système et nom d'hôte du nœud partenaire HA

## Fichiers joints

Les informations clés d'un message AutoSupport sont contenues dans des fichiers compressés dans un fichier 7z appelé `body.7z` et joints au message.

Les fichiers contenus dans la pièce jointe sont spécifiques au type de message AutoSupport.

## Types de gravité AutoSupport

Les messages AutoSupport ont des types de gravité qui vous aident à comprendre l'objet de chaque message : par exemple, pour attirer l'attention immédiate sur un problème d'urgence ou uniquement pour fournir des informations.

Les messages ont l'un des niveaux de gravité suivants :

- **Alerte** : les messages d'alerte indiquent qu'un événement de niveau supérieur peut se produire si vous ne prenez pas d'action.

Vous devez prendre une action contre les messages d'alerte dans les 24 heures.

- **Urgence** : les messages d'urgence sont affichés lorsqu'une interruption s'est produite.

Vous devez agir immédiatement contre les messages d'urgence.

- **Erreur** : les conditions d'erreur indiquent ce qui peut se produire si vous ignorez.
- **Avis** : condition normale mais significative.
- **Info** : Message d'information fournit des détails sur le problème, que vous pouvez ignorer.
- **Debug** : les messages au niveau du débogage fournissent des instructions que vous devez effectuer.

Si votre service de support interne reçoit des messages AutoSupport par e-mail, la gravité apparaît dans l'objet de l'e-mail.

## Lire les descriptions de messages AutoSupport

Les descriptions des messages AutoSupport que vous recevez sont disponibles via le convertisseur Syslog ONTAP.

## Étapes

1. Accédez au ["Traducteur syslog"](#).

2. Dans le champ **version**, entrez la version de ONTAP que vous utilisez. Dans le champ **Search String**, entrez « callhome ». Sélectionnez **Translate**.
3. Syslog Translator répertorie par ordre alphabétique tous les événements correspondant à la chaîne de message que vous avez saisie.

## Commandes de gestion de AutoSupport

Vous utilisez le `system node autosupport` Commandes permettant de modifier ou d'afficher la configuration AutoSupport, d'afficher des informations sur les messages AutoSupport précédents et d'envoyer, de renvoyer ou d'annuler un message AutoSupport.

### Configurez AutoSupport

| Les fonctions que vous recherchez...                                                                                                                                                                                                                                                                             | Utilisez cette commande...                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Contrôlez si des messages AutoSupport sont envoyés                                                                                                                                                                                                                                                               | <code>system node autosupport modify</code> avec le <code>-state</code> paramètre   |
| Contrôlez si les messages AutoSupport sont envoyés au support technique                                                                                                                                                                                                                                          | <code>system node autosupport modify</code> avec le <code>-support</code> paramètre |
| Configurer AutoSupport ou modifier la configuration de AutoSupport                                                                                                                                                                                                                                               | <code>system node autosupport modify</code>                                         |
| Activez et désactivez les messages AutoSupport à votre organisation de support interne pour les événements de déclenchement individuels. Vous pouvez également spécifier des rapports de sous-système supplémentaires à inclure dans les messages envoyés en réponse aux événements de déclenchement individuels | <code>system node autosupport trigger modify</code>                                 |

### Affiche des informations sur la configuration AutoSupport


| Les fonctions que vous recherchez...                                                                                           | Utilisez cette commande...                                                     |
|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Afficher la configuration AutoSupport                                                                                          | <code>system node autosupport show</code> avec le <code>-node</code> paramètre |
| Afficher un récapitulatif de toutes les adresses et URL qui reçoivent des messages AutoSupport                                 | <code>system node autosupport destinations show</code>                         |
| Affichez les messages AutoSupport envoyés à votre organisation de support interne pour des événements déclencheurs individuels | <code>system node autosupport trigger show</code>                              |


| Les fonctions que vous recherchez...                                                                        | Utilisez cette commande...                              |
|-------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| Affichage de l'état de la configuration AutoSupport ainsi que de la livraison vers différentes destinations | <code>system node autosupport check show</code>         |
| Affiche l'état détaillé de la configuration AutoSupport ainsi que la livraison à différentes destinations   | <code>system node autosupport check show-details</code> |

#### Affiche les informations relatives aux messages AutoSupport précédents

| Les fonctions que vous recherchez...                                                                                                                                                           | Utilisez cette commande...                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Affiche des informations sur un ou plusieurs des 50 messages AutoSupport les plus récents                                                                                                      | <code>system node autosupport history show</code>                |
| Affiche des informations sur les messages AutoSupport récents générés pour télécharger les fichiers core dump ou archive des performances vers le site de support technique ou un URI spécifié | <code>system node autosupport history show-upload-details</code> |
| Affichez les informations des messages AutoSupport, y compris le nom et la taille de chaque fichier collecté pour le message, ainsi que toute erreur                                           | <code>system node autosupport manifest show</code>               |

#### Envoyer, renvoyer ou annuler des messages AutoSupport

| Les fonctions que vous recherchez...                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Utilisez cette commande...                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| <p>Retransmettez un message AutoSupport stocké localement, identifié par son numéro de séquence AutoSupport</p> <div>  <p>Si vous retransmettez un message AutoSupport et que le support a déjà reçu ce message, le système de support ne crée pas de dossier en double. Si, par contre, le support ne recevait pas ce message, le système AutoSupport analysera le message et créera un dossier, si nécessaire.</p> </div> | <code>system node autosupport history retransmit</code> |

| Les fonctions que vous recherchez...                                       | Utilisez cette commande...                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Générer et envoyer un message AutoSupport, par exemple, à des fins de test | <pre>system node autosupport invoke</pre> <div>  <p>Utilisez le <code>-force</code> Paramètre permettant d'envoyer un message même si AutoSupport est désactivé. Utilisez le <code>-uri</code> paramètre pour envoyer le message à la destination que vous spécifiez au lieu de la destination configurée.</p> </div> |
| Annuler un message AutoSupport                                             | <pre>system node autosupport history cancel</pre>                                                                                                                                                                                                                                                                                                                                                      |

### Informations associées

["Référence de commande ONTAP"](#)

### Informations incluses dans le manifeste AutoSupport

Le manifeste AutoSupport vous offre une vue détaillée des fichiers collectés pour chaque message AutoSupport. Le manifeste AutoSupport contient également des informations sur les erreurs de collecte lorsque AutoSupport ne peut pas collecter les fichiers dont il a besoin.

Le manifeste du AutoSupport inclut les informations suivantes :

- Numéro de séquence du message AutoSupport
- Fichiers AutoSupport inclus dans le message AutoSupport
- Taille de chaque fichier, en octets
- Statut de la collection du manifeste AutoSupport
- Description de l'erreur, si AutoSupport n'a pas pu collecter un ou plusieurs fichiers

Vous pouvez afficher le manifeste AutoSupport en utilisant le `system node autosupport manifest show` commande.

Le manifeste AutoSupport est inclus avec chaque message AutoSupport et présenté au format XML, ce qui signifie que vous pouvez soit utiliser un visualiseur XML générique pour le lire, soit l'afficher à l'aide du portail Active IQ (précédemment appelé My AutoSupport).

## Planification

### Préparez-vous à utiliser AutoSupport

Vous pouvez configurer un cluster ONTAP pour qu'il puisse transmettre des messages AutoSupport à NetApp. Dans ce cadre, vous pouvez également envoyer une copie des messages aux adresses e-mail locales, généralement au sein de votre entreprise. Vous devez préparer la configuration de AutoSupport en consultant les options disponibles.

## Transmettre les messages AutoSupport à NetApp

Les messages AutoSupport peuvent être transmis à NetApp à l'aide du protocole HTTP ou SMTP. Pour améliorer la sécurité, vous pouvez utiliser TLS avec HTTP. À partir de ONTAP 9.15.1, vous pouvez également utiliser TLS avec SMTP.



Utilisez HTTP avec TLS (HTTPS) autant que possible.

Notez également ce qui suit :

- Un seul canal de distribution vers NetApp peut être configuré pour les messages AutoSupport. Vous ne pouvez pas utiliser deux protocoles pour transmettre des messages AutoSupport à NetApp.
- AutoSupport limite la taille maximale de fichier pour chaque protocole. Si la taille d'un message AutoSupport dépasse la limite configurée, AutoSupport transmet autant de messages que possible, mais une troncature se produit.
- Vous pouvez modifier la taille maximale du fichier si nécessaire. Voir la commande `system node autosupport modify` pour en savoir plus.
- Les deux protocoles peuvent être transportés sur IPv4 ou IPv6 en fonction de la famille d'adresses à laquelle le nom résout.
- La connexion TCP établie par ONTAP pour envoyer des messages AutoSupport est temporaire et de courte durée.

## HTTP

Cela fournit les fonctionnalités les plus robustes. Notez ce qui suit :

- AutoSupport OnDemand et le transfert de fichiers volumineux sont pris en charge.
- Une requête HTTP PUT est tentée en premier. Si la demande échoue pendant la transmission, la demande redémarre à l'endroit où elle s'est arrêtée.
- Si le serveur ne prend pas en charge PUT, la méthode HTTP POST est utilisée à la place.
- La limite par défaut pour les transferts HTTP est de 50 Mo.
- Le protocole HTTP non sécurisé utilise le port 80.

## SMTP

En règle générale, vous devez utiliser SMTP uniquement si HTTPS/HTTP n'est pas autorisé ou non pris en charge pour une raison quelconque. Notez ce qui suit :

- AutoSupport OnDemand et les transferts de fichiers volumineux ne sont pas pris en charge.
- Si les informations d'identification de connexion SMTP sont configurées, elles sont envoyées sans cryptage et en clair.
- La limite par défaut pour les transferts HTTP est de 5 Mo.
- Le protocole SMTP non sécurisé utilise le port 25.

## Améliorer la sécurité avec TLS

Lorsque vous utilisez HTTP ou SMTP, tout le trafic est non chiffré et peut être facilement intercepté et lu. Lorsque vous utilisez HTTP, vous devez toujours configurer le protocole pour qu'il utilise également TLS (HTTPS).





À partir de ONTAP 9.15.1, vous pouvez également utiliser TLS avec SMTP (SMTPS). Dans ce cas, *Explicit TLS* est utilisé pour activer le canal sécurisé une fois la connexion TCP établie.

### Ports pour les protocoles sécurisés

Les ports suivants sont généralement utilisés pour les versions sécurisées de ces protocoles :

- HTTPS - port 443
- SMTPS - port 587

### Validation du certificat

Avec TLS, le certificat téléchargé à partir du serveur est validé par ONTAP sur la base du certificat de l'autorité de certification racine. Avant d'utiliser HTTPS ou SMTPS, vous devez vous assurer que le certificat racine est installé dans ONTAP. Voir [Installez le certificat du serveur](#) pour en savoir plus.

### Autres considérations relatives à la configuration

D'autres considérations sont à prendre en compte lors de la configuration de AutoSupport.

### Envoi d'une copie locale par e-mail

Quel que soit le protocole utilisé pour transmettre des messages AutoSupport à NetApp, vous pouvez également envoyer une copie de chaque message à une ou plusieurs adresses e-mail locales. Par exemple, vous pouvez envoyer des messages à votre service de support interne ou à une entreprise partenaire.



Si vous transmettez des messages à NetApp à l'aide de SMTP (ou SMTPS) et que vous envoyez également des copies locales de ces messages, la même configuration de serveur de messagerie est utilisée.

### Proxy HTTP

Selon la configuration de votre réseau, le protocole HTTPS peut nécessiter une configuration supplémentaire d'une URL proxy. Si HTTPS est utilisé pour envoyer des messages AutoSupport au support technique et que vous disposez d'un proxy, vous devez identifier l'URL du proxy. Si le proxy utilise un port autre que le port par défaut (port 3128), vous pouvez spécifier le port de ce proxy. Vous pouvez également spécifier un nom d'utilisateur et un mot de passe pour l'authentification proxy.

### Installez le certificat du serveur

Si vous utilisez TLS (HTTPS ou SMTPS), vous devez vous assurer que ONTAP peut valider le certificat du serveur. Cette validation est effectuée sur la base de l'autorité de certification qui a signé le certificat du serveur.

ONTAP inclut un grand nombre de certificats d'autorité de certification racine pré-installés. Ainsi, dans de nombreux cas, le certificat de votre serveur sera immédiatement reconnu par ONTAP sans configuration supplémentaire. Mais selon la façon dont le certificat de serveur a été signé, vous devrez peut-être installer un certificat d'autorité de certification racine et tous les certificats intermédiaires.

Suivez les instructions ci-dessous pour installer le certificat si nécessaire. Vous devez installer tous les certificats requis au niveau du cluster.

## Exemple 30. Étapes

### System Manager

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Faites défiler jusqu'à la section **sécurité**.
3. Sélectionnez ➔ en regard de **certificats**.
4. Sous l'onglet **autorités de certification approuvées**, cliquez sur **Ajouter**.
5. Cliquez sur **Importer** et sélectionnez le fichier de certificat.
6. Renseignez les paramètres de configuration de votre environnement.
7. Cliquez sur **Ajouter**.

### CLI

1. Commencez l'installation :

```
security certificate install -type server-ca
```

2. Recherchez le message de console suivant :

```
Please enter Certificate: Press <Enter> when done
```

3. Ouvrez le fichier de certificat à l'aide d'un éditeur de texte.
4. Copiez l'intégralité du certificat, y compris les lignes suivantes :

```
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
```

5. Collez le certificat dans le terminal après l'invite de commande.
6. Appuyez sur **entrée** pour terminer l'installation.
7. Vérifiez que le certificat est installé à l'aide de l'une des méthodes suivantes :

```
security certificate show-user-installed

security certificate show
```

## Configurer AutoSupport

Vous pouvez configurer un cluster ONTAP pour qu'il envoie des messages AutoSupport au support technique NetApp et envoie des copies à votre service de support interne. Dans ce cadre, vous pouvez également tester la configuration avant de l'utiliser dans un environnement de production.

### Description de la tâche

Depuis ONTAP 9.5, vous activez et configurez AutoSupport pour tous les nœuds d'un cluster simultanément. Lorsqu'un nouveau nœud rejoint le cluster, il hérite automatiquement de la même configuration AutoSupport. Pour cela, le périmètre de la commande CLI `system node autosupport modify` est au niveau du cluster. Le `-node` l'option de commande est conservée pour la compatibilité descendante, mais elle est ignorée.



Dans ONTAP 9.4 et versions antérieures, la commande `system node autosupport modify` est spécifique à chaque nœud. Si votre cluster exécute ONTAP 9.4 ou une version antérieure, vous devez activer et configurer AutoSupport sur chaque nœud du cluster.

## Avant de commencer

La configuration de transport recommandée pour la transmission des messages AutoSupport à NetApp est HTTPS (HTTP avec TLS). Cette option offre les fonctionnalités les plus robustes et la meilleure sécurité.

Révision "[Préparez-vous à utiliser AutoSupport](#)" Pour plus d'informations avant de configurer votre cluster ONTAP.

## Étapes

1. Assurez-vous que AutoSupport est activé :

```
system node autosupport modify -state enable
```

2. Si vous souhaitez que le support technique NetApp reçoive des messages AutoSupport, utilisez la commande suivante :

```
system node autosupport modify -support enable
```

Vous devez activer cette option si vous souhaitez permettre à AutoSupport de travailler avec AutoSupport OnDemand ou si vous souhaitez télécharger des fichiers volumineux, tels que les fichiers core dump et d'archivage des performances, vers le support technique ou une URL spécifiée.

3. Si le support technique NetApp est activé pour recevoir des messages AutoSupport, spécifiez le protocole de transport à utiliser pour les messages.

Vous pouvez choisir parmi les options suivantes :

| Les fonctions que vous recherchez...   | Définissez ensuite les paramètres suivants du <code>system node autosupport modify</code> commande...                                                                                                                                                                                                                                       |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Utilisez le protocole HTTPS par défaut | <ol style="list-style-type: none"><li>a. Réglez <code>-transport</code> à <code>https</code>.</li><li>b. Si vous utilisez un proxy, définissez <code>-proxy -url</code> À l'URL de votre proxy.<br/>Cette configuration prend en charge la communication avec AutoSupport OnDemand et les téléchargements de fichiers volumineux.</li></ol> |
| Utiliser SMTP                          | Réglez <code>-transport</code> à <code>smtp</code> .<br><br>Cette configuration ne prend pas en charge AutoSupport OnDemand ni les téléchargements de fichiers volumineux.                                                                                                                                                                  |

4. Si vous souhaitez que votre service de support interne ou un partenaire de support reçoive les messages

AutoSupport, effectuez les opérations suivantes :

- a. Identifiez les destinataires de votre organisation en définissant les paramètres suivants de l' `system node autosupport modify` commande :

| Définir ce paramètre...       | À ceci...                                                                                                                                                                                                                                                               |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-to</code>              | Jusqu'à cinq adresses e-mail ou listes de distribution individuelles séparées par des virgules dans votre service de support interne qui recevront des messages AutoSupport clés                                                                                        |
| <code>-noteto</code>          | Jusqu'à cinq adresses e-mail ou listes de distribution individuelles séparées par des virgules dans votre service d'assistance interne qui recevront une version abrégée des messages clés AutoSupport conçus pour les téléphones portables et autres appareils mobiles |
| <code>-partner-address</code> | Jusqu'à cinq adresses e-mail ou listes de distribution séparées par des virgules dans votre organisation partenaire de support qui recevront tous les messages AutoSupport                                                                                              |

- b. Vérifiez que les adresses sont correctement configurées en répertoriant les destinations à l'aide de l' `system node autosupport destinations show` commande.

5. Si vous envoyez des messages à votre organisation de support interne ou si vous avez choisi le transport SMTP pour les messages au support technique, configurez SMTP en définissant les paramètres suivants de l' `system node autosupport modify` commande :

- Réglez `-mail-hosts` à un ou plusieurs hôtes de messagerie, séparés par des virgules.

Vous pouvez définir un maximum de cinq.

Vous pouvez configurer une valeur de port pour chaque hôte de messagerie en spécifiant un point-virgule et un numéro de port après le nom d'hôte de messagerie : par exemple, `mymailhost.example.com:5678`, où 5678 est le port de l'hôte de messagerie.

- Réglez `-from` À l'adresse e-mail qui envoie le message AutoSupport.

6. Configurez DNS.

7. Vous pouvez également ajouter des options de commande si vous souhaitez modifier des paramètres spécifiques :

|              |                                                                                                       |
|--------------|-------------------------------------------------------------------------------------------------------|
| Pour cela... | Définissez ensuite les paramètres suivants du <code>system node autosupport modify</code> commande... |
|--------------|-------------------------------------------------------------------------------------------------------|

|                                                                                                         |                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Masquez des données privées en supprimant, masquant ou encodant des données sensibles dans les messages | Réglez <code>-remove-private-data</code> à <code>true</code> . Si vous changez de <code>false</code> à <code>true</code> , Tous les fichiers historiques AutoSupport et tous les fichiers associés sont supprimés. |
| Arrêt de l'envoi des données de performance dans des messages AutoSupport périodiques                   | Réglez <code>-perf</code> à <code>false</code> .                                                                                                                                                                   |

8. Si vous utilisez SMTP pour envoyer des messages AutoSupport à NetApp, vous pouvez éventuellement activer TLS pour améliorer la sécurité.

- a. Afficher les valeurs disponibles pour le nouveau paramètre :

```
cluster1::> system node autosupport modify -smtp-encryption ?
```

- b. Activer TLS pour la livraison des messages SMTP :

```
cluster1::> system node autosupport modify -smtp-encryption start_tls
```

- c. Afficher la configuration actuelle :

```
cluster1::> system node autosupport show -fields smtp-encryption
```

9. Vérifiez la configuration globale à l'aide du `system node autosupport show` commande avec `-node` paramètre.

10. Vérifier le fonctionnement de AutoSupport à l'aide de l' `system node autosupport check show` commande.

Si des problèmes sont signalés, utilisez le `system node autosupport check show-details` pour afficher plus d'informations.

11. Vérifiez que les messages AutoSupport sont en cours d'envoi et de réception :

- a. Utilisez le `system node autosupport invoke` commande avec `-type` paramètre défini sur `test`:

```
cluster1::> system node autosupport invoke -type test -node node1
```

- b. Vérifiez que NetApp reçoit vos messages AutoSupport :

```
system node autosupport history show -node local
```

Le statut du dernier message AutoSupport sortant doit finalement être défini sur `sent-successful` pour toutes les destinations de protocole appropriées.

- c. Vous pouvez également vérifier que les messages AutoSupport sont envoyés à votre service de support interne ou à votre partenaire de support en consultant l'e-mail de toute adresse configurée pour le `-to`, `-noteto`, ou `-partner-address` paramètres du `system node autosupport modify` commande.

## Configurer

### Gérer les paramètres AutoSupport

Vous pouvez utiliser System Manager pour gérer les paramètres de votre compte AutoSupport.

Vous pouvez effectuer les opérations suivantes :

#### Afficher les paramètres AutoSupport

Vous pouvez utiliser System Manager pour afficher les paramètres de votre compte AutoSupport.

#### Étapes

1. Dans System Manager, cliquez sur **Cluster > Paramètres**.

Dans la section **AutoSupport**, les informations suivantes sont affichées :

- État
- Protocole de transport
- Serveur proxy
- De l'adresse e-mail


2. Dans la section **AutoSupport**, sélectionnez , puis **plus d'options**.

Des informations supplémentaires s'affichent sur la connexion AutoSupport et les paramètres de messagerie. De plus, l'historique des transferts de messages est répertorié.

### Générez et envoyez des données AutoSupport

Dans System Manager, vous pouvez lancer la génération de messages AutoSupport et choisir entre le nœud de cluster ou les nœuds où les données sont collectées.


#### Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, sélectionnez , puis **générer et Envoyer**.
3. Saisissez un objet.
4. Cochez la case sous **collecter les données de** pour spécifier les nœuds à partir desquels collecter les données.

#### Testez la connexion à AutoSupport

Depuis System Manager, vous pouvez envoyer un message de test pour vérifier la connexion à AutoSupport.

#### Étapes

1. Dans System Manager, cliquez sur **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, sélectionnez , puis **Tester la connectivité**.
3. Saisissez un objet pour le message.

### Activez ou désactivez le protocole AutoSupport

AutoSupport offre aux clients NetApp des avantages éprouvés, notamment l'identification proactive d'éventuels problèmes de configuration et l'accélération de la résolution des dossiers de support. AutoSupport est activé par défaut sur les nouveaux systèmes. Si nécessaire, vous pouvez utiliser System Manager pour désactiver la fonction AutoSupport de surveillance de l'état de santé du système de stockage et vous envoyer des messages de notification. Vous pouvez à nouveau activer AutoSupport après sa désactivation.

### Description de la tâche

Avant de désactiver AutoSupport, vous devez savoir que vous désactivez le système d'appel à distance NetApp et que vous perdrez les avantages suivants :

- **Surveillance de l'état** : AutoSupport surveille l'état de santé de votre système de stockage et envoie des notifications au support technique et à votre service de support interne.
- **Automatisation** : AutoSupport automatise le reporting des dossiers de support. La plupart des dossiers de demande de support sont ouverts automatiquement avant que les clients n'aient conscience d'un problème.
- **Résolution plus rapide** : les dossiers de support des systèmes qui envoient des données AutoSupport sont résolus en deux fois moins de temps que ceux des systèmes qui n'envoient pas de données AutoSupport.
- **Mises à niveau plus rapides** : AutoSupport optimise les flux de travail en libre-service des clients, tels que les mises à niveau de version, les modules complémentaires, les renouvellements et l'automatisation des mises à jour de firmware dans System Manager.
- **Autres fonctions** : certaines fonctions d'autres outils ne fonctionnent que lorsque AutoSupport est activé, par exemple, certains flux de travail dans BlueXP.

### Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, sélectionnez , puis **Désactiver**.
3. Si vous souhaitez réactiver AutoSupport, dans la section **AutoSupport**, sélectionnez , puis **Activer**.

### Supprimez la génération des dossiers de demande de support

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour envoyer une demande à AutoSupport afin de supprimer la génération des dossiers de demande de support.


### Description de la tâche

Pour supprimer la génération de dossiers de demande de support, vous spécifiez les nœuds et le nombre d'heures pour lesquels la suppression doit avoir lieu.

La suppression de dossiers de demande de support peut être particulièrement utile si vous ne souhaitez pas que AutoSupport crée des dossiers automatisés pendant que vous effectuez la maintenance de vos systèmes.

### Étapes


1. Sélectionnez **Cluster > Paramètres**.

2. Dans la section **AutoSupport**, sélectionnez , puis **Supprimer la génération de cas de support**.
3. Saisissez le nombre d'heures pendant lesquelles vous souhaitez que la suppression se produise.
4. Sélectionnez les nœuds pour lesquels vous souhaitez que la suppression se produise.

#### Reprendre la génération des dossiers de demande de support

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour reprendre la génération d'demandes de support avec AutoSupport si elles ont été supprimées.



#### Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, sélectionnez , puis **reprendre la génération de cas de support**.
3. Sélectionnez les nœuds pour lesquels vous souhaitez que la génération reprenne.

#### Modifier les paramètres AutoSupport

System Manager permet de modifier les paramètres de connexion et de messagerie de votre compte AutoSupport.

#### Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, sélectionnez , puis **plus d'options**.
3. Dans la section **connexions** ou **Courriel**, sélectionnez  **Edit** pour modifier les paramètres de l'une ou l'autre section.

#### Supprimer la création de cas AutoSupport pendant les fenêtres de maintenance planifiées

La suppression de dossier AutoSupport vous permet d'arrêter la création de dossiers inutiles provenant de messages AutoSupport déclenchés lors des fenêtres de maintenance planifiées.

#### Étapes

1. Appelez manuellement un message AutoSupport avec la chaîne de texte `MAINT=xh`, où x correspond à la durée de la fenêtre de maintenance en heures. Remplacer <node> par le nom du nœud à partir duquel envoyer le message AutoSupport :

```
system node autosupport invoke -node <node> -message MAINT=xh
```

#### Informations associées

- ["Référence de commande ONTAP"](#)
- ["Comment supprimer la création automatique de dossier pendant les fenêtres de maintenance planifiées"](#)

## Téléchargez des fichiers à l'aide de AutoSupport

### Charger les fichiers core dump

Lorsqu'un fichier « core dump » est enregistré, un message d'événement est généré. Si



le service AutoSupport est activé et configuré pour envoyer des messages au support NetApp, un message AutoSupport est transmis, ainsi qu'un e-mail de confirmation automatique vous est envoyé.

### Ce dont vous avez besoin

- Vous devez avoir configuré AutoSupport avec les paramètres suivants :
  - AutoSupport est activé sur le nœud.
  - AutoSupport est configuré pour envoyer des messages au support technique.
  - AutoSupport est configuré pour utiliser le protocole de transport HTTP ou HTTPS.

Le protocole de transport SMTP n'est pas pris en charge lors de l'envoi de messages contenant des fichiers volumineux, tels que des fichiers de vidage de mémoire.

### Description de la tâche

Vous pouvez également charger le fichier « core dump » via le service AutoSupport via HTTPS en utilisant le `system node autosupport invoke-core-upload` Si le support NetApp en a besoin.

### "Télécharger un fichier vers NetApp"

#### Étapes

1. Afficher les fichiers « core dump » d'un nœud en utilisant le `system node coredump show` commande.

Dans l'exemple suivant, les fichiers « core dump » sont affichés pour le nœud local :

```
cluster1::> system node coredump show -node local
Node:Type Core Name Saved Panic Time

node:kernel
core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
```

2. Générez un message AutoSupport et téléchargez un fichier « core dump » à l'aide de `system node autosupport invoke-core-upload` commande.

Dans l'exemple suivant, un message AutoSupport est généré et envoyé à l'emplacement par défaut, qui est le support technique, et le fichier core dump est téléchargé vers l'emplacement par défaut, qui est le site du support NetApp :

```
cluster1::> system node autosupport invoke-core-upload -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

Dans l'exemple suivant, un message AutoSupport est généré et envoyé à l'emplacement spécifié dans l'URI, et le fichier core dump est chargé dans l'URI :

```
cluster1::> system node autosupport invoke-core-upload -uri
https://files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

## Téléchargez les fichiers d'archivage des performances

Vous pouvez générer et envoyer un message AutoSupport contenant un archivage des performances. Par défaut, le support technique NetApp reçoit le message AutoSupport, et l'archivage des performances est téléchargé sur le site du support NetApp. Vous pouvez spécifier une autre destination pour le message et le téléchargement.

### Ce dont vous avez besoin

- Vous devez avoir configuré AutoSupport avec les paramètres suivants :
  - AutoSupport est activé sur le nœud.
  - AutoSupport est configuré pour envoyer des messages au support technique.
  - AutoSupport est configuré pour utiliser le protocole de transport HTTP ou HTTPS.

Le protocole de transport SMTP n'est pas pris en charge lors de l'envoi de messages contenant des fichiers volumineux, tels que des fichiers d'archivage de performance.

### Description de la tâche

Vous devez spécifier une date de début pour les données d'archive de performances que vous souhaitez télécharger. La plupart des systèmes de stockage conservent des archives de performances pendant deux semaines. Vous pouvez ainsi spécifier une date de démarrage il y a deux semaines. Par exemple, si aujourd'hui est janvier 15, vous pouvez spécifier une date de début de janvier 2.

### Étape

1. Générez un message AutoSupport et téléchargez le fichier d'archivage des performances à l'aide de `system node autosupport invoke-performance-archive` commande.

Dans l'exemple suivant, 4 heures de fichiers d'archivage des performances date du 12 janvier 2015 sont ajoutés à un message AutoSupport et téléchargés sur l'emplacement par défaut, qui est le site de support NetApp :

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h
```

Dans l'exemple suivant, 4 heures de fichiers d'archive de performances à partir du 12 janvier 2015 sont ajoutés à un message AutoSupport et chargés à l'emplacement spécifié par l'URI :

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h -uri
https://files.company.com
```

## Résoudre les problèmes

### Dépanner AutoSupport lorsque les messages ne sont pas reçus

Si le système n'envoie pas le message AutoSupport, vous pouvez déterminer si c'est parce que AutoSupport ne peut pas générer le message ou ne peut pas le transmettre.

#### Étapes

1. Vérifiez l'état de transmission des messages à l'aide de `system node autosupport history show` commande.
2. Lire l'état.

| Ce statut                | Signifie                                                                                                                                                                                                                                                                                         |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| initialisation           | Le processus de collecte démarre. Si cet état est temporaire, tout est bien. Toutefois, si cet état persiste, il y a un problème.                                                                                                                                                                |
| echec de la collecte     | AutoSupport ne peut pas créer le contenu AutoSupport dans le répertoire spoule. Vous pouvez afficher ce que AutoSupport tente de collecter en entrant dans le <code>system node autosupport history show -detail</code> commande.                                                                |
| collecte en cours        | AutoSupport collecte du contenu AutoSupport. Vous pouvez afficher les données collectées par AutoSupport en entrant <code>system node autosupport manifest show</code> commande.                                                                                                                 |
| en file d'attente        | Les messages AutoSupport sont placés en file d'attente pour livraison, mais pas encore livrés.                                                                                                                                                                                                   |
| transmission             | AutoSupport fournit actuellement des messages.                                                                                                                                                                                                                                                   |
| envoi réussi             | AutoSupport a envoyé le message avec succès. Pour savoir où AutoSupport a envoyé le message, entrez la <code>system node autosupport history show -delivery</code> commande.                                                                                                                     |
| ignorer                  | AutoSupport n'a aucune destination pour le message. Vous pouvez afficher les détails de livraison en entrant le <code>system node autosupport history show -delivery</code> commande.                                                                                                            |
| mise en file d'attente   | AutoSupport a tenté de livrer des messages, mais la tentative a échoué. Par conséquent, AutoSupport a replacé les messages dans la file d'attente de livraison pour une autre tentative. Vous pouvez afficher l'erreur en entrant le <code>system node autosupport history show</code> commande. |
| transmission défectueuse | AutoSupport n'a pas réussi à transmettre le message le nombre spécifié de fois et a cessé d'essayer de le transmettre. Vous pouvez afficher l'erreur en entrant le <code>system node autosupport history show</code> commande.                                                                   |

| Ce statut       | Signifie                                                                                                     |
|-----------------|--------------------------------------------------------------------------------------------------------------|
| ondemand-ignore | Le message AutoSupport a été traité avec succès, mais le service AutoSupport OnDemand a choisi de l'ignorer. |

3. Effectuez l'une des opérations suivantes :

| Pour ce statut                                                         | Faites ça                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| échec de l'initialisation ou de la collecte                            | <p>Contactez le support NetApp, car AutoSupport ne peut pas générer le message. Mentionner l'article suivant de la base de connaissances :</p> <p><a href="#">"Échec de la livraison d'AutoSupport : l'état est bloqué en cours d'initialisation"</a></p> |
| échec de l'ignorer, de la mise en file d'attente ou de la transmission | Vérifiez que les destinations sont correctement configurées pour SMTP, HTTP ou HTTPS car AutoSupport ne peut pas transmettre le message.                                                                                                                  |

## Dépanner la distribution des messages AutoSupport via HTTP ou HTTPS

Si le système n'envoie pas le message AutoSupport attendu et que vous utilisez HTTP ou HTTPS ou si la fonction de mise à jour automatique ne fonctionne pas, vous pouvez vérifier un certain nombre de paramètres pour résoudre le problème.

### Ce dont vous avez besoin

Vous devez avoir confirmé la connectivité réseau de base et la recherche DNS :

- Votre LIF de node-management doit être active et administrative.
- Vous devez pouvoir envoyer une requête ping à un hôte opérationnel sur le même sous-réseau à partir de la LIF de gestion du cluster (il ne s'agit pas d'une LIF sur un des nœuds).
- Vous devez pouvoir envoyer des requêtes ping à un hôte opérationnel en dehors du sous-réseau à partir de la LIF de gestion du cluster.
- Vous devez pouvoir ping un hôte opérationnel hors du sous-réseau depuis la LIF de gestion du cluster utilisant le nom de l'hôte (pas l'adresse IP).

### Description de la tâche

Ces étapes sont pour les cas où vous avez déterminé que AutoSupport peut générer le message, mais que vous ne pouvez pas le transmettre via HTTP ou HTTPS.

Si vous rencontrez des erreurs ou si vous ne parvenez pas à effectuer une étape de cette procédure, déterminez et traitez le problème avant de passer à l'étape suivante.

### Étapes

1. Afficher l'état détaillé du sous-système AutoSupport :

```
system node autosupport check show-details
```

Cela inclut la vérification de la connectivité aux destinations AutoSupport via l'envoi de messages de test et la liste des erreurs possibles dans les paramètres de configuration de AutoSupport.

2. Vérifier l'état du LIF node management :

```
network interface show -home-node local -role node-mgmt -fields
vserver,lif,status-oper,status-admin,address,role
```

Le status-oper et status-admin les champs doivent retourner « up ».

3. Enregistrer le nom du SVM, le nom de la LIF et l'adresse IP de la LIF pour une utilisation ultérieure.

4. Assurez-vous que le DNS est activé et configuré correctement :

```
vserver services name-service dns show
```

5. Corriger toute erreur renvoyée par le message AutoSupport :

```
system node autosupport history show -node * -fields node,seq-
num,destination,last-update,status,error
```

Pour obtenir de l'aide sur le dépannage des erreurs renvoyées, reportez-vous au ["Guide de résolution ONTAP AutoSupport \(transport HTTPS et HTTP\)"](#).

6. Vérifiez que le cluster peut accéder aux serveurs dont il a besoin et à Internet :

a. `network traceroute -lif node-management_LIF -destination DNS server`

b. `network traceroute -lif node_management_LIF -destination support.netapp.com`



L'adresse `support.netapp.com` elle-même ne répond pas à la commande ping/traceroute, mais l'information par saut est utile.

c. `system node autosupport show -fields proxy-url`

d. `network traceroute -node node_management_LIF -destination proxy_url`

Si l'une de ces routes ne fonctionne pas, essayez la même route à partir d'un hôte en fonctionnement sur le même sous-réseau que le cluster, en utilisant l'utilitaire « traceroute » ou « tracert » situé sur la plupart des clients réseau tiers. Cela vous aide à déterminer si le problème se situe dans votre configuration réseau ou dans votre configuration de cluster.

7. Si vous utilisez HTTPS pour votre protocole de transport AutoSupport, assurez-vous que le trafic HTTPS peut quitter le réseau :

a. Configurez un client web sur le même sous-réseau que la LIF de gestion du cluster.

Assurez-vous que tous les paramètres de configuration sont les mêmes que pour la configuration AutoSupport, y compris en utilisant le même serveur proxy, le même nom d'utilisateur, le même mot de passe et le même port.

b. L'accès `https://support.netapp.com` avec le client web.

L'accès doit être réussi. Si ce n'est pas le cas, assurez-vous que tous les pare-feu sont correctement configurés pour autoriser le trafic HTTPS et DNS et que le serveur proxy est configuré correctement. Pour plus d'informations sur la configuration de la résolution statique des noms pour

support.netapp.com, consultez l'article de la base de connaissances "[Comment ajouter une entrée D'HÔTE dans ONTAP pour support.netapp.com?](#)"

8. Depuis ONTAP 9.10.1, si vous avez activé la fonction mise à jour automatique, assurez-vous que vous disposez de la connectivité HTTPS aux URL supplémentaires suivantes :

- <https://support-sg-emea.netapp.com>
- <https://support-sg-naeast.netapp.com>
- <https://support-sg-nawest.netapp.com>

## Dépanner la transmission des messages AutoSupport via SMTP

Si le système ne parvient pas à transmettre les messages AutoSupport via SMTP, vous pouvez vérifier un certain nombre de paramètres pour résoudre le problème.

### Ce dont vous avez besoin

Vous devez avoir confirmé la connectivité réseau de base et la recherche DNS :

- Votre LIF de node-management doit être active et administrative.
- Vous devez pouvoir envoyer une requête ping à un hôte opérationnel sur le même sous-réseau à partir de la LIF de gestion du cluster (il ne s'agit pas d'une LIF sur un des nœuds).
- Vous devez pouvoir envoyer des requêtes ping à un hôte opérationnel en dehors du sous-réseau à partir de la LIF de gestion du cluster.
- Vous devez pouvoir ping un hôte opérationnel hors du sous-réseau depuis la LIF de gestion du cluster utilisant le nom de l'hôte (pas l'adresse IP).

### Description de la tâche

Ces étapes sont destinées aux cas où vous avez déterminé que AutoSupport peut générer le message, mais ne peut pas le transmettre via SMTP.

Si vous rencontrez des erreurs ou si vous ne parvenez pas à effectuer une étape de cette procédure, déterminez et traitez le problème avant de passer à l'étape suivante.

Toutes les commandes sont saisies au niveau de l'interface de ligne de commandes ONTAP, sauf indication contraire.

### Étapes

1. Vérifier l'état du LIF node management :

```
network interface show -home-node local -role node-mgmt -fields
vservers,lif,status-oper,status-admin,address,role
```

Le status-oper et status-admin vous devriez y retourner up.

2. Enregistrer le nom du SVM, le nom de la LIF et l'adresse IP de la LIF pour une utilisation ultérieure.

3. Assurez-vous que le DNS est activé et configuré correctement :

```
vservers services name-service dns show
```

4. Afficher tous les serveurs configurés pour être utilisés par AutoSupport :

```
system node autosupport show -fields mail-hosts
```

Enregistrer tous les noms de serveur affichés.

5. Pour chaque serveur affiché par l'étape précédente, et `support.netapp.com`, Assurez-vous que le serveur ou l'URL peut être atteint par le noeud :

```
network traceroute -node local -destination server_name
```

Si l'une de ces routes ne fonctionne pas, essayez la même route à partir d'un hôte en fonctionnement sur le même sous-réseau que le cluster, en utilisant l'utilitaire « traceroute » ou « tracert » situé sur la plupart des clients réseau tiers. Cela vous aide à déterminer si le problème se situe dans votre configuration réseau ou dans votre configuration de cluster.

6. Connectez-vous à l'hôte désigné comme hôte de messagerie et assurez-vous qu'il peut traiter les demandes SMTP :

```
netstat -aAn|grep 25
```

25 Est le numéro de port SMTP du port d'écoute.

Un message similaire au texte suivant s'affiche :

```
ff64878c tcp 0 0 *.25 *.* LISTEN.
```

7. À partir d'un autre hôte, ouvrez une session Telnet avec le port SMTP de l'hôte de messagerie :

```
telnet mailhost 25
```

Un message similaire au texte suivant s'affiche :

```
220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
10:49:04 PST
```

8. À l'invite telnet, assurez-vous qu'un message peut être relayé depuis votre hôte de messagerie :

```
HELO domain_name
```

```
MAIL FROM: your_email_address
```

```
RCPT TO: autosupport@netapp.com
```

`domain_name` est le nom de domaine de votre réseau.

Si une erreur est renvoyée indiquant que la retransmission est refusée, la retransmission n'est pas activée sur l'hôte de messagerie. Contactez votre administrateur système.

9. À l'invite telnet, envoyez un message de test :

```
DATA
```

**SUBJECT: TESTING**

**THIS IS A TEST**

.



Assurez-vous d'entrer la dernière période (.) sur une ligne par elle-même. La période indique à l'hôte de messagerie que le message est terminé.

Si une erreur est renvoyée, votre hôte de messagerie n'est pas configuré correctement. Contactez votre administrateur système.

10. À partir de l'interface de ligne de commande ONTAP, envoyez un message de test AutoSupport à une adresse e-mail de confiance à laquelle vous avez accès :

```
system node autosupport invoke -node local -type test
```

11. Recherchez le numéro de séquence de la tentative :

```
system node autosupport history show -node local -destination smtp
```

Recherchez le numéro de séquence de votre tentative en fonction de l'horodatage. C'est probablement la tentative la plus récente.

12. Afficher l'erreur de votre tentative de message de test :

```
system node autosupport history show -node local -seq-num seq_num -fields error
```

Si l'erreur affichée est de `Login denied`, Votre serveur SMTP n'accepte pas les requêtes d'envoi de la LIF de gestion du cluster. Si vous ne souhaitez pas passer à utiliser HTTPS comme protocole de transport, contactez votre administrateur réseau de site pour configurer les passerelles SMTP afin de résoudre ce problème.

Si ce test réussit mais que le même message envoyé à `mailto:autosupport@netapp.com` ne le fait pas, assurez-vous que le relais SMTP est activé sur tous vos hôtes de messagerie SMTP ou utilisez HTTPS comme protocole de transport.

Si même le message du compte de messagerie géré localement ne fonctionne pas, vérifiez que vos serveurs SMTP sont configurés pour transférer les pièces jointes avec les deux caractéristiques suivantes :

- Le suffixe « 7z »
- Le type MIME « application/x-7X-compressé ».

## Dépanner le sous-système AutoSupport

Le `system node check show` Les commandes permettent de vérifier et de résoudre tous les problèmes liés à la configuration et à la livraison de AutoSupport.

### Étape

1. Utiliser les commandes suivantes pour afficher l'état du sous-système AutoSupport.



| Utilisez cette commande...                              | Pour cela...                                                                                                                                                                                                       |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>system node autosupport check show</code>         | Affiche l'état général du sous-système AutoSupport, tel que l'état de la destination AutoSupport HTTP ou HTTPS, les destinations SMTP AutoSupport, le serveur AutoSupport OnDemand et la configuration AutoSupport |
| <code>system node autosupport check show-details</code> | Affiche l'état détaillé du sous-système AutoSupport, notamment des descriptions détaillées des erreurs et des actions correctives                                                                                  |

## Contrôle de l'état du système

### Surveillez l'état de santé de votre système

Cette fonction surveille de manière proactive certaines conditions critiques du cluster et déclenche des alertes en cas de défaillance ou de risque. Si des alertes sont actives, l'état de l'état du système signale un état dégradé pour le cluster. Les alertes incluent les informations dont vous avez besoin pour répondre à la dégradation de l'état du système.

Si l'état est dégradé, vous pouvez afficher des détails sur le problème, y compris la cause probable et les actions de récupération recommandées. Une fois le problème résolu, l'état de l'état du système revient automatiquement à OK.

L'état de l'état du système reflète plusieurs moniteurs d'état distincts. Un état dégradé au sein d'un moniteur d'état entraîne un état dégradé pour l'état global du système.

Pour plus de détails sur la prise en charge des commutateurs de cluster par ONTAP pour le contrôle de l'état du système dans votre cluster, reportez-vous au *Hardware Universe*.

["Commutateurs pris en charge dans le Hardware Universe"](#)

Pour plus d'informations sur les causes des messages AutoSupport du moniteur d'intégrité des commutateurs de cluster (CSHM) et sur les actions nécessaires pour résoudre ces alertes, consultez l'article de la base de connaissances.

["Message AutoSupport : processus de surveillance de l'état CSHM"](#)

### Fonctionnement de la surveillance de l'état

Les moniteurs de santé individuels disposent d'un ensemble de règles qui déclenchent des alertes lorsque certaines conditions se produisent. Comprendre le fonctionnement de la surveillance de l'état de santé peut vous aider à résoudre les problèmes et à contrôler les alertes futures.

La surveillance de l'état des systèmes comprend les composants suivants :

- Chaque état de santé surveille pour des sous-systèmes spécifiques, chacun ayant son propre état d'intégrité

Par exemple, le sous-système de stockage dispose d'un contrôle de l'état de la connectivité des nœuds.

- Un contrôle de l'état global du système qui consolide l'état d'intégrité des différents moniteurs de santé

Un état dégradé dans un seul sous-système entraîne un état dégradé pour tout le système. Si aucun sous-système n'a d'alertes, l'état global du système est OK.

Chaque contrôle de l'état est constitué des éléments clés suivants :

- Alertes que le contrôle de l'état peut potentiellement générer

Chaque alerte a une définition, qui inclut des détails tels que la gravité de l'alerte et sa cause probable.

- Règles de santé qui identifient quand chaque alerte est déclenchée

Chaque règle de santé dispose d'une expression de règle, qui est la condition ou la modification exacte qui déclenche l'alerte.

Un contrôle de l'état surveille et valide en permanence les ressources de son sous-système à des fins de modification de l'état ou des conditions. Lorsqu'une condition ou une modification d'état correspond à une expression de règle dans une politique de santé, le contrôle de l'état génère une alerte. Une alerte provoque l'état de l'état de santé du sous-système et l'état global de l'intégrité du système.

## Moyens de répondre aux alertes d'intégrité du système

Lorsqu'une alerte d'intégrité du système se produit, vous pouvez la valider, en savoir plus sur celui-ci, réparer l'état sous-jacent et éviter qu'elle ne se reproduise.

Lorsqu'un contrôle de l'état soulève une alerte, vous pouvez répondre de l'une des manières suivantes :

- Obtenez des informations sur l'alerte, qui inclut la ressource affectée, la gravité de l'alerte, la cause probable, l'effet possible et les actions correctives.
- Obtenez des informations détaillées sur l'alerte, telles que l'heure à laquelle l'alerte a été générée et si quelqu'un d'autre a déjà reconnu l'alerte.
- Consultez les informations relatives à l'état de la ressource ou du sous-système affecté, par exemple un tiroir ou un disque spécifique.
- Reconnaissez l'alerte pour indiquer qu'une personne travaille sur le problème et identifiez-vous comme « vérificateur ».
- Résolvez le problème en prenant les mesures correctives fournies dans l'alerte, telles que la résolution du câblage pour résoudre un problème de connectivité.
- Supprimez l'alerte si le système ne l'a pas supprimée automatiquement.
- Supprimez une alerte pour l'empêcher d'affecter l'état de santé d'un sous-système.

La suppression est utile lorsque vous comprenez un problème. Après avoir supprimé une alerte, elle peut toujours se produire, mais l'état de santé du sous-système s'affiche sous la forme « ok-avec-supprimé » lorsque l'alerte supprimée se produit.

## Personnalisation des alertes d'intégrité du système

Vous pouvez contrôler les alertes qu'un contrôle de l'état génère en activant et en

désactivant les politiques d'intégrité du système qui définissent lorsque les alertes sont déclenchées. Cela vous permet de personnaliser le système de surveillance de l'état de santé pour votre environnement particulier.

Pour connaître le nom d'une règle, vous pouvez afficher des informations détaillées sur une alerte générée ou afficher les définitions de règles pour un contrôle de l'état, un nœud ou un ID d'alerte spécifique.

La désactivation des politiques de santé est différente de la suppression des alertes. Lorsque vous supprimez une alerte, elle n'a pas d'impact sur l'état de santé du sous-système, mais l'alerte peut toujours se produire.

Si vous désactivez une règle, la condition ou l'état défini dans son expression de règle de gestion ne déclenche plus d'alerte.

### **Exemple d'alerte que vous souhaitez désactiver**

Par exemple, supposons qu'une alerte ne vous soit pas utile. Vous utilisez le `system health alert show -instance` Commande pour obtenir l'ID de la règle pour l'alerte. Vous utilisez l'ID de la police dans le `system health policy definition show` commande pour afficher les informations relatives à la règle. Après avoir vérifié l'expression de règle et d'autres informations sur la stratégie, vous décidez de la désactiver. Vous utilisez le `system health policy definition modify` commande pour désactiver la règle.

## **Le mode d'alerte de santé déclenche des messages et des événements AutoSupport**

Les alertes d'intégrité du système déclenchent des messages AutoSupport et des événements dans le système de gestion des événements (EMS), ce qui vous permet de surveiller l'état du système à l'aide des messages AutoSupport et du système EMS en plus d'utiliser directement le système de contrôle de l'état.

Votre système envoie un message AutoSupport dans les cinq minutes qui suivent une alerte. Le message AutoSupport inclut toutes les alertes générées depuis le message AutoSupport précédent, à l'exception des alertes qui dupliquent une alerte pour la même ressource et la même cause probable au cours de la semaine précédente.

Certaines alertes ne déclenchent pas de messages AutoSupport. Une alerte ne déclenche pas de message AutoSupport si sa politique d'intégrité désactive l'envoi de messages AutoSupport. Par exemple, une politique de santé peut désactiver les messages AutoSupport par défaut, car AutoSupport génère déjà un message lorsque le problème se produit. Vous pouvez configurer des règles pour ne pas déclencher de messages AutoSupport à l'aide de `system health policy definition modify` commande.

Vous pouvez afficher la liste de tous les messages AutoSupport déclenchés par les alertes envoyés au cours de la semaine précédente à l'aide du `system health autosupport trigger history show` commande.

Les alertes déclenchent également la génération d'événements au SGE. Un événement est généré chaque fois qu'une alerte est créée et chaque fois qu'une alerte est effacée.

## **Contrôles disponibles de l'état du cluster**

Plusieurs moniteurs d'état permettent de surveiller différentes parties d'un cluster. Les contrôles d'état vous aident à corriger des erreurs au sein des systèmes ONTAP en détectant des événements, en vous envoyant des alertes et en supprimant les

événements tels qu'ils sont clairs.

| Nom du contrôle de l'état (identifiant)        | Nom du sous-système (identifiant)                                                                                                         | Objectif                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Commutateur du cluster(commutateur du cluster) | Commutateur (commutateur - état)                                                                                                          | <p>Surveille les commutateurs du réseau de cluster et les commutateurs du réseau de gestion en termes de température, d'utilisation, de configuration des interfaces, de redondance (commutateurs du réseau de cluster uniquement), et de fonctionnement des ventilateurs et de l'alimentation. Le contrôle de l'état du commutateur de cluster communique avec les commutateurs via SNMP. SNMPv2c est le paramètre par défaut.</p> <div>  <p>Depuis ONTAP 9.2, ce moniteur peut détecter et signaler le redémarrage d'un commutateur de cluster depuis la dernière période d'interrogation.</p> </div> |
| Structure MetroCluster                         | Commutateur                                                                                                                               | Surveille la topologie de la configuration MetroCluster back-end de la structure et détecte les erreurs de configuration, comme le câblage et la segmentation incorrects ou les défaillances ISL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| État de santé du MetroCluster                  | Interconnexion, RAID et stockage                                                                                                          | Surveille les adaptateurs FC-VI, les adaptateurs d'initiateurs FC, les agrégats et disques situés derrière le côté gauche et les ports d'intercluster                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Connectivité nœud(nœud-Connect)                | Continuité de l'activité CIFS                                                                                                             | Surveille les connexions SMB afin de garantir la continuité de l'activité aux applications Hyper-V.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Stockage (SAS-Connect)                         | Surveille les tiroirs, les disques et les adaptateurs au niveau du nœud pour s'assurer que les chemins et les connexions sont appropriés. | Système                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Nom du contrôle de l'état (identifiant) | Nom du sous-système (identifiant)                       | Objectif                              |
|-----------------------------------------|---------------------------------------------------------|---------------------------------------|
| sans objet                              | Rassemble les informations d'autres moniteurs de santé. | Connectivité système (system-Connect) |

## Recevez automatiquement les alertes d'état du système

Vous pouvez afficher manuellement les alertes d'état du système en utilisant le `system health alert show` commande. Vous devez toutefois vous abonner à des messages EMS pour recevoir automatiquement des notifications lorsqu'un contrôle de l'état génère une alerte.

### Description de la tâche

La procédure suivante vous indique comment configurer les notifications pour tous les messages `hm.Alert.déclenché` et pour tous les messages `hm.Alert.effacé`.

Tous les messages `hm.Alert.déclenché` et tous les messages `hm.Alert.décoché` comprennent une interruption SNMP. Les noms des traps SNMP sont `HealthMonitorAlertRaised` et `HealthMonitorAlertCleared`. Pour plus d'informations sur les interruptions SNMP, consultez le *Network Management Guide*.

### Étapes

1. Utilisez le `event destination create` Commande pour définir la destination à laquelle vous souhaitez envoyer les messages EMS.

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. Utilisez le `event route add-destinations` commande permettant d'acheminer le `hm.alert.raised` message et le `hm.alert.cleared` message vers une destination.

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

### Informations associées

["Gestion du réseau"](#)

## Répondez à la dégradation de l'état du système

Lorsque l'état de santé de votre système est dégradé, vous pouvez afficher des alertes, lire les informations sur la cause probable et les actions correctives, afficher des informations sur le sous-système dégradé et résoudre le problème. Les alertes supprimées s'affichent également pour vous permettre de les modifier et de vérifier si elles ont été acquittées.

### Description de la tâche

Vous pouvez découvrir qu'une alerte a été générée en visualisant un message AutoSupport ou un événement EMS, ou en utilisant le `system health` commandes.

## Étapes

1. Utilisez le `system health alert show` commande pour afficher les alertes qui compromettre l'intégrité du système
2. Lisez la cause probable, l'effet possible et les actions correctives de l'alerte pour déterminer si vous pouvez résoudre le problème ou si vous avez besoin d'informations supplémentaires.
3. Si vous avez besoin de plus d'informations, utilisez le `system health alert show -instance` pour afficher les informations supplémentaires disponibles pour l'alerte.
4. Utilisez le `system health alert modify` commande avec `-acknowledge` paramètre pour indiquer que vous travaillez sur une alerte spécifique.
5. Prendre des mesures correctives pour résoudre le problème comme décrit dans le `Corrective Actions` champ dans l'alerte.

Les actions correctives peuvent inclure le redémarrage du système.

Une fois le problème résolu, l'alerte est automatiquement effacée. Si le sous-système n'a pas d'autres alertes, l'intégrité du sous-système devient OK. Si l'intégrité de tous les sous-systèmes est correcte, l'état d'intégrité globale du système passe à OK.

6. Utilisez le `system health status show` commande pour vérifier que l'état de l'intégrité du système est OK.

Si l'état de l'état de santé du système n'est pas OK, répéter cette procédure.

## Exemple de réponse à une dégradation de l'état du système

En examinant un exemple spécifique de l'état du système dégradé après un tiroir qui manque deux chemins d'accès à un nœud, vous pouvez voir ce que l'interface de ligne de commandes affiche lorsque vous répondez à une alerte.

Après avoir démarré ONTAP, vous vérifiez l'état du système et vous découvrez que son état est dégradé :

```
cluster1::>system health status show
Status

degraded
```

Vous affichez les alertes pour déterminer l'emplacement du problème et vous voyez que le tiroir 2 n'a pas deux chemins d'accès au nœud 1 :

```
cluster1::>system health alert show
 Node: node1
 Resource: Shelf ID 2
 Severity: Major
 Indication Time: Mon Nov 10 16:48:12 2013
 Probable Cause: Disk shelf 2 does not have two paths to controller
 node1.
 Possible Effect: Access to disk shelf 2 via controller node1 will be
 lost with a single hardware component failure (e.g.
 cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
 to disk shelf 2.
 2. Connect disk shelf 2 to controller node1 via two
 paths following the rules in the Universal SAS and ACP Cabling Guide.
 3. Reboot the halted controllers.
 4. Contact support personnel if the alert persists.
```

Vous affichez des informations détaillées sur l'alerte pour obtenir plus d'informations, notamment l'ID d'alerte :

```

cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
 Node: node1
 Monitor: node-connect
 Alert ID: DualPathToDiskShelf_Alert
 Alerting Resource: 50:05:0c:c1:02:00:0f:02
 Subsystem: SAS-connect
 Indication Time: Mon Mar 21 10:26:38 2011
 Perceived Severity: Major
 Probable Cause: Connection_establishment_error
 Description: Disk shelf 2 does not have two paths to controller
node1.
 Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
 2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
 3. Reboot the halted controllers.
 4. Contact support personnel if the alert
persists.
 Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
 Acknowledge: false
 Suppress: false
 Policy: DualPathToDiskShelf_Policy
 Acknowledger: -
 Suppressor: -
 Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
 Shelf id: 2
 Shelf Name: 4d.shelf2
 Number of Paths: 1
 Number of Disks: 6
 Adapter connected to IOMA:
 Adapter connected to IOMB: 4d
 Alerting Resource Name: Shelf ID 2

```

Vous reconnaissez l'alerte pour indiquer que vous y travaillez.

```

cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true

```

Vous avez résolu le câblage entre le tiroir 2 et le nœud 1, puis redémarré le système. Ensuite, vous vérifiez de nouveau l'état du système et voyez que son état est OK:



```
cluster1::>system health status show
Status

OK
```

## Configurer la détection des commutateurs du réseau de gestion et du cluster

Le contrôle de l'état du switch de cluster tente automatiquement de détecter les commutateurs du réseau de gestion et de cluster à l'aide du protocole CDP (Cisco Discovery Protocol). Vous devez configurer le contrôle de l'état s'il ne peut pas détecter automatiquement un switch ou si vous ne souhaitez pas utiliser CDP pour la découverte automatique.

### Description de la tâche

Le `system cluster-switch show` la commande répertorie les switchs détectés par le contrôle de l'état. Si vous ne voyez pas de commutateur que vous aviez prévu dans cette liste, le contrôle de l'état ne peut pas le détecter automatiquement.

### Étapes

1. Si vous souhaitez utiliser CDP pour la découverte automatique, procédez comme suit :

- a. Assurez-vous que le Cisco Discovery Protocol (CDP) est activé sur vos commutateurs.

Reportez-vous à la documentation de votre commutateur pour obtenir des instructions.

- b. Exécutez la commande suivante sur chaque nœud du cluster pour vérifier si CDP est activée ou désactivée :

```
run -node node_name -command options cdpd.enable
```

Si CDP est activé, passez à l'étape d. Si le CDP est désactivé, passez à l'étape c.

- c. Exécutez la commande suivante pour activer CDP :

```
run -node node_name -command options cdpd.enable on
```

Attendez cinq minutes avant de passer à l'étape suivante.

- a. Utilisez le `system cluster-switch show` Commande pour vérifier si ONTAP peut désormais détecter automatiquement les commutateurs.

2. Si le contrôle de l'état ne peut pas détecter automatiquement un commutateur, utilisez le `system cluster-switch create` commande pour configurer la découverte du commutateur :

```
cluster1::> system cluster-switch create -device switch1 -address
192.0.2.250 -snmp-version SNMPv2c -community cshml! -model NX5020 -type
cluster-network
```

Attendez cinq minutes avant de passer à l'étape suivante.

3. Utilisez le `system cluster-switch show` Commande pour vérifier que ONTAP peut détecter le switch pour lequel vous avez ajouté des informations.

### Une fois que vous avez terminé

Vérifiez que le contrôle de l'état peut surveiller vos commutateurs.

## Vérifier la surveillance du cluster et des commutateurs du réseau de gestion

Le contrôle de l'état du commutateur de cluster tente automatiquement de surveiller les commutateurs qu'il détecte ; toutefois, la surveillance peut ne pas se produire automatiquement si les commutateurs ne sont pas configurés correctement. Vérifiez que le contrôle de l'état est correctement configuré pour surveiller les commutateurs.

### Étapes

1. Pour identifier les switchs détectés par le contrôle de l'état du commutateur de cluster, entrez la commande suivante :

#### ONTAP 9.8 et versions ultérieures

```
system switch ethernet show
```

#### ONTAP 9.7 et versions antérieures

```
system cluster-switch show
```

Si le `Model` affiche la valeur `OTHER`, ONTAP ne peut pas surveiller le commutateur. ONTAP définit la valeur sur `OTHER` si un commutateur qu'il détecte automatiquement n'est pas pris en charge pour le contrôle de l'état de santé.



Si un commutateur ne s'affiche pas dans la sortie de la commande, vous devez configurer la détection du commutateur.

2. Effectuez une mise à niveau vers la dernière version du logiciel de commutateur pris en charge et consultez le fichier de configuration (RCF) disponible sur le site de support NetApp.

### ["Page des téléchargements du support NetApp"](#)

La chaîne de communauté dans le RCF du commutateur doit correspondre à la chaîne de communauté que le moniteur d'état est configuré pour utiliser. Par défaut, le contrôle de l'état utilise la chaîne de communauté `cshml` !.



Actuellement, le moniteur de santé ne prend en charge que SNMPv2.

Si vous avez besoin de modifier les informations concernant un commutateur que le cluster surveille, vous pouvez modifier la chaîne de communauté utilisée par le contrôle de l'état à l'aide de la commande suivante :

**ONTAP 9.8 et versions ultérieures**

```
system switch ethernet modify
```

**ONTAP 9.7 et versions antérieures**

```
system cluster-switch modify
```

3. Vérifiez que le port de gestion du commutateur est connecté au réseau de gestion.

Cette connexion est requise pour exécuter des requêtes SNMP.

## Commandes permettant de contrôler l'état de santé de votre système

Vous pouvez utiliser le `system health` commandes permettant d'afficher des informations relatives à l'état de santé des ressources système, de répondre aux alertes et de configurer les alertes futures. L'utilisation des commandes de l'interface de ligne de commandes vous permet d'afficher des informations détaillées sur la configuration de la surveillance de l'état. Les pages de manuels des commandes contiennent plus d'informations.

### Affiche l'état de l'état de santé du système

| Les fonctions que vous recherchez...                                                                | Utilisez cette commande...                |
|-----------------------------------------------------------------------------------------------------|-------------------------------------------|
| Affiche l'état de santé du système, qui reflète l'état global des moniteurs d'intégrité individuels | <code>system health status show</code>    |
| Affiche l'état d'intégrité des sous-systèmes pour lesquels la surveillance de l'état est disponible | <code>system health subsystem show</code> |

### Affiche l'état de la connectivité du nœud

| Les fonctions que vous recherchez...                                                                                                                                                                                    | Utilisez cette commande...                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Affiche des informations détaillées sur la connectivité du nœud au tiroir de stockage, notamment les informations relatives aux ports, la vitesse du port HBA, le débit d'E/S et le taux d'opérations d'E/S par seconde | <code>storage shelf show -connectivity</code><br><br>Utilisez le <code>-instance</code> paramètre pour afficher des informations détaillées sur chaque tiroir. |
| Affiche des informations sur les disques et les LUN de baie, y compris l'espace utilisable, les numéros de tiroir et de compartiment, ainsi que le nom de nœud propriétaire                                             | <code>storage disk show</code><br><br>Utilisez le <code>-instance</code> paramètre pour afficher des informations détaillées sur chaque lecteur.               |

| Les fonctions que vous recherchez...                                                                                       | Utilisez cette commande...                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Affiche des informations détaillées sur les ports des tiroirs de stockage, notamment le type de port, la vitesse et l'état | <pre>storage port show</pre> <p>Utilisez le <code>-instance</code> paramètre pour afficher des informations détaillées sur chaque adaptateur.</p> |

## Gérer la détection des commutateurs de cluster, de stockage et de réseau de gestion

| Les fonctions que vous recherchez...                                                                                                                                                                                                                                                                                                                                                          | Utilisez cette commande.<br>(ONTAP 9.8 et versions ultérieures) | Utilisez cette commande.<br>(ONTAP 9.7 et versions antérieures) |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|-----------------------------------------------------------------|
| Afficher les commutateurs surveillés par le bloc d'instruments                                                                                                                                                                                                                                                                                                                                | <pre>system switch ethernet show</pre>                          | <pre>system cluster-switch show</pre>                           |
| Afficher les commutateurs actuellement surveillés par le cluster, notamment les commutateurs que vous avez supprimés (indiqués dans la colonne raison de la sortie de la commande) et les informations de configuration dont vous avez besoin pour accéder au réseau au cluster et aux commutateurs du réseau de gestion.<br><br>Cette commande est disponible au niveau de privilège avancé. | <pre>system switch ethernet show-all</pre>                      | <pre>system cluster-switch show-all</pre>                       |
| Configurer la détection d'un commutateur non découvert                                                                                                                                                                                                                                                                                                                                        | <pre>system switch ethernet create</pre>                        | <pre>system cluster-switch create</pre>                         |
| Modifier les informations relatives à un commutateur que le cluster surveille (par exemple, nom de périphérique, adresse IP, version SNMP et chaîne de communauté)                                                                                                                                                                                                                            | <pre>system switch ethernet modify</pre>                        | <pre>system cluster-switch modify</pre>                         |
| Désactiver la surveillance d'un commutateur                                                                                                                                                                                                                                                                                                                                                   | <pre>system switch ethernet modify -disable-monitoring</pre>    | <pre>system cluster-switch modify -disable-monitoring</pre>     |
| Désactiver la détection et la surveillance d'un commutateur et supprimer les informations de configuration du commutateur                                                                                                                                                                                                                                                                     | <pre>system switch ethernet delete</pre>                        | <pre>system cluster-switch delete</pre>                         |

| Les fonctions que vous recherchez...                                                                                                                                            | Utilisez cette commande.<br>(ONTAP 9.8 et versions ultérieures) | Utilisez cette commande.<br>(ONTAP 9.7 et versions antérieures) |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|-----------------------------------------------------------------|
| Supprimez définitivement les informations de configuration du commutateur stockées dans la base de données (ce qui permet de réactiver la détection automatique du commutateur) | <code>system switch ethernet delete -force</code>               | <code>system cluster-switch delete -force</code>                |
| Activez la journalisation automatique pour envoyer des messages AutoSupport.                                                                                                    | <code>system switch ethernet log</code>                         | <code>system cluster-switch log</code>                          |




## Répondez aux alertes générées

| Les fonctions que vous recherchez...                                                                                                                                                | Utilisez cette commande...                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| Affiche des informations sur les alertes générées, telles que la ressource et le nœud où l'alerte a été déclenchée, ainsi que la gravité et la cause probable de l'alerte           | <code>system health alert show</code>                       |
| Affiche des informations sur chaque alerte générée                                                                                                                                  | <code>system health alert show -instance</code>             |
| Indique que quelqu'un travaille sur une alerte                                                                                                                                      | <code>system health alert modify</code>                     |
| Accuser réception d'une alerte                                                                                                                                                      | <code>system health alert modify -acknowledge</code>        |
| Supprimez une alerte ultérieure afin qu'elle n'affecte pas l'état de santé d'un sous-système                                                                                        | <code>system health alert modify -suppress</code>           |
| Supprimez une alerte qui n'a pas été automatiquement effacée                                                                                                                        | <code>system health alert delete</code>                     |
| Affiche des informations sur les messages AutoSupport qui déclenchent les alertes la semaine dernière, par exemple pour déterminer si une alerte a déclenché un message AutoSupport | <code>system health autosupport trigger history show</code> |

## Configurez les alertes futures

| Les fonctions que vous recherchez...                                                                        | Utilisez cette commande...                          |
|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Activez ou désactivez la règle qui contrôle si un état de ressource spécifique génère une alerte spécifique | <code>system health policy definition modify</code> |

## Affiche des informations sur la configuration de la surveillance de l'état

| Les fonctions que vous recherchez...                                                                                          | Utilisez cette commande...                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Affiche des informations relatives aux contrôles d'état, telles que leurs nœuds, leurs noms, leurs sous-systèmes et leur état | <pre>system health config show</pre> <div> Utilisez le <code>-instance</code> paramètre pour afficher des informations détaillées sur chaque contrôle de l'état.</div>                                                                                                                                                           |
| Affiche des informations sur les alertes qu'un contrôle de l'état peut générer                                                | <pre>system health alert definition show</pre> <div> Utilisez le <code>-instance</code> paramètre pour afficher des informations détaillées sur chaque définition d'alerte.</div>                                                                                                                                                |
| Affiche des informations sur les règles de contrôle de l'état, qui déterminent l'heure à laquelle les alertes sont émises     | <pre>system health policy definition show</pre> <div> Utilisez le <code>-instance</code> paramètre pour afficher des informations détaillées sur chaque règle. Utilisez d'autres paramètres pour filtrer la liste des alertes, par exemple en fonction de l'état (activé ou non), du contrôle de l'état, de l'alerte, etc.</div> |

## Affiche des informations environnementales

Les capteurs vous aident à surveiller les composants environnementaux de votre système. Les informations que vous pouvez afficher concernant les capteurs environnementaux incluent leur type, leur nom, leur état, leur valeur et les avertissements de seuil.

### Étape

1. Pour afficher des informations sur les capteurs environnementaux, utilisez le `system node environment sensors show` commande.

## Analytique du système de fichiers

### Présentation de l'analytique du système de fichiers

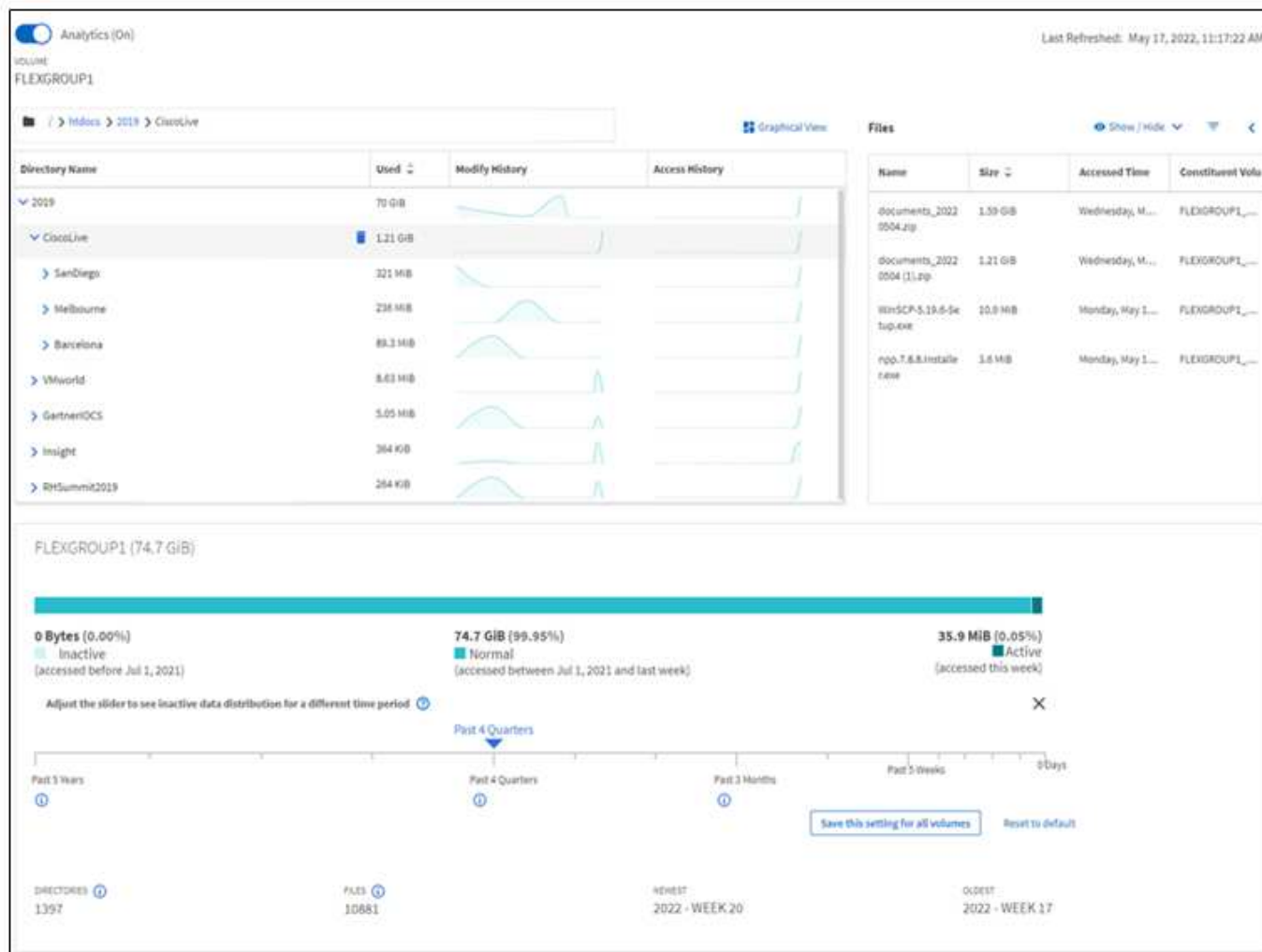
Le service File System Analytics (FSA) a été intégré à ONTAP 9.8 pour fournir une visibilité en temps réel sur l'utilisation des fichiers et les tendances en matière de capacité de stockage au sein des volumes ONTAP FlexGroup ou FlexVol. Cette fonctionnalité native élimine la nécessité de disposer d'outils externes et fournit des informations essentielles sur l'utilisation du stockage et sur les possibilités d'optimisation du stockage en fonction des besoins de l'entreprise.

Avec FSA, vous disposez d'une visibilité à tous les niveaux de la hiérarchie du système de fichiers d'un volume dans NAS. Par exemple, vous pouvez obtenir des informations sur l'utilisation et la capacité au niveau des VM de stockage (SVM), des volumes, des répertoires et des fichiers. Ce compte vous permet de répondre à des questions telles que :

- Qu'est-ce qui remplit mon système de stockage et y a-t-il des fichiers volumineux que je peux déplacer vers un autre emplacement de stockage ?
- Quels sont mes volumes, répertoires et fichiers les plus actifs ? Mes performances de stockage sont-elles optimisées pour répondre aux besoins de mes utilisateurs ?
- Quelle quantité de données ont été ajoutées au mois dernier ?
- Qui sont mes utilisateurs de stockage les plus actifs ou les moins actifs ?
- Quel est le volume de données inactives ou inactives sur mon stockage primaire ? Puis-je déplacer ces données vers un niveau à froid moins coûteux ?
- Les modifications planifiées de la qualité de service auront-elles une incidence négative sur l'accès aux fichiers stratégiques fréquemment utilisés ?

L'analytique du système de fichiers est intégrée à ONTAP System Manager. Les vues dans System Manager fournissent les éléments suivants :

- Visibilité en temps réel pour une gestion et un fonctionnement efficaces des données
- Collecte et agrégation des données en temps réel
- Tailles et nombres de fichiers et de sous-répertoires, ainsi que les profils de performances associés
- Classez les histogrammes d'âge pour modifier et accéder aux historiques



## Types de volume pris en charge

L'analytique du système de fichiers est conçue pour fournir une visibilité sur les volumes contenant des données NAS actives, à l'exception des caches FlexCache et des volumes de destination SnapMirror.

## Disponibilité des fonctions d'analytique du système de fichiers

Chaque version d'ONTAP étend l'étendue de l'analytique des systèmes de fichiers.

|                                                                 | ONTAP 9.15.1 | ONTAP 9.14.1 | ONTAP 9.13.1 | ONTAP 9.12.1 | ONTAP 9.11.1 | ONTAP 9.10.1 | ONTAP 9.9.1 | ONTAP 9.8 |
|-----------------------------------------------------------------|--------------|--------------|--------------|--------------|--------------|--------------|-------------|-----------|
| Visualisation dans System Manager                               | ✓            | ✓            | ✓            | ✓            | ✓            | ✓            | ✓           | ✓         |
| Analyse de la capacité                                          | ✓            | ✓            | ✓            | ✓            | ✓            | ✓            | ✓           | ✓         |
| Informations sur les données inactives                          | ✓            | ✓            | ✓            | ✓            | ✓            | ✓            | ✓           | ✓         |
| La prise en charge des volumes a migré depuis Data ONTAP 7-mode | ✓            | ✓            | ✓            | ✓            | ✓            | ✓            | ✓           |           |



|                                                                         | ONTAP<br>9.15.1 | ONTAP<br>9.14.1 | ONTAP<br>9.13.1 | ONTAP<br>9.12.1 | ONTAP<br>9.11.1 | ONTAP<br>9.10.1 | ONTAP<br>9.9.1 | ONTAP<br>9.8 |
|-------------------------------------------------------------------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|----------------|--------------|
| Personnalisation de la période inactive dans System Manager             | ✓               | ✓               | ✓               | ✓               | ✓               | ✓               | ✓              |              |
| Suivi des activités au niveau du volume                                 | ✓               | ✓               | ✓               | ✓               | ✓               | ✓               |                |              |
| Téléchargez les données de suivi d'activité au format CSV               | ✓               | ✓               | ✓               | ✓               | ✓               | ✓               |                |              |
| Suivi d'activité au niveau de SVM                                       | ✓               | ✓               | ✓               | ✓               | ✓               |                 |                |              |
| De la chronologie                                                       | ✓               | ✓               | ✓               | ✓               | ✓               |                 |                |              |
| Analyse de l'utilisation                                                | ✓               | ✓               | ✓               | ✓               |                 |                 |                |              |
| Option permettant d'activer l'analyse du système de fichiers par défaut | ✓               | ✓               | ✓               |                 |                 |                 |                |              |
| Moniteur de progression de l'acquisition d'initialisation               | ✓               | ✓               |                 |                 |                 |                 |                |              |

## En savoir plus sur l'analytique des systèmes de fichiers

# ONTAP File System Analytics

Daniel Tennant  
 Director of Software Engineering  
 December 13, 2020

© 2020 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL —






## Plus de lecture

- ["Tr 4687 : recommandations sur les meilleures pratiques pour l'analytique des systèmes de fichiers ONTAP"](#)

- ["Base de connaissances : latence élevée ou variable après l'activation de l'analytique du système de fichiers ONTAP de NetApp"](#)

## Activez l'analyse du système de fichiers

Pour collecter et afficher des données d'utilisation telles que l'analyse de la capacité, vous devez activer l'analytique du système de fichiers sur un volume.

### Description de la tâche

- Depuis ONTAP 9.8, vous pouvez activer l'analytique du système de fichiers sur un volume nouveau ou existant. Si vous mettez à niveau un système vers ONTAP 9.8 ou une version ultérieure, assurez-vous que tous les processus de mise à niveau sont terminés avant d'activer l'analyse du système de fichiers.
- Le temps nécessaire à l'activation de l'analyse dépend de la taille et du contenu du volume. System Manager affiche la progression et présente les données analytiques une fois terminées. Pour des informations plus précises sur la progression de l'acquisition lors de l'initialisation, utilisez la commande de l'interface de ligne de commande ONTAP `volume analytics show`.
  - À partir de ONTAP 9.14.1, ONTAP assure le suivi de la progression de l'analyse d'initialisation en plus des notifications relatives aux événements de limitation qui affectent la progression de l'analyse.
  - À partir de ONTAP 9.15.1, vous ne pouvez effectuer que quatre acquisitions d'initialisation simultanément sur un nœud. Vous devez attendre la fin d'une numérisation avant de lancer une nouvelle numérisation. ONTAP s'assure également que l'espace disponible sur le volume est suffisant et affiche un message d'erreur s'il n'y en a pas. Assurez-vous qu'au moins 5 à 8 % de l'espace disponible du volume est libre. Si la taille automatique est activée sur le volume, calculez la taille disponible en fonction de la taille maximale de la croissance automatique.
  - Pour plus d'informations sur l'acquisition d'initialisation, voir [Considérations relatives à l'analyse](#).

### Activez l'analyse du système de fichiers sur un volume existant

Vous pouvez activer l'analytique du système de fichiers avec ONTAP System Manager ou l'interface de ligne de commande.

Exemple 31. Étape

System Manager

| À ONTAP 9.8 et 9.9.1                                                                                                                                                                                                                                   | À partir de ONTAP 9.10.1                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"><li>1. Sélectionnez <b>stockage &gt; volumes</b>.</li><li>2. Sélectionnez le volume souhaité, puis <b>Explorer</b>.</li><li>3. Sélectionnez <b>Activer les analyses</b> ou <b>Désactiver les analyses</b>.</li></ol> | <ol style="list-style-type: none"><li>1. Sélectionnez <b>stockage &gt; volumes</b>.</li><li>2. Sélectionnez le volume souhaité. Dans le menu volume individuel, sélectionnez <b>système de fichiers &gt; Explorateur</b>.</li><li>3. Sélectionnez <b>Activer les analyses</b> ou <b>Désactiver les analyses</b>.</li></ol> |

CLI

Activez l'analyse du système de fichiers à l'aide de la CLI

1. Exécutez la commande suivante :  

```
volume analytics on -vserver svm_name -volume volume_name [-foreground {true|false}]
```

Par défaut, la commande s'exécute au premier plan ; ONTAP affiche la progression et présente les données analytiques une fois l'opération terminée. Si vous avez besoin d'informations plus précises, vous pouvez exécuter la commande en arrière-plan à l'aide de la `-foreground false` puis utilisez l'`volume analytics show` Commande permettant d'afficher la progression de l'initialisation dans l'interface de ligne de commandes.
2. Une fois l'analyse du système de fichiers terminée, utilisez System Manager ou l'API REST ONTAP pour afficher les données analytiques.

Modifier les paramètres par défaut de l'analyse du système de fichiers


À partir de la version ONTAP 9.13.1, vous pouvez modifier les paramètres des SVM ou des clusters pour activer l'analytique du système de fichiers par défaut sur les nouveaux volumes.

## Exemple 32. Étapes

### System Manager

Si vous utilisez System Manager, vous pouvez modifier les paramètres de la machine virtuelle de stockage ou du cluster pour activer l'analyse de la capacité et le suivi des activités lors de la création du volume par défaut. L'activation par défaut s'applique uniquement aux volumes créés après la modification des paramètres, et non aux volumes existants.

#### Modifier les paramètres d'analyse du système de fichiers sur un cluster

1. Dans System Manager, accédez à **Paramètres de cluster**.
2. Dans **Paramètres du cluster**, consultez l'onglet Paramètres du système de fichiers. Pour modifier les paramètres, sélectionnez l'  icône.
3. Dans le champ **Activity Tracking**, entrez les noms des SVM pour lequel le suivi des activités est activé par défaut. Si vous ne renseignez pas ce champ, le suivi d'activité sera désactivé sur tous les SVM.

Décochez la case **Activer sur les nouveaux ordinateurs virtuels de stockage** pour désactiver le suivi des activités par défaut sur les nouveaux ordinateurs virtuels de stockage.

4. Dans le champ **Analytics**, entrez les noms des machines virtuelles de stockage pour lesquels l'analyse des capacités doit être activée par défaut. Si vous ne renseignez pas ce champ, l'analyse de la capacité est désactivée sur tous les SVM.

Décochez la case **Activer sur les nouvelles machines virtuelles de stockage** pour désactiver l'analyse des capacités par défaut sur les nouvelles machines virtuelles de stockage.

5. Sélectionnez **Enregistrer**.

#### Modification des paramètres d'analytique du système de fichiers sur une SVM

1. Sélectionner le SVM à modifier puis **Storage VM settings**.
2. Dans la carte **File System Analytics**, utilisez les commutateurs pour activer ou désactiver le suivi des activités et l'analyse des capacités pour tous les nouveaux volumes de la machine virtuelle de stockage.

### CLI

Vous pouvez configurer la machine virtuelle de stockage pour activer l'analytique du système de fichiers par défaut sur les nouveaux volumes à l'aide de l'interface de ligne de commande ONTAP.

#### Activer l'analytique des systèmes de fichiers par défaut sur une SVM

1. Modifier le SVM pour activer l'analytique de capacité et le suivi des activités par défaut sur tous les volumes nouvellement créés :  

```
vserver modify -vserver svm_name -auto-enable-activity-tracking true -auto-enable-analytics true
```

## Afficher l'activité du système de fichiers

Une fois que File System Analytics (FSA) est activé, vous pouvez afficher le contenu du répertoire racine d'un volume sélectionné trié par espace utilisé dans chaque sous-arborescence.

Sélectionnez un objet système de fichiers pour parcourir le système de fichiers et afficher des informations détaillées sur chaque objet d'un répertoire. Les informations sur les répertoires peuvent également être affichées graphiquement. Au fil du temps, les données historiques sont affichées pour chaque sous-arbre. L'espace utilisé n'est pas trié s'il y a plus de 3000 répertoires.

## Explorateur

L'écran File System Analytics **Explorer** comprend trois zones :

- Arborescence des répertoires et sous-répertoires ; liste extensible indiquant le nom, la taille, l'historique des modifications et l'historique des accès.
- Fichiers ; affichage du nom, de la taille et du temps d'accès de l'objet sélectionné dans la liste de répertoires.
- Comparaison des données actives et inactives pour l'objet sélectionné dans la liste des répertoires.

Depuis ONTAP 9.9.1, vous pouvez personnaliser la plage à laquelle vous souhaitez faire état. La valeur par défaut est un an. En fonction de ces personnalisations, il est possible d'effectuer des actions correctives, telles que le déplacement de volumes et la modification de la règle de hiérarchisation.

L'heure d'accès est affichée par défaut. Cependant, si la valeur par défaut du volume a été modifiée à partir de l'interface de ligne de commande (en définissant le paramètre `-atime-update` option à `false` avec le `volume modify` commande), seule la dernière heure modifiée est affichée. Par exemple :

- L'arborescence n'affiche pas l'historique **Access**.
- La vue fichiers sera modifiée.
- La vue des données actives/inactives est basée sur l'heure modifiée (`mtime`).

Ces affichages permettent d'examiner les éléments suivants :

- Les emplacements des systèmes de fichiers consomment le plus d'espace
- Informations détaillées sur une arborescence de répertoires, y compris le nombre de fichiers et de sous-répertoires dans les répertoires et sous-répertoires
- Emplacements des systèmes de fichiers contenant d'anciennes données (par exemple, égratignures, temporaires ou arborescences des journaux)

Gardez à l'esprit les points suivants lors de l'interprétation des résultats de FSA :

- FSA affiche où et quand vos données sont en cours d'utilisation, pas la quantité de données traitées. Par exemple, la consommation d'espace importante pour les fichiers récemment utilisés ou modifiés n'indique pas nécessairement des charges de traitement système élevées.
- La façon dont l'onglet **Volume Explorer** calcule la consommation d'espace pour FSA peut différer des autres outils. En particulier, il peut y avoir des différences significatives par rapport à la consommation indiquée dans **Volume Overview** si les fonctions d'efficacité du stockage du volume sont activées. Cela est dû au fait que l'onglet **Volume Explorer** n'inclut pas les économies d'efficacité.
- En raison des limitations d'espace dans l'affichage du répertoire, il n'est pas possible d'afficher une profondeur de répertoire supérieure à 8 niveaux dans *List View*. Pour afficher des répertoires de plus de 8 niveaux au fond, vous devez passer à *Graphical View*, localiser le répertoire souhaité, puis revenir à *List View*. Cela permet d'ajouter de l'espace à l'écran.

## Étapes

1. Afficher le contenu du répertoire racine d'un volume sélectionné :

| À ONTAP 9.8 et 9.9.1                                                                                           | À partir de ONTAP 9.10.1                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cliquez sur <b>stockage &gt; volumes</b> , sélectionnez le volume souhaité, puis cliquez sur <b>Explorer</b> . | Sélectionnez <b>stockage &gt; volumes</b> , puis sélectionnez le volume souhaité. Dans le menu volume individuel, sélectionnez <b>système de fichiers &gt; Explorateur</b> . |

## Activer le suivi des activités

À partir de ONTAP 9.10.1, l'analyse du système de fichiers inclut une fonction de suivi des activités qui vous permet d'identifier les objets sensibles et de télécharger les données sous forme de fichier CSV. Depuis ONTAP 9.11.1, le suivi de l'activité est étendu au périmètre de la SVM. À partir de ONTAP 9.11.1, System Manager propose également une chronologie pour le suivi des activités, vous permettant d'examiner jusqu'à cinq minutes de données de suivi des activités.

Le suivi des activités permet la surveillance en quatre catégories :

- Répertoires
- Fichiers
- Clients
- Utilisateurs

Pour chaque catégorie surveillée, Activity Tracking affiche les IOPS en lecture, les IOPS en écriture, les débits de lecture et les débits d'écriture. Les requêtes sur le suivi d'activité se réactualisent toutes les 10 à 15 secondes en rapport avec les points sensibles observés dans le système au cours de l'intervalle de cinq secondes précédent.

Les informations de suivi d'activité sont approximatives et la précision des données dépend de la distribution du trafic d'E/S entrant.

Lors de l'affichage du suivi d'activité dans System Manager au niveau du volume, seul le menu du volume étendu est actualisé activement. Si l'affichage d'un volume est réduit, il ne sera pas actualisé tant que l'affichage du volume n'aura pas été développé. Vous pouvez arrêter les actualisations à l'aide du bouton **Pause Rafraîchir**. Les données d'activité peuvent être téléchargées au format CSV pour afficher toutes les données ponctuelles capturées pour le volume sélectionné.

La fonction de chronologie proposée sous ONTAP 9.11.1 vous permet de conserver un enregistrement d'activité de zone sensible sur un volume ou une SVM, en mettant à jour en continu environ toutes les cinq secondes et en conservant les données des cinq minutes précédentes. Les données de chronologie ne sont conservées que pour les champs qui sont une zone visible de la page. Si vous réduisez une catégorie de suivi ou faites défiler de façon à ce que la chronologie ne soit plus en vue, la chronologie arrête de collecter les données. Par défaut, les délais sont désactivés et sont automatiquement désactivés lorsque vous vous éloignez de l'onglet activité.

## Activez le suivi des activités pour un seul volume

Vous pouvez activer le suivi des activités avec ONTAP System Manager ou l'interface de ligne de commande.

## Description de la tâche

Si vous utilisez le RBAC avec l'API REST de ONTAP ou System Manager, vous devez créer des rôles personnalisés pour gérer l'accès au suivi des activités. Voir [Contrôle d'accès basé sur des rôles](#) pour ce processus.

### System Manager

#### Étapes

1. Sélectionnez **stockage > volumes**. Sélectionnez le volume souhaité. Dans le menu volume individuel, sélectionnez système de fichiers, puis sélectionnez l'onglet activité.
2. Assurez-vous que **suivi d'activité** est activé pour afficher des rapports individuels sur les répertoires, les fichiers, les clients et les utilisateurs supérieurs.
3. Pour analyser des données plus en profondeur sans actualiser, sélectionnez **Pause Rafraîchir**. Vous pouvez également télécharger les données pour obtenir un enregistrement CSV du rapport.

### CLI

#### Étapes

1. Activer le suivi d'activité :

```
volume activity-tracking on -vserver svm_name -volume volume_name
```

2. Vérifiez si l'état suivi d'activité d'un volume est activé ou désactivé à l'aide de la commande :

```
volume activity-tracking show -vserver svm_name -volume volume_name -state
```

3. Une fois activée, utilisez ONTAP System Manager ou l'API REST ONTAP pour afficher les données de suivi d'activité.

## Activez le suivi des activités pour plusieurs volumes

Vous pouvez activer le suivi des activités pour plusieurs volumes avec System Manager ou l'interface de ligne de commande.

## Description de la tâche

Si vous utilisez le RBAC avec l'API REST de ONTAP ou System Manager, vous devez créer des rôles personnalisés pour gérer l'accès au suivi des activités. Voir [Contrôle d'accès basé sur des rôles](#) pour ce processus.

## System Manager

### Activez pour des volumes spécifiques

1. Sélectionnez **stockage > volumes**. Sélectionnez le volume souhaité. Dans le menu volume individuel, sélectionnez système de fichiers, puis sélectionnez l'onglet activité.
2. Sélectionnez les volumes sur lesquels vous souhaitez activer le suivi d'activité. En haut de la liste des volumes, sélectionnez le bouton **plus d'options**. Sélectionnez **Activer le suivi d'activité**.
3. Pour afficher le suivi des activités au niveau du SVM, sélectionnez le SVM spécifique que vous souhaitez afficher dans **Storage > volumes**. Naviguez jusqu'à l'onglet système de fichiers, puis activité et vous verrez les données des volumes sur lesquels le suivi d'activité est activé.

### Activer pour tous les volumes

1. Sélectionnez **stockage > volumes**. Sélectionner un SVM dans le menu.
2. Accédez à l'onglet **système de fichiers**, choisissez l'onglet **plus** pour activer le suivi d'activité sur tous les volumes de la SVM.

## CLI

À partir de ONTAP 9.13.1, vous pouvez activer le suivi d'activité pour plusieurs volumes à l'aide de l'interface de ligne de commande ONTAP.

### Étapes

1. Activer le suivi d'activité :

```
volume activity-tracking on -vserver svm_name -volume [*|!volume_names]
```

Utiliser \* Pour activer le suivi des activités pour tous les volumes de la machine virtuelle de stockage spécifiée.

Utiliser ! Suivi des noms de volumes pour activer le suivi d'activité pour tous les volumes du SVM à l'exception des volumes nommés.

2. Confirmez que l'opération a réussi :

```
volume show -fields activity-tracking-state
```

3. Une fois activée, utilisez ONTAP System Manager ou l'API REST ONTAP pour afficher les données de suivi d'activité.

## Analytique de l'utilisation

À partir de ONTAP 9.12.1, vous pouvez activer l'analyse de l'utilisation pour voir quels répertoires d'un volume utilisent le plus d'espace. Vous pouvez afficher le nombre total de répertoires d'un volume ou le nombre total de fichiers d'un volume. La création de rapports est limitée aux répertoires 25 qui utilisent le plus d'espace.

Les analyses des répertoires volumineux sont actualisées toutes les 15 minutes. Vous pouvez contrôler l'actualisation la plus récente en vérifiant l'horodatage de la dernière actualisation en haut de la page. Vous pouvez également cliquer sur le bouton Télécharger pour télécharger des données dans un classeur Excel. L'opération de téléchargement s'exécute en arrière-plan et présente les informations les plus récentes pour le volume sélectionné. Si l'analyse revient sans résultat, vérifiez que le volume est en ligne. Des événements tels



que SnapRestore entraînent la reconstruction de la liste de grands répertoires par l'analytique système de fichiers.

### Étapes

1. Sélectionnez **stockage > volumes**. Sélectionnez le volume souhaité.
2. Dans le menu volume individuel, sélectionnez **système de fichiers**. Sélectionnez ensuite l'onglet **usage**.
3. Activez l'option **Analytics** pour activer l'analyse de l'utilisation.
4. System Manager affiche un graphique à barres identifiant les répertoires dont la taille est la plus grande dans l'ordre décroissant.



ONTAP peut afficher des données partielles ou aucune donnée du tout pendant la collecte de la liste des principaux répertoires. La progression de l'acquisition peut se trouver dans l'onglet **usage** qui s'affiche pendant l'acquisition.

Pour obtenir plus d'informations sur un répertoire spécifique, vous pouvez le faire [afficher l'activité sur un système de fichiers](#).

## Prendre les mesures correctives basées sur l'analytique

Depuis ONTAP 9.9.1, vous pouvez effectuer des actions correctives en fonction des données actuelles et des résultats souhaités, directement à partir des affichages d'analytique du système de fichiers.

### Supprimez des répertoires et des fichiers

Dans l'écran de l'Explorateur, vous pouvez sélectionner des répertoires ou des fichiers individuels à supprimer. Les répertoires sont supprimés avec une fonctionnalité de suppression rapide des répertoires à faible latence. (La suppression rapide des répertoires est également disponible depuis ONTAP 9.9.1, sans activation des analyses.)

### Étapes

1. Cliquez sur **Storage > volumes**, puis sur **Explorer**.

Lorsque vous placez le pointeur de la souris sur un fichier ou un dossier, l'option de suppression apparaît. Vous ne pouvez supprimer qu'un seul objet à la fois.



Lorsque des répertoires et des fichiers sont supprimés, les nouvelles valeurs de capacité de stockage ne sont pas affichées immédiatement.

## Attribuez le coût du support dans les tiers de stockage pour comparer les coûts des emplacements de stockage de données inactifs

Le coût du support est une valeur que vous attribuez en fonction de votre évaluation des coûts de stockage, représentée comme la devise par Go de votre choix. Lorsqu'il est défini, System Manager utilise le coût de support attribué pour projeter les économies estimées lors du déplacement des volumes.

Le coût de support que vous avez défini n'est pas persistant ; il ne peut être défini que pour une seule session de navigateur.

### Étapes

1. Cliquez sur **stockage > niveaux**, puis cliquez sur **définir le coût du support** dans les mosaïques de niveau local (agrégat) souhaitées.

Veillez à sélectionner les tiers actifs et inactifs pour permettre la comparaison.

2. Entrez un type de devise et un montant.


Lorsque vous saisissez ou modifiez le coût du support, la modification est effectuée dans tous les types de support.

## Déplacez des volumes pour réduire les coûts de stockage

En se basant sur des analyses et des comparaisons des coûts des supports, vous pouvez déplacer des volumes vers un stockage moins coûteux au niveau local.

Vous ne pouvez comparer et déplacer qu'un seul volume à la fois.

### Étapes

1. Une fois l'affichage du coût du support pris en charge, cliquez sur **stockage > niveaux**, puis sur **volumes**.
2. Pour comparer les options de destination d'un volume, cliquez sur  pour le volume, puis cliquez sur **déplacer**.
3. Dans l'écran **Sélectionner le niveau local** de destination, sélectionnez les niveaux de destination pour afficher la différence de coût estimée.
4. Après avoir comparé les options, sélectionnez le niveau souhaité et cliquez sur **déplacer**.

## Contrôle d'accès basé sur des rôles avec File System Analytics

À partir de ONTAP 9.12.1, ONTAP inclut un rôle de contrôle d'accès basé sur des rôles (RBAC) prédéfini appelé `admin-no-fsa`. Le `admin-no-fsa` le rôle accorde des privilèges de niveau administrateur mais empêche l'utilisateur d'effectuer des opérations liées à l'`files` Terminal (analytique du système de fichiers) dans l'interface de ligne de commande ONTAP, l'API REST et dans System Manager.

Pour plus d'informations sur le `admin-no-fsa` rôle, voir [Rôles prédéfinis pour les administrateurs du cluster](#).

Si vous utilisez une version de ONTAP antérieure à ONTAP 9.12.1, vous devrez créer un rôle dédié pour contrôler l'accès à l'analyse du système de fichiers. Dans les versions de ONTAP antérieures à ONTAP 9.12.1, vous devez configurer les autorisations RBAC via l'interface de ligne de commande d'ONTAP ou l'API REST d'ONTAP.

## System Manager

À partir de ONTAP 9.12.1, vous pouvez configurer les autorisations RBAC pour l'analyse du système de fichiers à l'aide de System Manager.

### Étapes

1. Sélectionnez **Cluster > Paramètres**. Sous **sécurité**, naviguez jusqu'à **utilisateurs et rôles** et sélectionnez ➔.
2. Sous **rôles**, sélectionnez **+ Add**.
3. Indiquez un nom pour le rôle. Sous attributs de rôle, configurez l'accès ou les restrictions pour le rôle d'utilisateur en fournissant le approprié "**Terminaux d'API**". Consultez le tableau ci-dessous pour connaître les chemins principaux et secondaires permettant de configurer l'accès ou les restrictions de l'analyse du système de fichiers.

| Restriction                                            | Chemin primaire      | Chemin secondaire                                                                                                                                                                           |
|--------------------------------------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Suivi d'activité sur les volumes                       | /api/storage/volumes | <ul style="list-style-type: none"><li>• /:uuid/top-metrics/directories</li><li>• /:uuid/top-metrics/files</li><li>• /:uuid/top-metrics/clients</li><li>• /:uuid/top-metrics/users</li></ul> |
| Suivi de l'activité sur les SVM                        | /api/svm/svms        | <ul style="list-style-type: none"><li>• /:uuid/top-metrics/directories</li><li>• /:uuid/top-metrics/files</li><li>• /:uuid/top-metrics/clients</li><li>• /:uuid/top-metrics/users</li></ul> |
| Toutes les opérations d'analyse du système de fichiers | /api/storage/volumes | /:uuid/files                                                                                                                                                                                |

Vous pouvez utiliser `/*` Au lieu d'un UUID afin de définir la règle pour tous les volumes ou SVM sur le terminal.

Choisissez les privilèges d'accès pour chaque noeud final.

4. Sélectionnez **Enregistrer**.
5. Pour attribuer le rôle à un ou plusieurs utilisateurs, voir [Contrôlez l'accès administrateur](#).

### CLI

Si vous utilisez une version de ONTAP antérieure à ONTAP 9.12.1, créez un rôle personnalisé à l'aide de

l'interface de ligne de commandes de ONTAP.

## Étapes

1. Créez un rôle par défaut pour accéder à toutes les fonctions.

Cette opération doit être effectuée avant de créer le rôle restrictif afin de garantir que le rôle n'est que restrictif sur le suivi d'activité :

```
security login role create -cmddirname DEFAULT -access all -role
storageAdmin
```

2. Créer le rôle restrictif :

```
security login role create -cmddirname "volume file show-disk-usage"
-access none -role storageAdmin
```

3. Autoriser les rôles à accéder aux services web du SVM :

- `rest` Pour les appels API REST
- `security` pour la protection par mot de passe
- `sysmgr` Pour accéder à System Manager

```
vserver services web access create -vserver svm-name -name_ -name rest
-role storageAdmin
```

```
vserver services web access create -vserver svm-name -name security
-role storageAdmin
```

```
vserver services web access create -vserver svm-name -name sysmgr -role
storageAdmin
```

4. Créer un utilisateur.

Vous devez exécuter une commande de création distincte pour chaque application que vous souhaitez appliquer à l'utilisateur. Les appels créent plusieurs fois sur le même utilisateur appliquent simplement toutes les applications à cet utilisateur et ne créent pas de nouvel utilisateur à chaque fois. Le `http` Le paramètre pour le type d'application s'applique à l'API REST ONTAP et à System Manager.

```
security login create -user-or-group-name storageUser -authentication
-method password -application http -role storageAdmin
```

5. Avec les nouvelles informations d'identification utilisateur, vous pouvez désormais vous connecter à System Manager ou utiliser l'API REST de ONTAP pour accéder aux données d'analytique des systèmes de fichiers.

## Plus d'informations

- [Rôles prédéfinis pour les administrateurs du cluster](#)
- [Contrôle de l'accès administrateur avec System Manager](#)
- ["En savoir plus sur les rôles RBAC et l'API REST de ONTAP"](#)

## Considérations relatives à l'analytique des systèmes de fichiers

Vous devez connaître les limites d'utilisation et les impacts potentiels sur les performances associés à l'implémentation de File System Analytics.

### Relations protégées par un SVM

Si vous avez activé File System Analytics sur les volumes dont le SVM contient fait partie d'une relation de protection, les données d'analytique ne sont pas répliquées vers le SVM de destination. Si le SVM source doit être resynchronisé dans une opération de restauration, vous devez de nouveau activer manuellement l'analytique sur les volumes souhaités après sa restauration.

### Performances

Dans certains cas, l'activation d'une analytique système de fichiers peut avoir un impact négatif sur les performances lors de la collecte de métadonnées initiale. Cela est généralement le plus fréquemment observé sur les systèmes qui atteignent une utilisation maximale. Pour éviter l'activation de l'analytique sur ces systèmes, vous pouvez utiliser les outils de contrôle des performances de ONTAP System Manager.

Si vous constatez une augmentation notable de la latence, consultez l'article de la base de connaissances ["Latence élevée ou variable après l'activation de l'analytique système de fichiers ONTAP de NetApp"](#).

### Considérations relatives à l'analyse

Lorsque vous activez l'analyse de la capacité, ONTAP effectue une analyse d'initialisation pour l'analyse de la capacité. L'analyse accède aux métadonnées de tous les fichiers des volumes pour lesquels l'analyse de capacité est activée. Aucune donnée de fichier n'est lue pendant l'acquisition. À partir de ONTAP 9.14.1, vous pouvez suivre la progression de l'analyse avec l'API REST, dans l'onglet **Explorer** du Gestionnaire système ou avec le `volume analytics show` Commande CLI. En cas d'événement d'accélération, ONTAP envoie une notification.

Lorsque vous activez l'analyse du système de fichiers sur un volume, assurez-vous qu'au moins 5 à 8 % de l'espace disponible du volume est libre. Si la taille automatique est activée sur le volume, calculez la taille disponible en fonction de la taille maximale de la croissance automatique. Depuis ONTAP 9.15.1, ONTAP affiche un message d'erreur si l'espace disponible est insuffisant lorsque vous activez l'analyse du système de fichiers sur un volume.

Une fois l'analyse terminée, l'analyse du système de fichiers est continuellement mise à jour en temps réel à mesure que le système de fichiers change.

Le temps requis pour l'analyse est proportionnel au nombre de répertoires et de fichiers sur le volume. Étant donné que l'analyse collecte des métadonnées, la taille du fichier n'a pas d'incidence sur le temps d'analyse.

Pour plus d'informations sur l'acquisition d'initialisation, reportez-vous à la section ["Tr-4867 : recommandations sur les bonnes pratiques pour l'analytique de système de fichiers"](#).

### Et des meilleures pratiques

Vous devez démarrer l'analyse sur des volumes qui ne partagent pas d'agrégats. Vous pouvez voir quels agrégats hébergent actuellement les volumes à l'aide de la commande :

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

Pendant l'analyse, les volumes continuent de transmettre le trafic client. Il est recommandé de démarrer

l'analyse pendant les périodes où vous prévoyez un trafic client plus faible.

Si le trafic client augmente, il consomme les ressources système et allonge l'analyse.

À partir de ONTAP 9.12.1, vous pouvez interrompre la collecte de données dans System Manager et via l'interface de ligne de commandes ONTAP.

- Si vous utilisez l'interface de ligne de commandes ONTAP :
  - Vous pouvez interrompre la collecte de données à l'aide de la commande : `volume analytics initialization pause -vserver svm_name -volume volume_name`
  - Une fois le trafic client ralenti, vous pouvez reprendre la collecte de données à l'aide de la commande : `volume analytics initialization resume -vserver svm_name -volume volume_name`
- Si vous utilisez System Manager, dans la vue **Explorer** du menu volume, vous utilisez les boutons **Pause collecte de données** et **reprendre collecte de données** pour gérer l'acquisition.

# Configuration EMS

## Présentation de la configuration EMS

Vous pouvez configurer ONTAP 9 pour envoyer des notifications d'événements EMS (Event Management System) importantes directement à une adresse e-mail, un serveur syslog, un traphost SNMP (simple Management Network Protocol) ou une application webhook afin que vous soyez immédiatement averti des problèmes système nécessitant une intervention rapide.

Comme les notifications d'événements importantes ne sont pas activées par défaut, vous devez configurer l'EMS pour qu'il envoie des notifications à une adresse e-mail, à un serveur syslog, à un traphost SNMP ou à une application webhook.

Examiner les versions spécifiques à la version du ["Référence EMS ONTAP 9"](#).

Si votre mappage d'événements EMS utilise des jeux de commandes ONTAP obsolètes (comme la destination de l'événement, la route des événements), il est recommandé de mettre à jour votre mappage. ["Découvrez comment mettre à jour votre mappage EMS à partir de commandes ONTAP obsolètes"](#).

## Configurez les notifications d'événement EMS et les filtres avec System Manager

Vous pouvez utiliser System Manager pour configurer la manière dont le système EMS (Event Management System) envoie des notifications d'événements afin de vous informer des problèmes système qui nécessitent une intervention rapide.

| Version ONTAP                        | Grâce à System Manager, vous pouvez...                                                                                |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| ONTAP 9.12.1 et versions ultérieures | Spécifiez le protocole TLS (transport Layer Security) lors de l'envoi d'événements vers des serveurs syslog distants. |
| ONTAP 9.10.1 et versions ultérieures | Configurez les adresses électroniques, les serveurs syslog et les applications webhook, ainsi que les Traphosts SNMP. |

|                    |                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ONTAP 9.7 à 9.10.0 | Configurez uniquement les Traphosts SNMP. Vous pouvez configurer d'autres destinations EMS à l'aide de l'interface de ligne de commande ONTAP. Voir " <a href="#">Présentation de la configuration EMS</a> ". |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Vous pouvez effectuer les opérations suivantes :

- [\[add-ems-destination\]](#)
- [\[create-ems-filter\]](#)
- [\[edit-ems-destination\]](#)
- [\[edit-ems-filter\]](#)
- [\[delete-ems-destination\]](#)
- [\[delete-ems-filter\]](#)

#### Informations associées



- "[Référence ONTAP EMS](#)"
- "[Utilisation de l'interface de ligne de commande pour configurer les Traphosts SNMP pour recevoir des notifications d'événements](#)"

### Ajouter une destination de notification d'événement EMS

Vous pouvez utiliser System Manager pour spécifier l'emplacement d'envoi des messages EMS.

Depuis ONTAP 9.12.1, les événements EMS peuvent être envoyés vers un port désigné sur un serveur syslog distant via le protocole TLS (transport Layer Security). Pour plus d'informations, reportez-vous à la [event notification destination create](#) page de manuel.

#### Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Dans la section **gestion des notifications**, cliquez sur , puis sur **Afficher les destinations des événements**.
3. Sur la page **gestion des notifications**, sélectionnez l'onglet **destinations d'événements**.
4. Cliquez sur  **Add**.
5. Spécifiez un nom, un type de destination EMS et des filtres.



Si nécessaire, vous pouvez ajouter un nouveau filtre. Cliquez sur **Ajouter un nouveau filtre d'événements**.

6. En fonction du type de destination EMS que vous avez sélectionné, spécifiez ce qui suit :



| Pour configurer... | Spécifiez ou sélectionnez...                                     |
|--------------------|------------------------------------------------------------------|
| Traphost SNMP      | <ul style="list-style-type: none"> <li>• Nom TrapHost</li> </ul> |


|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| E-mail<br>(À partir de la version 9.10.1)         | <ul style="list-style-type: none"> <li>• Adresse e-mail de destination</li> <li>• Serveur de messagerie</li> <li>• De l'adresse e-mail</li> </ul>                                                                                                                                                                                                                                                                                    |
| Serveur Syslog<br>(À partir de la version 9.10.1) | <ul style="list-style-type: none"> <li>• Nom d'hôte ou adresse IP du serveur</li> <li>• Port Syslog (commençant par 9.12.1)</li> <li>• Transport Syslog (à partir de 9.12.1)</li> </ul> <p>La sélection de <b>TCP chiffré</b> active le protocole TLS (transport Layer Security). Si aucune valeur n'est saisie pour <b>Syslog port</b>, une valeur par défaut est utilisée en fonction de la sélection <b>Syslog transport</b>.</p> |
| Webhook<br>(À partir de la version 9.10.1)        | <ul style="list-style-type: none"> <li>• URL de Webhook</li> <li>• Authentification client (sélectionnez cette option pour spécifier un certificat client)</li> </ul>                                                                                                                                                                                                                                                                |

## Créer un nouveau filtre de notification d'événement EMS

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour définir de nouveaux filtres personnalisés spécifiant les règles de gestion des notifications EMS.

### Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Dans la section **gestion des notifications**, cliquez sur , puis sur **Afficher les destinations des événements**.
3. Sur la page **gestion des notifications**, sélectionnez l'onglet **filtres d'événements**.
4. Cliquez sur  **Add**.
5. Spécifiez un nom et indiquez si vous souhaitez copier des règles à partir d'un filtre d'événements existant ou ajouter de nouvelles règles.
6. Selon votre choix, effectuez les opérations suivantes :



| Si vous choisissez....                                            | Puis, effectuez ces étapes...                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Copier les règles à partir du filtre d'événements existant</b> | <ol style="list-style-type: none"> <li>1. Sélectionnez un filtre d'événement existant.</li> <li>2. Modifier les règles existantes.</li> <li>3. Ajoutez d'autres règles, si nécessaire, en cliquant sur  <b>Add</b>.</li> </ol> |
| <b>Ajouter de nouvelles règles</b>                                | Spécifiez le type, le modèle de nom, les niveaux de gravité et le type d'interruption SNMP pour chaque nouvelle règle.                                                                                                                                                                                            |



## Modifier une destination de notification d'événement EMS

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour modifier les données de destination de la notification d'événement.

### Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Dans la section **gestion des notifications**, cliquez sur , puis sur **Afficher les destinations des événements**.
3. Sur la page **Notifications Management**, sélectionnez l'onglet **Événements destinations**.
4. En regard du nom de la destination de l'événement, cliquez sur , puis sur **Modifier**.
5. Modifiez les informations de destination de l'événement, puis cliquez sur **Enregistrer**.



## Modifier un filtre de notification d'événement EMS

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour modifier les filtres personnalisés afin de modifier le mode de traitement des notifications d'événements.



Vous ne pouvez pas modifier les filtres définis par le système.

### Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Dans la section **gestion des notifications**, cliquez sur , puis sur **Afficher les destinations des événements**.
3. Sur la page **gestion des notifications**, sélectionnez l'onglet **filtres d'événements**.
4. En regard du nom du filtre d'événement, cliquez sur , puis sur **Modifier**.
5. Modifiez les informations de filtre d'événement, puis cliquez sur **Enregistrer**.



## Supprimer une destination de notification d'événement EMS

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour supprimer une destination de notification d'événement EMS.



Vous ne pouvez pas supprimer des destinations SNMP.

### Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Dans la section **gestion des notifications**, cliquez sur , puis sur **Afficher les destinations des événements**.
3. Sur la page **gestion des notifications**, sélectionnez l'onglet **destinations d'événements**.
4. En regard du nom de la destination de l'événement, cliquez sur , puis sur **Supprimer**.



## Supprimer un filtre de notification d'événement EMS

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour supprimer des filtres personnalisés.



Vous ne pouvez pas supprimer des filtres définis par le système.

## Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Dans la section **gestion des notifications**, cliquez sur , puis sur **Afficher les destinations des événements**.
3. Sur la page **gestion des notifications**, sélectionnez l'onglet **filtres d'événements**.
4. En regard du nom du filtre d'événement, cliquez sur , puis sur **Supprimer**.

## Configurez les notifications d'événements EMS avec l'interface de ligne de commande

### Flux de travail de configuration EMS

Vous devez configurer les notifications d'événements EMS importantes pour qu'elles soient envoyées par e-mail, envoyées à un serveur syslog, transférées à un hôte de transfert SNMP ou transmises à une application de connexion Web. Cela vous permet d'éviter toute interruption du système en prenant des actions correctives en temps opportun.

### Description de la tâche

Si votre environnement contient déjà un serveur syslog permettant d'agréger les événements journaux d'autres systèmes, tels que des serveurs et des applications, il est plus facile d'utiliser ce serveur syslog également pour recevoir des notifications d'événements importantes provenant des systèmes de stockage.

Si votre environnement ne contient pas encore de serveur syslog, il est plus facile d'utiliser le courrier électronique pour les notifications d'événements importantes.

Si vous transférez déjà des notifications d'événement à un Traphost SNMP, il se peut que vous souhaitiez surveiller ce Traphost pour les événements importants.



## Choix

- Configurez EMS pour envoyer des notifications d'événement.

| Les fonctions que vous recherchez...                                                                | Reportez-vous à ceci...                                                                                                 |
|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| L'EMS doit envoyer des notifications d'événements importantes à une adresse e-mail                  | <a href="#">Configurez les événements EMS importants pour envoyer des notifications par e-mail</a>                      |
| L'EMS doit transmettre des notifications d'événements importantes à un serveur syslog               | <a href="#">Configurez les événements EMS importants pour transférer des notifications à un serveur syslog</a>          |
| Si vous souhaitez que l'EMS envoie des notifications d'événement à un Traphost SNMP                 | <a href="#">Configurez les Traphosts SNMP pour recevoir des notifications d'événement</a>                               |
| Si vous souhaitez que l'EMS envoie des notifications d'événement à une application de connexion Web | <a href="#">Configurez les événements EMS importants pour transférer les notifications vers une application webhook</a> |

## Configurez les événements EMS importants pour envoyer des notifications par e-mail

Pour recevoir des notifications par e-mail des événements les plus importants, vous devez configurer l'EMS pour qu'il envoie des e-mails pour les événements qui signalent une activité importante.

### Ce dont vous avez besoin

Le DNS doit être configuré sur le cluster pour résoudre les adresses e-mail.

### Description de la tâche

Vous pouvez effectuer cette tâche à tout moment du cluster en entrant les commandes sur la ligne de commande ONTAP.

### Étapes

1. Configurez les paramètres du serveur de messagerie SMTP d'événement :

```
event config modify -mail-server mailhost.your_domain -mail-from
cluster_admin@your_domain
```

2. Créer une destination e-mail pour les notifications d'événements :

```
event notification destination create -name storage-admins -email
your_email@your_domain
```

3. Configurez les événements importants pour envoyer des notifications par e-mail :

```
event notification create -filter-name important-events -destinations storage-
admins
```

### Configuration des événements EMS importants pour transférer des notifications à un serveur syslog

Pour enregistrer les notifications des événements les plus graves sur un serveur syslog, vous devez configurer l'EMS pour transférer les notifications des événements qui signalent une activité importante.

### Ce dont vous avez besoin

Le DNS doit être configuré sur le cluster pour résoudre le nom du serveur syslog.

### Description de la tâche

Si votre environnement ne contient pas encore de serveur syslog pour les notifications d'événements, vous devez d'abord en créer un. Si votre environnement contient déjà un serveur syslog pour la journalisation des événements à partir d'autres systèmes, vous pouvez l'utiliser pour les notifications d'événements importantes.

Vous pouvez effectuer cette tâche à n'importe quel moment du cluster en entrant les commandes sur l'interface de ligne de commandes de ONTAP.

Depuis ONTAP 9.12.1, les événements EMS peuvent être envoyés vers un port désigné sur un serveur syslog distant via le protocole TLS (transport Layer Security). Deux nouveaux paramètres sont disponibles :

#### **tcp-encrypted**

Quand `tcp-encrypted` est spécifié pour le `syslog-transport`, ONTAP vérifie l'identité de l'hôte de destination en validant son certificat. La valeur par défaut est `udp-unencrypted`.

#### **syslog-port**

La valeur par défaut `syslog-port` le paramètre dépend du réglage de l' `syslog-transport` paramètre. Si `syslog-transport` est défini sur `tcp-encrypted`, `syslog-port` a la valeur par défaut 6514.

Pour plus d'informations, reportez-vous à la [event notification destination create](#) page de manuel.

## Étapes

1. Créer une destination de serveur syslog pour les événements importants :

```
event notification destination create -name syslog-ems -syslog syslog-server-address -syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}
```

À partir de ONTAP 9.12.1, les valeurs suivantes peuvent être spécifiées pour `syslog-transport`:

- ° `udp-unencrypted` - Protocole de datagramme utilisateur sans sécurité
- ° `tcp-unencrypted` - Protocole de contrôle de transmission sans sécurité
- ° `tcp-encrypted` - Protocole de contrôle de transmission avec TLS (transport Layer Security)

Le protocole par défaut est `udp-unencrypted`.

2. Configurez les événements importants pour transférer des notifications au serveur syslog :

```
event notification create -filter-name important-events -destinations syslog-ems
```

## Configurez les Traphosts SNMP pour recevoir des notifications d'événement

Pour recevoir des notifications d'événements sur un Traphost SNMP, vous devez configurer un Traphost.

### Ce dont vous avez besoin

- Les traps SNMP doivent être activés sur le cluster.



Les interruptions SNMP et SNMP sont activées par défaut.

- Le DNS doit être configuré sur le cluster pour résoudre les noms de Traphost.

### Description de la tâche

Si aucun Traphost SNMP n'est déjà configuré pour recevoir des notifications d'événements (traps SNMP), vous devez en ajouter un.

Vous pouvez effectuer cette tâche à tout moment du cluster en entrant les commandes sur la ligne de commande ONTAP.

### Étape

1. Si votre environnement ne dispose pas déjà d'un Traphost SNMP configuré pour recevoir des notifications d'événement, ajoutez-en un :

```
system snmp traphost add -peer-address snmp_traphost_name
```

Toutes les notifications d'événements prises en charge par SNMP par défaut sont transmises au Traphost SNMP.

## Configurez les événements EMS importants pour transférer les notifications vers une application webhook

Vous pouvez configurer ONTAP pour transférer des notifications d'événements importantes vers une application de connexion Web. Les étapes de configuration nécessaires dépendent du niveau de sécurité que vous choisissez.

### Préparez-vous à configurer le transfert d'événements EMS

Vous devez tenir compte de plusieurs concepts et exigences avant de configurer ONTAP pour transférer les notifications d'événements vers une application webhook.

### Application Webhook

Vous avez besoin d'une application webhook capable de recevoir les notifications d'événements ONTAP. Un webhook est une routine de rappel définie par l'utilisateur qui étend la capacité de l'application ou du serveur distant où il s'exécute. Les patrons sont appelés ou activés par le client (dans ce cas ONTAP) en envoyant une requête HTTP à l'URL de destination. Plus précisément, ONTAP envoie une requête HTTP POST au serveur hébergeant l'application webhook avec les détails de notification d'événement formatés en XML.

### Options de sécurité

Plusieurs options de sécurité sont disponibles en fonction de l'utilisation du protocole TLS (transport Layer Security). L'option choisie détermine la configuration ONTAP requise.



TLS est un protocole cryptographique largement utilisé sur Internet. Il assure la confidentialité ainsi que l'intégrité et l'authentification des données à l'aide d'un ou de plusieurs certificats de clé publique. Les certificats sont émis par les autorités de certification de confiance.

### HTTP

Vous pouvez utiliser HTTP pour transporter les notifications d'événement. Avec cette configuration, la connexion n'est pas sécurisée. Les identités du client ONTAP et de l'application webhook ne sont pas vérifiées. En outre, le trafic réseau n'est pas chiffré ni protégé. Voir ["Configurez une destination de connexion Web pour utiliser HTTP"](#) pour en savoir plus sur la configuration.

### HTTPS

Pour plus de sécurité, vous pouvez installer un certificat sur le serveur hébergeant la routine webhook. Le protocole HTTPS est utilisé par ONTAP pour vérifier l'identité du serveur d'application webhook ainsi que par les deux parties pour assurer la confidentialité et l'intégrité du trafic réseau. Voir ["Configurez une destination Webhook pour utiliser HTTPS"](#) pour en savoir plus sur la configuration.

### HTTPS avec authentification mutuelle

Vous pouvez améliorer encore la sécurité HTTPS en installant un certificat client sur le système ONTAP émettant les requêtes webhook. En plus de la vérification par ONTAP de l'identité du serveur d'applications webhook et de la protection du trafic réseau, l'application webhook vérifie l'identité du client ONTAP. Cette authentification bidirectionnelle par poste est appelée *Mutual TLS*. Voir ["Configurez une destination de connexion Web pour utiliser HTTPS avec authentification mutuelle"](#) pour en savoir plus sur la configuration.

### Informations associées

- ["Protocole TLS \(transport Layer Security\) version 1.3"](#)

## Configurez une destination de connexion Web pour utiliser HTTP

Vous pouvez configurer ONTAP pour transférer des notifications d'événements vers une application de webhook à l'aide de HTTP. Il s'agit de l'option la moins sécurisée, mais la plus simple à configurer.

### Étapes

1. Créer une nouvelle destination `restapi-ems` pour recevoir les événements :

```
event notification destination create -name restapi-ems -rest-api-url
http://<webhook-application>
```

Dans la commande ci-dessus, vous devez utiliser le schéma **HTTP** pour la destination.

2. Créez une notification reliant le `important-events` filtrer avec le `restapi-ems` destination :

```
event notification create -filter-name important-events -destinations restapi-
ems
```

## Configurez une destination Webhook pour utiliser HTTPS

Vous pouvez configurer ONTAP pour transférer les notifications d'événements vers une application de connexion Internet à l'aide de HTTPS. ONTAP utilise le certificat de serveur pour confirmer l'identité de l'application webhook et sécuriser le trafic réseau.

### Avant de commencer

- Générez une clé privée et un certificat pour le serveur d'applications webhook
- Disponibilité du certificat racine pour l'installation dans ONTAP

### Étapes

1. Installez la clé privée du serveur et les certificats appropriés sur le serveur hébergeant votre application webhook. Les étapes de configuration spécifiques dépendent du serveur.
2. Installez le certificat racine du serveur dans ONTAP :

```
security certificate install -type server-ca
```

La commande demande le certificat.

3. Créer le `restapi-ems` destination pour recevoir les événements :

```
event notification destination create -name restapi-ems -rest-api-url
https://<webhook-application>
```

Dans la commande ci-dessus, vous devez utiliser le schéma **HTTPS** pour la destination.

4. Créez la notification qui lie le `important-events` filtrer avec le nouveau `restapi-ems` destination :

```
event notification create -filter-name important-events -destinations restapi-
ems
```

## Configurez une destination de connexion Web pour utiliser HTTPS avec authentification mutuelle

Vous pouvez configurer ONTAP pour transférer les notifications d'événements vers une application webhook en utilisant HTTPS avec authentification mutuelle. Avec cette configuration, il y a deux certificats. ONTAP utilise le certificat de serveur pour confirmer l'identité de l'application webhook et sécuriser le trafic réseau. De plus, l'application hébergeant le webhook utilise le certificat client pour confirmer l'identité du client ONTAP.

### Avant de commencer

Vous devez effectuer les opérations suivantes avant de configurer ONTAP :

- Générez une clé privée et un certificat pour le serveur d'applications webhook
- Disponibilité du certificat racine pour l'installation dans ONTAP
- Générez une clé privée et un certificat pour le client ONTAP

### Étapes

1. Effectuez les deux premières étapes de la tâche "[Configurez une destination Webhook pour utiliser HTTPS](#)" Pour installer le certificat de serveur afin que ONTAP puisse vérifier l'identité du serveur.
2. Installez les certificats racine et intermédiaire appropriés sur l'application webhook pour valider le certificat client.
3. Installez le certificat client dans ONTAP :

```
security certificate install -type client
```

La commande demande la clé privée et le certificat.

4. Créer le `restapi-ems` destination pour recevoir les événements :

```
event notification destination create -name restapi-ems -rest-api-url
https://<webhook-application> -certificate-authority <issuer of the client
certificate> -certificate-serial <serial of the client certificate>
```

Dans la commande ci-dessus, vous devez utiliser le schéma **HTTPS** pour la destination.

5. Créez la notification qui lie le `important-events` filtrer avec le nouveau `restapi-ems` destination :

```
event notification create -filter-name important-events -destinations restapi-
ems
```

## Mettre à jour le mappage d'événements EMS obsolète

### Modèles de mappage d'événements EMS

Avant ONTAP 9.0, les événements EMS ne pouvaient être mappés qu'à des destinations d'événement en fonction de la correspondance du modèle de nom d'événement. La commande ONTAP définit (`event destination`, `event route`) Qui utilisent ce modèle continue d'être disponible dans les dernières versions de ONTAP, mais ils ont été obsolètes à partir de ONTAP 9.0.

Depuis ONTAP 9.0, la meilleure pratique pour le mappage de destination d'événements EMS ONTAP consiste à utiliser le modèle de filtre d'événements plus évolutif dans lequel la correspondance de modèles est



effectuée sur plusieurs champs, à l'aide du `event filter`, `event notification`, et `event notification destination` jeux de commandes.

Si votre mappage EMS est configuré à l'aide des commandes obsolètes, vous devez mettre à jour votre mappage pour utiliser le `event filter`, `event notification`, et `event notification destination` jeux de commandes.

Il existe deux types de destinations d'événements :

**1. Destinations générées par le système** : il existe cinq destinations d'événements générées par le système (créées par défaut)

- ° `allevents`
- ° `asup`
- ° `criticals`
- ° `pager`
- ° `traphost`

Certaines des destinations générées par le système sont à des fins spéciales. Par exemple, la destination d'`asup` achemine les événements `callhome.*` vers le module AutoSupport dans ONTAP pour générer des messages AutoSupport.

**2. Destinations créées par l'utilisateur** : elles sont créées manuellement à l'aide de `event destination create` commande.

```
cluster-1::event*> destination show
```

| Name | Mail Dest. | SNMP Dest. | Syslog Dest. | Hide |
|------|------------|------------|--------------|------|
|------|------------|------------|--------------|------|

Params

|       |       |       |       |       |
|-------|-------|-------|-------|-------|
| ----- | ----- | ----- | ----- | ----- |
|-------|-------|-------|-------|-------|

allevents

-

-

-

false

asup

-

-

-

false

criticals

-

-

-

false

pager

-

-

-

false

traphost

-

-

-

false

5 entries were displayed.

+

```
cluster-1::event*> destination create -name test -mail test@xyz.com
```

This command is deprecated. Use the "event filter", "event notification destination" and "event notification" commands, instead.

+

```
cluster-1::event*> destination show
```

+

Hide

| Name | Mail Dest. | SNMP Dest. | Syslog Dest. |
|------|------------|------------|--------------|
|------|------------|------------|--------------|

Params

|       |       |       |       |
|-------|-------|-------|-------|
| ----- | ----- | ----- | ----- |
|-------|-------|-------|-------|

allevents

-

-

-

false

asup

-

-

-

false

criticals

-

-

-

false

pager

-

-

-

false

test

test@xyz.com

-

-

false

traphost

-

-

-

false

6 entries were displayed.

Dans le modèle obsolète, les événements EMS sont mappés individuellement vers une destination à l'aide de l'event route add-destinations commande.

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.
```

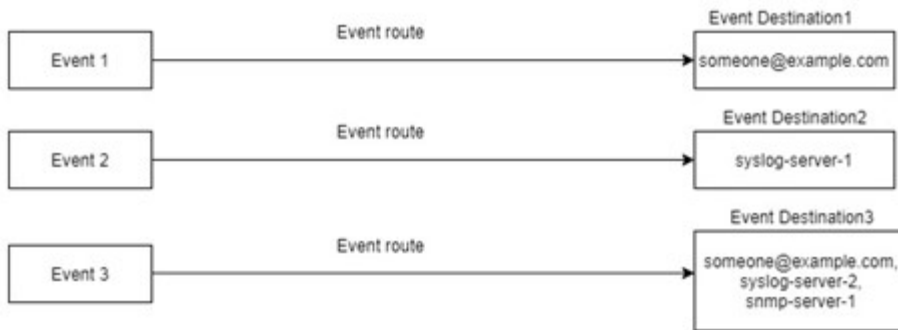
```
cluster-1::event*> route show -message-name raid.aggr.*
```

| Time  | Message                    | Severity      | Destinations | Freq  | Threshd |
|-------|----------------------------|---------------|--------------|-------|---------|
| ----- | -----                      | -----         | -----        | ----- | -----   |
| ----- | -----                      | -----         | -----        | ----- | -----   |
|       | raid.aggr.autoGrow.abort   | NOTICE        | test         | 0     | 0       |
|       | raid.aggr.autoGrow.success | NOTICE        | test         | 0     | 0       |
|       | raid.aggr.lock.conflict    | INFORMATIONAL | test         | 0     | 0       |
|       | raid.aggr.log.CP.count     | DEBUG         | test         | 0     | 0       |
|       | 4 entries were displayed.  |               |              |       |         |

Le nouveau mécanisme plus évolutif de notification d'événements EMS est basé sur des filtres d'événements et des destinations de notification d'événements. Pour plus d'informations sur le nouveau mécanisme de notification d'événements, reportez-vous à l'article suivant de la base de connaissances :

- ["Présentation du système de gestion des événements pour ONTAP 9"](#)

Legacy routing based model



Event notification based model



## Mettre à jour le mappage des événements EMS à partir des commandes ONTAP obsolètes

Si votre mappage d'événements EMS est actuellement configuré à l'aide des jeux de commandes ONTAP obsolètes (`event destination`, `event route`), vous devez suivre cette procédure pour mettre à jour votre mappage pour utiliser l' `event filter`, `event notification`, et `event notification destination` jeux de commandes.

### Étapes

1. Répertoriez toutes les destinations d'événements du système à l'aide du `event destination show` commande.

```
cluster-1::event*> destination show
```

Hide

| Name | Mail Dest. | SNMP Dest. | Syslog Dest. |
|------|------------|------------|--------------|
|------|------------|------------|--------------|

Params

|           |              |   |   |
|-----------|--------------|---|---|
| allevents | -            | - | - |
| false     |              |   |   |
| asup      | -            | - | - |
| false     |              |   |   |
| criticals | -            | - | - |
| false     |              |   |   |
| pager     | -            | - | - |
| false     |              |   |   |
| test      | test@xyz.com | - | - |
| false     |              |   |   |
| traphost  | -            | - | - |
| false     |              |   |   |

6 entries were displayed.

2. Pour chaque destination, répertoriez les événements qui lui sont mappés à l'aide de l' `event route show -destinations <destination name>` commande.

```
cluster-1::event*> route show -destinations test
```

| Time                       | Message       | Severity | Destinations | Threshd | Freq |
|----------------------------|---------------|----------|--------------|---------|------|
| raid.aggr.autoGrow.abort   | NOTICE        | test     | 0            | 0       |      |
| raid.aggr.autoGrow.success | NOTICE        | test     | 0            | 0       |      |
| raid.aggr.lock.conflict    | INFORMATIONAL | test     | 0            | 0       |      |
| raid.aggr.log.CP.count     | DEBUG         | test     | 0            | 0       |      |

4 entries were displayed.

3. Créer un correspondant `event filter` qui inclut tous ces sous-ensembles d'événements.  
Par exemple, si vous souhaitez inclure uniquement le `raid.aggr.*` les événements, utilisez un caractère générique pour le `message-name` paramètre lors de la création du filtre. Vous pouvez également créer des filtres pour des événements uniques.



Vous pouvez créer jusqu'à 50 filtres d'événements.

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule Rule Message Name SNMP Trap Type
Severity
 Position Type

test_events
 1 include raid.aggr.* * *
 2 exclude * * *
2 entries were displayed.
```

4. Créez un event notification destination pour chacune des event destination Terminaux (SMTP/SNMP/syslog)

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name Type Destination

dest1 email test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost snmp - (from "system snmp traphost")
2 entries were displayed.
```

5. Créez une notification d'événement en mappant le filtre d'événement à la destination de notification d'événement.

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID Filter Name Destinations

1 default-trap-events snmp-traphost
2 asup_events dest1
2 entries were displayed.
```

6. Répétez les étapes 1 à 1-5 pour chaque event destination cela a un event route mappage.



Les événements routés vers des destinations SNMP doivent être mappés à l' snmp-traphost destination de la notification d'événement. La destination de Traphost SNMP utilise le Traphost configuré par le système.

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
 scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135> Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

 Destination Name: snmp-traphost
 Type of Destination: snmp
 Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
 Client Certificate Issuing CA: -
 Client Certificate Serial Number: -
 Client Certificate Valid?: -
```

# Référence de commande ONTAP

Pour chaque version majeure de ONTAP, les commandes CLI les plus courantes (pages de manuel ONTAP ou pages de manuel) sont regroupées dans un *command Reference*. Ces références de commandes expliquent comment utiliser les commandes CLI dans chaque version de ONTAP. Les pages man sont également disponibles sur la ligne de commande ONTAP avec le `man` commande.

## Références des commandes pour les versions prises en charge de ONTAP

- ["ONTAP 9.15.1"](#)
- ["ONTAP 9.14.1"](#)
- ["ONTAP 9.13.1"](#)
- ["ONTAP 9.12.1"](#)
- ["ONTAP 9.11.1"](#)
- ["ONTAP 9.10.1"](#)
- ["ONTAP 9.9.1"](#)
- ["ONTAP 9.8"](#)
- ["ONTAP 9.7"](#)
- ["ONTAP 9.6"](#)
- ["ONTAP 9.5"](#)
- ["ONTAP 9.3"](#)

## Références des commandes pour les versions de support limitées de ONTAP (PDF uniquement)

- ["ONTAP 9.4"](#)
- ["ONTAP 9.2"](#)
- ["ONTAP 9.1"](#)

## Outil de comparaison CLI

Pour en savoir plus sur les modifications apportées aux commandes de l'interface de ligne de commandes entre les versions de ONTAP, consultez le ["Outil de comparaison CLI"](#) Sur le site de support NetApp.

### Plus de lecture

- [Utilisez l'interface de ligne de commande ONTAP](#)
- [Méthodes de navigation dans les répertoires de commandes CLI](#)



# Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

## Droits d'auteur

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l'adresse suivante :

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Politique de confidentialité

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## Source ouverte

Les fichiers de notification fournissent des informations sur les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp.

### ONTAP

["Avis pour ONTAP 9.15.1"](#)

["Avis pour ONTAP 9.15.0"](#)

["Avis pour ONTAP 9.14.1"](#)

["Avis pour ONTAP 9.14.0"](#)

["Avis pour ONTAP 9.13.1"](#)

["Notification relative à ONTAP 9.12.1"](#)

["Notification relative à ONTAP 9.12.0"](#)

["Notification relative à ONTAP 9.11.1"](#)

["Notification relative à ONTAP 9.10.1"](#)

["Avis pour ONTAP 9.10.0"](#)

["Notification relative à ONTAP 9.9.1"](#)

["Notification relative à ONTAP 9.8"](#)

["Avis pour ONTAP 9.7"](#)

["Avis pour ONTAP 9.6"](#)

["Avis pour ONTAP 9.5"](#)

["Avis pour ONTAP 9.4"](#)

"Avis pour ONTAP 9.3"

"Avis pour ONTAP 9.2"

"Avis pour ONTAP 9.1"

## **ONTAP Mediator pour les configurations IP MetroCluster**

"9.9.1 Avis concernant le médiateur ONTAP pour les configurations IP MetroCluster" "9.8 Avis concernant le médiateur ONTAP pour les configurations IP MetroCluster" "9.7 Avis concernant le médiateur ONTAP pour les configurations IP MetroCluster"

## Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

**LÉGENDE DE RESTRICTION DES DROITS :** L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.