Rapports techniques de ONTAP

ONTAP Technical Reports

NetApp
January 23, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/ontap-technical-reports/index.html on January 23, 2026. Always check docs.netapp.com for the latest.

Sommaire

Rapports techniques de ONTAP

ONTAP et rapports techniques sur les applications et les bases de données

ONTAP constitue le socle de la gestion et de la protection des données pour de nombreuses applications d'entreprise et technologies de base de données. Ces rapports techniques fournissent des conseils sur les pratiques recommandées par NetApp et les procédures d'implémentation pour Microsoft SQL Server, MySQL, Oracle, PostgreSQL, SAP HANA et Epic.

Microsoft SQL Server

SQL Server constitue le socle de la plateforme de données Microsoft. Il apporte les performances stratégiques grâce aux technologies in-memory et permet d'obtenir plus rapidement des informations sur toutes les données, qu'elles soient sur site ou dans le cloud.

"Bonne pratique pour Microsoft SQL Server avec ONTAP" Découvrez comment les administrateurs du stockage et des bases de données peuvent réussir le déploiement de Microsoft SQL Server sur un système de stockage ONTAP.

Cette documentation remplace le rapport technique *TR-4590 : guide des meilleures pratiques pour Microsoft SQL Server avec ONTAP.*

"Tr-4976 : performances de Microsoft SQL Server virtualisé sur les systèmes NetApp AFF A-Series et C-Series"
Découvrez les caractéristiques de performances de Microsoft SQL Server avec les systèmes NetApp AFF A-Series et C-Series, ainsi que des conseils pour sélectionner le système adapté à la charge de travail.

"Tr-4714 : meilleures pratiques pour Microsoft SQL Server avec SnapCenter"
Apprenez à déployer Microsoft SQL Server sur un système de stockage ONTAP à l'aide de la technologie SnapCenter pour la protection des données.

MySQL

Ce document décrit la configuration requise et fournit des conseils sur le réglage et la configuration du stockage pour le déploiement de MySQL sur ONTAP.

"Base de données MySQL sur les bonnes pratiques NetApp ONTAP" MySQL et ses variantes, dont MariaDB et Percona, sont largement utilisés pour de nombreuses applications d'entreprise. Ces applications vont des sites de réseaux sociaux mondiaux, des systèmes de commerce électronique massifs aux systèmes d'hébergement SMB contenant des milliers d'instances de base de données. Découvrez la configuration requise et les conseils d'ajustement et de configuration du stockage pour le déploiement de MySQL sur ONTAP.

Cette documentation remplace le rapport technique *TR-4722 : base de données MySQL sur les meilleures pratiques NetApp ONTAP.*

Oracle

ONTAP est conçu pour les bases de données Oracle. Pendant des décennies, ONTAP a été optimisé pour les demandes uniques d'E/S de bases de données relationnelles. Plusieurs fonctionnalités ONTAP ont été créées spécifiquement pour répondre aux besoins des bases de données Oracle, et même à la demande d'Oracle Inc. Elle-même.

"Bases de données Oracle sur ONTAP" Découvrez les pratiques recommandées pour déployer Oracle sur un système de stockage ONTAP par les administrateurs de bases de données et de stockage.

"Protection des données Oracle avec ONTAP" Découvrez les pratiques recommandées pour permettre aux administrateurs du stockage et des bases de données de sauvegarder, restaurer, répliquer et fournir une reprise après incident dans Oracle sur le stockage ONTAP.

"Reprise après incident Oracle avec ONTAP" Découvrez les pratiques recommandées, les procédures de test et d'autres considérations à prendre en compte pour l'exploitation de bases de données Oracle sur une continuité de l'activité MetroCluster et SnapMirror.

"Migration des bases de données Oracle vers des systèmes de stockage ONTAP" Découvrez les facteurs généraux à prendre en compte lors de la planification d'une stratégie de migration, les trois niveaux de déplacement des données et quelques-unes des procédures disponibles.

> La documentation décrite ci-dessus remplace les rapports techniques *TR-3633 : bases de données Oracle sur ONTAP ; TR-4591 : protection des données Oracle : sauvegarde, restauration, réplication ; TR-4592 : Oracle sur MetroCluster ; et TR-4534 : migration des bases de données Oracle vers des systèmes de stockage NetApp*

"Tr-4969 : performances des bases de données Oracle sur les systèmes AFF A-Series et C-Series"
ONTAP est une puissante plateforme de gestion des données dont les fonctionnalités natives comprennent la compression à la volée, les mises à niveau matérielles sans interruption et l'importation d'un LUN à partir d'une baie de stockage étrangère. Il est possible de mettre en cluster jusqu'à 24 nœuds pour assurer le service de données simultanément via les protocoles NFS (Network File System), SMB (Server message Block), iSCSI, FC (Fibre Channel) et NVMe (Nonvolatile Memory Express). De plus, la technologie Snapshot constitue la base de la création de dizaines de milliers de sauvegardes en ligne et de clones de bases de données entièrement opérationnels. Outre l'ensemble de fonctionnalités avancées de ONTAP, les besoins des utilisateurs sont très variés, notamment en termes de taille, de performances et de protection des données. Découvrez les performances des bases de données sans système d'exploitation grâce aux systèmes de stockage AFF, y compris Les Gammes A-Series et C-Series. Elles couvrent les valeurs maximales et la différence pratique entre les deux options AFF.

"Tr-4971 : performances des bases de données Oracle virtualisées sur les systèmes AFF A-Series et C-Series"
ONTAP est une puissante plateforme de gestion des données dont les fonctionnalités natives comprennent la compression à la volée, les mises à niveau matérielles sans interruption et l'importation d'un LUN à partir d'une baie de stockage étrangère. Il est possible de mettre en cluster jusqu'à 24 nœuds pour assurer le service de données simultanément via les protocoles NFS (Network File System), SMB (Server message Block), iSCSI, FC (Fibre Channel) et NVMe (Nonvolatile Memory Express). De plus, la technologie Snapshot constitue la base de la création de dizaines de milliers de sauvegardes en ligne et de clones de bases de données entièrement opérationnels. Outre l'ensemble de fonctionnalités avancées de ONTAP, les besoins des utilisateurs sont très variés, notamment en termes de taille, de performances et de protection des données. Découvrez les performances des bases de données virtualisées grâce aux systèmes de stockage AFF, y compris Les Gammes A-Series et C-Series. Elles couvrent les valeurs maximales et la différence pratique entre les deux options AFF.

"Tr-4695 : hiérarchisation du stockage de base de données avec FabricPool"
Découvrez les avantages et les options de configuration de FabricPool avec diverses bases de données, notamment le système de gestion de bases de données relationnelles (SGBDR) d'Oracle.

"Tr-4899 : basculement transparent des applications de la base de données Oracle avec synchronisation active SnapMirror" La synchronisation active SnapMirror (anciennement SM-BC) et Oracle Real application Cluster (RAC) permettent un basculement transparent des applications et une continuité en cas de panne sur site ou d'incident. Découvrez les conseils de configuration et les pratiques recommandées pour une baie de stockage AFF avec SnapMirror Active Sync comme composant de stockage d'Oracle RAC.

"Tr-4876 : meilleures pratiques de déploiement et de colocation Oracle avec la solution ONTAP"
Découvrez les pratiques recommandées par la solution pour provisionner, gérer et protéger les bases de données Oracle mutualisées à l'aide du stockage ONTAP afin d'optimiser les avantages des bases de données Oracle mutualisées et des fonctionnalités du logiciel ONTAP.

PostgreSQL

PostgreSQL est fourni avec des variantes incluant PostgreSQL, PostgreSQL plus et EDB Postgres Advanced Server (EPAS). PostgreSQL est généralement déployé en tant que base de données interne pour les applications multiniveaux. NetApp ONTAP constitue un excellent choix pour l'exécution des bases de données PostgreSQL et ses fonctionnalités de gestion des données fiables, performantes et efficaces.

"Base de données PostgreSQL sur les bonnes pratiques ONTAP" PostgreSQL est fourni avec des variantes incluant PostgreSQL, PostgreSQL plus et EDB Postgres Advanced Server (EPAS). PostgreSQL est généralement déployé en tant que base de données interne pour les applications à plusieurs niveaux. Il est pris en charge par les logiciels middleware courants (tels que PHP, Java, Python, Tcl/TK, ODBC, Et JDBC) et a toujours été un choix populaire pour les systèmes de gestion de bases de données open source. Découvrez les exigences de configuration et les conseils sur l'ajustement et la configuration du stockage pour le déploiement de PostgreSQL sur ONTAP.

Cette documentation remplace le rapport technique *TR-4770 : base de données PostgreSQL sur les meilleures pratiques ONTAP*.

SAP HANA

"Solutions de base de données SAP HANA sur ONTAP" Les bonnes pratiques de configuration, de gestion et d'automatisation des solutions SAP sont disponibles sur la page Solutions SAP de NetApp.

Epic

"Meilleures pratiques Epic sur ONTAP" Guide pour comprendre les bonnes pratiques de déploiement d'Epic sur site et dans le cloud, tout en respectant les normes de configuration et en vue d'un déploiement correct sur ONTAP.

Cette documentation remplace le rapport technique *TR-3923 : meilleures pratiques NetApp pour Epic*.

Rapports techniques sur la continuité de l'activité

NetApp propose une large gamme de solutions permettant de choisir l'emplacement optimal pour vos applications et vos données de manière à améliorer les performances à moindre coût. Protection des données, réplication et disponibilité continue : la gestion des données ONTAP simplifie la protection des données à l'aide d'une gestion des règles en une seule étape, tout en assurant la continuité de l'activité avec la synchronisation active MetroCluster et SnapMirror.

Ces rapports techniques étendent la documentation sur "Synchronisation active de ONTAP SnapMirror" les produits et "ONTAP MetroCluster" .

SnapMirror actif sync (anciennement SM-BC)

"Tr-4878 : synchronisation active SnapMirror" SnapMirror Active Sync est une solution de stockage disponible en continu avec une granularité au niveau des applications. Elle est disponible pour ONTAP sur les systèmes de stockage AFF ou ASA, afin de répondre aux besoins RPO 0 et RTO 0 des applications d'entreprise les plus stratégiques.

MetroCluster

"Tr-4705 : architecture et conception de la solution NetApp MetroCluster"
Ce document présente l'architecture générale et les concepts de conception des fonctionnalités MetroCluster dans ONTAP.

Les IP dans MetroCluster

"Tr-4689 : IP NetApp MetroCluster" MetroCluster est une solution de stockage disponible en continu pour ONTAP sur les systèmes FAS et AFF. MetroCluster IP est la dernière évolution qui utilise un fabric de stockage back-end basé sur Ethernet. MetroCluster IP fournit une configuration hautement redondante afin de répondre aux besoins des applications d'entreprise les plus stratégiques. MetroCluster IP est inclus dans ONTAP et fournit une connectivité NAS et SAN pour les clients et les serveurs qui utilisent le stockage ONTAP.

Les FC dans MetroCluster

"Tr-4375 : FC NetApp MetroCluster" MetroCluster assure une disponibilité continue des données dans les data centers répartis géographiquement pour les applications stratégiques. Découvrez les pratiques recommandées, les décisions de conception et les configurations prises en charge par MetroCluster FC.

Rapports techniques sur la protection des données et la reprise après incident ONTAP

SnapMirror est une solution de réplication unifiée économique et facile à utiliser dans l'environnement Data Fabric. Il réplique les données à haute vitesse sur un WAN ou un LAN. Vous bénéficiez ainsi de données hautement disponibles et d'une réplication rapide des données de vos applications stratégiques, comme Microsoft Exchange, Microsoft SQL Server et Oracle, dans les environnements traditionnels et virtualisés. En répliquant vos données sur un ou plusieurs systèmes de stockage ONTAP, puis en les mettant régulièrement à jour, vous disposez de données actualisées et accessibles dès que vous en avez besoin. Aucun serveur de réplication externe n'est requis.

Ces rapports techniques sont détaillés dans "Protection des données et reprise après incident ONTAP"la documentation produit.

SnapMirror

Réplication asynchrone SnapMirror

"Tr-4015 : configuration asynchrone SnapMirror et bonnes pratiques" Découvrez les pratiques recommandées pour la configuration de la réplication asynchrone SnapMirror (SM-A) des volumes, des groupes de cohérence et des machines virtuelles de stockage (reprise après incident de SVM).

"Tr-4678 : protection des données et sauvegarde des volumes ONTAP FlexGroup"
Découvrez les recommandations de protection et de sauvegarde des données pour les volumes FlexGroup. Et notamment les copies Snapshot, SnapMirror ainsi que d'autres solutions de protection et de sauvegarde des données.

SnapMirror synchrone

"Tr-4733 : configuration synchrone SnapMirror et bonnes pratiques" Découvrez les pratiques recommandées pour la configuration de la réplication synchrone SnapMirror (SM-S).

Reprise après incident SnapMirror à trois data centers

"Tr-4832 : reprise après incident à trois data centers avec SnapMirror NetApp pour ONTAP 9.7" Découvrez une configuration de reprise après incident à trois data centers qui utilise la technologie ONTAP SnapMirror pour la réplication.

Application et infrastructure avec SnapMirror

"Tr-4900 : VMware site Recovery Manager avec ONTAP" Depuis son introduction dans le data Center moderne en 2002, ONTAP est une solution de stockage leader pour les environnements VMware vSphere. De plus, il continue d'ajouter des fonctionnalités innovantes pour simplifier la gestion tout en réduisant les coûts. Découvrez les recommandations de la solution ONTAP pour VMware site Recovery Manager (SRM), le logiciel de reprise après incident de pointe de VMware, notamment les dernières informations produit et les pratiques recommandées pour rationaliser le déploiement, réduire les risques et simplifier la gestion au quotidien.

Cyber-coffre ONTAP

"Cyber-coffre ONTAP" Le cyber-coffre basé sur ONTAP de NetApp offre aux entreprises une solution complète et flexible pour protéger leurs données les plus stratégiques. En exploitant la « Air gapping » logique associée à des méthodologies de renforcement solides, ONTAP vous permet de créer des environnements de stockage isolés et sécurisés, résilients face aux cybermenaces en constante évolution. Avec ONTAP, vous pouvez assurer la confidentialité, l'intégrité et la disponibilité de vos données tout en conservant l'agilité et l'efficacité de votre infrastructure de stockage.

Rapports techniques de volume sur ONTAP FlexCache et FlexGroup

Grâce à ces solutions, vous pouvez simplifier la gestion des données et suivre le rythme de la croissance tout en optimisant les coûts. NetApp Les solutions ONTAP NAS assurent la continuité de l'activité, améliorent l'efficacité et offrent une évolutivité transparente, le tout dans une architecture unifiée. Optimisé par ONTAP, le stockage NAS scale-out tire parti de l'énorme écosystème ONTAP, avec une avance significative en matière d'innovation et une vision pour l'innovation future agressive.

Ces rapports techniques étendent la documentation sur "Volume ONTAP FlexCache" les produits et "Volume ONTAP FlexGroup" .

FlexCache

"Tr-4743 : FlexCache dans ONTAP"
FlexCache est une technologie de mise en cache qui crée des répliques inscriptibles clairsemées de volumes sur les mêmes clusters ONTAP ou sur des clusters différents. Il peut rapprocher les données et les fichiers de l'utilisateur pour un débit plus rapide et une empreinte moindre. Découvrez comment FlexCache peut être utilisé, les pratiques recommandées, les limites et les considérations à prendre en compte pour la conception et l'implémentation.

Réécriture de code FlexCache

"Réécriture de code FlexCache" Introduit dans ONTAP 9.15.1, l'écriture différée FlexCache est un autre mode de fonctionnement pour l'écriture au niveau du cache. L'écriture différée permet d'engager l'écriture sur un stockage stable au niveau du cache et d'en accuser réception au client sans attendre que les données soient à l'origine. Les données sont transférées de manière asynchrone vers l'origine. Le résultat est un système de fichiers distribué à l'échelle mondiale qui permet aux écritures d'effectuer des opérations à des vitesses proches de celles locales pour des charges de travail et des environnements spécifiques, et qui offre des avantages considérables en termes de performances.

Volumes FlexGroup

"Tr-4571a : les dix meilleures pratiques de FlexGroup"
Ce rapport technique est une version condensée du document TR-4571 : meilleures pratiques des volumes NetApp ONTAP FlexGroup et guide d'implémentation pour une consommation rapide.

"Tr-4557 : volumes NetApp ONTAP FlexGroup : présentation technique"
Découvrez FlexGroup volumes, un conteneur NAS scale-out ONTAP, qui allie une capacité quasi illimitée et des performances prévisibles à faible latence pour les charges de travail consommatrices de métadonnées.

"Tr-4571 : guide des meilleures pratiques et d'implémentation des volumes NetApp ONTAP FlexGroup"
Découvrez les volumes FlexGroup, les pratiques recommandées et des conseils d'implémentation. Les volumes FlexGroup font partie de l'évolution des conteneurs NAS scale-out de ONTAP. Ils allient une capacité presque illimitée et des performances prévisibles à une faible latence pour les charges de travail consommatrices de métadonnées.

"Tr-4678 : protection des données et sauvegarde des volumes FlexGroup"

Découvrez la protection et la sauvegarde des données pour les volumes FlexGroup, notamment les copies Snapshot, SnapMirror et d’autres solutions de protection et de sauvegarde des données.

Rapports techniques sur ONTAP NAS

Grâce à ces solutions, vous pouvez simplifier la gestion des données et suivre le rythme de la croissance tout en optimisant les coûts. NetApp Les solutions NAS de ONTAP assurent la continuité de l'activité, l'efficacité et une évolutivité transparente au sein d'une architecture unifiée. Optimisé par NetApp ONTAP, le stockage NAS scale-out tire parti de l'énorme écosystème ONTAP, avec une avance significative en matière d'innovation et une vision pour l'innovation future agressive.

Ces rapports techniques étendent la documentation sur "Gestion du stockage NAS ONTAP" les produits et "Gestion du stockage ONTAP S3" .

NFS

"Tr-4067 : guide des bonnes pratiques et d'implémentation NFS dans ONTAP"
Découvrez les concepts de base, les informations de support, des conseils de configuration et les recommandations pour NFS dans ONTAP.

"Tr-4962 : attributs étendus NFSv4.2"
Découvrez comment activer et utiliser les attributs étendus NFSv4.2 dans ONTAP 9.12.1 et versions ultérieures.

PME

"Tr-4740 : multicanal SMB 3.0"
Microsoft a introduit Multicanal dans le protocole SMB 3.0 dans le but d'améliorer le protocole SMB3 en répondant aux limites de performances et de fiabilité de SMB1 et SMB2. Découvrez la fonctionnalité multicanal de ONTAP, notamment ses fonctionnalités, ses pratiques recommandées et les résultats des tests de performances.

Multiprotocole

"Tr-4887 : présentation et bonnes pratiques du stockage NAS multiprotocole dans ONTAP"
Découvrez le fonctionnement de l'accès NAS multiprotocole dans ONTAP et les pratiques recommandées pour les environnements multiprotocoles.

ONTAP S3

"Tr-4814 : S3 dans les bonnes pratiques ONTAP" Découvrez les pratiques recommandées pour l'utilisation d'Amazon simple Storage Service (S3) avec le logiciel ONTAP ainsi que les fonctionnalités et configurations pour l'utilisation d'ONTAP en tant que magasin d'objets avec les applications S3 natives ou en tant que destination de Tiering pour FabricPool.

Nommer les services

"Tr-4523 : équilibrage de la charge DNS dans ONTAP"
Découvrez comment configurer ONTAP pour une utilisation avec les méthodologies d'équilibrage de la charge DNS, y compris DNS dans ONTAP, les différentes méthodes de configuration et les pratiques recommandées.

"Tr-4668 : guide des meilleures pratiques des services de noms"
Découvrez les pratiques recommandées, les limites et les considérations à prendre en compte lors de l'implémentation de solutions de stockage NAS (Network-Attached Storage), telles que CIFS/SMB et NFS dans ONTAP.

"Tr-4835 : configuration du protocole LDAP dans la gestion multiprotocole des identités NAS de ONTAP"
Découvrez comment configurer la gestion des identités LDAP (Lightweight Directory Access Protocol) dans ONTAP pour NAS multiprotocole.

Sécurité NAS

"Tr-4616 : NFS Kerberos dans ONTAP"
Découvrez le protocole Kerberos NFS dans ONTAP, notamment les étapes de configuration avec les clients Active Directory et Red Hat Enterprise Linux (RHEL).

Rapports techniques sur la mise en réseau ONTAP

ONTAP propose une vaste gamme de fonctionnalités et de configurations réseau pour répondre aux besoins des applications scale-out les plus exigeantes. Grâce aux fonctionnalités et fonctionnalités de mise en réseau, les entreprises peuvent créer un accès fiable et sécurisé à leurs données.

Ces rapports techniques sont détaillés dans "Gestion de réseau ONTAP"la documentation produit.

"Tr-4949 : BGP/VIP avec ONTAP dans le data Center"
Apprenez à déployer rapidement une configuration BGP de base dans ONTAP.

Rapports techniques sur les SAN ONTAP

Le stockage SAN de ONTAP offre une expérience SAN simplifiée qui assure la haute disponibilité des bases de données stratégiques de votre entreprise et d'autres workloads SAN. Grâce à l'intégration de services de données exceptionnels avec les bases de données Oracle, SAP et Microsoft SQL Server, ainsi que l'utilisation de VMware et d'autres hyperviseurs de premier plan, les systèmes SAN ONTAP accélèrent le retour sur investissement des applications de bases de données d'entreprise.

Ces rapports techniques sont détaillés dans "Gestion du stockage SAN ONTAP"la documentation produit.

"Tr-4080 : bonnes pratiques pour le SAN moderne dans ONTAP"
Découvrez les protocoles de niveau bloc dans ONTAP ainsi que des recommandations.

"Tr-4684 : implémentation et configuration de SAN modernes avec NVMe over Fabrics (NVMe-of)"
Découvrez comment implémenter et configurer le transport NVMe over Fabrics (NVMe over Fibre Channel et NVMe over TCP). Il aborde des thèmes tels que la conception, l'implémentation, la configuration, les instructions de gestion, ainsi que les pratiques recommandées pour créer des solutions SAN modernes haute disponibilité et haute performance basées sur les protocoles et les transports NVMe.

"Tr-4968 : disponibilité et intégrité des données des baies 100 % SAN NetApp"
Découvrez comment les différentes fonctionnalités de protection et d'intégrité des données des systèmes SAN fonctionnent pour optimiser la continuité des applications, ainsi que les pratiques recommandées pour la conception, l'implémentation et la gestion d'un réseau SAN.

"Solution Flash connectée au cloud SAN moderne"
Cette architecture vérifiée NetApp a été conçue et vérifiée conjointement par NetApp, VMware et Broadcom. Elle utilise les dernières solutions technologiques Brocade, Emulex et VMware vSphere ainsi que le stockage 100 % Flash NetApp, qui définit un nouveau standard en matière de stockage SAN d'entreprise et de protection des données pour une plus grande valeur commerciale.

Sécurité

Rapports techniques sur la sécurité ONTAP

ONTAP continue d'évoluer, et la sécurité fait partie intégrante de la solution. Les dernières versions d'ONTAP comprennent bon nombre de nouvelles fonctions de sécurité essentielles pour protéger les données de l'entreprise dans le cloud hybride, éviter les attaques par ransomware et se conformer aux pratiques recommandées par le secteur. Ces nouvelles fonctionnalités contribuent également à l'adoption d'un modèle « zéro confiance ».

Ces rapports techniques sont détaillés dans "Sécurité et chiffrement des données ONTAP"la documentation produit.

Cyber-coffre ONTAP

"Cyber-coffre ONTAP" Le cyber-coffre basé sur ONTAP de NetApp offre aux entreprises une solution complète et flexible pour protéger leurs données les plus stratégiques. En exploitant la « Air gapping » logique associée à des méthodologies de renforcement solides, ONTAP vous permet de créer des environnements de stockage isolés et sécurisés, résilients face aux cybermenaces en constante évolution. Avec ONTAP, vous pouvez assurer la confidentialité, l'intégrité et la disponibilité de vos données tout en conservant l'agilité et l'efficacité de votre infrastructure de stockage.

Attaques par ransomware

"Tr-4572 : la solution NetApp pour ransomware" Découvrez l'évolution des ransomwares et comment identifier les attaques, prévenir la propagation et restaurer les données aussi rapidement que possible grâce à la solution NetApp pour ransomware. Les conseils et solutions fournis dans ce document sont conçus pour aider les entreprises à disposer de solutions de cyberrésilience tout en respectant leurs objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité des systèmes d'information.

"Tr-4526 : stockage WORM conforme avec NetApp SnapLock"
De nombreuses entreprises ont recours au stockage des données WORM (Write Once, Read Many) pour respecter les exigences de conformité réglementaires, ou simplement pour ajouter une couche supplémentaire à leur stratégie de protection des données. Découvrez comment intégrer SnapLock, la solution WORM de ONTAP, dans des environnements qui nécessitent le stockage de données WORM.

Zéro confiance

"NetApp et le modèle « zéro confiance »" La solution « zéro confiance » s'est traditionnellement orientée réseau pour structurer les microsegments et le périmètre (MCAP) afin de protéger les données, les services, les applications ou les ressources grâce à des contrôles appelés « passerelle de segmentation ». ONTAP adopte une approche « zéro confiance » centrée sur les données, dans laquelle le système de gestion du stockage devient la passerelle de segmentation pour protéger et surveiller l'accès aux données de nos clients. Le moteur « zéro confiance » FPolicy et l'écosystème de partenaires FPolicy deviennent un centre de contrôle pour obtenir une compréhension détaillée des modèles d'accès aux données normaux et aberrants et identifier les menaces internes.

Authentification multifacteur

"Tr-4647 : guide d'implémentation et des bonnes pratiques pour l'authentification multifacteur dans ONTAP"
Découvrez la fonctionnalité d'authentification multifacteur d'ONTAP pour un accès administratif via System Manager, Active IQ Unified Manager et l'authentification CLI ONTAP Secure Shell (SSH).

"Tr-4717 : authentification ONTAP SSH avec une carte d'accès commune"
Découvrez comment configurer et tester des clients SSH tiers, en association avec le logiciel ActivClient, pour authentifier un administrateur de stockage ONTAP via la clé publique stockée sur une carte d'accès commun (CAC) lorsqu'elle est configurée dans ONTAP.

Colocation

"Tr-4160 : Colocation sécurisée dans ONTAP"
Découvrez comment implémenter la colocation sécurisée à l'aide des VM de stockage dans ONTAP, y compris les considérations de conception et les pratiques recommandées.

Normes

"Tr-4401 : PCI-DSS 4.0 et ONTAP"
Découvrez comment valider un système par rapport à la norme PCI DSS 4.0 et répondre aux exigences des contrôles que vous appliquez à un système NetApp ONTAP.

Contrôle d'accès basé sur les attributs

"Contrôle d'accès basé sur les attributs avec ONTAP" Apprenez à configurer les étiquettes de sécurité NFSv4.2 et les attributs étendus (xattrs) pour prendre en charge le contrôle d'accès basé sur les rôles (RBAC) et le contrôle d'accès basé sur les attributs (ABAC), une stratégie d'autorisation qui définit des autorisations basées sur les attributs utilisateur, ressource et environnement.

Solution NetApp pour ransomware

Attaques par ransomware et portefeuille de solutions de protection de NetApp

Les ransomwares restent l'une des menaces les plus importantes qui ont entraîné des interruptions d'activité pour les entreprises en 2024. D'après le "Sophos : État des ransomware 2024", les attaques par ransomware ont affecté 72 % de leur public interrogé. Les attaques par ransomware ont évolué pour être plus sophistiquées et ciblées : les acteurs de menaces utilisent des techniques avancées, telles que l'intelligence artificielle, pour optimiser leur impact et leurs bénéfices.

Les entreprises doivent regarder l'ensemble de leur posture de sécurité du périmètre, du réseau, de l'identité, des applications et de l'emplacement des données au niveau du stockage, et sécuriser ces couches. L'adoption d'une approche axée sur les données en matière de cybersécurité au niveau de la couche de stockage est cruciale dans le paysage actuel des menaces. Bien qu'aucune solution ne puisse déjouer toutes les attaques, l'utilisation d'un portefeuille de solutions, notamment des partenariats et des tiers, offre une défense multicouche.

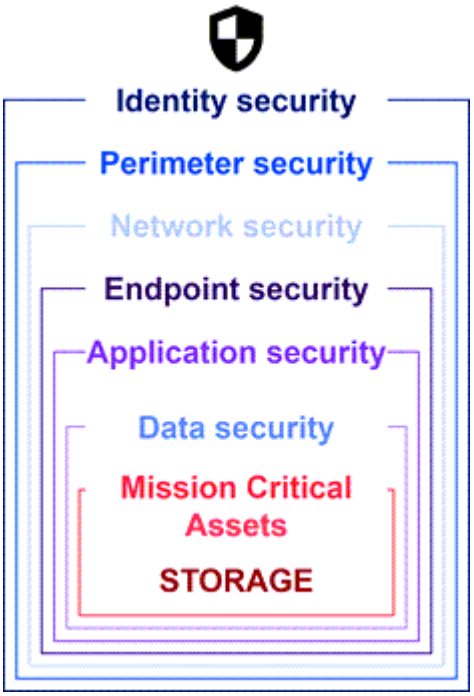
Le Gamme de produits NetApp fournit divers outils efficaces pour la visibilité, la détection et la résolution des problèmes, ce qui vous aide à détecter rapidement les ransomware, à prévenir la propagation et à restaurer rapidement, si nécessaire, pour éviter les interruptions coûteuses. Les solutions de défense à plusieurs

couches classiques restent répandues, tout comme les solutions tierces et partenaires pour la visibilité et la détection. Une solution efficace reste une partie essentielle de la réponse à toute menace. L'approche unique du secteur qui repose sur la technologie NetApp Snapshot immuable et la solution SnapLock Logical Air Gap est un atout concurrentiel dans le secteur et constitue la bonne pratique du secteur pour la résolution des problèmes par ransomware.

À partir de juillet 2024, le contenu du rapport technique *TR-4572: NetApp ransomware protection*, qui a été publié au format PDF, est disponible sur docs.netapp.com.

Les données sont la cible principale

Les cybercriminels ciblent de plus en plus directement les données, en reconnaissant leur valeur. Bien que la sécurité du périmètre, du réseau et des applications soit importante, il est possible de les contourner. La couche de stockage, qui se concentre sur la protection des données à la source, constitue une dernière ligne de défense critique. Les attaques par ransomware ont pour objectif d'accéder aux données de production et de les chiffrer ou de les rendre inaccessibles. Pour y parvenir, les attaquants doivent déjà avoir percé les défenses existantes déployées par les entreprises aujourd'hui, du périmètre à la sécurité des applications.



Malheureusement, de nombreuses entreprises ne tirent pas parti des fonctionnalités de sécurité au niveau de la couche de données. C'est là qu'intervient la gamme de solutions NetApp pour la protection contre les ransomwares, pour vous protéger dans votre dernier domaine de défense.

Le vrai coût des ransomwares

Le paiement d'une rançon en elle-même n'a pas le plus grand effet financier sur une entreprise. Bien que le paiement ne soit pas insignifiant, il reste insignifiant comparé au coût des temps d'indisponibilité liés à un incident d'ransomware.

Le paiement d'une rançon n'est qu'un élément du coût de la récupération lorsqu'il s'agit de faire face à des attaques par ransomware. En excluant toute rançon payée, les entreprises ont déclaré en 2024 un coût moyen de restauration suite à une attaque par ransomware de 2,7 millions de dollars, soit une augmentation de près de 1 million de dollars par rapport aux 1,2 million de dollars rapportés en 2023 "2024 Sophos State of ransomware". Les coûts peuvent être 10 fois plus élevés pour les entreprises qui dépendent fortement de la

disponibilité INFORMATIQUE, telles que l'e-commerce, les actions boursières et les soins de santé.

Les coûts de la cyberassurance continuent également d'augmenter, étant donné la très réelle probabilité d'une attaque par ransomware sur les entreprises assurées.

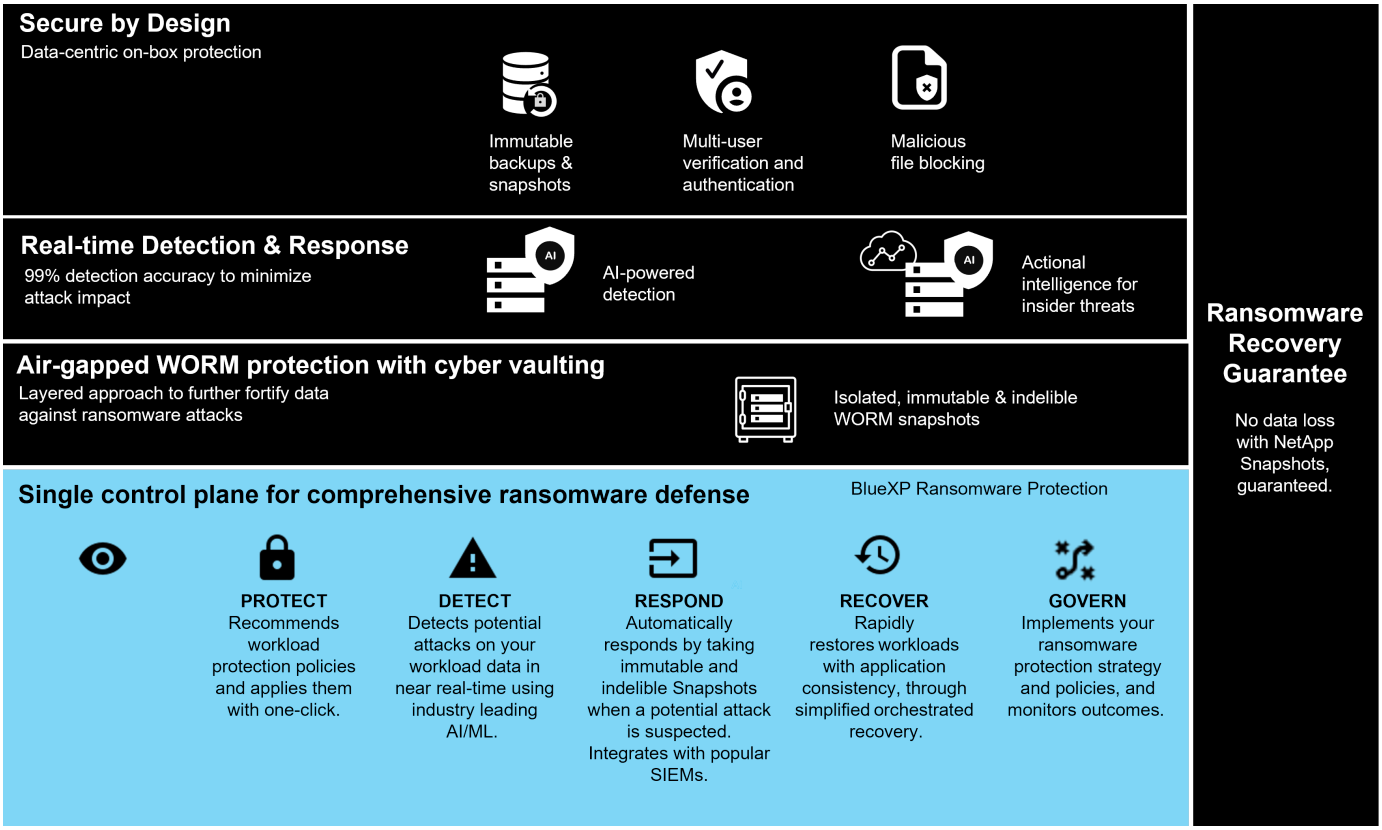
Protection contre les ransomware au niveau de la couche de données

NetApp comprend que la sécurité de votre entreprise est vaste et approfondie dans tout le périmètre, jusqu'à l'emplacement des données au niveau de la couche de stockage. Votre pile de sécurité est complexe et doit assurer la sécurité à tous les niveaux de votre pile technologique.

La protection en temps réel au niveau de la couche de données est encore plus importante et a des exigences uniques. Pour être efficace, les solutions de cette couche doivent offrir les attributs critiques suivants :

- **Sécurité par conception** pour minimiser les risques d'attaque réussie
- **Détection et réponse en temps réel** pour minimiser l'impact d'une attaque réussie
- **Protection WORM à air Gap** pour isoler les sauvegardes de données critiques
- **Un seul plan de contrôle** pour une défense complète contre les ransomware

NetApp peut vous offrir tout cela et bien plus encore.



Le portefeuille de solutions NetApp pour la protection contre les ransomwares

NetApp "protection intégrée contre les ransomware"propose une défense à facettes et robuste en temps réel pour vos données stratégiques. Au cœur de ces outils, des algorithmes avancés de détection optimisés par l'IA surveillent en continu les modèles de données, ce qui permet d'identifier rapidement les menaces de ransomware avec une précision de 99 %. En réagissant rapidement aux attaques, notre stockage peut créer rapidement des snapshots de données et sécuriser les copies, assurant ainsi une restauration rapide.

Pour renforcer encore davantage les données, la "cyber-archivage" capacité de NetApp isole les données avec un air Gap logique. En protégeant les données stratégiques, nous assurons une continuité rapide de l'activité.

NetApp"Protection contre les ransomwares NetApp" réduit les charges opérationnelles avec un plan de contrôle unique pour coordonner et exécuter intelligemment une défense contre les ransomwares centrée sur la charge de travail de bout en bout, afin que vous puissiez identifier et protéger les données de charge de travail critiques à risque en un seul clic, détecter et répondre avec précision et automatiquement pour limiter l'impact d'une attaque potentielle et récupérer les charges de travail en quelques minutes, et non en quelques jours, en protégeant vos précieuses données de charge de travail et en minimisant les perturbations coûteuses.

En tant que solution ONTAP intégrée native pour protéger les accès non autorisés à vos données, "Vérification multiadministrateur" bénéficiez de fonctionnalités robustes qui assurent l'exécution des opérations telles que la suppression de volumes, la création d'utilisateurs administratifs ou la suppression de snapshots uniquement après approbation d'un second administrateur désigné. Cela empêche les administrateurs compromis, malveillants ou peu expérimentés d'effectuer des modifications ou de supprimer des données indésirables. Vous pouvez configurer autant d'approbateurs administrateurs désignés que vous le souhaitez avant de supprimer un instantané.

> NetApp ONTAP répond à la condition requise pour "Authentification multifacteur (MFA)" l'authentification Web dans System Manager et l'authentification via l'interface de ligne de commandes SSH.

Avec la protection contre les ransomwares de NetApp, travaillez sereinement dans un environnement aux menaces qui ne cesse d'évoluer. Son approche globale ne se contente pas de vous défendre contre les variantes actuelles des ransomwares. Elle s'adapte également aux menaces émergentes, assurant ainsi la sécurité à long terme de votre infrastructure de données.

Découvrez les autres options de protection

- "Protection contre les ransomware via Digital Advisor"
- "Data Infrastructure Insights Stockage Charge de travail Sécurité"
- "FPolicy"
- "SnapLock et copies Snapshot inviolables"

Garantie de restauration contre les ransomwares

NetApp garantit la restauration des données Snapshot en cas d'attaque par ransomware. Notre garantie : si nous ne pouvons pas vous aider à restaurer vos données de snapshot, nous nous engageons à trouver la solution. La garantie est disponible pour tout achat de systèmes AFF A-Series, AFF C-Series, ASA et FAS.

En savoir plus >>

- "Description du service de garantie de récupération"
- "Blog sur la garantie de restauration contre les ransomwares".

Informations associées

- "Page des ressources du site de support NetApp"
- "Sécurité des produits NetApp"

SnapLock et copies Snapshot inviolables pour la protection contre les ransomwares

SnapLock, l'une des armes essentielles de l'arsenal de NetApp Snap, s'est avéré très efficace pour protéger les données contre les menaces de ransomware. En empêchant la suppression non autorisée des données, SnapLock fournit une couche de sécurité supplémentaire qui garantit l'intégrité et l'accessibilité des données critiques, même en cas d'attaques malveillantes.

Conformité SnapLock

SnapLock Compliance (SLC) assure une protection indélébile de vos données. SLC interdit la suppression de données même lorsqu'un administrateur tente de réinitialiser la baie. Contrairement à d'autres produits concurrents, SnapLock Compliance n'est pas vulnérable aux piratages d'ingénierie sociale par l'intermédiaire des équipes de support de ces produits. Les données protégées par des volumes SnapLock Compliance peuvent être récupérables jusqu'à leur date d'expiration.

Pour activer SnapLock, une "ONTAP One" licence est requise.

En savoir plus >>

- "Documentation SnapLock"

Des snapshots inviolables

Les copies Snapshot inviolables constituent un moyen pratique et rapide de protéger vos données contre les actes malveillants. Contrairement à SnapLock Compliance, TPS est généralement utilisé sur les systèmes principaux où l'utilisateur peut protéger les données pendant un temps déterminé et les laisser localement pour des restaurations rapides ou où les données n'ont pas besoin d'être répliquées hors du système principal. TPS utilise les technologies SnapLock pour empêcher la suppression du snapshot principal, même par un administrateur ONTAP, pendant la même période d'expiration de la rétention SnapLock. La suppression de Snapshot est impossible même si le volume n'est pas activé sur SnapLock, bien que les snapshots ne possèdent pas la même nature indélébile que les volumes SnapLock Compliance.

Pour rendre les snapshots inviolables, une "ONTAP One" licence est requise.

En savoir plus >>

- "Verrouillez une copie Snapshot pour vous protéger contre les attaques par ransomware".

Blocage des fichiers FPolicy

FPolicy empêche le stockage des fichiers indésirables sur votre appliance de stockage haute performance. FPolicy vous permet également de bloquer les extensions de fichiers ransomware connues. Un utilisateur dispose toujours des autorisations d'accès complètes au dossier de départ, mais FPolicy ne permet pas à un utilisateur de stocker les fichiers marqués par votre administrateur comme bloqués. Le cas échéant, il n'est pas important que ces fichiers soient des fichiers MP3 ou des extensions de fichiers ransomware connues.

Bloquez les fichiers malveillants avec le mode natif FPolicy

Le mode natif NetApp FPolicy (une évolution du nom, la stratégie de fichiers) est un framework de blocage

d'extension de fichiers qui vous permet de bloquer les extensions de fichiers indésirables dans votre environnement. Fait partie de ONTAP depuis plus de dix ans, il est incroyablement utile pour vous protéger contre les ransomware. Ce moteur « zéro confiance » est très utile, car vous bénéficiez de mesures de sécurité supplémentaires qui vont au-delà des autorisations de liste de contrôle d'accès (ACL).

Dans ONTAP System Manager et la NetApp Console, une liste de plus de 3 000 extensions de fichiers est disponible pour référence.

> Certaines extensions peuvent être légitimes dans votre environnement et leur blocage peut entraîner des problèmes inattendus. Créez votre propre liste adaptée à votre environnement avant de configurer FPolicy natif.

Le mode natif FPolicy est inclus dans toutes les licences ONTAP.

En savoir plus >>

- "Blog : lutter contre les ransomware : troisième partie : ONTAP FPolicy, un autre outil puissant et natif (appelé gratuitement)"

Activez l'analyse du comportement des utilisateurs et des entités (UEBA) avec le mode externe FPolicy

Le mode externe FPolicy est un framework de notification et de contrôle de l'activité des fichiers qui offre une visibilité sur l'activité des fichiers et des utilisateurs. Ces notifications peuvent être utilisées par une solution externe pour effectuer des analyses basées sur l'IA afin de détecter les comportements malveillants.

Le mode externe FPolicy peut également être configuré pour attendre l'approbation du serveur FPolicy avant de permettre l'exécution d'activités spécifiques. Vous pouvez configurer plusieurs règles de ce type sur un cluster, ce qui vous apporte une grande flexibilité.

> Les serveurs FPolicy doivent répondre aux requêtes FPolicy s'ils sont configurés pour être approuvés. Sinon, les performances du système de stockage risquent d'être affectées.

Le mode externe FPolicy est inclus dans "Toutes les licences ONTAP".

En savoir plus >>

- "Blog : lutter contre les ransomware : quatrième partie — UBA et ONTAP avec le mode externe FPolicy."

Data Infrastructure Insights Stockage Charge de travail Sécurité

Storage Workload Security (SWS) est une fonctionnalité de NetApp Data Infrastructure Insights qui améliore considérablement la posture de sécurité, la récupérabilité et la responsabilité d'un environnement ONTAP . SWS adopte une approche centrée sur l'utilisateur, en suivant toutes les activités des fichiers de chaque utilisateur authentifié dans l'environnement. Il utilise des analyses avancées pour établir des modèles d'accès normaux et saisonniers pour chaque utilisateur. Ces modèles sont utilisés pour identifier rapidement les comportements suspects sans avoir besoin de signatures de ransomware.

Lorsque SWS détecte un ransomware potentiel ou une suppression de données, il peut prendre des mesures automatiques telles que :

- Prenez un instantané du volume affecté.

- Bloquez le compte utilisateur et l'adresse IP suspectés d'activité malveillante.
- Envoyez une alerte aux administrateurs.

Comme il peut prendre des mesures automatisées pour arrêter rapidement une menace interne et suivre chaque activité de fichier, SWS simplifie et accélère la restauration suite à un événement de ransomware. Grâce aux outils avancés d'audit et d'analyse intégrés, les utilisateurs peuvent immédiatement voir quels volumes et fichiers ont été affectés par une attaque, quel compte d'utilisateur l'attaque a été et quelle action malveillante a été exécutée. Les snapshots automatiques atténuent les dommages et accélèrent la restauration des fichiers.

Les alertes issues de la protection anti-ransomware autonome (ARP) de ONTAP sont également visibles dans SWS, fournissant une interface unique aux clients qui utilisent à la fois ARP et SWS pour se protéger contre les attaques par ransomware.

En savoir plus >>

- "Data Infrastructure Insights NetApp"

Détection et réponse basées sur l'IA intégrées à NetApp ONTAP

Comme les menaces de ransomware sont de plus en plus sophistiquées, vos mécanismes de défense aussi devraient-ils le faire. La protection anti-ransomware autonome (ARP) de NetApp est optimisée par l'IA avec la détection d'anomalies intelligente intégrée à ONTAP. Activez-la pour ajouter une couche de défense supplémentaire à votre cyberrésilience.

ARP et ARP/ai sont configurables via l'interface de gestion intégrée ONTAP, System Manager et activées par volume.

Protection autonome contre les ransomwares (ARP)

La protection anti-ransomware autonome (ARP), une autre solution ONTAP intégrée native depuis 9.10.1, examine l'activité des fichiers de workloads de volume de stockage NAS et l'entropie des données pour détecter automatiquement les ransomwares. ARP fournit aux administrateurs une détection en temps réel, des informations et un point de restauration des données pour une détection intégrée sans précédent des ransomwares.

Pour ONTAP 9.15.1 et les versions antérieures qui prennent en charge ARP, ARP démarre en mode d'apprentissage pour apprendre l'activité typique des données de charge de travail. Cela peut prendre sept jours pour la plupart des environnements. Une fois le mode d'apprentissage terminé, le protocole ARP passe automatiquement en mode actif et commence à rechercher les activités anormales des workloads qui

pourraient être des ransomware.

En cas d'activité anormale, un snapshot automatique est immédiatement pris, ce qui fournit un point de restauration aussi proche que possible du moment de l'attaque avec un minimum de données infectées. Simultanément, une alerte automatique (configurable) est générée et permet aux administrateurs de voir l'activité anormale des fichiers afin qu'ils puissent déterminer si l'activité est malveillante et prendre les mesures appropriées.

Si l'activité correspond à une charge de travail attendue, les administrateurs peuvent facilement la marquer comme un faux positif. ARP apprend ce changement comme une activité normale de la charge de travail et ne le signale plus comme une attaque potentielle à l'avenir.

Pour activer ARP, une "ONTAP One" licence est requise.

En savoir plus >>

- "Protection autonome contre les ransomwares"

Protection anti-ransomware autonome/IA (ARP/ai)

Présenté en tant que préversion technologique d'ONTAP 9.15.1, ARP/ai va encore plus loin avec la détection en temps réel intégrée des systèmes de stockage NAS. La nouvelle technologie de détection optimisée par l'IA est entraînée sur plus d'un million de fichiers et diverses attaques par ransomware connues. En plus des signaux utilisés dans ARP, ARP/ai détecte également le chiffrement des en-têtes. La puissance ai et les signaux supplémentaires permettent à ARP/ai d'offrir une précision de détection supérieure à 99 %. Ce résultat a été validé par se Labs, un laboratoire de test indépendant qui a donné à ARP/ai son meilleur classement AAA.

L'entraînement des modèles étant effectué en continu dans le cloud, l'ARP/l'IA ne requiert pas de mode d'apprentissage. Elle est active dès sa mise sous tension. La formation continue implique également que l'ARP/l'IA est toujours validée contre les nouveaux types d'attaques par ransomware dès qu'ils surviennent. ARP/ai est également fourni avec des fonctionnalités de mise à jour automatique qui fournissent de nouveaux paramètres à tous les clients pour maintenir la détection des ransomware à jour. Toutes les autres fonctionnalités de détection, d'aperçu et de point de restauration des données d'ARP sont conservées pour ARP/ai.

Pour activer ARP/ai, une "ONTAP One" licence est requise.

En savoir plus >>

- "Blog : la solution NetApp de détection des ransomwares en temps réel basée sur l'IA classe AAA"

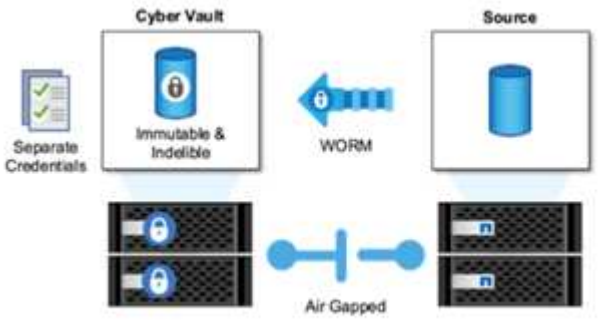
Protection WORM protégée par air avec archivage électronique dans ONTAP

L'approche de NetApp en matière de cyber-coffre est une architecture de référence dédiée pour un cyber-coffre à air Gap logique. Cette approche tire parti des technologies de renforcement de la sécurité et de conformité, telles que SnapLock, pour permettre des snapshots immuables et indélébiles.

Cyber-archivage avec SnapLock Compliance et un air Gap logique

La tendance est de plus en plus marquée aux pirates informatiques qui détruisent les copies de sauvegarde et, dans certains cas, même les chiffrent. C'est pourquoi beaucoup dans le secteur de la cybersécurité recommandent d'utiliser des sauvegardes « air Gap » dans le cadre d'une stratégie globale de cyberrésilience.

Le problème, c'est que les lacunes traditionnelles (bandes et supports hors ligne) peuvent considérablement augmenter le temps de restauration, augmentant ainsi les temps d'indisponibilité et les coûts globaux associés. Même une approche plus moderne de la solution de l'air Gap peut s'avérer problématique. Par exemple, si le coffre-fort de sauvegarde est temporairement ouvert pour recevoir de nouvelles copies de sauvegarde, puis déconnecte et ferme sa connexion réseau aux données primaires pour être à nouveau « à air Gap », un attaquant pourrait tirer parti de l'ouverture temporaire. Au cours de la connexion, un attaquant pourrait frapper pour compromettre ou détruire les données. Ce type de configuration ajoute également généralement une complexité indésirable. L'air Gap logique est un excellent substitut à un air Gap traditionnel ou moderne car il possède les mêmes principes de protection de sécurité tout en conservant la sauvegarde en ligne. Avec NetApp, simplifiez les opérations de « air gapping » sur bande ou sur disque grâce à des opérations de « air gapping » logiques, réalisables avec des snapshots et des NetApp SnapLock Compliance immuables.



NetApp a publié la fonctionnalité SnapLock il y a plus de 10 ans pour répondre aux exigences de conformité des données, telles que la loi HIPAA (Health Insurance Portability and Accountability Act), la loi Sarbanes-Oxley et d'autres règles relatives aux données réglementaires. Vous pouvez également archiver les snapshots primaires de façon sécurisée sur des volumes SnapLock de façon à ce que ces copies puissent être validées sur WORM, empêchant ainsi la suppression. Il existe deux versions de licence SnapLock : SnapLock Compliance et SnapLock Enterprise. Pour la protection contre les ransomwares, NetApp recommande SnapLock Compliance, car vous pouvez définir une période de conservation spécifique pendant laquelle les snapshots sont verrouillés et ne peuvent pas être supprimés, même par les administrateurs ONTAP ou par le support NetApp.

En savoir plus >>

- "Blog : présentation du cyber-coffre-fort ONTAP"

Des snapshots inviolables

Si l'utilisation de SnapLock Compliance comme air Gap logique offre une protection ultime pour empêcher les pirates de supprimer vos copies de sauvegarde, il est nécessaire de déplacer les snapshots à l'aide de SnapVault vers un volume secondaire compatible SnapLock. Par conséquent, de nombreux clients déploient cette configuration sur un système de stockage secondaire sur le réseau. Cela peut entraîner des temps de restauration plus longs qu'avec la restauration d'un Snapshot de volume primaire sur le système de stockage primaire.

À partir de ONTAP 9.12.1, les copies Snapshot inviolables assurent une protection proche du niveau SnapLock Compliance pour vos copies Snapshot sur le stockage primaire et dans les volumes primaires. Il n'est pas nécessaire d'archiver l'instantané à l'aide de SnapVault sur un volume secondaire SnapLocaché. Les snapshots inviolables utilisent la technologie SnapLock pour empêcher la suppression du snapshot principal, même par un administrateur ONTAP complet, pendant toute la durée de conservation SnapLock. Cela permet des délais de restauration plus rapides et la possibilité de sauvegarder un volume FlexClone à l'aide d'une copie Snapshot protégée et inviolable, ce que vous ne pouvez pas faire avec une copie Snapshot stockage SnapLock Compliance classique.

La principale différence entre les snapshots SnapLock Compliance et inviolables est que SnapLock Compliance n'autorise pas l'initialisation et la suppression de la baie ONTAP si des volumes SnapLock Compliance existent avec des snapshots voûtés qui n'ont pas encore atteint leur date d'expiration. Pour rendre les snapshots inviolables, une licence SnapLock Compliance est requise.

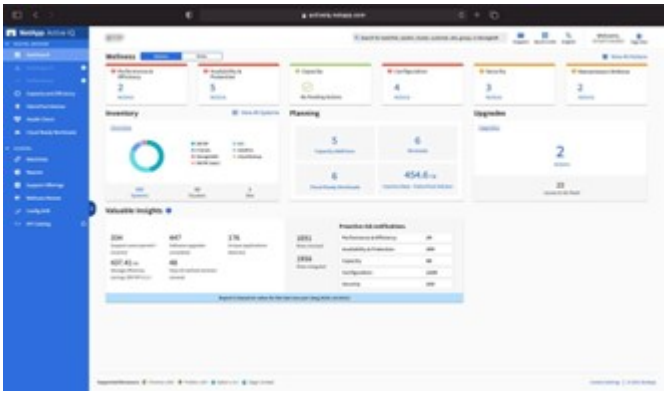
En savoir plus >>

- "Verrouillez une copie Snapshot pour vous protéger contre les attaques par ransomware"

Protection contre les ransomware via Digital Advisor

Digital Advisor optimisé par Active IQ simplifie la maintenance proactive et l'optimisation du stockage NetApp avec des informations exploitables pour une gestion des données optimale. S'appuyant sur les données de télémétrie de notre base installée très diversifiée, il utilise des techniques avancées d'IA et de ML pour identifier les opportunités de réduction des risques et d'amélioration des performances et de l'efficacité de votre environnement de stockage.

Non seulement peut "Conseiller digital NetApp" vous y aider "éliminez les failles de sécurité", mais il fournit également des informations et des recommandations spécifiques pour vous protéger contre les ransomwares. Une carte d'intégrité dédiée présente les actions nécessaires et les risques résolus. Vous êtes ainsi sûr que vos systèmes respectent ces recommandations en matière de bonnes pratiques.



Les risques et les actions suivis sur la page ransomware Defense Wellness incluent notamment les éléments suivants :

- Le nombre de copies Snapshot des volumes est faible, ce qui réduit la protection potentielle contre les ransomware.
- FPolicy n'est pas activé pour toutes les machines virtuelles de stockage (SVM) configurées pour les protocoles NAS.

Pour voir la protection contre les ransomware en action, voir "Conseiller digital".

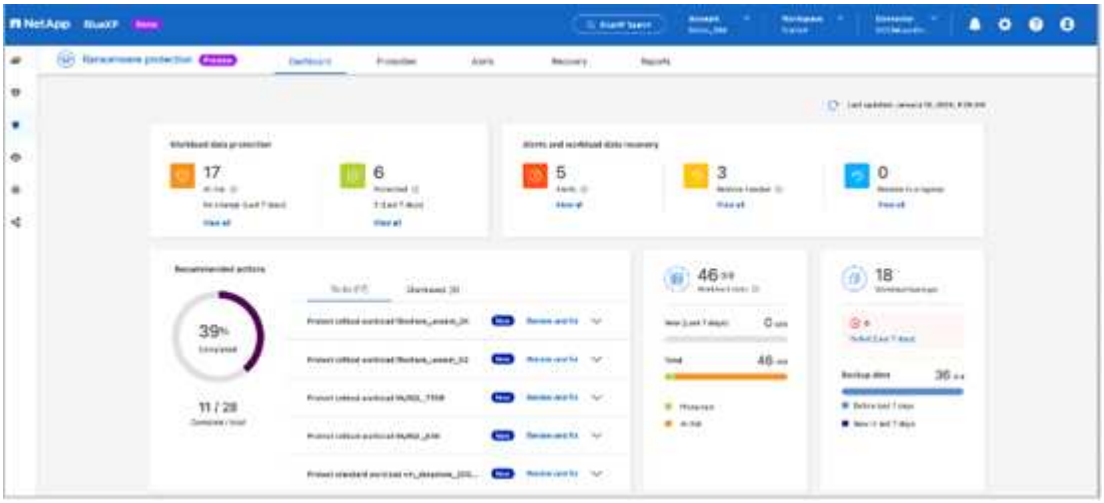
Résilience complète avec la protection contre les ransomwares NetApp

Il est important que la détection des ransomwares ait lieu le plus tôt possible afin de pouvoir empêcher leur propagation et éviter des temps d'arrêt coûteux. Une stratégie efficace de détection des ransomwares doit toutefois inclure plus d'une seule couche de protection. La protection contre les ransomwares de NetApp adopte une approche globale qui comprend des fonctionnalités en temps réel, intégrées, s'étendant aux

services de données à l'aide de la NetApp Console et une solution isolée et en couches pour le cyber-coffre-fort.

Protection contre les ransomwares NetApp

La NetApp Console est un plan de contrôle unique permettant d'orchestrer intelligemment une défense complète contre les ransomwares centrée sur la charge de travail. La protection contre les ransomwares NetApp rassemble les puissantes fonctionnalités de cyber-résilience d' ONTAP, telles que ARP, FPolicy et les snapshots inviolables, et les services de données NetApp , tels que NetApp Backup and Recovery. Il ajoute également des recommandations et des conseils avec des flux de travail automatisés pour fournir une défense de bout en bout via une interface utilisateur unique. Il fonctionne au niveau de la charge de travail pour garantir que les applications qui font fonctionner votre entreprise sont protégées et peuvent être récupérées le plus rapidement possible en cas d'attaque.



Avantages pour le client :

- La préparation assistée par ransomware réduit la surcharge opérationnelle et améliore l'efficacité
- La détection d'anomalies optimisée par l'IA et le ML améliore la précision et accélère la réponse pour maîtriser les risques
- La restauration guidée cohérente au niveau des applications vous permet de restaurer les workloads plus facilement et en quelques minutes

"Protection contre les ransomwares NetApp"rend ces fonctions NIST plus faciles à réaliser :

- Automatiquement **découvrir** et hiérarchiser les données dans le stockage NetApp **en mettant l'accent sur les principales charges de travail basées sur les applications**.
- **Protection en un clic** de la sauvegarde des données de la charge de travail la plus importante, immuable, configuration sécurisée, blocage des fichiers malveillants et domaine de sécurité différent.
- **Détectez avec précision** les ransomware au plus vite * en utilisant **la détection d'anomalies basée sur l'IA nouvelle génération.**
- Réponse automatisée et flux de travail et intégration avec les meilleures solutions * SIEM et XDR.*
- Restaurez rapidement les données à l'aide d'une récupération * orchestrée simplifiée* pour accélérer la continuité des applications.
- Mettez en œuvre votre **stratégie** et **politiques** de protection contre les ransomware et **surveillez les résultats**.

NetApp et le modèle « zéro confiance »

NetApp et le modèle « zéro confiance »

La solution « zéro confiance » s'est traditionnellement orientée réseau pour structurer les microsegments et le périmètre (MCAP) afin de protéger les données, les services, les applications ou les ressources grâce à des contrôles appelés « passerelle de segmentation ». NetApp ONTAP adopte une approche « zéro confiance » centrée sur les données, dans laquelle le système de gestion du stockage devient la passerelle de segmentation pour protéger et surveiller l'accès aux données de nos clients. Le moteur « zéro confiance » FPolicy et l'écosystème de partenaires FPolicy deviennent un centre de contrôle pour obtenir une compréhension détaillée des modèles d'accès aux données normaux et aberrants et identifier les menaces internes.

À partir de juillet 2024, le contenu du rapport technique *TR-4829: NetApp and Zero Trust: Enabling a data-Centric Zero Model*, qui a été publié au format PDF, est disponible sur docs.netapp.com.

Les données constituent les ressources les plus importantes de votre entreprise. Selon le 2022 , les menaces internes sont la cause de 18 % des violations de données "Rapport d'enquête sur les violations de données Verizon". Les entreprises peuvent améliorer leur vigilance en déployant des contrôles « zéro confiance » de pointe sur les données à l'aide du logiciel de gestion des données NetApp ONTAP.

Qu'est-ce que le principe zéro confiance ?

Le modèle Zero Trust a été développé pour la première fois par John Kindervag, de Forrester Research. Le service informatique envisage la sécurité du réseau de l'intérieur vers l'extérieur plutôt que de l'extérieur vers l'intérieur. L'approche « zéro confiance » de l'intérieur identifie un micronoyau et un périmètre (MCAP). Le MCAP est une définition intérieure des données, des services, des applications et des ressources à protéger avec un ensemble complet de contrôles. Le concept de périmètre extérieur sécurisé est obsolète. Les entités fiables et autorisées à s'authentifier avec succès via le périmètre peuvent alors rendre l'organisation vulnérable aux attaques. Les initiés, par définition, sont déjà à l'intérieur du périmètre sécurisé. Les employés, prestataires et partenaires sont des initiés, et ils doivent être autorisés à opérer avec des contrôles appropriés pour remplir leurs rôles au sein de l'infrastructure de votre entreprise.

Zéro confiance a été mentionné comme une technologie qui offre une promesse au DoD en septembre 2019 "FY19-23 Stratégie de modernisation numérique du Département de la Défense des États-Unis". Le modèle « zéro confiance » est défini comme « Une stratégie de cybersécurité qui intègre la sécurité dans l'ensemble de l'architecture dans le but d'enrayer les fuites de données. Ce modèle de sécurité centré sur les données élimine l'idée de réseaux, périphériques, rôles ou processus fiables ou non approuvés, et passe à des niveaux de confiance basés sur plusieurs attributs qui activent des stratégies d'authentification et d'autorisation dans le concept d'accès le moins privilégié. Mettre en œuvre la confiance zéro exige de repenser la façon dont nous utilisons l'infrastructure existante pour mettre en œuvre la sécurité en simplifiant et en améliorant l'efficacité tout en assurant la continuité des opérations. »

En août 2020, le NIST a publié "Architecture Zero Trust Pub 800-207 spéciale" (ZTA). ZTA se concentre sur la protection des ressources, et non des segments de réseau, car l'emplacement du réseau n'est plus considéré comme le composant principal de la posture de sécurité de la ressource. Les ressources sont des données et de l'informatique. Les stratégies ZTA sont destinées aux architectes de réseaux d'entreprise. ZTA présente une nouvelle terminologie issue des concepts originaux de Forrester. Les mécanismes de protection appelés le point de décision de la politique (PDP) et le point d'application de la politique (PEP) sont analogues à une

passerelle de segmentation Forrester. ZTA présente quatre modèles de déploiement :

- Déploiement basé sur un agent ou une passerelle
- Déploiement basé sur l'enclave (un peu similaire au MCAP de Forrester)
- Déploiement sur portail de ressources
- Sandbox d'application de périphérique

Pour les besoins de cette documentation, nous utilisons les concepts et la terminologie de Forrester Research plutôt que le NIST ZTA.

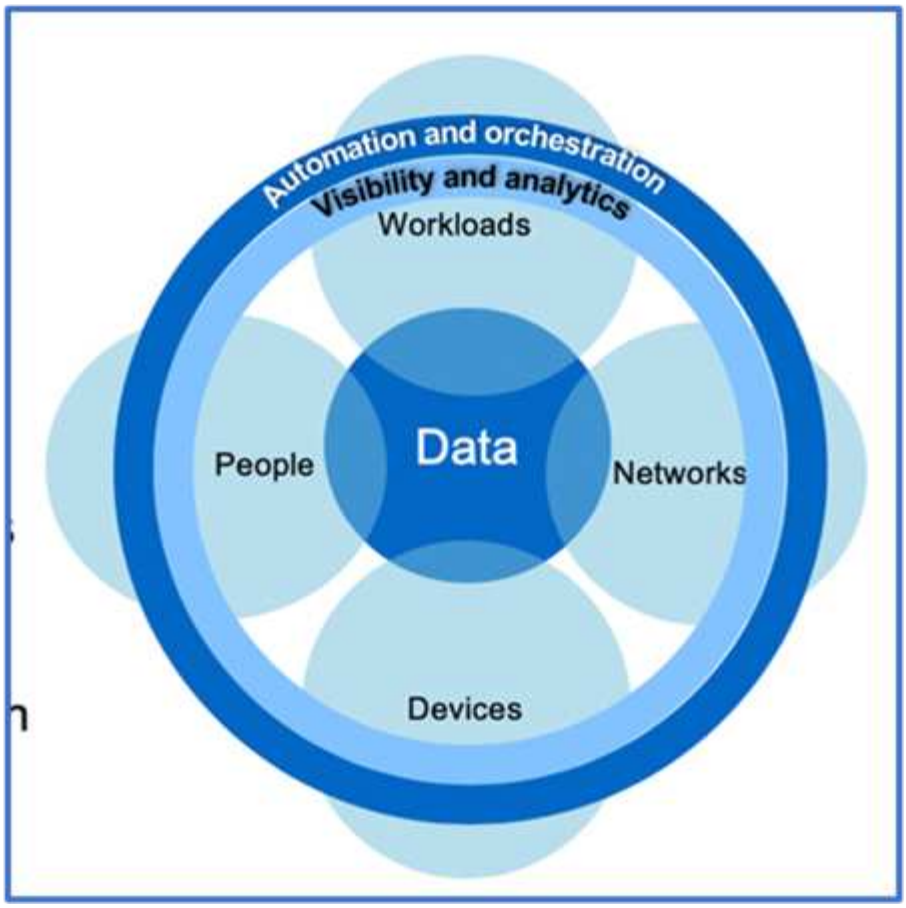
Ressources de sécurité

Pour plus d'informations sur le signalement de vulnérabilités et d'incidents, les réponses de sécurité NetApp et la confidentialité des clients, consultez le "Portail de sécurité NetApp".

Concevez une approche « zéro confiance » centrée sur les données avec ONTAP

Un réseau « zéro confiance » est défini par une approche centrée sur les données dans laquelle les contrôles de sécurité doivent être aussi proches que possible des données. Les fonctionnalités de ONTAP, associées à l'écosystème de partenaires NetApp FPolicy, peuvent fournir les contrôles nécessaires au modèle « zéro confiance » centré sur les données.

ONTAP est le logiciel de gestion des données riche en fonctions de sécurité de NetApp, et le moteur « zéro confiance » FPolicy est une fonctionnalité ONTAP de pointe qui offre une interface de notification d'événements granulaire et basée sur des fichiers. Les partenaires NetApp FPolicy peuvent utiliser cette interface pour obtenir un niveau d'éclairage plus élevé de l'accès aux données dans ONTAP.



Concevez un MCAP « zéro confiance » centré sur les données

Pour concevoir un MCAP Zero Trust axé sur les données, procédez comme suit :

1. Identifiez l'emplacement de toutes les données de l'entreprise.
2. Classez vos données.
3. Supprimez en toute sécurité les données dont vous n'avez plus besoin.
4. Comprendre quels rôles doivent avoir accès aux classifications de données.
5. Appliquez le principe du privilège minimum pour appliquer les contrôles d'accès.
6. Utilisez l'authentification multifacteur pour l'accès administratif et l'accès aux données.
7. Utilisez le chiffrement pour les données au repos et en transit.
8. Contrôlez et consignez tous les accès.
9. Alertez les accès suspects ou les comportements à adopter.

Identifiez l'emplacement de toutes les données de l'entreprise

La fonctionnalité FPolicy de ONTAP associée à l'écosystème de partenaires Alliance NetApp de FPolicy vous permet d'identifier l'emplacement des données de votre entreprise et les personnes qui y ont accès. Cette opération est effectuée à l'aide d'une analyse comportementale des utilisateurs qui identifie si les modèles d'accès aux données sont valides. Pour plus d'informations sur l'analyse comportementale des utilisateurs, reportez-vous à la section contrôle et journalisation de tous les accès. Si vous ne comprenez pas où se trouvent vos données et qui y a accès, l'analyse comportementale des utilisateurs peut fournir une base pour établir une classification et une politique à partir d'observations empiriques.

Classez vos données

Dans la terminologie du modèle Zero Trust, la classification des données implique l'identification des données toxiques. Les données toxiques sont des données sensibles qui ne sont pas destinées à être exposées en dehors d'une organisation. La divulgation de données toxiques pourrait violer la conformité réglementaire et nuire à la réputation d'une organisation. En termes de conformité réglementaire, les données toxiques incluent les données des titulaires de cartes pour le "Norme de sécurité de l'industrie des cartes de paiement (PCI-DSS)" , données personnelles pour l'UE "Règlement général sur la protection des données (RGPD)" , ou des données de santé pour le "Loi américaine sur la transférabilité et la responsabilité en matière d'assurance maladie (HIPAA)" . Vous pouvez utiliser NetApp "NetApp Data Classification" (anciennement connu sous le nom de Cloud Data Sense), une boîte à outils basée sur l'IA, pour numériser, analyser et catégoriser automatiquement vos données.

Supprimez les données dont vous n'avez plus besoin en toute sécurité

Une fois les données de votre entreprise classifiées, vous pouvez découvrir que certaines de vos données ne sont plus nécessaires ou pertinentes pour le fonctionnement de votre entreprise. La conservation de données inutiles est une responsabilité et ces données doivent être supprimées. Pour obtenir un mécanisme avancé d'effacement cryptographique des données, consultez la description de la suppression sécurisée dans le chiffrement des données au repos.

Comprendre quels rôles doivent avoir accès aux classifications de données et appliquer le principe du privilège minimum pour appliquer les contrôles d'accès

Mapper l'accès aux données sensibles et appliquer le principe du privilège minimum implique de donner aux personnes de votre entreprise l'accès aux seules données requises pour accomplir leur travail. Ce processus implique le contrôle d'accès basé sur les rôles ("RBAC"), qui s'applique à l'accès aux données et à l'accès administratif.

Avec ONTAP, un SVM (Storage Virtual machine) peut être utilisé pour segmenter l'accès aux données de l'entreprise par les locataires au sein d'un cluster ONTAP. Le RBAC peut être appliqué à l'accès aux données ainsi qu'à l'accès administratif à la SVM. Le RBAC peut également être appliqué au niveau administratif du cluster.

En plus de RBAC, vous pouvez utiliser ONTAP "vérification multiadministrateur" (MAV) pour demander à un ou plusieurs administrateurs d'approuver des commandes telles que `volume delete` ou `volume snapshot delete`. Une fois MAV activé, la modification ou la désactivation de MAV nécessite l'approbation de l'administrateur MAV.

ONTAP est un autre moyen de protéger les snapshots"verrouillage des copies snapshot". Le verrouillage des snapshots est une fonctionnalité SnapLock dans laquelle les snapshots sont rendus indélébiles manuellement ou automatiquement avec une période de conservation définie dans la règle Snapshot du volume. Le verrouillage des snapshots est également appelé verrouillage inviolable des snapshots. Le verrouillage des snapshots permet d'empêcher les administrateurs peu scrupuleux ou non approuvés de supprimer des snapshots sur les systèmes ONTAP primaires et secondaires. Il est possible d'effectuer une restauration rapide des copies Snapshot verrouillées sur les systèmes primaires afin de restaurer les volumes corrompus par des ransomwares.

Utilisez l'authentification multifacteur pour l'accès administratif et l'accès aux données

Outre le RBAC d'administration de cluster, "Authentification multifacteur (MFA)" peut être déployé pour l'accès administratif web ONTAP et l'accès à la ligne de commande SSH (Secure Shell). L'authentification multifacteur en matière d'accès administratif est obligatoire pour les organisations du secteur public américain ou celles qui doivent suivre la norme PCI-DSS. L'authentification multifacteur empêche un attaquant de compromettre un compte en utilisant uniquement un nom d'utilisateur et un mot de passe. L'authentification MFA nécessite au

moins deux facteurs indépendants. Un exemple d'authentification à deux facteurs est quelque chose qu'un utilisateur possède, comme une clé privée, et quelque chose qu'un utilisateur sait, comme un mot de passe. L'accès administratif Web à ONTAP System Manager ou à ActiveIQ Unified Manager est activé par le langage SAML (Security assertion Markup Language) 2.0. L'accès en ligne de commande SSH utilise une authentification à deux facteurs chaînée avec une clé publique et un mot de passe.

Vous pouvez contrôler l'accès des utilisateurs et des machines via des API dotées des fonctionnalités de gestion des identités et des accès de ONTAP :

- Utilisateur :
  - **Authentification et autorisation.** Grâce aux fonctionnalités de protocole NAS pour SMB et NFS.
  - **Vérification.** Syslog d'accès et d'événements. Une journalisation d'audit détaillée du protocole CIFS pour tester les règles d'authentification et d'autorisation. Audit précis et granulaire de l'accès NAS détaillé dans FPolicy au niveau des fichiers.
- Périphérique :
  - **Authentification.** Authentification basée sur certificat pour l'accès à l'API.
  - **Autorisation.** Contrôle d'accès basé sur des rôles (RBAC) par défaut ou personnalisé.
  - **Vérification.** Syslog de toutes les actions entreprises.

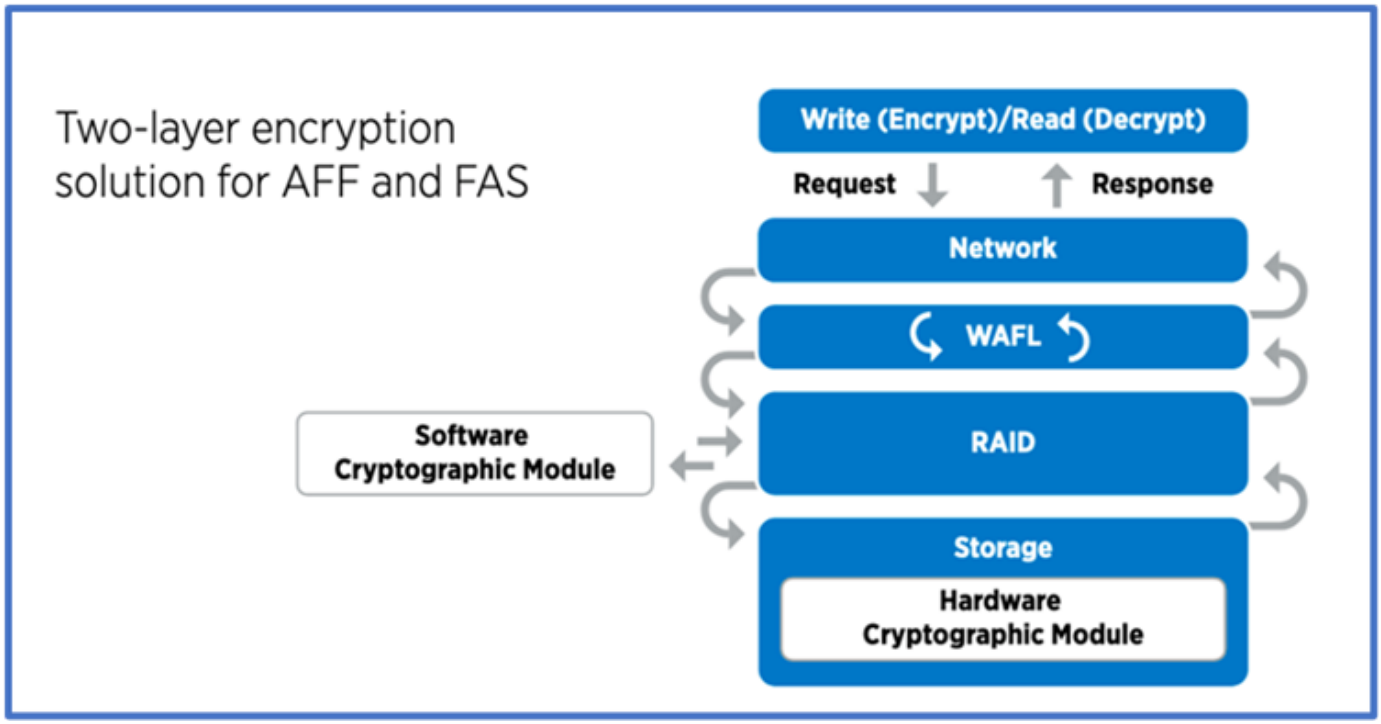
Utilisez le chiffrement pour les données au repos et en transit

Chiffrement des données au repos

Chaque jour, lorsqu'une entreprise réutilise des disques, renvoie des disques défectueux ou effectue des mises à niveau vers des disques de plus grande capacité, elle doit satisfaire de nouvelles exigences afin de réduire les risques liés aux systèmes de stockage et les écarts d'infrastructure. En tant qu'administrateurs et opérateurs de ressources de données, les ingénieurs du stockage doivent gérer et maintenir les données en toute sécurité tout au long de leur cycle de vie. "Chiffrement de stockage NetApp (NSE) ;#44 ; NetApp Volume Encryption (NVE) ;#44 ; et chiffrement d'agrégat NetApp" vous aider à chiffrer toutes vos données au repos en permanence, qu'elles soient toxiques ou non, et sans affecter les opérations quotidiennes. "NSE" Est une solution matérielle ONTAP "données au repos" qui utilise des disques auto-cryptés conformes à la norme FIPS 140-2 de niveau 2. "NVE et NAE" Sont une solution logicielle ONTAP "données au repos" qui utilise le "Module cryptographique NetApp conforme à la norme FIPS 140-2 de niveau 1". Avec NVE et NAE, vous pouvez utiliser des disques durs ou des disques SSD pour le chiffrement des données au repos. De plus, les disques NSE peuvent être utilisés pour fournir une solution de chiffrement à plusieurs couches native qui assure la redondance du chiffrement et une sécurité supplémentaire. Si l'une des couches est rompue, la seconde couche sécurise toujours les données. Ces fonctionnalités font de ONTAP une solution bien positionnée pour "chiffrement prêt pour le quantum".

NVE propose également une fonctionnalité appelée "suppression sécurisée" qui supprime de manière cryptographique les données toxiques des fuites de données lorsque les fichiers sensibles sont écrits sur un volume non classifié.

Soit le "Gestionnaire de clés intégré Onboard Key Manager (OKM)", qui est le gestionnaire de clés intégré dans ONTAP, soit un "approuvée" tiers "gestionnaires de clés externes" peut être utilisé avec NSE et NVE pour stocker des clés en toute sécurité.



Comme le montre la figure ci-dessus, le chiffrement matériel et logiciel peut être combiné. Cette fonctionnalité a permis à l' "Validation de ONTAP dans les solutions commerciales de la NSA pour le programme classifié" de stocker des données les plus secrètes.

Chiffrement des données à la volée

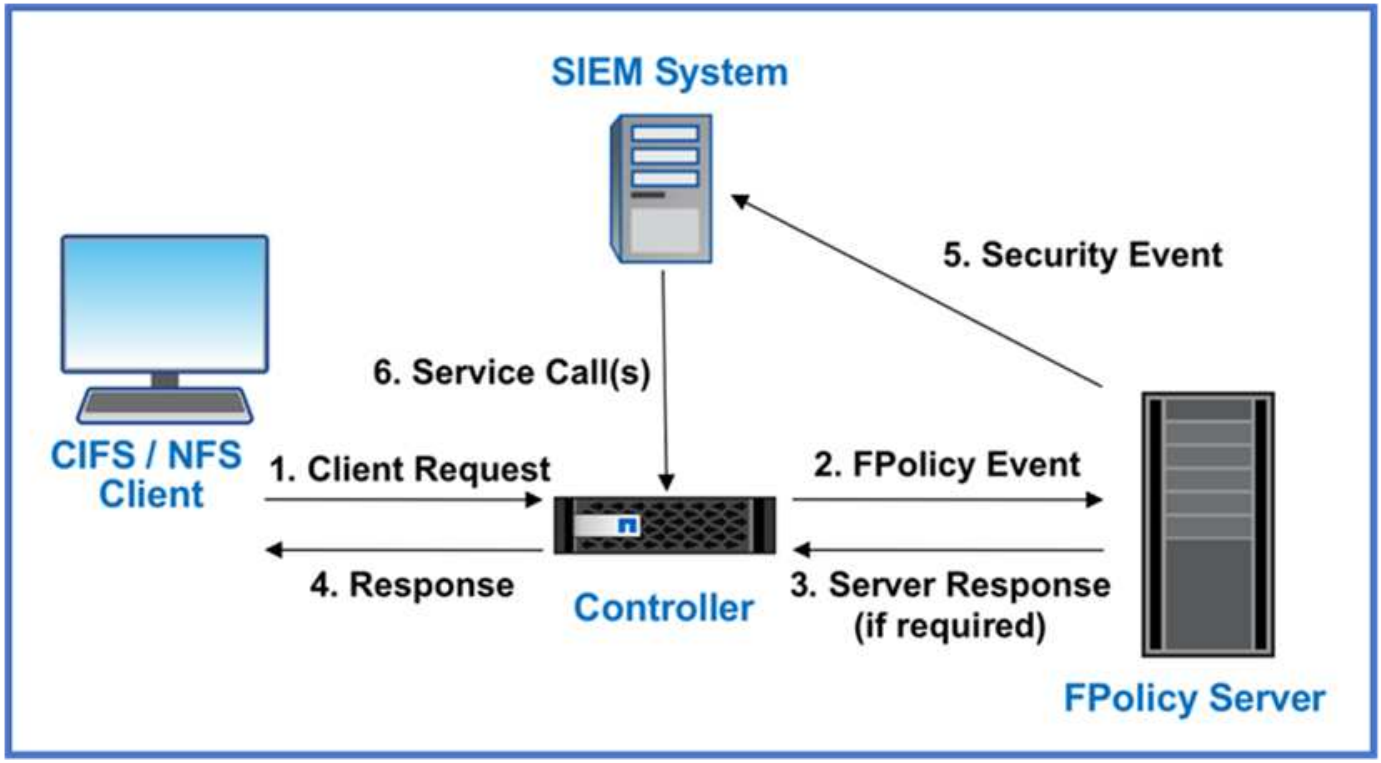
Le chiffrement des données à la volée ONTAP protège l'accès aux données utilisateur et l'accès au plan de contrôle. L'accès aux données utilisateur peut être chiffré par chiffrement SMB 3.0 pour l'accès aux partages Microsoft CIFS ou par krb5P pour NFS Kerberos 5. L'accès aux données utilisateur peut également être chiffré avec "IPSec" pour CIFS, NFS et iSCSI. L'accès au plan de contrôle est chiffré avec TLS (transport Layer Security). ONTAP fournit "FIPS"le mode de conformité pour l'accès au plan de contrôle, qui active les algorithmes approuvés FIPS et désactive les algorithmes non approuvés FIPS. La réplication des données est chiffrée avec "chiffrement des pairs de cluster". Cela assure le cryptage pour les technologies ONTAP SnapVault et SnapMirror.

Contrôlez et consignez tous les accès

Une fois les règles RBAC en place, vous devez déployer des fonctionnalités actives de surveillance, d'audit et d'alerte. Le moteur « zéro confiance » FPolicy de NetApp ONTAP, couplé au "Écosystème de partenaires NetApp FPolicy", fournit les contrôles nécessaires au modèle « zéro confiance » centré sur les données. NetApp ONTAP est un logiciel de gestion des données riche en fonctions de sécurité. Il "FPolicy" s'agit d'une fonctionnalité ONTAP de pointe qui offre une interface de notification d'événements granulaire basée sur des fichiers. Les partenaires NetApp FPolicy peuvent utiliser cette interface pour obtenir un niveau d'éclairage plus élevé de l'accès aux données dans ONTAP. La fonctionnalité FPolicy de ONTAP, associée à l'écosystème de partenaires Alliance NetApp de FPolicy, vous permet d'identifier l'emplacement et l'accès aux données de votre entreprise. Cette opération est effectuée à l'aide d'une analyse comportementale des utilisateurs qui identifie si les modèles d'accès aux données sont valides. L'analyse comportementale des utilisateurs peut être utilisée pour alerter l'utilisateur en cas d'accès aux données suspect ou aberrant qui ne correspond pas au modèle normal et, si nécessaire, prendre des mesures pour refuser l'accès.

Les partenaires FPolicy vont au-delà de l'analyse comportementale des utilisateurs et s'orientent vers le machine learning (ML) et l'intelligence artificielle (IA) pour assurer la fidélité des événements et réduire le nombre de faux positifs, voire de faux positifs. Tous les événements doivent être consignés sur un serveur

syslog ou sur un système de gestion des informations et des événements de sécurité (SIEM) pouvant également utiliser le ML et l'IA.



NetApp "Sécurité de la charge de travail de stockage DII" utilise l'interface FPolicy et l'analyse du comportement des utilisateurs sur les systèmes de stockage ONTAP cloud et sur site pour vous fournir des alertes en temps réel sur le comportement malveillant des utilisateurs. Storage Workload Security protège les données de l'organisation contre toute utilisation abusive par des utilisateurs malveillants ou compromis grâce à l'apprentissage automatique avancé et à la détection des anomalies. Storage Workload Security peut identifier les attaques de ransomware ou d'autres comportements malveillants, invoquer des instantanés et mettre en quarantaine les utilisateurs malveillants. Storage Workload Security dispose également d'une capacité d'analyse médico-légale permettant de visualiser en détail les activités des utilisateurs et des entités. La sécurité des charges de travail de stockage fait partie de NetApp Data Infrastructure Insights.

Outre la sécurité des workloads de stockage, ONTAP dispose d'une fonctionnalité intégrée de détection des ransomwares appelée "Protection autonome contre les ransomwares" ARP. ARP utilise le machine learning pour déterminer si une activité anormale sur les fichiers indique qu'une attaque par ransomware est en cours, puis appelle une copie Snapshot et une alerte aux administrateurs. Storage Workload Security s'intègre à ONTAP pour recevoir des événements ARP et fournit une couche supplémentaire d'analytique et de réponses automatiques.

Pour en savoir plus sur les commandes décrites dans cette procédure"Référence des commandes ONTAP", reportez-vous à la .

Contrôles d'orchestration et d'automatisation de la sécurité NetApp externes à ONTAP

L'automatisation vous permet d'effectuer un processus ou une procédure avec une assistance humaine minimale. L'automatisation permet aux entreprises d'étendre les déploiements « zéro confiance » bien au-delà des procédures manuelles pour se défendre contre les activités imcretes également automatisées.

Ansible est un outil open source de provisionnement logiciel, de gestion de la configuration et de déploiement des applications. Il fonctionne sur de nombreux systèmes Unix et peut configurer à la fois les systèmes Unix et Microsoft Windows. Il comprend son propre langage déclaratif pour décrire la configuration du système. Ansible a été écrit par Michael DeHaan et acquis par Red Hat en 2015. Ansible se connecte temporairement à distance sans agent via SSH ou Windows Remote Management (permettant l'exécution à distance de PowerShell). NetApp a développé plus de "150 modules Ansible pour le logiciel ONTAP", permettant une intégration supplémentaire avec la structure d'automatisation Ansible. Les modules Ansible pour NetApp fournissent un ensemble d'instructions sur la manière de définir l'état souhaité et de le relayer vers l'environnement NetApp cible. Les modules sont conçus pour prendre en charge des tâches telles que la configuration de licences, la création d'agrégats et de machines virtuelles de stockage, la création de volumes et la restauration de snapshots, pour n'en nommer que quelques-uns. Un rôle Ansible a été "Publié sur GitHub" spécifique au guide de déploiement des fonctionnalités unifiées du Ministère de la Défense NetApp.

En utilisant la bibliothèque de modules disponibles, les utilisateurs peuvent facilement développer des playbooks Ansible et les personnaliser en fonction de leurs propres applications et des besoins de l'entreprise pour automatiser des tâches courantes. Une fois qu'un PlayBook est écrit, vous pouvez l'exécuter pour exécuter la tâche spécifiée, ce qui permet de gagner du temps et d'améliorer la productivité. NetApp a créé et partagé des exemples de playbooks pouvant être utilisés directement ou personnalisés en fonction de vos besoins.

Data Infrastructure Insights est un outil de surveillance de l'infrastructure qui vous donne une visibilité sur l'ensemble de votre infrastructure. Avec Data Infrastructure Insights, vous pouvez surveiller, dépanner et optimiser toutes vos ressources, y compris vos instances de cloud public et vos centres de données privés. Data Infrastructure Insights peut réduire le temps moyen de résolution de 90 % et empêcher 80 % des problèmes de cloud d'affecter les utilisateurs finaux. Il peut également réduire les coûts d'infrastructure cloud de 33 % en moyenne et réduire votre exposition aux menaces internes en protégeant vos données grâce à des renseignements exploitables. La fonctionnalité de sécurité de la charge de travail de stockage de Data Infrastructure Insights permet l'analyse du comportement des utilisateurs avec l'IA et le ML pour alerter lorsque des comportements d'utilisateur aberrants se produisent en raison d'une menace interne. Pour ONTAP, Storage Workload Security utilise le moteur Zero Trust FPolicy.

Zero Trust et déploiements de cloud hybride

NetApp est l'autorité en matière de données pour le cloud hybride. NetApp propose une variété d'options pour étendre les systèmes de gestion de données sur site au cloud hybride avec Amazon Web Services (AWS), Microsoft Azure, Google Cloud et d'autres fournisseurs de cloud de premier plan. Les solutions cloud hybrides NetApp prennent en charge les mêmes contrôles de sécurité Zero Trust que ceux disponibles avec les systèmes ONTAP sur site et le stockage défini par logiciel ONTAP Select .

Vous pouvez facilement étendre la capacité des clouds publics sans contraintes CAPEX typiques en utilisant des services de fichiers cloud natifs de classe entreprise pour AWS (FSxN), Google Cloud (GCNV) et Azure NetApp Files pour Microsoft Azure. Idéals pour les charges de travail gourmandes en données telles que l'analyse et DevOps, ces services de données cloud combinent le stockage élastique à la demande en tant que service de NetApp avec la gestion des données ONTAP dans une offre entièrement gérée.

ONTAP permet le déplacement de données entre vos systèmes ONTAP sur site et l'environnement de stockage AWS, Google Cloud ou Azure avec le logiciel de réplication de données NetApp SnapMirror .

Contrôle d'accès basé sur les attributs

Contrôle d’accès basé sur les attributs avec ONTAP

À partir de la version 9.12.1, vous pouvez configurer ONTAP avec les étiquettes de sécurité NFSv4.2 et les attributs étendus (xattrs) pour prendre en charge le contrôle d’accès basé sur les rôles (RBAC) avec des attributs et le contrôle d’accès basé sur les attributs (ABAC).

ABAC est une stratégie d’autorisation qui définit les autorisations en fonction des attributs utilisateur, des attributs de ressource et des conditions environnementales. L’intégration de ONTAP avec les étiquettes de sécurité NFS v4.2 et les xattrs est conforme aux normes NIST pour les solutions ABAC, comme indiqué dans la publication spéciale NIST 800-162.

Vous pouvez utiliser les étiquettes de sécurité NFS v4.2 et les xattrs pour attribuer des attributs et des étiquettes définis par l’utilisateur de fichiers. ONTAP peut s’intégrer au logiciel de gestion des accès et des identités orienté ABAC pour appliquer des règles de contrôle d’accès granulaires aux fichiers et dossiers en fonction de ces attributs et étiquettes.

Informations associées

- "Approches de l’ABAC avec ONTAP"
- "NFS dans NetApp ONTAP : guide des bonnes pratiques et d’implémentation"

Approches du contrôle d’accès basé sur les attributs (ABAC) dans ONTAP

ONTAP propose plusieurs approches pour assurer le contrôle d’accès basé sur des attributs (ABAC) au niveau des fichiers, notamment les étiquettes de sécurité NFS v4.2 et les attributs étendus (xattrs) à l’aide de NFS.

Étiquettes de sécurité NFS v4.2

À partir de ONTAP 9.9.1, la fonctionnalité NFS v4.2 appelée NFS est prise en charge.

Les étiquettes de sécurité NFS v4.2 permettent de gérer l’accès granulaire aux fichiers et dossiers à l’aide d’étiquettes SELinux et de MAC (obligatoire Access Control). Ces étiquettes MAC sont stockées avec des fichiers et des dossiers et fonctionnent en conjonction avec les autorisations UNIX et les listes de contrôle d’accès NFS v4.x.

La prise en charge des étiquettes de sécurité NFS v4.2 signifie que ONTAP reconnaît et comprend désormais les paramètres d’étiquette SELinux du client NFS. Les étiquettes de sécurité NFS v4.2 sont couvertes par la norme RFC-7204.

Voici quelques cas d’utilisation des étiquettes de sécurité NFS v4.2 :

- Étiquetage MAC des images de machines virtuelles (VM)
- Classification de sécurité des données pour le secteur public (secret, secret et autres classifications)
- Conformité en matière de sécurité
- Linux sans disque

Activez les étiquettes de sécurité NFS v4.2

Vous pouvez activer ou désactiver les étiquettes de sécurité NFS v4.2 à l’aide de la commande suivante (privilège avancé requis) :

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel <disabled|enabled>
```

Pour en savoir plus, `vserver nfs modify` consultez le "Référence des commandes ONTAP".

Modes d'application pour les étiquettes de sécurité NFS v4.2

À partir de ONTAP 9.9.1, ONTAP prend en charge les modes d'application suivants :

- **Mode serveur limité** : ONTAP ne peut pas appliquer les étiquettes mais peut les stocker et les transmettre.

  La possibilité de modifier les étiquettes MAC revient au client de les appliquer.

- **Mode invité** : si le client n'est pas étiqueté NFS-Aware (v4.1 ou inférieur), les étiquettes MAC ne sont pas transmises.

  ONTAP ne prend actuellement pas en charge le mode complet (stockage et application des étiquettes MAC).

Exemples d'étiquettes de sécurité NFS v4.2

L'exemple de configuration suivant illustre les concepts d'utilisation de Red Hat Enterprise Linux version 9.3 (Plough).

L'utilisateur `jrsmith`, créé à partir des informations d'identification de John R. Smith, possède le compte Privileges suivant :

- Nom d'utilisateur = `jrsmith`
- Privileges = `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

Il existe deux rôles : le compte admin qui est un utilisateur privilégié et un utilisateur `jrsmith` comme décrit dans le tableau Privileges MLS suivant :

Utilisateurs	Rôle	Type	Niveaux
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

Dans cet exemple d'environnement, l'utilisateur `jrsmith` a accès aux fichiers aux niveaux de `s0 s3` . Nous pouvons améliorer les classifications de sécurité existantes, comme décrit ci-dessous, afin de nous assurer que les administrateurs n'ont pas accès aux données spécifiques aux utilisateurs.

- s0 = données utilisateur admin des privilèges
- s0 = données non classées
- s1 = confidentiel

- s2 = données secrètes
- s3 = données les plus secrètes

Exemple d'étiquettes de sécurité NFS v4.2 avec MCS

Outre la sécurité multi-niveaux (MLS), une autre fonctionnalité appelée sécurité multi-catégories (MCS) vous permet de définir des catégories telles que des projets.

Étiquette de sécurité NFS	Valeur
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

Attributs étendus (xattrs)

À partir de ONTAP 9.12.1, ONTAP prend en charge xattrs. Xattrs permet d'associer des métadonnées à des fichiers et des répertoires au-delà de ce qui est fourni par le système, tels que les listes de contrôle d'accès (ACL) ou les attributs définis par l'utilisateur.

Pour implémenter xattrs, vous pouvez utiliser `setfattr` et `getfattr` les utilitaires de ligne de commande sous Linux. Ces outils fournissent un moyen puissant de gérer des métadonnées supplémentaires pour les fichiers et les répertoires. Elles doivent être utilisées avec précaution, car une utilisation inappropriée peut entraîner des comportements inattendus ou des problèmes de sécurité. Reportez-vous toujours aux `setfattr` pages de manuel et `getfattr` ou à toute autre documentation fiable pour obtenir des instructions d'utilisation détaillées.

Lorsque xattrs est activé sur un système de fichiers ONTAP, les utilisateurs peuvent définir, modifier et récupérer des attributs arbitraires sur les fichiers. Ces attributs peuvent être utilisés pour stocker des informations supplémentaires sur le fichier qui ne sont pas capturées par l'ensemble standard d'attributs de fichier, telles que les informations de contrôle d'accès.

Il existe plusieurs exigences et limites pour l'utilisation de xattrs dans ONTAP :

- Red Hat Enterprise Linux 8.4 ou version ultérieure
- Ubuntu 22.04 ou version ultérieure
- Chaque fichier peut avoir jusqu'à 128 xattrs
- Les clés xattr sont limitées à 255 octets
- La taille de la clé ou de la valeur combinée est de 1,729 octets par xattr
- Les répertoires et les fichiers peuvent avoir des xattrs
- Pour définir et récupérer les xattrs, `w` ou les bits de mode d'écriture doivent être activés pour l'utilisateur et le groupe

Les Xattrs sont utilisés dans l'espace de nom de l'utilisateur et n'ont aucune signification intrinsèque à ONTAP lui-même. Au lieu de cela, leurs applications pratiques sont déterminées et gérées exclusivement par l'application côté client qui interagit avec le système de fichiers.

Exemples de cas d'utilisation de xattr :

- Enregistrement du nom de l'application responsable de la création d'un fichier

- Conservation d'une référence à l'e-mail à partir duquel un fichier a été obtenu
- Établissement d'un cadre de catégorisation pour l'organisation des objets de fichier
- Étiquetage des fichiers avec l'URL de leur source de téléchargement d'origine

Commandes de gestion des xattrs

- `setfattr` définit un attribut étendu d'un fichier ou d'un répertoire :

  ```
  setfattr -n <attribute_name> -v <attribute_value> <file or directory name>
  ```

  Exemple de commande :

  ```
  setfattr -n user.comment -v test example.txt
  ```

- `getfattr` récupère la valeur d'un attribut étendu spécifique ou répertorie tous les attributs étendus d'un fichier ou d'un répertoire :

  Attribut spécifique :
  `getfattr -n <attribute_name> <file or directory name>`

  Tous les attributs :
  `getfattr <file or directory name>`

  Exemple de commande :

  ```
  getfattr -n user.comment example.txt
  ```

Exemples de paires de valeurs de clé xattr

Le tableau suivant présente deux exemples de paire de valeurs de clé xattr :

xattr	Valeur
`user.digitalIdentifier`	`CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US`
`user.countryOfAffiliations`	`USA`

Autorisations utilisateur avec ACE pour xattrs

Une entrée de contrôle d'accès (ACE) est un composant d'une liste de contrôle d'accès qui définit les droits ou autorisations d'accès accordés à un utilisateur individuel ou à un groupe d'utilisateurs pour une ressource spécifique, comme un fichier ou un répertoire. Chaque ACE spécifie le type d'accès autorisé ou refusé et est associé à une entité de sécurité particulière (identité d'utilisateur ou de groupe).

Entrée de contrôle d'accès (ACE) requise pour les xattrs

- Retrieve xattr : autorisations requises pour qu'un utilisateur puisse lire les attributs étendus d'un fichier ou d'un répertoire. Le « R » signifie que l'autorisation de lecture est nécessaire.
- Set xattrs : les autorisations nécessaires pour modifier ou définir les attributs étendus. « A », « W » et « T » représentent différents exemples d'autorisations, telles que l'ajout, l'écriture et une autorisation spécifique liée aux xattrs.
- Fichiers : les utilisateurs doivent ajouter, écrire et éventuellement accorder une autorisation spéciale liée aux xattrs pour définir des attributs étendus.
- Répertoires : une autorisation spécifique « T » est requise pour définir des attributs étendus.

Type de fichier	Récupérer xattr	Définissez xattrs
Fichier	R	A,W,T
Répertoire	R	T

Intégration au logiciel ABAC Identity and Access Control

Pour exploiter pleinement les capacités d'ABAC, ONTAP peut s'intégrer à un logiciel de gestion des identités et des accès orienté ABAC.

Dans un système ABAC, le point d'application de la politique (PEP) et le point de décision de la politique (PDP) jouent des rôles cruciaux. Le PPE est responsable de l'application des politiques de contrôle d'accès, tandis que le PDP prend la décision d'accorder ou de refuser l'accès en fonction des politiques.

Dans la pratique, une entreprise utiliserait un mélange d'étiquettes de sécurité NFS et de xattrs. Ils sont utilisés pour représenter une variété de métadonnées, y compris la classification, la sécurité, l'application et le contenu, qui sont tous des éléments essentiels dans la prise de décisions ABAC. Xattrs, par exemple, peut être utilisé pour stocker les attributs de ressource que le PDP utilise pour son processus de prise de décision. Un attribut peut être défini pour représenter le niveau de classification d'un fichier (par exemple, « non classé », « confidentiel », « secret » ou « secret supérieur »). Le PDP pourrait alors utiliser cet attribut pour appliquer une stratégie qui limite les utilisateurs à accéder uniquement aux fichiers dont le niveau de classification est égal ou inférieur à leur niveau d'autorisation.

Ce contenu suppose que l'identité, l'authentification et les services d'accès du client incluent au moins une PPE et un PDP qui servent d'intermédiaires pour l'accès au système de fichiers.

Exemple de flux de processus pour ABAC

1. L'utilisateur présente les informations d'identification (par exemple, PKI, OAuth, SAML) pour accéder au système à PEP et obtient les résultats du PDP.

   Le rôle du PPE est d'intercepter la demande d'accès de l'utilisateur et de la transférer au PDP.

2. Le PDP évalue ensuite cette demande par rapport aux politiques établies de l'ABAC.

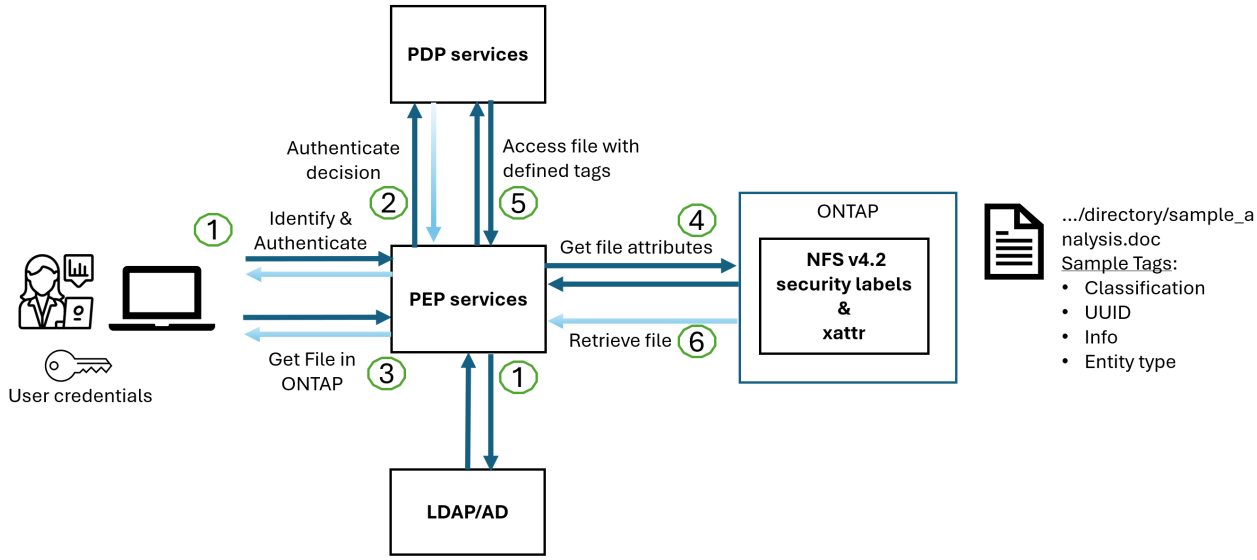
   Ces stratégies tiennent compte de divers attributs liés à l'utilisateur, à la ressource en question et à l'environnement environnant. En fonction de ces politiques, le PDP prend une décision d'accès d'autoriser ou de refuser, puis communique cette décision à la PPE.

   PDP fournit une politique à PEP pour qu'elle l'applique. Le PPE applique ensuite cette décision, en accordant ou en refusant la demande d'accès de l'utilisateur conformément à la décision du PDP.

3. Après une demande réussie, l'utilisateur demande un fichier stocké dans ONTAP (AFF, AFF-C, par exemple).

4. Si la demande réussit, PEP obtient des étiquettes de contrôle d'accès à grain fin à partir du document.
5. PEP demande la politique de l'utilisateur en fonction des certificats de cet utilisateur.
6. PEP prend une décision en fonction de la politique et des balises si l'utilisateur a accès au fichier et permet à l'utilisateur de le récupérer.

L'accès réel peut être effectué à l'aide de jetons.



Clonage ONTAP et SnapMirror

Les technologies de clonage et de SnapMirror de ONTAP sont conçues pour offrir des fonctionnalités de réplication et de clonage des données efficaces et fiables, garantissant que tous les aspects des données de fichiers, y compris les xattrs, sont conservés et transférés avec le fichier. Les xattrs sont essentiels car ils stockent des métadonnées supplémentaires associées à un fichier, telles que des étiquettes de sécurité, des informations de contrôle d'accès et des données définies par l'utilisateur, qui sont essentielles pour maintenir le contexte et l'intégrité du fichier.

Lorsqu'un volume est cloné à l'aide de la technologie FlexClone de ONTAP, une réplique inscriptible exacte du volume est créée. Ce processus de clonage est instantané et compact. Il inclut toutes les données de fichiers et métadonnées, garantissant ainsi la réplication complète des fichiers xattrs. De même, SnapMirror garantit la mise en miroir parfaite des données vers un système secondaire. Cela inclut les xattrs, qui sont essentiels pour que les applications qui s'appuient sur ces métadonnées fonctionnent correctement.

En incluant les xattrs dans les opérations de clonage et de réplication, NetApp ONTAP s'assure que l'ensemble du dataset, avec toutes ses caractéristiques, est disponible et cohérent sur l'ensemble des systèmes de stockage primaire et secondaire. Cette approche globale de la gestion des données est cruciale pour les entreprises qui ont besoin d'une protection cohérente des données, d'une restauration rapide et du respect des normes de conformité et réglementaires. Elle simplifie également la gestion des données entre différents environnements, sur site ou dans le cloud, garantissant ainsi aux utilisateurs que leurs données sont complètes et non modifiées au cours de ces processus.

Les étiquettes de sécurité NFS v4.2 présentent les restrictions définies dans le Étiquettes de sécurité NFS v4.2.

Audit des modifications apportées aux étiquettes

L'audit des modifications apportées aux étiquettes de sécurité xattrs ou NFS constitue un aspect essentiel de la gestion et de la sécurité du système de fichiers. Les outils d'audit standard du système de fichiers permettent de surveiller et de consigner toutes les modifications apportées à un système de fichiers, y compris les modifications apportées aux xattrs et aux étiquettes de sécurité.

Dans les environnements Linux, le `auditd` démon est généralement utilisé pour établir un audit pour les événements du système de fichiers. Il permet aux administrateurs de configurer des règles pour surveiller des appels système spécifiques liés aux modifications xattr, telles que `setxattr`, `lsetxattr` et pour définir des attributs et, `lremovexattr` et `fsetxattr` `fremovexattr` pour supprimer des attributs `removexattr`.

ONTAP FPolicy étend ces fonctionnalités en fournissant une structure robuste pour la surveillance et le contrôle en temps réel des opérations de fichiers. FPolicy peut être configuré pour prendre en charge divers événements xattr, offrant un contrôle granulaire des opérations sur fichiers et la possibilité d'appliquer des règles complètes de gestion des données.

Pour les utilisateurs utilisant xattrs, en particulier dans les environnements NFS v3 et NFS v4, seules certaines combinaisons d'opérations et de filtres de fichiers sont prises en charge pour la surveillance. La liste des combinaisons de filtres et d'opérations de fichiers prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers NFS v3 et NFS v4 est détaillée ci-dessous :

Opérations de fichiers prises en charge	Filtres pris en charge
`setattr`	`offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory`

Exemple de fragment de journal auditd pour une opération setattr :

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

L'activation "ONTAP FPolicy" pour les utilisateurs travaillant avec xattrs fournit une couche de visibilité et de contrôle qui est essentielle au maintien de l'intégrité et de la sécurité du système de fichiers. Grâce aux fonctionnalités avancées de surveillance de FPolicy, les entreprises peuvent s'assurer que toutes les modifications apportées aux xattrs font l'objet d'un suivi, d'un audit et d'une mise en adéquation avec leurs normes de sécurité et de conformité. Cette approche proactive de la gestion du système de fichiers explique pourquoi l'activation de ONTAP FPolicy est fortement recommandée pour toute entreprise qui souhaite améliorer ses stratégies de gouvernance et de protection des données.

Exemples de contrôle de l'accès aux données

L'exemple d'entrée ci-dessous pour les données stockées dans le certificat PKI de John R. Smith montre comment l'approche de NetApp peut être appliquée à un fichier et fournit un contrôle d'accès précis.

Ces exemples sont fournis à titre d'exemple et il incombe au client de déterminer les métadonnées associées aux étiquettes de sécurité et aux fichiers xattrs NFS v4.2. Les détails sur la mise à jour et la conservation des étiquettes sont omis pour plus de simplicité.

Exemple de valeurs de certificat PKI

Clé	Valeur
EntitySecurityMark	t:s01 = non confidentiel

Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"emailAddresses": [
	{
	"value": "jrsmith@dod.mil"
	}
	],
	"employeeId": {
	"value": "00000387835"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"telephoneNumber": {
	"value": "938/260-9537"
	},
	"uid": {
	"value": "jrsmith"
	}
	}

spécifications	« DOD »
uuid	b4111349-7875-4115-ad30-0928565f2e15

Clé	Valeur

AdminOrganisation	{
	"value": "DoD"
	}

réunions d'information	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

État de la citoyenneté	{
	"value": "US"
	}

jeux	[
	{
	"value": "TS"
	},
	{
	"value": "S"
	},
	{
	"value": "C"
	},
	{
	"value": "U"
	}
	]

Clé	Valeur

PaysOfaffiliations	[
	  {
	  "value": "USA"
	  }
	]

Identificateur numérique	{
	  "classification": "UNCLASSIFIED",
	  "value": "cn=smith john r jrsmith, ou=dod, o=u.s. government, c=us"
	}

Démontez	{
	  "value": "DoD"
	}

DutyOrganisation	{
	  "value": "DoD"
	}

EntityType	{
	  "value": "GOV"
	}

Clé	Valeur

FineAccessControls	[
	{
	"value": "SI"
	},
	{
	"value": "TK"
	},
	{
	"value": "NSYS"
	}
	]

Ces droits ICP montrent les détails d'accès de John R. Smith, y compris l'accès par type de données et l'attribution.

Dans les cas où les métadonnées IC-TDF sont stockées séparément du fichier, NetApp préconise une couche supplémentaire de contrôle d'accès granulaire. Cela implique le stockage des informations de contrôle d'accès au niveau du répertoire et en association avec chaque fichier. Prenons l'exemple des balises suivantes liées à un fichier :

- Étiquettes de sécurité NFS v4.2 : utilisées pour prendre les décisions relatives à la sécurité
- Xattrs : fournir des renseignements supplémentaires pertinents au dossier et aux exigences du programme organisationnel

Les paires clé-valeur suivantes sont des exemples de métadonnées qui peuvent être stockées sous forme de xattrs et fournissent des informations détaillées sur le créateur du fichier et les classifications de sécurité associées. Ces métadonnées peuvent être exploitées par les applications client pour prendre des décisions éclairées en matière d'accès et organiser les fichiers en fonction des normes et des exigences de l'entreprise.

Exemple de paires clé-valeur xattr

Clé	Valeur
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`
`user.specification`	`"INFO"`

Clé	Valeur

user.Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"currentOrganization": {
	"value": "TUV33"
	},
	"displayName": {
	"value": "John Smith"
	},
	"emailAddresses": [
	"jrsmith@example.org"
	],
	"employeeId": {
	"value": "00000405732"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"managers": [
	{
	"value": ""
	}
	],
	"organizations": [
	{
	"value": "TUV33"
	},
	{
	"value": "WXY44"
	}
	],
	"personalTitle": {
	"value": ""
	},
	"secureTelephoneNumber": {
	"value": "506-7718"
	},
	"telephoneNumber": {
	"value": "264/160-7187"
	},
	"title": {
	"value": "Software Engineer"
	},

Clé	Valeur
`user.geo_point`	`[-78.7941, 35.7956]`

```
    }
}
```

Informations associées

- "NFS dans NetApp ONTAP : guide des bonnes pratiques et d'implémentation"
- "Référence des commandes ONTAP"
- Demande de commentaires (RFC)
  - "RFC 7204 : exigences pour le protocole NFS étiqueté"
  - "RFC 2203 : spécification du protocole RPCSEC_GSS"
  - "RFC 3530 : protocole NFS (Network File System) version 4"

Renforcement de la sécurité

Guides ONTAP sur le renforcement de la sécurité

Ces rapports techniques vous indiquent comment renforcer NetApp ONTAP et les autres produits NetApp.

Ces rapports techniques sont détaillés dans "Sécurité et chiffrement des données ONTAP"la documentation produit.

Guides de durcissement

"Tr-4569 : guide sur le renforcement de la sécurité pour NetApp ONTAP" Découvrez comment configurer NetApp ONTAP pour aider les entreprises à atteindre les objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité des systèmes d'information.

"Guide de renforcement de la sécurité des outils ONTAP pour VMware vSphere" Découvrez comment configurer les outils ONTAP pour VMware vSphere pour aider les entreprises à atteindre les objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité des systèmes d'information.

"Tr-4957 : guide sur le renforcement de la sécurité pour NetApp SnapCenter"
Découvrez comment configurer le logiciel NetApp SnapCenter pour aider les entreprises à atteindre les objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité des systèmes d'information.

"TR-4963 : Guide de renforcement de la sécurité : NetApp Backup and Recovery pour les applications"Découvrez comment configurer NetApp Cloud Backup for Applications pour aider les organisations à atteindre les objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité des systèmes d'information.

"Tr-4943 : guide sur le renforcement de la sécurité pour NetApp Active IQ Unified Manager"
Découvrez comment configurer NetApp Active IQ Unified Manager pour aider les entreprises à atteindre les objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité des systèmes d'information.

"Tr-4945 : guide de renforcement de la sécurité pour le SDK de gestion NetApp"
Découvrez comment configurer le SDK de gestion NetApp (NMSDK) pour aider les entreprises à atteindre les objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité des systèmes d'information.

"Guide de renforcement de la sécurité pour l'hôte et la base de données MetroCluster Tiebreaker" Découvrez comment configurer l'hôte et la base de données NetApp MetroCluster Tiebreaker pour aider les entreprises à atteindre les objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité des systèmes d'information.

Instructions de renforcement de la sécurité ONTAP

Présentation du renforcement de la sécurité ONTAP

ONTAP propose un ensemble de commandes qui vous permettent d'utiliser en toute

sécurité le système d'exploitation du stockage ONTAP, le logiciel de gestion des données n° 1 du secteur. Utilisez les conseils et les paramètres de configuration de ONTAP pour aider votre entreprise à atteindre les objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité des systèmes d'information.

L'évolution du paysage actuel des menaces présente à une entreprise des défis uniques pour protéger ses ressources les plus précieuses : les données et les informations. Les menaces et vulnérabilités dynamiques et avancées auxquelles nous sommes confrontés sont de plus en plus sophistiquées. Associés à une augmentation de l'efficacité des techniques d'obfuscation et de reconnaissance de la part des intrus potentiels, les gestionnaires de systèmes doivent aborder de façon proactive la sécurité des données et de l'information.

À partir de juillet 2024, le contenu du rapport technique *TR-4569: Security durcissante guide for ONTAP*, qui a été publié au préalable en format PDF, est disponible sur docs.netapp.com.

Validation des images ONTAP

ONTAP fournit des mécanismes permettant de s'assurer que l'image ONTAP est valide lors de la mise à niveau et au démarrage.

Validation des images de mise à niveau

La signature de code permet de vérifier que les images ONTAP installées via des mises à jour d'images sans interruption ou des mises à jour d'images automatisées sans interruption, des interfaces de ligne de commande ou des API ONTAP sont produites de manière authentique par NetApp et n'ont pas été falsifiées. La validation des images de mise à niveau a été introduite dans ONTAP 9.3.

Cette fonction est une amélioration de la sécurité sans intervention de la mise à niveau ou de la restauration ONTAP. L'utilisateur ne doit rien faire différemment, sauf pour vérifier éventuellement la signature de premier niveau `image.tgz` .

Validation de l'image de démarrage

À partir de ONTAP 9.4, le démarrage sécurisé UEFI (Unified extensible Firmware interface) est activé pour les systèmes NetApp AFF A800, AFF A220, FAS2750 et FAS2720, ainsi que pour les systèmes nouvelle génération qui utilisent le BIOS UEFI.

Lors de la mise sous tension, le chargeur d'amorçage valide la base de données de la liste blanche des clés d'amorçage sécurisées avec la signature associée à chaque module chargé. Une fois que chaque module est validé et chargé, le processus de démarrage continue avec l'initialisation ONTAP. Si la validation de la signature échoue pour un module, le système redémarre.

Ces éléments s'appliquent aux images ONTAP et au BIOS de la plate-forme.

Comptes d'administrateur du stockage local

Rôles, applications et authentification ONTAP

ONTAP offre aux entreprises soucieuses de leur sécurité la possibilité de fournir un accès granulaire à différents administrateurs via différentes applications et méthodes de connexion. Les clients peuvent ainsi créer un modèle zéro confiance centré sur les données.

Il s'agit des rôles disponibles pour les administrateurs admin et Storage Virtual machine. Les méthodes d'application de connexion et les méthodes d'authentification de connexion sont spécifiées.

Rôles

Grâce au contrôle d'accès basé sur des rôles (RBAC), les utilisateurs n'ont accès qu'aux systèmes et aux options requis pour leurs rôles et fonctions. La solution RBAC d'ONTAP limite l'accès administratif des utilisateurs au niveau correspondant à leur rôle, ce qui permet aux administrateurs de gérer les utilisateurs par rôle attribué. ONTAP fournit plusieurs rôles prédéfinis. Les opérateurs et les administrateurs peuvent créer, modifier ou supprimer des rôles de contrôle d'accès personnalisés et peuvent spécifier des restrictions de compte pour des rôles spécifiques.

Rôles prédéfinis pour les administrateurs du cluster

Ce rôle…	Dispose de ce niveau d'accès…	Aux commandes ou répertoires de commandes suivants
`admin`	Tout	Tous les répertoires de commandes (`DEFAULT`)
`admin-no-fsa` (Disponible à partir de ONTAP 9.12.1)	Lecture/écriture	• Tous les répertoires de commandes (`DEFAULT`) • `security login rest-role` • `security login role`

Lecture seule	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	Aucune
`volume file show-disk-usage`	`autosupport`	Tout
• `set` • `system node autosupport`	Aucune	Tous les autres répertoires de commandes (`DEFAULT`)
`backup`	Tout	`vserver services ndmp`
Lecture seule	`volume`	Aucune
Tous les autres répertoires de commandes (`DEFAULT`)	`readonly`	Tout
• `security login password` Pour la gestion du mot de passe local et des informations clés du compte utilisateur • `set`	Aucune	`security`

Lecture seule	Tous les autres répertoires de commandes (`DEFAULT`)	`none`

Le `autosupport` rôle est attribué au compte prédéfini `autosupport`, qui est utilisé par AutoSupport OnDemand. ONTAP vous empêche de modifier ou de supprimer le `autosupport` compte. ONTAP vous empêche également d'attribuer le `autosupport` rôle à d'autres comptes utilisateur.

Rôles prédéfinis pour les administrateurs des machines virtuelles de stockage (SVM)

Nom du rôle	Capacités
`vsadmin`	• Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gérez les volumes, à l'exception des déplacements de volumes • Gérez les quotas, les qtrees, les copies Snapshot et les fichiers • Gérer les LUN • Effectuer des opérations SnapLock, sauf la suppression privilégiée • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Surveiller les tâches • Surveiller les connexions réseau et l'interface réseau • Surveiller l'état de santé du SVM
`vsadmin-volume`	• Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gérez les volumes, à l'exception des déplacements de volumes • Gérez les quotas, les qtrees, les copies Snapshot et les fichiers • Gérer les LUN • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Interface réseau du moniteur • Surveiller l'état de santé du SVM

`vsadmin-protocol`	• Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Gérer les LUN • Interface réseau du moniteur • Surveiller l'état de santé du SVM
`vsadmin-backup`	• Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gestion des opérations NDMP • Effectuez une lecture/écriture de volume restauré • Gestion des relations SnapMirror et des copies Snapshot • Afficher les volumes et les informations réseau
`vsadmin-snaplock`	• Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gérez les volumes, à l'exception des déplacements de volumes • Gérez les quotas, les qtrees, les copies Snapshot et les fichiers • Effectuer des opérations SnapLock, y compris la suppression privilégiée • Configuration des protocoles : NFS et SMB • Configuration des services : DNS, LDAP et NIS • Surveiller les tâches • Surveiller les connexions réseau et l'interface réseau
`vsadmin-readonly`	• Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Surveiller l'état de santé du SVM • Interface réseau du moniteur • Vision des volumes et des LUN • Vision des services et protocoles

Méthodes d'application

La méthode d'application spécifie le type d'accès de la méthode de connexion. Les valeurs possibles incluent `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, et `telnet`.

La définition de ce paramètre sur accorde à `service-processor` l'utilisateur l'accès au processeur de service. Lorsque ce paramètre est défini sur `service-processor`, le `-authentication-method` paramètre doit être défini sur `password` car le processeur de service prend uniquement en charge `password` l'authentification. Les comptes utilisateurs SVM ne peuvent pas accéder au processeur de service. Par conséquent, les opérateurs et les administrateurs ne peuvent pas utiliser le `-vserver` paramètre lorsque ce paramètre est défini sur `service-processor`.

Pour restreindre davantage l'accès à l' `service-processor` , utilisez la commande `system service-processor ssh add-allowed-addresses`. La commande `system service-processor api-service` peut être utilisée pour mettre à jour les configurations et les certificats.

Pour des raisons de sécurité, Telnet et le shell distant (RSH) sont désactivés par défaut car NetApp recommande le shell sécurisé (SSH) pour un accès distant sécurisé. S'il existe une exigence ou un besoin unique de Telnet ou RSH, ils doivent être activés.

La `security protocol modify` commande modifie la configuration existante de RSH et Telnet au niveau du cluster. Activez RSH et Telnet dans le cluster en définissant le champ activé sur `true`.

Méthodes d'authentification

Le paramètre de méthode d'authentification spécifie la méthode d'authentification utilisée pour les connexions.

METHODE d'authentification	Description
`cert`	Authentification par certificat SSL
`community`	Chaînes de communauté SNMP
`domain`	Authentification Active Directory
`nsswitch`	Authentification LDAP ou NIS
`password`	Mot de passe
`publickey`	Authentification par clé publique
`usm`	Modèle de sécurité utilisateur SNMP

L'utilisation de NIS n'est pas recommandée en raison des faiblesses de sécurité du protocole.

À partir de la version ONTAP 9.3, une authentification à deux facteurs est disponible en chaîne pour les comptes SSH locaux `admin` à l'aide des `publickey` deux méthodes d'authentification et `password` . En plus du `-authentication-method` champ de la `security login` commande, un nouveau champ nommé `-second-authentication-method` a été ajouté. `publickey`Ou `password` peut être spécifié en tant que `-authentication-method` ou `-second-authentication-method`. Cependant, lors de l'authentification SSH, l'ordre est toujours `publickey` avec une authentification partielle, suivie de l'invite de mot de passe pour une authentification complète.

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

À partir de ONTAP 9.4, `nsswitch` peut être utilisé comme deuxième méthode d'authentification avec `publickey`.

A partir de ONTAP 9.12.1, FIDO2 peut également être utilisé pour l'authentification SSH à l'aide d'un dispositif d'authentification matérielle YubiKey ou d'autres appareils compatibles FIDO2.

À partir de ONTAP 9.13.1 :

- `domain` les comptes peuvent être utilisés comme deuxième méthode d'authentification avec `publickey`.
- Mot de passe à usage unique basé sur l'heure (`totp`) est un code d'accès temporaire généré par un algorithme qui utilise l'heure actuelle comme l'un de ses facteurs d'authentification pour la deuxième méthode d'authentification.
- La révocation des clés publiques est prise en charge avec les clés publiques SSH ainsi que les certificats qui seront vérifiés pour leur expiration/révocation au cours de SSH.

Pour plus d'informations sur l'authentification multifacteur (MFA) pour ONTAP System Manager, Active IQ Unified Manager et SSH, consultez la section "Tr-4647 : authentification multifacteur dans ONTAP 9".

Comptes d'administration par défaut

Le compte admin doit être restreint car le rôle d'administrateur est autorisé à accéder à l'aide de toutes les applications. Le compte diag permet l'accès à l'interpréteur de commandes du système et ne doit être réservé qu'au support technique pour effectuer les tâches de dépannage.

Il existe deux comptes d'administration par défaut : `admin` et `diag`.

Les comptes orphelins sont un vecteur de sécurité majeur qui entraîne souvent des vulnérabilités, y compris l'escalade des privilèges. Il s'agit de comptes inutiles et inutilisés qui restent dans le référentiel de comptes d'utilisateurs. Il s'agit principalement de comptes par défaut qui n'ont jamais été utilisés ou pour lesquels les mots de passe n'ont jamais été mis à jour ou modifiés. Pour résoudre ce problème, ONTAP prend en charge la suppression et le changement de nom des comptes.

Vous ne pouvez pas supprimer ni renommer les comptes intégrés. Si un administrateur supprime le compte, au redémarrage, le compte intégré sera recréé. **NetApp recommande** de verrouiller tout compte intégré inutile avec la commande lock.

Bien que les comptes orphelins constituent un problème de sécurité important, **NetApp recommande fortement** de tester l'effet de la suppression des comptes du référentiel de comptes local.

Répertorie les comptes locaux

Pour lister les comptes locaux, exécutez la `security login show` commande.

```
cluster1::*> security login show -vserver cluster1

vserver: cluster1
                             Authentication             Acct   Is-Nsswitch
User/Group Name  Application Method    Role Name        Locked Group
---------------- ----------- --------- ---------------- ------ -----------
admin            console     password  admin            no     no
admin            http        password  admin            no     no
admin            ontapi      password  admin            no     no
admin            service-processor password admin       no     no
admin            ssh         password  admin            no     no
autosupport      console     password  autosupport      no     no
6 entries were displayed.
```

Définissez le mot de passe du compte de diagnostic (diag)

Un compte de diagnostic nommé `diag` est fourni avec votre système de stockage. Vous pouvez utiliser le `diag` compte pour effectuer des tâches de dépannage dans `systemshell`. Le `diag` compte est le seul compte qui peut être utilisé pour accéder au systemshell via la `diag` commande Privileged `systemshell`.

> Le systemshell et le compte associé `diag` sont destinés à des fins de diagnostic de bas niveau. Leur accès requiert le niveau de privilège diagnostic et est réservé uniquement pour être utilisé avec l'aide du support technique pour effectuer des tâches de dépannage. Ni le compte ni le n' `diag` `systemshell` est destiné à des fins administratives générales.

Avant de commencer

Avant d'accéder au `systemshell`, vous devez définir le `diag` mot de passe du compte à l'aide de la `security login password` commande. Vous devez utiliser des principes de mot de passe forts et modifier le `diag` mot de passe à intervalles réguliers.

Étapes

1. Définissez le `diag` mot de passe de l'utilisateur du compte :

```
cluster1::> set -privilege diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? \{y|n}: y

cluster1::*> systemshell -node node-01
    (system node systemshell)
diag@node-01's password:

Warning: The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly. Use this environment
only when directed to do so by support personnel.

node-01%
```

Vérification multi-administrateurs

À partir de ONTAP 9.11.1, vous pouvez utiliser la vérification multiadministrateur pour permettre l'exécution de certaines opérations, telles que la suppression de volumes ou de snapshots, uniquement après approbation par les administrateurs désignés. Cela empêche les administrateurs compromis, malveillants ou peu expérimentés d'effectuer des modifications ou de supprimer des données indésirables.

La configuration de MAV comprend les éléments suivants :

- "Création d'un ou de plusieurs groupes d'approbation d'administrateur".
- "Activation de la fonctionnalité de vérification multiadministrateur".
- "Ajout ou modification de règles".

Après la configuration initiale, seuls les administrateurs d'un groupe d'approbation MAV (administrateurs MAV) peuvent modifier ces éléments.

Lorsque MAV est activé, la réalisation de chaque opération protégée nécessite trois étapes :

1. Lorsqu'un utilisateur lance l'opération, un "une demande est générée".
2. Avant de pouvoir l'exécuter, le nombre requis de "Les administrateurs MAV doivent approuver".
3. Après approbation, l'utilisateur termine l'opération.

La MAV n'est pas destinée à être utilisée avec des volumes ou des flux de travail qui impliquent une automatisation poussée car chaque tâche automatisée nécessite une approbation avant que l'opération ne puisse être terminée. Si vous souhaitez utiliser l'automatisation et la vérification multiniveau ensemble, NetApp vous recommande d'utiliser des requêtes pour des opérations de vérification multiniveau spécifiques. Par exemple, vous pouvez appliquer `volume delete` des règles MAV uniquement aux volumes pour lesquels l'automatisation n'est pas impliquée, et vous pouvez désigner ces volumes avec un schéma de nommage particulier.

Pour plus d'informations sur MAV, reportez-vous à la "Documentation de vérification multiadministrateur ONTAP".

Verrouillage des copies Snapshot

Le verrouillage des snapshots est une fonctionnalité SnapLock dans laquelle les snapshots sont rendus indélébiles manuellement ou automatiquement avec une période de conservation définie dans la règle Snapshot du volume. Le verrouillage des snapshots permet d'empêcher les administrateurs peu scrupuleux ou non approuvés de supprimer des snapshots sur le système ONTAP principal ou secondaire.

Le verrouillage des snapshots a été introduit dans ONTAP 9.12.1. Le verrouillage des snapshots est également appelé verrouillage inviolable des snapshots. Bien qu'il nécessite la licence SnapLock et l'initialisation de l'horloge de conformité, le verrouillage des snapshots n'est pas lié à SnapLock Compliance ou SnapLock Enterprise. Il n'existe aucun administrateur de confiance dans le stockage, comme pour SnapLock Enterprise, et il ne protège pas l'infrastructure de stockage physique sous-jacente, comme pour SnapLock Compliance. Il s'agit d'une amélioration par rapport aux snapshots SnapVauting sur un système secondaire. La restauration rapide des copies Snapshot verrouillées sur les systèmes primaires peut être effectuée pour restaurer les volumes corrompus par des ransomwares.

Pour plus de détails, voir "documentation sur le verrouillage des snapshots".

Configurez l'accès à l'API basée sur un certificat

Au lieu de l'authentification par ID utilisateur et mot de passe pour l'accès à ONTAP par l'API REST ou l'API du SDK de gestion NetApp, l'authentification basée sur certificat doit être utilisée.

Comme alternative à l'authentification basée sur certificat pour l'API REST, utilisez "Authentification par jeton OAuth 2.0".)

Vous pouvez générer et installer un certificat auto-signé sur ONTAP comme décrit dans ces étapes.

Étapes

1. À l'aide d'OpenSSL, générez un certificat en exécutant la commande suivante :

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"
Generating a 2048 bit RSA private key
..............+++
.........................+++
writing new private key to 'test.key'
```

   Cette commande génère un certificat public nommé `test.pem` et une clé privée nommée `key.out`. Le nom commun, CN, correspond à l'ID utilisateur ONTAP.

2. Installez le contenu du certificat public au format courrier amélioré confidentiel (pem) dans ONTAP en exécutant la commande suivante et en collant le contenu du certificat lorsque vous y êtes invité :

```
security certificate install -type client-ca -vserver cluster1

Please enter Certificate: Press <Enter> when done
```

3. Activez ONTAP pour autoriser l'accès client via SSL et définissez l'ID utilisateur pour l'accès API.

```
security ssl modify -vserver cluster1 -client-enabled true
security login create -user-or-group-name cert_user -application ontapi
-authmethod cert -role admin -vserver cluster1
```

Dans l'exemple suivant, l'ID utilisateur `cert_user` est désormais activé pour utiliser l'accès à l'API authentifié par certificat. Un script Python du SDK de gestion simple utilisant `cert_user` pour afficher la version ONTAP apparaît comme suit :

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

La sortie du script affiche la version ONTAP.

```
./version.py

V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. Pour effectuer une authentification basée sur un certificat avec l'API REST ONTAP, procédez comme suit :
   a. Dans ONTAP, définissez l'ID utilisateur pour l'accès http :

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

b. Sur votre client Linux, exécutez la commande suivante qui produit la version ONTAP en tant que sortie :

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key
./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
    "version": {
        "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
        "generation": 9,
        "major": 7,
        "minor": 0
    },
    "_links": {
        "self": {
            "href": "/api/cluster"
        }
    }
}
```

Plus d'informations

- "Authentification basée sur certificat avec le SDK de gestion NetApp pour ONTAP".

Authentification basée sur jeton OAuth 2.0 ONTAP pour l'API REST

En alternative à l'authentification basée sur certificat, vous pouvez utiliser l'authentification basée sur jeton OAuth 2.0 pour l'API REST.

Depuis ONTAP 9.14.1, vous avez la possibilité de contrôler l'accès à vos clusters ONTAP à l'aide de l'infrastructure d'autorisation ouverte (OAuth 2.0). Vous pouvez configurer cette fonctionnalité à l'aide de n'importe quelle interface d'administration ONTAP, notamment l'interface de ligne de commandes ONTAP, System Manager et l'API REST. Cependant, les décisions d'autorisation et de contrôle d'accès OAuth 2.0 ne peuvent être appliquées que lorsqu'un client accède à ONTAP à l'aide de l'API REST.

Les jetons OAuth 2.0 remplacent les mots de passe pour l'authentification des comptes utilisateur.

Pour plus d'informations sur l'utilisation d'OAuth 2.0, consultez le "Documentation ONTAP sur l'authentification et l'autorisation via OAuth 2.0".

Paramètres de connexion et de mot de passe

Une stratégie de sécurité efficace est conforme aux politiques, aux directives et à toute gouvernance ou norme établies de l'entreprise. La durée de vie du nom d'utilisateur, les exigences de longueur du mot de passe, les exigences en termes de caractères et le stockage de ces comptes sont des exemples de ces exigences. La solution ONTAP offre des fonctionnalités pour traiter ces constructions de sécurité.

Nouvelles fonctionnalités de compte local

Pour prendre en charge les stratégies, directives ou normes de compte utilisateur d'une entreprise, notamment la gouvernance, les fonctionnalités suivantes sont prises en charge dans ONTAP :

- Configuration des stratégies de mot de passe pour appliquer un nombre minimum de chiffres, de minuscules ou de majuscules
- Délai nécessaire après un échec de la tentative de connexion
- Définition de la limite d'inactivité du compte
- Expiration d'un compte utilisateur
- Affichage d'un message d'avertissement d'expiration de mot de passe
- Notification d'une connexion non valide

Les paramètres configurables sont gérés à l'aide de la commande Security login role config modify.

Prise en charge de SHA-512

Pour améliorer la sécurité des mots de passe, ONTAP 9 prend en charge la fonction de hachage SHA-2 et utilise par défaut la fonction SHA-512 pour hacher les nouveaux mots de passe ou les mots de passe modifiés. Les opérateurs et les administrateurs peuvent également expirer ou verrouiller les comptes selon les besoins.

Les comptes utilisateur ONTAP 9 préexistants avec des mots de passe inchangés continuent d'utiliser la fonction de hachage MD5 après la mise à niveau vers ONTAP 9.0 ou version ultérieure. Cependant, NetApp recommande vivement de migrer ces comptes utilisateur vers la solution SHA-512 plus sécurisée en demandant aux utilisateurs de modifier leur mot de passe.

La fonctionnalité de hachage de mot de passe vous permet d'effectuer les tâches suivantes :

- Afficher les comptes utilisateur correspondant à la fonction de hachage spécifiée :

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver  user-or-group-name application authentication-method hash-
function
-------- ----------------- ----------- --------------------
-------------
cluster1 NewAdmin          console     password             sha512
cluster1 NewAdmin          ontapi      password             sha512
cluster1 NewAdmin          ssh         password             sha512
```

- Comptes expirés utilisant une fonction de hachage spécifiée (MD5, par exemple), qui oblige les utilisateurs à modifier leur mot de passe lors de la connexion suivante :

```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```

- Verrouiller les comptes avec des mots de passe utilisant la fonction de hachage spécifiée.

```
cluster1::*> security login lock -vserver * -username * -hash-function
md5
```

La fonction de hachage password est inconnue pour l'utilisateur interne `autosupport` du SVM d'administration de votre cluster. Ce problème est cosmétique. La fonction de hachage est inconnue car cet utilisateur interne ne dispose pas d'un mot de passe configuré par défaut.

  - Pour afficher la fonction de hachage du mot de passe de l' `autosupport` utilisateur, exécutez les commandes suivantes :

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

                    Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: unknown
Second Authentication Method2: none
```

  - Pour définir la fonction de hachage du mot de passe (par défaut : sha512), exécutez la commande suivante :

```
::> security login password -username autosupport
```

La définition du mot de passe n'a pas d'importance.

```
security login show -user-or-group-name autosupport -instance

                      Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: sha512
Second Authentication Method2: none
```

Paramètres de mot de passe

La solution ONTAP prend en charge les paramètres de mot de passe qui répondent aux exigences et directives de l'entreprise et qui les prennent en charge.

Depuis 9.14.1, la complexité et les règles de verrouillage des mots de passe ne s'appliquent qu'aux nouvelles installations de ONTAP.

Tous les mots de passe doivent être distincts du nom d'utilisateur.

Attribut	Description	Valeur par défaut	Gamme
`username-minlength`	Longueur minimale du nom d'utilisateur requise	3	3-16
`username-alphanum`	Nom d'utilisateur alphanumérique	désactivé	Activé/Désactivé
`passwd-minlength`	Longueur minimale du mot de passe requise	8	3-64
`passwd-alphanum`	Mot de passe alphanumérique	activé	Activé/Désactivé
`passwd-min-special-chars`	Nombre minimum de caractères spéciaux requis dans le mot de passe	0	0-64
`passwd-expiry-time`	Heure d'expiration du mot de passe (en jours)	Illimité, ce qui signifie que les mots de passe n'expirent jamais	0-illimité 0 == expire maintenant
`require-initial-passwd-update`	Exiger la mise à jour initiale du mot de passe lors de la première connexion	Désactivé	Activé/Désactivé Modifications autorisées via la console ou SSH

Attribut	Description	Valeur par défaut	Gamme
`max-failed-login-attempts`	Nombre maximal de tentatives infructueuses	0, ne pas verrouiller le compte	-
`lockout-duration`	Durée maximale de verrouillage (en jours)	La valeur par défaut est 0, ce qui signifie que le compte est verrouillé pendant une journée	-
`disallowed-reuse`	Interdire les N derniers mots de passe	6	Le minimum est de 6
`change-delay`	Délai entre les modifications du mot de passe (en jours)	0	-
`delay-after-failed-login`	Délai après chaque tentative de connexion échouée (en secondes)	4	-
`passwd-min-lowercase-chars`	Nombre minimum de caractères alphabétiques minuscules requis dans le mot de passe	0, qui ne nécessite pas de caractères minuscules	0-64
`passwd-min-uppercase-chars`	Nombre minimum de caractères alphabétiques majuscules requis	0, qui ne nécessite pas de majuscules	0-64
`passwd-min-digits`	Nombre minimum de chiffres requis dans le mot de passe	0, qui ne nécessite pas de chiffres	0-64
`passwd-expiry-warn-time`	Afficher le message d'avertissement avant l'expiration du mot de passe (en jours)	Illimité, ce qui signifie ne jamais avertir de l'expiration du mot de passe	0, ce qui signifie avertir l'utilisateur de l'expiration du mot de passe à chaque connexion réussie
`account-expiry-time`	Le compte expire dans N jours	Illimité, ce qui signifie que les comptes n'expirent jamais	Le délai d'expiration du compte doit être supérieur à la limite d'inactivité du compte
`account-inactive-limit`	Durée maximale d'inactivité avant l'expiration du compte (en jours)	Illimité, ce qui signifie que les comptes inactifs n'expirent jamais	La limite d'inactivité du compte doit être inférieure à l'heure d'expiration du compte

Exemple

```
cluster1::*> security login role config show -vserver cluster1 -role admin

                                          Vserver: cluster1
                                        Role Name: admin
                  Minimum Username Length Required: 3
                            Username Alpha-Numeric: disabled
                  Minimum Password Length Required: 8
                            Password Alpha-Numeric: enabled
Minimum Number of Special Characters Required in the Password: 0
                       Password Expires In (Days): unlimited
   Require Initial Password Update on First Login: disabled
                Maximum Number of Failed Attempts: 0
                    Maximum Lockout Period (Days): 0
                      Disallow Last 'N' Passwords: 6
            Delay Between Password Changes (Days): 0
     Delay after Each Failed Login Attempt (Secs): 4
Minimum Number of Lowercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Uppercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Digits Required in the Password: 0
Display Warning Message Days Prior to Password Expiry (Days): unlimited
                        Account Expires in (Days): unlimited
Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```

Méthodes d’administration du système

Ce sont des paramètres importants pour renforcer l’administration du système ONTAP.

Accès en ligne de commande

L’établissement d’un accès sécurisé aux systèmes est un élément essentiel du maintien de la sécurité de la solution. Les options d’accès en ligne de commande les plus courantes sont SSH, Telnet et RSH. Parmi ces technologies, SSH est la meilleure pratique standard du secteur et la plus sécurisée pour l’accès à distance en ligne de commande. NetApp recommande vivement d’utiliser SSH pour l’accès en ligne de commande à la solution ONTAP.

Configurations SSH

La `security ssh show` commande affiche les configurations des algorithmes d’échange de clés SSH, du chiffrement et des algorithmes MAC pour le cluster et les SVM. La méthode d’échange de clés utilise ces algorithmes et ces chiffrements pour spécifier comment les clés de session à usage unique sont générées pour le cryptage et l’authentification et comment l’authentification du serveur a lieu.

```
cluster1::> security ssh show

Vserver       Ciphers       Key Exchange Algorithms     MAC Algorithms
--------  ----------------  --------------------------  --------------
nsadhanacluster-2
                aes256-ctr,   diffie-helman-group-      hmac-sha2-256
                aes192-ctr,    exchange-sha256,         hmac-sha2-512
                aes128-ctr    ecdh-sha2-nistp384
vs0             aes128-gcm    curve25519-sha256         hmac-sha1
vs1             aes256-ctr,   diffie-hellman-group-     hmac-sha1-96
                aes192-ctr,   exchange-sha256           hmac-sha2-256
                aes128-ctr,   ecdh-sha2-nistp384        hmac-sha2-256-
                3des-cbc,     ecdh-sha2-nistp512        etm
                aes128-gcm                              hmac-sha2-512
3 entries were displayed.
```

Bannières de connexion

Les bannières de connexion permettent aux entreprises de présenter aux opérateurs, administrateurs, voire même aux utilisateurs malveillants, les conditions d'utilisation. Elles indiquent qui est autorisé à accéder au système. Cette approche est utile pour établir les attentes en matière d'accès et d'utilisation du système. La `security login banner modify` commande modifie la bannière de connexion. La bannière de connexion s'affiche juste avant l'étape d'authentification lors du processus de connexion SSH et du périphérique de la console. Le texte de la bannière doit être entre guillemets (" "), comme dans l'exemple suivant.

```
cluster1::> security login banner modify -vserver cluster1 -message
"Authorized users ONLY!"
```

Paramètres de bannière de connexion

Paramètre	Description
`vserver`	Utiliser ce paramètre pour spécifier le SVM avec la bannière modifiée. Utiliser le nom du SVM admin du cluster pour modifier le message au niveau du cluster. La message au niveau du cluster est utilisée par défaut pour les SVM de données qui ne disposent pas de message défini.

Paramètre	Description
`message`	Ce paramètre facultatif peut être utilisé pour spécifier un message de bannière de connexion. Si le cluster a un ensemble de messages de bannière de connexion, la bannière de connexion au cluster est également utilisée par tous les SVM de données. La définition de la bannière de connexion d'un SVM de données remplace l'affichage de la bannière de connexion du cluster. Pour réinitialiser une bannière de connexion SVM de données afin d'utiliser la bannière de connexion au cluster, utilisez ce paramètre avec la valeur « - ». Si vous utilisez ce paramètre, la bannière de connexion ne peut pas contenir de nouvelles lignes (également appelées extrémités de lignes [EOL] ou sauts de ligne). Pour saisir un message de bannière de connexion avec des lignes de rappel, ne spécifiez aucun paramètre. Vous êtes invité à saisir le message de manière interactive. Les messages entrés de manière interactive peuvent contenir des nouvelles lignes. Les caractères non ASCII doivent utiliser Unicode UTF-8.
`uri`	`(ftp
http):///(hostname	IPv4` Utilisez ce paramètre pour spécifier l'URI à partir de laquelle la bannière de connexion est téléchargée. La longueur du message ne doit pas dépasser 2048 octets. Les caractères non ASCII doivent être fournis au format Unicode UTF-8.

Message du jour

La `security login motd modify` commande met à jour le message du jour (MOTD).

Il existe deux catégories de MOTD : le MOTD au niveau du cluster et le MOTD au niveau du SVM de données. Un utilisateur se connectant au cluster d'un SVM de données peut voir deux messages : le MOTD au niveau du cluster suivi du MOTD au niveau du SVM pour ce SVM.

L'administrateur du cluster peut activer ou désactiver le MOTD au niveau du cluster sur chaque SVM individuellement si nécessaire. Si l'administrateur du cluster désactive le MOTD au niveau du cluster pour un SVM, un utilisateur se connectant au SVM ne voit pas le message au niveau du cluster. Seul un administrateur de cluster peut activer ou désactiver le message au niveau du cluster.

Paramètre MOTD	Description
Un vServer	Utiliser ce paramètre pour spécifier le SVM pour lequel le MOTD est modifié. Utiliser le nom du SVM admin du cluster pour modifier le message au niveau du cluster.

Paramètre MOTD	Description
messagerie	Ce paramètre facultatif peut être utilisé pour spécifier un message. Si vous utilisez ce paramètre, le MOTD ne peut pas contenir de nouvelles lignes. Si vous ne spécifiez aucun paramètre autre que le `-vserver` paramètre, vous êtes invité à saisir le message de manière interactive. Les messages entrés de manière interactive peuvent contenir des nouvelles lignes. Les caractères non ASCII doivent être fournis au format Unicode UTF-8. Le message peut contenir du contenu généré de façon dynamique à l'aide des séquences d'échappement suivantes : • `\\` - Un seul caractère de jeu • `\b` - Pas de sortie (pris en charge pour la compatibilité avec Linux uniquement) • `\C` - Nom du cluster • `\d` - La date actuelle telle qu'elle est définie sur le nœud de connexion • `\t` - Heure actuelle définie sur le nœud de connexion • `\I` - Adresse IP de LIF entrante (imprime la console pour une `console` connexion) • `\l` - Nom du périphérique de connexion (imprime la console pour une `console` connexion) • `\L` - Dernière connexion de l'utilisateur sur n'importe quel nœud du cluster • `\m` - Architecture de la machine • `\n` - Nom du nœud ou du SVM de données • `\N` - Nom de l'utilisateur se connectant • `\o` - Identique à \O. Fourni pour la compatibilité Linux. • `\O` - Nom de domaine DNS du nœud. Notez que la sortie dépend de la configuration du réseau et peut être vide. • `\r` - Numéro de version du logiciel • `\s` - Nom du système d'exploitation • `\u` - Nombre de sessions clustershell actives sur le nœud local. Pour l'administrateur du cluster : tous les utilisateurs du cluster shell. Pour le SVM de données admin : sessions actives uniquement pour ce SVM de données. • `\U` - Identique à `\u`, mais a ou a `user users` ajouté • `\v` - Chaîne de version de cluster effective • `\W` - Sessions actives sur le cluster pour l'utilisateur se connectant (`who`)

Pour plus d'informations sur la configuration du message du jour dans ONTAP, reportez-vous au "Documentation ONTAP sur message du jour".

Expiration de la session CLI

Le délai d'expiration par défaut de la session CLI est de 30 minutes. Le délai d'expiration est important pour éviter les sessions obsolètes et le piggydorsal de session.

Utilisez `system timeout show` la commande pour afficher le délai d'expiration actuel de la session de l'interface de ligne de commande. Pour définir la valeur du délai d'expiration, utilisez la `system timeout modify -timeout <minutes>` commande.

Accès Internet avec NetApp ONTAP System Manager

Si un administrateur ONTAP préfère utiliser une interface graphique au lieu de l'interface de ligne de commandes pour accéder au cluster et le gérer, utilisez NetApp ONTAP System Manager. Il est inclus avec ONTAP en tant que service Web, activé par défaut et accessible à l'aide d'un navigateur. Pointez le navigateur sur le nom d'hôte si vous utilisez DNS ou l'adresse IPv4 ou IPv6 via `https://cluster-management-LIF`.

Si le cluster utilise un certificat numérique auto-signé, il est possible que le navigateur affiche un avertissement indiquant que le certificat n'est pas approuvé. Vous pouvez soit reconnaître le risque de continuer l'accès, soit installer un certificat numérique signé par l'autorité de certification (CA) sur le cluster pour l'authentification du serveur.

Depuis ONTAP 9.3, l'authentification SAML (Security assertion Markup Language) est une option disponible dans ONTAP System Manager.

Authentification SAML pour ONTAP System Manager

SAML 2.0 est une norme du secteur largement adoptée qui permet à tout fournisseur d'identités tiers conforme à la norme SAML d'effectuer un MFA à l'aide de mécanismes propres à l'IDP choisi par l'entreprise et en tant que source d'authentification unique (SSO).

Trois rôles sont définis dans la spécification SAML : le principal, l'IDP et le fournisseur de services. Dans l'implémentation de ONTAP, un principal est l'administrateur du cluster qui accède à ONTAP via ONTAP System Manager ou NetApp Active IQ Unified Manager. Le PDI est un logiciel tiers IDP. Depuis ONTAP 9.3, Microsoft Active Directory Federated Services (ADFS) et l'IDP open source Shibboleth sont des PDI pris en charge. À partir de ONTAP 9.12.1, Cisco DUO est un IDP pris en charge. Le fournisseur de services est la fonctionnalité SAML intégrée à ONTAP qui est utilisée par ONTAP System Manager ou l'application Web Active IQ Unified Manager.

Contrairement au processus de configuration à deux facteurs SSH, une fois l'authentification SAML activée, l'accès à ONTAP System Manager ou au processeur de service ONTAP requiert l'authentification de tous les administrateurs existants via ce protocole. Aucune modification n'est requise pour les comptes utilisateur du cluster. Lorsque l'authentification SAML est activée, une nouvelle méthode d'authentification de `saml` est ajoutée aux utilisateurs existants disposant des rôles d'administrateur pour `http` et `ontapi` les applications.

Une fois l'authentification SAML activée, les nouveaux comptes supplémentaires nécessitant l'accès SAML IDP doivent être définis dans ONTAP avec le rôle d'administrateur et la méthode d'authentification saml pour et les `http` `ontapi` applications. Si l'authentification SAML est désactivée à un moment ou à un autre, ces nouveaux comptes requièrent que la `password` méthode d'authentification soit définie avec le rôle d'administrateur pour `http` et `ontapi` les applications et qu'elle ajoute l' `console` application pour l'authentification ONTAP locale à ONTAP System Manager.

Une fois l'IDP SAML activé, il effectue l'authentification pour l'accès au Gestionnaire système ONTAP à l'aide des méthodes disponibles pour ce dernier, telles que le protocole LDAP (Lightweight Directory Access Protocol), Active Directory (AD), Kerberos, le mot de passe, etc. Les méthodes disponibles sont uniques au PDI. Il est important que les comptes configurés dans ONTAP aient des ID utilisateur qui correspondent aux méthodes d'authentification IDP.

Les PDI validés par NetApp sont Microsoft ADFS, Cisco DUO et Shibboleth IDP open source.

À partir de ONTAP 9.14.1, Cisco DUO peut être utilisé comme second facteur d'authentification pour SSH.

Pour plus d'informations sur MFA pour ONTAP System Manager, Active IQ Unified Manager et SSH, voir "Tr-4647 : authentification multifacteur dans ONTAP 9".

Informations ONTAP System Manager

À partir de ONTAP 9.11.1, ONTAP System Manager fournit des informations exploitables pour aider les administrateurs du cluster à rationaliser leurs tâches quotidiennes. Les informations de sécurité sont basées sur les recommandations de ce rapport technique.

Analyse de la sécurité	Détermination
Telnet est activé	NetApp recommande un accès sécurisé à distance (SSH).
Le shell distant (RSH) est activé	NetApp recommande SSH pour un accès distant sécurisé.
AutoSupport utilise un protocole non sécurisé	AutoSupport n'est pas configuré pour être envoyé via lien:HTTPS.
La bannière de connexion n'est pas configurée au niveau du cluster	Avertissement si la bannière de connexion n'est pas configurée pour le cluster.
SSH utilise des chiffrements non sécurisés	Avertissement si SSH utilise des chiffrements non sécurisés.
Trop peu de serveurs NTP sont configurés	Avertissement si le nombre de serveurs NTP configurés est inférieur à trois.
Utilisateur admin par défaut non verrouillé	Lorsque vous n'utilisez aucun compte d'administration par défaut (admin ou diag) pour vous connecter à System Manager et que ces comptes ne sont pas verrouillés, il est recommandé de les verrouiller.
Défense contre les ransomwares : les volumes n'ont pas de règles Snapshot	Aucune règle Snapshot adéquate n'est associée à un ou plusieurs volumes.
Défense anti-ransomware : désactivez la suppression automatique de Snapshot	La suppression automatique des snapshots est définie pour un ou plusieurs volumes.
Les attaques par ransomware ne font pas l'objet d'une surveillance des volumes	La protection anti-ransomware autonome est prise en charge sur plusieurs volumes, mais pas encore configurée.
Les SVM ne sont pas configurés pour la protection autonome contre les ransomware	La protection anti-ransomware autonome est prise en charge sur plusieurs SVM, mais elle n'est pas encore configurée.
FPolicy natif n'est pas configuré	FPolicy n'est pas défini pour les SVM NAS.
Activez le mode actif de protection anti-ransomware autonome	Plusieurs volumes ont terminé leur mode d'apprentissage et vous pouvez activer le mode actif
La conformité à la norme FIPS 140-2 globale est désactivée	La conformité à la norme FIPS 140-2 globale n'est pas activée.
Le cluster n'est pas configuré pour les notifications	Les e-mails, les webhooks ou les traphosts SNMP ne sont pas configurés pour recevoir des notifications.

Pour plus d'informations sur ONTAP System Manager Insights, consultez le "Informations exploitables avec ONTAP System Manager".

Expiration de la session System Manager

Vous pouvez modifier le délai d'inactivité de la session System Manager. Le délai d'inactivité par défaut est de

30 minutes. Un délai d'expiration est important pour éviter les sessions obsolètes et le retour de session.

Si SAML est configuré, le délai d'inactivité est contrôlé par les paramètres de l'IDP.

Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Dans **UI settings**, sélectionnez .
3. Dans la zone **délai d'inactivité**, saisissez une valeur de minutes comprise entre 2 et 180 ou entrez "0" pour désactiver le délai d'inactivité.
4. Sélectionnez **Enregistrer**.

La protection anti-ransomware autonome de ONTAP

Pour compléter l'analytique du comportement des utilisateurs pour Storage Workload Security, la protection anti-ransomware autonome de ONTAP analyse les workloads de volume et l'entropie pour détecter les ransomware, effectue une copie Snapshot et notifie l'administrateur lorsqu'une attaque est suspectée.

Outre la détection et la prévention des ransomwares à l'aide de l'analyse comportementale des utilisateurs FPolicy externes (UBA) avec NetApp Data Infrastructure Insights Storage Workload Security et l'écosystème de partenaires NetApp FPolicy, ONTAP 9.10.1 introduit une protection autonome contre les ransomwares. La protection autonome contre les ransomwares ONTAP utilise une capacité d'apprentissage automatique (ML) intégrée qui examine l'activité de la charge de travail du volume ainsi que l'entropie des données pour détecter automatiquement les ransomwares. Il surveille les activités différentes de celles de l'UBA afin de pouvoir détecter les attaques que l'UBA ne détecte pas.

Pour plus d'informations sur cette fonctionnalité, voir "Solutions NetApp pour ransomware" ou "Documentation sur la protection anti-ransomware autonome de ONTAP".

Audit du système d'administration du stockage

Assurez l'intégrité de l'audit des événements en transférant les événements ONTAP vers un serveur syslog distant. Ce serveur peut être un système de gestion des événements liés aux informations de sécurité tel que Splunk.

Envoyer syslog

Les informations d'audit et de journalisation sont extrêmement précieuses pour le support et la disponibilité. En outre, les informations figurant dans les journaux (syslog) ainsi que dans les rapports et résultats d'audit sont généralement sensibles. Pour préserver les contrôles et le niveau de sécurité, les entreprises doivent impérativement gérer les données de journalisation et d'audit de manière sécurisée.

Le délestage des données des syslog est nécessaire pour limiter l'impact d'une faille à un seul système ou une seule solution. Par conséquent, NetApp recommande de décharger des informations syslog en toute sécurité vers un emplacement de stockage ou de conservation sécurisé.

Créez une destination de transfert de journaux

Utilisez `cluster log-forwarding create` la commande pour créer des destinations de transfert de journaux pour la journalisation à distance.

Paramètres

Utiliser les paramètres suivants pour configurer la `cluster log-forwarding create` commande :

- **Hôte de destination.** Ce nom est le nom d'hôte ou l'adresse IPv4 ou IPv6 du serveur vers lequel transférer les journaux.

```
-destination <Remote InetAddress>
```

- **Port de destination.** Il s'agit du port sur lequel le serveur de destination écoute.

```
[-port <integer>]
```

- **Protocole de transfert de journaux.** Ce protocole est utilisé pour envoyer des messages à la destination.

```
[-protocol \{udp-unencrypted|tcp-unencrypted|tcp-encrypted}]
```

  Le protocole de transfert de journaux peut utiliser l'une des valeurs suivantes :

  - `udp-unencrypted`. Protocole de datagramme utilisateur sans sécurité.
  - `tcp-unencrypted`. TCP sans sécurité.
  - `tcp-encrypted`. TCP avec TLS (transport Layer Security).

- **Vérifiez l'identité du serveur de destination.** Lorsque ce paramètre est défini sur true, l'identité de la destination de transfert de journaux est vérifiée en validant son certificat. La valeur peut être définie sur vrai uniquement lorsque la `tcpencrypted` valeur est sélectionnée dans le champ de protocole.

```
[-verify-server \{true|false}]
```

- **Fonction Syslog.** Cette valeur est la fonction syslog à utiliser pour les journaux transmis.

```
[-facility <Syslog Facility>]
```

- **Ignorez le test de connectivité.** Normalement, la `cluster log-forwarding create` commande vérifie que la destination est accessible en envoyant une requête ping ICMP (Internet Control message Protocol) et échoue si elle n'est pas accessible. La définition de cette valeur `true` permet de contourner la vérification ping afin que vous puissiez configurer la destination lorsqu'elle est inaccessible.

```
[-force [true]]
```

NetApp recommande d'utiliser la `cluster log-forwarding` commande pour forcer la connexion à un `-tcp-encrypted` type.

Notification d'événement

La sécurisation des informations et des données quittant un système est essentielle au maintien et à la gestion du niveau de sécurité du système. Les événements générés par la solution ONTAP sont une mine d'informations sur le problème rencontré par la solution, les informations traitées, etc. La vitalité de ces données souligne la nécessité de les gérer et de les migrer de manière sécurisée.

La `event notification create` commande envoie une nouvelle notification d'un ensemble d'événements défini par un filtre d'événements à une ou plusieurs destinations de notification. Les exemples suivants illustrent la configuration de la notification d'événements et la `event notification show` commande, qui affiche les destinations et les filtres de notification d'événements configurés.

```
cluster1::> event notification create -filter-name filter1 -destinations
 email_dest,syslog_dest,snmp-traphost

cluster1::> event notification show
ID     Filter Name       Destinations
-----  ----------------  -----------------
1 filter1 email_dest, syslog_dest, snmp-traphost
```

Chiffrement du stockage dans ONTAP

Pour protéger les données sensibles en cas de vol, de retour ou de reconversion d'un disque, utilisez le chiffrement de stockage NetApp matériel ou le chiffrement logiciel de volume NetApp/chiffrement d'agrégat NetApp. Ces deux mécanismes sont validés conformément à la norme FIPS-140-2 et lors de l'utilisation de mécanismes matériels avec des mécanismes logiciels, la solution est admissible au programme CSfC (commercial Solutions for Classified Program). Il offre une protection renforcée des données secrètes et les plus secrètes au repos, à la fois au niveau du matériel et des logiciels.

Le chiffrement des données au repos est important pour protéger les données sensibles en cas de vol, de retour ou de reconversion d'un disque.

ONTAP 9 propose trois solutions de chiffrement des données au repos conformes à la norme FIPS 140-2 :

- NetApp Storage Encryption (NSE) est une solution matérielle qui utilise des disques à chiffrement automatique.
- NetApp Volume Encryption (NVE) est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque où il est activé avec une clé unique pour chaque volume.
- NetApp Aggregate Encryption (NAE) est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque grâce à des clés uniques pour chaque agrégat.

NSE, NVE et NAE peuvent utiliser soit la gestion des clés externe, soit le gestionnaire de clés intégré (OKM). L'utilisation de NSE, NVE et NAE n'affecte pas les fonctionnalités d'efficacité du stockage ONTAP. Toutefois, les volumes NVE sont exclus de la déduplication dans les agrégats. Les volumes NAE participent à la déduplication dans les agrégats et en tirent profit.

Le gestionnaire de clés intégré OKM fournit une solution de chiffrement autonome pour les données au repos

avec NSE, NVE ou NAE.

NVE, NAE et OKM utilisent le module de chiffrement ONTAP. CryptoMod figure dans la liste des modules validés CCVP FIPS 140-2. Voir "FIPS 140-2 Cert. No 4144".

Pour commencer la configuration de OKM, utilisez la `security key-manager onboard enable` commande. Pour configurer les gestionnaires de clés KMIP (Key Management Interoperability Protocol) externes, utilisez la `security key-manager external enable` commande. À partir de ONTAP 9.6, la colocation est prise en charge pour les gestionnaires de clés externes. Utiliser le `-vserver <vserver name>` paramètre pour activer la gestion externe des clés pour un SVM spécifique. Avant la version 9.6, la `security key-manager setup` commande servait à configurer OKM et des gestionnaires de clés externes. Pour la gestion intégrée des clés, cette configuration guide l'opérateur ou l'administrateur tout au long de la configuration de la phrase de passe et des paramètres supplémentaires pour la configuration de OKM.

Une partie de la configuration est fournie dans l'exemple suivant :

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default
or omit a question, do not enter a value.

Would you like to configure onboard key management? {yes, no} [yes]:
Enter the cluster-wide passphrase for onboard key management. To continue
the configuration, enter the passphrase, otherwise
type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, save the encrypted configuration
data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager backup show"
command.
```

À partir de ONTAP 9.4, vous pouvez utiliser l' `-enable-cc-mode` option vrai avec `security key-manager setup` pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage. Pour ONTAP 9.6 et versions ultérieures, la syntaxe de la commande est `security key-manager onboard enable -cc-mode-enabled yes`.

À partir de ONTAP 9.4, vous pouvez utiliser la `secure-purge` fonctionnalité avec privilèges avancés pour « nettoyer » les données sur des volumes NVE sans interruption. Le nettoyage des données sur un volume chiffré garantit qu'elles ne peuvent pas être restaurées à partir du support physique. La commande suivante purge de manière sécurisée les fichiers supprimés sur vol1 sur SVM vs1 :

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

À partir de ONTAP 9.7, NAE et NVE sont activés par défaut si la licence VE est en place, OKM ou des gestionnaires de clés externes sont configurés et NSE n'est pas utilisé. Les volumes NAE sont créés par défaut sur les agrégats NAE et les volumes NVE sont créés par défaut sur des agrégats non NAE. Vous pouvez le remplacer en saisissant la commande suivante :

```
cluster1::*> options -option-name
encryption.data_at_rest_encryption.disable_by_default true
```

À partir de la version ONTAP 9.6, vous pouvez utiliser une étendue SVM pour configurer la gestion externe des clés pour un SVM de données dans le cluster. Cette configuration est idéale pour les environnements mutualisés dans lesquels chaque locataire utilise un SVM différent (ou un ensemble de SVM) pour le service des données. Seul l'administrateur du SVM pour un locataire donné peut accéder aux clés pour ce locataire. Pour plus d'informations, reportez-vous à la section "Activez la gestion externe des clés dans ONTAP 9.6 et versions ultérieures" de la documentation ONTAP.

À partir de ONTAP 9.11.1, vous pouvez configurer la connectivité aux serveurs de gestion externe des clés en cluster en désignant des serveurs clés principaux et secondaires sur une SVM. Pour plus d'informations, reportez-vous à la section "configurez les serveurs de clés externes en cluster" de la documentation ONTAP.

À partir de ONTAP 9.13.1, vous pouvez configurer des serveurs de gestionnaire de clés externes dans le gestionnaire de système. Pour plus d'informations, reportez-vous à la section "Gestion de gestionnaires de clés externes" de la documentation ONTAP.

Chiffrement de réplication des données

Pour compléter le chiffrement des données au repos, vous pouvez chiffrer le trafic de réplication des données ONTAP entre les clusters à l'aide de TLS 1.2 avec une clé prépartagée pour SnapMirror, SnapVault ou FlexCache.

Lors de la réplication de données pour la reprise sur incident, la mise en cache ou la sauvegarde, vous devez protéger ces données lors du transport sur le réseau entre un cluster ONTAP et un autre. Cela permet d'éviter les attaques de l'homme du milieu malveillantes contre les données sensibles lorsqu'elles sont en transit.

À partir de ONTAP 9.6, le chiffrement de peering de cluster prend en charge le chiffrement TLS 1.2 AES-256 GCM pour les fonctionnalités de réplication des données ONTAP telles que SnapMirror, SnapVault et FlexCache. Le chiffrement est configuré au moyen d'une clé pré-partagée (PSK) entre deux pairs de cluster.

Les clients qui utilisent des technologies comme NSE, NVE et NAE pour protéger les données au repos peuvent également utiliser le chiffrement des données de bout en bout en passant à ONTAP 9.6 ou version ultérieure pour utiliser le chiffrement de cluster.

Le cluster peering chiffre toutes les données entre les pairs de cluster. Par exemple, lorsque vous utilisez SnapMirror, toutes les informations de peering ainsi que toutes les relations SnapMirror entre l'homologue du

cluster source et l'homologue du cluster destination sont chiffrées. Vous ne pouvez pas envoyer de données en texte clair entre les pairs de cluster lorsque le chiffrement de peering de cluster est activé.

Depuis ONTAP 9.6, le chiffrement est activé par défaut pour les nouvelles relations entre clusters. Pour activer le chiffrement sur les relations entre clusters créées avant ONTAP 9.6, vous devez mettre à niveau le cluster source et le cluster de destination vers la version 9.6. En outre, vous devez utiliser `cluster peer modify` la commande pour modifier les pairs de cluster source et cible afin d'utiliser le chiffrement de peering de cluster.

Vous pouvez convertir une relation de pairs existante pour utiliser le chiffrement de peering de clusters dans ONTAP 9.6, comme illustré dans l'exemple suivant :

```
On the Destination Cluster Peer

cluster2::> cluster peer modify cluster1 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter a passphrase.

On the Source Cluster Peer

cluster1::> cluster peer modify cluster2 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter the same passphrase you created in the previous step.
```

Chiffrement IPsec des données en transit

Les clients qui utilisent des technologies de chiffrement des données au repos, telles que NetApp Storage Encryption (NSE) ou NetApp Volume Encryption (NVE) et Cluster Peering Encryption (CPE) pour le trafic de réplication des données peuvent désormais utiliser le chiffrement de bout en bout entre le client et le stockage dans l'ensemble de leur structure de données multicloud hybride en passant à ONTAP 9.8 ou version ultérieure et en utilisant IPSec : IPSec offre une alternative au chiffrement NFS ou SMB/CIFS et est la seule option de chiffrement à la volée pour le trafic iSCSI.

Dans certains cas, il peut être nécessaire de protéger toutes les données client transportées sur le réseau (ou en transit) vers le SVM ONTAP. Vous empêchez ainsi les attaques par réexécution et les attaques de l'homme du milieu malveillantes contre les données sensibles lorsqu'elles sont en transit.

À partir de la version ONTAP 9.8, IPsec offre la prise en charge du chiffrement de bout en bout pour l'ensemble du trafic IP entre un client et un SVM ONTAP. Le cryptage de données IPSec pour tout le trafic IP inclut les protocoles NFS, iSCSI et SMB/CIFS. IPSec fournit la seule option de cryptage en vol pour le trafic iSCSI.

Le chiffrement NFS sur le réseau est l'un des principaux cas d'utilisation d'IPsec. Avant ONTAP 9.8, le chiffrement NFS over-the-wire exigeait l'installation et la configuration de Kerberos pour utiliser krb5p afin de chiffrer les données NFS à la volée. Ce n'est pas toujours simple ou facile à accomplir dans chaque environnement client.

Les clients qui utilisent des technologies de chiffrement des données au repos, telles que NetApp Storage Encryption (NSE) ou NetApp Volume Encryption (NVE) et Cluster Peering Encryption (CPE) pour le trafic de réplication des données peuvent désormais utiliser le chiffrement de bout en bout entre le client et le stockage dans l'ensemble de leur structure de données multicloud hybride en passant à ONTAP 9.8 ou version ultérieure et en utilisant IPSec :

IPSec est une norme IETF. ONTAP utilise IPsec en mode transport. Il utilise également le protocole Internet Key Exchange (IKE) version 2, qui utilise une clé communiquée à l'avance (PSK) pour négocier les éléments clés entre le client et ONTAP avec IPv4 ou IPv6. Par défaut, IPsec utilise le chiffrement Suite-B AES-GCM 256 bits. Les normes Suite-B AES-GMAC256 et AES-CBC256 avec cryptage 256 bits sont également prises en charge.

Bien que la fonctionnalité IPsec doive être activée sur le cluster, elle s'applique aux adresses IP de SVM individuelles via l'utilisation d'une entrée de base de données de stratégie de sécurité (SPD). L'entrée de règle (SPD) contient l'adresse IP du client (sous-réseau IP distant), l'adresse IP du SVM (sous-réseau IP local), la suite de chiffrement à utiliser et le secret prépartagé (PSK) requis pour l'authentification via IKEv2 et l'établissement de la connexion IPsec. En plus de l'entrée de stratégie IPSec, le client doit être configuré avec les mêmes informations (IP locale et distante, PSK et suite de chiffrement) avant que le trafic puisse circuler sur la connexion IPsec. À partir de ONTAP 9.10.1, la prise en charge de l'authentification par certificat IPsec est ajoutée. Ceci supprime les limites de stratégie IPsec et active la prise en charge du système d'exploitation Windows pour IPsec.

S'il y a un pare-feu entre le client et l'adresse IP du SVM, il doit permettre aux protocoles ESP et UDP (port 500 et 4500), tant entrants (entrée) que sortants (sortie), de réussir la négociation IKEv2 et ainsi d'autoriser le trafic IPsec.

Pour NetApp SnapMirror et le chiffrement du trafic de peering de cluster, le chiffrement de peering de cluster (CPE) est toujours recommandé sur IPsec pour assurer la sécurité en transit sur le réseau. CPE fonctionne mieux pour ces charges de travail que IPSec. Vous n'avez pas besoin d'une licence pour IPsec et il n'y a pas de restrictions d'importation ou d'exportation.

Vous pouvez activer IPsec sur le cluster et créer une entrée SPD pour un seul client et une adresse IP de SVM unique, comme dans l'exemple suivant :

```
On the Destination Cluster Peer

cluster1::> security ipsec config modify -is-enabled true

cluster1::> security ipsec policy create -vserver vs1 -name test34 -local
-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32

When prompted enter and confirm the pre shared secret (PSK).
```

Informations associées

"Préparez-vous à utiliser la sécurité IP sur le réseau ONTAP"

Mode FIPS et gestion TLS et SSL dans ONTAP

La norme FIPS 140-2 spécifie les exigences de sécurité pour les modules cryptographiques dans les systèmes de sécurité qui protègent les informations sensibles dans les systèmes informatiques et de télécommunication. La norme FIPS 140-2

s'applique *spécifiquement* au module cryptographique plutôt qu'au produit, à l'architecture, aux données ou à l'écosystème. Le module cryptographique est le composant spécifique (matériel, logiciel, micrologiciel ou une combinaison des trois) qui implémente les fonctions de sécurité approuvées par le NIST.

L'activation de la conformité FIPS 140-2 a des effets sur d'autres systèmes et communications internes et externes à ONTAP 9. NetApp recommande vivement de tester ces paramètres sur un système hors production disposant d'un accès à la console.

À partir de la prise en charge de ONTAP 9.11.1 et TLS 1.3, vous pouvez valider FIPS 140-3.

La configuration FIPS s'applique à ONTAP et au contrôleur BMC de la plate-forme.

La configuration NetApp ONTAP FIPS-mode

NetApp ONTAP dispose d'une configuration FIPS-mode qui instancie un niveau de sécurité supplémentaire dans le plan de contrôle :

- À partir de ONTAP 9.11.1 lorsque le mode de conformité FIPS 140-2 est activé, TLSv1, TLSv1.1 et SSLv3 sont désactivés et seuls TSLv1.2 et TSLv1.3 restent activés. Elle affecte d'autres systèmes et communications internes et externes à ONTAP 9. Si vous activez le mode de conformité FIPS 140-2 puis désactivez-le, TLSv1, TLSv1.1 et SSLv3 restent désactivés. TLSv1.2 ou TLSSS3.3 restent activés en fonction de la configuration précédente.
- Pour les versions de ONTAP antérieures à 9.11.1 lorsque le mode de conformité FIPS 140-2 est activé, TLSv1 et SSLv3 sont désactivés et seuls TLSv1.1 et TLSv1.2 restent activés. ONTAP vous empêche d'activer à la fois TLSv1 et SSLv3 lorsque le mode de conformité FIPS 140-2 est activé. Si vous activez le mode de conformité FIPS 140-2 puis désactivez-le, TLSv1 et SSLv3 restent désactivés, mais TLSv1.2 ou les deux TLSv1.1 et TLSv1.2 sont activés en fonction de la configuration précédente.
- "Module de chiffrement NetApp (NCSM)", Qui est certifié conforme à la norme FIPS 140-2 de niveau 1, assure la conformité logicielle.

Le NIST a soumis une norme FIPS-140-3 et NCSM sera conforme aux normes FIPS-140-2 et FIPS-140-3. Toutes les validations conformes à la norme FIPS 140-2 seront transférées à l'état historique le 21 septembre 2026, soit cinq ans après le dernier jour de soumission de nouveaux certificats.

Activez le mode de conformité FIPS-140-2 et FIPS-140-3

À partir de ONTAP 9, vous pouvez activer le mode de conformité FIPS-140-2 et FIPS-140-3 pour les interfaces du plan de contrôle au niveau du cluster.

- "Activez le protocole FIPS"
- "Afficher le statut FIPS"

Protocoles et activation FIPS

La `security config modify` commande permet de modifier la configuration de sécurité existante au niveau du cluster. Si vous activez le mode conforme FIPS, le cluster ne sélectionne automatiquement que les protocoles TLS.

- Utilisez le `-supported-protocols` paramètre pour inclure ou exclure des protocoles TLS

indépendamment du mode FIPS. Par défaut, le mode FIPS est désactivé et les protocoles TLSv1.3 (à partir de ONTAP 9.11.1) et TLSv1.2 sont activés.

- Les protocoles TLS suivants étaient activés par défaut dans les versions précédentes de ONTAP :
  - TLSv1.1 (désactivé par défaut à partir de ONTAP 9.12.1)
  - TLSv1 (désactivé par défaut à partir de ONTAP 9.8)
- Pour une compatibilité descendante, ONTAP prend en charge l'ajout de SSLv3 à la liste des protocoles pris en charge lorsque le mode FIPS est désactivé.

Activation et chiffrement FIPS

- Utilisez le `-supported-cipher-suites` paramètre pour configurer uniquement AES (Advanced Encryption Standard) ou AES et 3DES.
- Vous pouvez désactiver les chiffrements faibles tels que RC4 en spécifiant `!RC4`. Par défaut, le paramètre de chiffrement pris en charge est `ALL:!LOW:!aNULL:!EXP:!eNULL`. Ce paramètre signifie que toutes les suites de chiffrement prises en charge pour les protocoles sont activées, sauf celles utilisant des algorithmes de cryptage 64 bits ou 56 bits sans authentification, sans chiffrement, sans exportation et avec des suites de chiffrement à faible cryptage.
- Sélectionnez une suite de chiffrement disponible avec le protocole sélectionné correspondant. Une configuration non valide peut entraîner l'échec de certaines fonctionnalités.
- Pour connaître la syntaxe correcte de la chaîne de chiffrement, reportez-vous à "page chiffrement" la section sur OpenSSL (publiée par la base logicielle OpenSSL). Depuis ONTAP 9.9.1 et les versions ultérieures, il n'est plus nécessaire de redémarrer manuellement tous les nœuds après avoir modifié la configuration de sécurité.

Renforcement de la sécurité SSH et TLS

L'administration SSH de ONTAP 9 nécessite un client OpenSSH 5.7 ou une version ultérieure. Les clients SSH doivent négocier avec l'algorithme de clé publique ECDSA (Elliptic Curve Digital Signature Algorithm) pour que la connexion réussisse.

Pour renforcer la sécurité TLS, activez uniquement TLS 1.2 et utilisez des suites de chiffrement capables de traiter le secret PFS (Perfect Forward Secret). PFS est une méthode d'échange de clés qui, lorsqu'elle est utilisée en combinaison avec des protocoles de chiffrement tels que TLS 1.2, empêche un attaquant de déchiffrer toutes les sessions réseau entre un client et un serveur.

Activez les suites de chiffrement compatibles TLSv1.2 et PFS

Pour activer uniquement les suites de chiffrement compatibles TLS 1.2 et PFS, utilisez la `security config modify` commande du niveau de privilège avancé.

> Avant de modifier la configuration de l'interface SSL, assurez-vous que le client prend en charge les chiffrements DHE et ECDHE lors de la connexion à ONTAP pour maintenir la connectivité avec ONTAP.

Exemple

```
cluster1::*> security config modify -interface SSL -supported-protocols
TLSv1.2 -supported-cipher-suites
PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

Confirmez `y` pour chaque invite. Pour plus d'informations sur PFS, voir "Blog NetApp" .

Informations associées

"Norme fédérale de traitement de l'information (FIPS) publication 140"

Créez un certificat numérique signé par une autorité de certification

Pour de nombreuses organisations, le certificat numérique auto-signé pour l'accès au Web ONTAP n'est pas conforme à leurs politiques InfoSec. Sur les systèmes de production, il est recommandé d'installer un certificat numérique signé par une autorité de certification pour l'authentification du cluster ou du SVM en tant que serveur SSL pour NetApp.

Vous pouvez utiliser `security certificate generate-csr` la commande pour générer une requête de signature de certificat (CSR) et la `security certificate install` commande pour installer le certificat que vous recevez de l'autorité de certification.

Étapes

1. Pour créer un certificat numérique signé par l'autorité de certification de l'organisation, procédez comme suit :
   a. Générer une RSC.
   b. Suivez la procédure de votre organisation pour demander un certificat numérique à l'aide de la RSC auprès de l'autorité de certification de votre organisation. Par exemple, à l'aide de l'interface Web Microsoft Active Directory Certificate Services, accédez à `<CA_server_name>/certsrv` et demandez un certificat.
   c. Installez le certificat numérique dans ONTAP.

Protocole d'état du certificat en ligne

Le protocole OCSP (Online Certificate Status Protocol) permet aux applications ONTAP qui utilisent des communications TLS ou LDAP de recevoir le statut du certificat numérique lorsque OCSP est activé. L'application reçoit une réponse signée indiquant que le certificat demandé est valide, révoqué ou inconnu.

OCSP permet de déterminer le statut actuel d'un certificat numérique sans nécessiter de listes de révocation de certificats.

Par défaut, la vérification du statut du certificat OCSP est désactivée. Il peut être activé à l'aide de la commande `security config ocsp enable -app name`, où le nom de l'application peut être `autosupport`, `audit_log` `fabricpool` `ems`, , , , , `kmip` `ldap_ad` `ldap_nis_namemap`, , ou `all`. La commande nécessite un niveau de privilège avancé.

Gestion SSHv2

`security ssh modify`La commande remplace les configurations existantes des algorithmes d'échange de clés SSH, des chiffrements ou des algorithmes MAC pour le cluster ou un SVM par les paramètres de configuration que vous spécifiez.

Recommandation NetApp :

- Utilisez des mots de passe pour les sessions utilisateur.
- Utiliser une clé publique pour accéder à la machine.

Chiffrements et échanges de clés pris en charge

Chiffrement	Échange de clés
aes256-ctr	diffie-hellman-group-Exchange-sha256 (SHA-2)
aes192-ctr	diffie-hellman-Group-Exchange-sha1 (SHA-1)
aes128-ctr	diffie-hellman-groupe14-sha1 (SHA-1)
aes256-cbc	diffie-hellman-groupe1-sha1 (SHA-1)
aes192-cbc	-
aes128-cbc	-
aes128-gcm	-
aes256-gcm	-
3des-cbc	-

Cryptage symétrique AES et 3DES pris en charge

ONTAP prend également en charge les types de chiffrement symétrique AES et 3DES suivants (également appelés chiffrement) :

- hmac-sha1
- hmac-sha1-96
- hmac-md5
- hmac-md5-96
- hmac-ripemd160
- umac-64
- umac-64
- umac-128
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1-etm
- hmac-sha1-96-etm

- hmac-sha2-256-etm
- hmac-sha2-512-etm
- hmac-md5-etm
- hmac-md5-96-etm
- hmac-ripemd160-etm
- umac-64-etm
- umac-128-etm

La configuration de gestion SSH s'applique à ONTAP et au contrôleur BMC de la plate-forme.

NetApp AutoSupport

La fonction AutoSupport de ONTAP vous permet de contrôler de manière proactive l'état de votre système et d'envoyer automatiquement des messages et des détails au support technique NetApp, à l'équipe de support interne de votre entreprise ou à un partenaire de support. Par défaut, les messages AutoSupport envoyés au support technique NetApp sont activés lorsque le système de stockage est configuré pour la première fois. De plus, AutoSupport commence à envoyer des messages au support technique NetApp 24 heures après son activation. Cette période de 24 heures est configurable. Pour tirer parti de la communication avec l'équipe de support interne d'une entreprise, la configuration de l'hôte de messagerie doit être effectuée.

Seul l'administrateur du cluster peut effectuer la gestion AutoSupport (configuration). L'administrateur du SVM n'a pas accès à AutoSupport. La fonction AutoSupport peut être désactivée. Toutefois, NetApp recommande de l'activer, car AutoSupport accélère l'identification et la résolution des problèmes en cas de problème sur le système de stockage. Par défaut, le système collecte les informations AutoSupport et les stocke localement même si vous désactivez AutoSupport.

Pour plus d'informations sur les messages AutoSupport, notamment sur ce qui se trouve dans les différents messages et sur l'emplacement d'envoi des différents types de messages, reportez-vous à la "Conseiller digital NetApp" documentation.

Les messages AutoSupport contiennent des données sensibles, notamment, mais sans s'y limiter, les éléments suivants :

- Fichiers journaux
- Données contextuelles concernant des sous-systèmes spécifiques
- Données de configuration et d'état
- Les données de performance

AutoSupport prend en charge HTTPS et SMTP pour les protocoles de transport. En raison des nature sensibles des messages AutoSupport, NetApp recommande fortement d'utiliser HTTPS comme protocole de transport par défaut pour l'envoi des messages AutoSupport au support NetApp.

De plus, vous devez utiliser `system node autosupport modify` la commande pour spécifier les cibles des données AutoSupport (par exemple, le support technique NetApp, les opérations internes d'une entreprise ou les partenaires). Cette commande vous permet également d'indiquer quelles informations AutoSupport spécifiques envoyer (par exemple, données de performances, fichiers journaux, etc.).

Pour désactiver entièrement AutoSupport, utilisez `system node autosupport modify -state disable` la commande.

Protocole de temps réseau

Bien que ONTAP vous permette de définir manuellement le fuseau horaire, la date et l'heure sur le cluster, vous devez configurer les serveurs NTP (Network Time Protocol) afin de synchroniser l'heure du cluster avec au moins trois serveurs NTP externes.

Les problèmes peuvent survenir lorsque l'heure du cluster est incorrecte. Bien que ONTAP vous permette de définir manuellement le fuseau horaire, la date et l'heure sur le cluster, vous devez configurer les serveurs NTP (Network Time Protocol) afin de synchroniser l'heure du cluster avec les serveurs NTP externes.

Depuis ONTAP 9.5, vous pouvez configurer votre serveur NTP avec une authentification symétrique.

Vous pouvez associer un maximum de 10 serveurs NTP externes à l'aide de la `cluster time-service ntp server create` commande. Pour la redondance et la qualité du service de temps, vous devez associer au moins trois serveurs NTP externes au cluster.

Pour plus de détails sur la configuration de NTP dans ONTAP, reportez-vous à la section "Gestion de l'heure du cluster (administrateurs du cluster uniquement)".

Comptes locaux du système de fichiers NAS (groupe de travail CIFS)

L'authentification des clients de groupe de travail offre une couche de sécurité supplémentaire à la solution ONTAP, qui est conforme à une posture d'authentification de domaine traditionnelle. Utilisez `vserver cifs session show` la commande pour afficher de nombreuses informations relatives au positionnement, notamment les informations IP, le mécanisme d'authentification, la version du protocole et le type d'authentification.

À partir de ONTAP 9, vous pouvez configurer un serveur CIFS dans un groupe de travail avec des clients CIFS qui s'authentifient auprès du serveur à l'aide d'utilisateurs et de groupes définis localement. L'authentification des clients de groupe de travail offre une couche de sécurité supplémentaire à la solution ONTAP, qui est conforme à une posture d'authentification de domaine traditionnelle. Pour configurer le serveur CIFS, utilisez `vserver cifs create` la commande. Une fois le serveur CIFS créé, vous pouvez le joindre à un domaine CIFS ou le joindre à un groupe de travail. Pour rejoindre un groupe de travail, utilisez le `-workgroup` paramètre. Voici un exemple de configuration :

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-workgroup Sales
```

Un serveur CIFS en mode groupe de travail prend uniquement en charge l'authentification Windows NT LAN Manager (NTLM) et ne prend pas en charge l'authentification Kerberos.

NetApp recommande d'utiliser la fonction d'authentification NTLM avec des groupes de travail CIFS pour maintenir la sécurité de votre entreprise. Pour valider la posture de sécurité CIFS, NetApp recommande d'utiliser la `vserver cifs session show` commande pour afficher de nombreuses informations relatives au positionnement, notamment les informations IP, le mécanisme d'authentification, la version du protocole et

le type d'authentification.

Audit du système de fichiers NAS

Les systèmes de fichiers NAS occupent une place de plus en plus importante dans le paysage actuel des menaces. Les fonctions d'audit sont essentielles pour assurer la visibilité des menaces.

La sécurité exige une validation. ONTAP fournit des événements d'audit plus nombreux et plus détaillés pour l'ensemble de la solution. Étant donné que les systèmes de fichiers NAS occupent une encombrement accru dans le paysage des menaces actuel, les fonctions d'audit sont essentielles pour garantir la visibilité. Grâce à la capacité d'audit améliorée dans ONTAP, les détails d'audit CIFS sont plus nombreux que jamais. Les informations clés, notamment les suivantes, sont consignées avec les événements créés :

- Accès aux fichiers, aux dossiers et au partage
- Fichiers créés, modifiés ou supprimés
- Accès en lecture du fichier réussi
- Échec des tentatives de lecture ou d'écriture des fichiers
- Modification des autorisations sur les dossiers

Créer une configuration d'audit

Vous devez activer l'audit CIFS pour générer des événements d'audit. Utiliser `vserver audit create` la commande pour créer une configuration d'audit. Par défaut, le journal d'audit utilise une méthode de rotation basée sur la taille. Vous pouvez utiliser une option de rotation basée sur le temps si elle est spécifiée dans le champ Paramètres de rotation. Les détails supplémentaires de la configuration de rotation de l'audit de journal incluent le planning de rotation, les limites de rotation, les jours de rotation de la semaine et la taille de rotation. Le texte suivant fournit un exemple de configuration d'audit utilisant une rotation mensuelle planifiée pour tous les jours de la semaine à 12:30.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule
-hour 12 -rotate-schedule-minute 30
```

Événements d'audit CIFS

Les événements d'audit CIFS sont les suivants :

- **Partage de fichiers** : génère un événement d'audit lorsqu'un partage réseau CIFS est ajouté, modifié ou supprimé à l'aide des commandes associées `vserver cifs share` .
- **Changement de stratégie d'audit** : génère un événement d'audit lorsque la stratégie d'audit est désactivée, activée ou modifiée à l'aide des commandes associées `vserver audit` .
- **Compte utilisateur** : génère un événement d'audit lorsqu'un utilisateur CIFS ou UNIX local est créé ou supprimé ; un compte utilisateur local est activé, désactivé ou modifié ; ou un mot de passe est réinitialisé ou modifié. Cet événement utilise la `vserver cifs users-and-groups local-group` commande ou la commande associée `vserver services name-service unix-user` .
- **Groupe de sécurité** : génère un événement d'audit lorsqu'un groupe de sécurité local CIFS ou UNIX est créé ou supprimé à l'aide de la `vserver cifs users-and-groups local-group` commande ou de

la commande associée `vserver services name-service unix-group`.

- **Changement de stratégie d'autorisation** : génère un événement d'audit lorsque des droits sont accordés ou révoqués pour un utilisateur CIFS ou un groupe CIFS à l'aide de la `vserver cifs users-and-groups privilege` commande.

> Cette fonctionnalité est basée sur la fonction d'audit du système, qui permet à un administrateur de vérifier ce que le système autorise et exécute du point de vue d'un utilisateur de données.

Effet des API REST sur l'audit NAS

ONTAP permet aux comptes d'administrateur d'accéder aux fichiers SMB/CIFS ou NFS et de les manipuler à l'aide d'API REST. Bien que les API REST puissent uniquement être exécutées par les administrateurs ONTAP, les commandes de l'API REST contournent le journal d'audit NAS du système. En outre, les administrateurs ONTAP peuvent également ignorer les autorisations liées aux fichiers lors de l'utilisation des API REST. Cependant, les actions de l'administrateur avec les API REST sur les fichiers sont capturées dans le journal de l'historique des commandes du système.

Créez un rôle d'API REST sans accès

Vous pouvez empêcher les administrateurs ONTAP d'utiliser des API REST pour l'accès aux fichiers en créant un rôle d'API REST qui n'a pas accès aux volumes ONTAP via REST. Pour configurer ce rôle, procédez comme suit.

> L'API REST /api/storage/volumes est utilisée pour plus que l'accès aux fichiers. Elle est utilisée par System Manager et d'autres interfaces graphiques pour créer, visualiser et modifier des volumes.

Étapes

1. Créez un nouveau rôle REST qui n'a pas accès aux volumes de stockage mais qui dispose de tout autre accès API REST.

```
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api/storage/volumes" -access none
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api" -access all
```

2. Attribuez le compte administrateur au nouveau rôle d'API REST que vous avez créé à l'étape précédente.

```
cluster1::> security login modify -user-or-group-name user1 -application
http -authentication-method password -vserver cluster1 -role nofile
```

> Pour empêcher le compte d'administrateur de cluster ONTAP intégré d'utiliser les API REST pour accéder aux fichiers, vous devez d'abord "créez un nouveau compte administrateur et désactivez ou supprimez le compte intégré".

Configuration et activation de la signature et du chiffrement SMB CIFS

Vous pouvez configurer et activer la signature SMB qui protège la sécurité de la Data Fabric en veillant à ce que le trafic entre les systèmes de stockage et les clients ne soit pas compromis par des attaques par réexécution ou des attaques de l'homme du milieu. La signature SMB assure la protection en vérifiant que les messages SMB ont une signature valide.

Description de la tâche

Le protocole SMB constitue un vecteur de menaces courant pour les systèmes de fichiers et les architectures. Pour résoudre ce problème, la solution ONTAP 9 utilise la signature et le chiffrement SMB standard. La signature SMB protège la sécurité du maillage Data Fabric en s'assurant que le trafic entre les systèmes de stockage et les clients n'est pas compromis par des attaques par réexécution ou des attaques de l'homme du milieu. Il vérifie que les messages SMB ont une signature valide.

Bien que la signature SMB soit désactivée par défaut dans l'intérêt des performances, NetApp vous recommande fortement de l'activer. En outre, la solution ONTAP prend en charge le chiffrement SMB. Cette approche permet le transport sécurisé des données partage par partage. Le chiffrement SMB est désactivé par défaut. Cependant, NetApp vous recommande d'activer le chiffrement SMB.

La signature et le chiffrement LDAP sont désormais pris en charge dans SMB 2.0 et versions ultérieures. La signature (protection contre toute falsification) et le chiffrement (chiffrement) assurent une communication sécurisée entre les SVM et les serveurs Active Directory. Le chiffrement accéléré des nouvelles instructions AES (Intel AES ni) est désormais pris en charge par SMB 3.0 et les versions ultérieures. Intel AES ni améliore l'algorithme AES et accélère le chiffrement des données pour toute la gamme de processeurs compatibles.

Étapes

1. Pour configurer et activer la signature SMB, utilisez `vserver cifs security modify` la commande et vérifiez que le `-is-signing-required` paramètre est défini sur `true`. Voir l'exemple de configuration suivant :

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -is-signing-required true
```

2. Pour configurer et activer le chiffrement SMB et le chiffrement, utilisez `vserver cifs security modify` la commande et vérifiez que le `-is-smb-encryption-required` paramètre est défini sur `true`. Voir l'exemple de configuration suivant :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

Sécurisation NFS

Les règles d'exportation sont les éléments fonctionnels d'une export-policy. Les règles d'exportation correspondent aux demandes d'accès client d'un volume par rapport à des paramètres spécifiques que vous configurez pour déterminer comment gérer les demandes d'accès client. Une export-policy doit contenir au moins une règle d'exportation pour permettre l'accès aux clients. Si une export-policy contient plusieurs règles, celles-ci sont traitées dans l'ordre dans lequel elles apparaissent dans l'export-policy.

Le contrôle d'accès est essentiel au maintien d'une posture de sécurité. Par conséquent, ONTAP utilise la fonctionnalité export policy pour limiter l'accès au volume NFS aux clients correspondant à des paramètres spécifiques. Les export-policy contiennent une ou plusieurs règles d'exportation qui traitent chaque requête d'accès client. Une export policy est associée à chaque volume afin de configurer l'accès client au volume. Le résultat de ce processus détermine si le client est autorisé ou refusé (avec un message d'autorisation refusée) à accéder au volume. Ce processus détermine également le niveau d'accès fourni au volume.

Pour que les clients puissent accéder aux données, une export policy doit exister sur un SVM. Un SVM peut contenir plusieurs export policies.

L'ordre des règles est dicté par le numéro d'index des règles. Si une règle correspond à un client, les autorisations de cette règle sont utilisées et aucune autre règle n'est traitée. Si aucune règle ne correspond, l'accès au client est refusé.

Les règles d'exportation déterminent les autorisations d'accès client en appliquant les critères suivants :

- Protocole d'accès aux fichiers utilisé par le client qui envoie la requête (par exemple, NFSv4 ou SMB)
- Un identifiant client (par exemple, le nom d'hôte ou l'adresse IP)
- Type de sécurité utilisé par le client pour l'authentification (par exemple, Kerberos v5, NTLM ou AUTH_SYS)

Si une règle spécifie plusieurs critères et que le client ne correspond pas à un ou plusieurs d'entre eux, la règle ne s'applique pas.

Un exemple de export-policy contient une règle d'export avec les paramètres suivants :

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Le type de sécurité détermine le niveau d'accès qu'un client reçoit. Les trois niveaux d'accès sont lecture seule, lecture-écriture et superutilisateur (pour les clients avec l'ID utilisateur `0`). Comme le niveau d'accès déterminé par le type de sécurité est évalué dans cet ordre, vous devez respecter les règles répertoriées :

Règles pour les paramètres de niveau d'accès dans les règles d'exportation

Pour qu'un client obtienne les niveaux d'accès suivants	Ces paramètres d'accès doivent correspondre au type de sécurité du client
Lecture seule normale par l'utilisateur	Lecture seule (`-rorule`)
Lecture-écriture utilisateur normale	Lecture seule (`-rorule`) et lecture-écriture)(`-rwrule`
Super-utilisateur en lecture seule	Lecture seule (`-rorule`) et `-superuser`
Super-utilisateur lecture-écriture	Lecture seule (`-rorule`) et lecture-écriture (`-rwrule`) et `-superuser`

Les types de sécurité suivants sont valides pour chacun de ces trois paramètres d'accès :

- Toutes
- Aucune
- Jamais

Ces types de sécurité ne peuvent pas être utilisés avec le `-superuser` paramètre :

- krb5
- ntlm
- system

Règles pour les résultats des paramètres d'accès

Si le type de sécurité du client …	Alors …
Correspond à un type de sécurité spécifié dans le paramètre d'accès.	Le client reçoit l'accès pour ce niveau avec son propre ID utilisateur.
Ne correspond pas à un type de sécurité spécifié, mais le paramètre d'accès inclut l'option `none`.	Le client reçoit l'accès pour ce niveau et reçoit l'utilisateur anonyme avec l'ID utilisateur spécifié par le `-anon` paramètre.
Ne correspond pas à un type de sécurité spécifié et le paramètre d'accès n'inclut pas l'option `none`.	Le client ne reçoit aucun accès pour ce niveau. Cette restriction ne s'applique pas au `-superuser` paramètre car ce paramètre n'inclut toujours aucune, même si elle n'est pas spécifiée.

Kerberos 5 et Krb5p

À partir de ONTAP 9, l'authentification Kerberos 5 avec service Privacy (krb5p) est prise en charge. Le mode d'authentification krbp5 est sécurisé et offre une protection contre la falsification et l'espionnage des données. Il utilise des checksums pour chiffrer l'ensemble du trafic entre le client et le serveur. La solution ONTAP prend en charge le chiffrement AES 128 bits et 256 bits pour Kerberos. Le service de confidentialité comprend la

vérification de l'intégrité des données reçues, l'authentification des utilisateurs et le cryptage des données avant leur transmission.

L'option krb5p est la plus présente dans la fonctionnalité export policy, où elle est définie comme option de cryptage. La méthode d'authentification krb5p peut être utilisée comme paramètre d'authentification, comme illustré dans l'exemple suivant :

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method krb5p -protocol nfs3
-access- type read
```

Activez la signature et le chiffrement du protocole d'accès aux répertoires légers

La signature et le chiffrement sont pris en charge pour permettre la sécurité des sessions lors de requêtes vers un serveur LDAP. Cette approche offre une alternative à la sécurité des sessions LDAP-over-TLS.

La signature valide l'intégrité des données LDAP à l'aide d'une technologie à clé secrète. Le chiffrement crypte les données LDAP afin de ne pas transmettre de données sensibles en clair. Les paramètres de sécurité de session sur un SVM correspondent à ceux disponibles sur le serveur LDAP. Par défaut, la signature et le chiffrement LDAP sont désactivés.

Étapes

1. Pour activer cette fonction, exécutez la `vserver cifs security modify` commande avec le `session-security-for-ad-ldap` paramètre.

   Options des fonctions de sécurité LDAP :

   - **Aucun** : par défaut, pas de signature ou de chiffrement
   - **Sign** : signer le trafic LDAP
   - **Sceau** : signer et crypter le trafic LDAP

   > Les paramètres de signe et de sceau sont cumulatifs, ce qui signifie que si l'option de signe est utilisée, le résultat est LDAP avec signature. Cependant, si l'option de joint est utilisée, le résultat est à la fois signe et joint. En outre, si aucun paramètre n'est spécifié pour cette commande, la valeur par défaut est aucun.

   Voici un exemple de configuration :

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -session-security-for-ad-ldap seal
```

Créez et utilisez un NetApp FPolicy

Vous pouvez créer et utiliser un composant d'infrastructure FPolicy de la solution ONTAP, qui permet à des applications partenaires de surveiller et définir les autorisations d'accès aux fichiers. L'une des applications les plus puissantes est Storage Workload Security,

une application SaaS NetApp qui offre une visibilité et un contrôle centralisés sur tous les accès aux données de l'entreprise dans les environnements de cloud hybride afin d'assurer la conformité et la sécurité.

Le contrôle d'accès est un concept de sécurité clé. La visibilité des accès aux fichiers et des opérations sur fichiers ainsi que la possibilité d'y réagir sont critiques pour maintenir le niveau de sécurité requis. Pour fournir cette visibilité et ce contrôle d'accès aux fichiers, la solution ONTAP utilise la fonction NetApp FPolicy.

Les règles peuvent être définies en fonction des types de fichiers. FPolicy détermine la façon dont le système de stockage gère les requêtes de chaque système client pour des opérations telles que les créations, ouvertures, renommages et suppressions. Depuis ONTAP 9, le système de notification d'accès aux fichiers FPolicy possède des commandes de filtrage et supporte de brèves coupures de réseau.

Étapes

1. Pour exploiter la fonction FPolicy, vous devez d'abord créer la règle FPolicy avec la `vserver fpolicy policy create` commande.

   > En outre, utilisez le `-events` paramètre si vous utilisez FPolicy pour la visibilité et la collecte des événements. La granularité supplémentaire fournie par ONTAP permet de filtrer les données et d'accéder au niveau de contrôle par nom d'utilisateur. Pour contrôler les privilèges et l'accès avec des noms d'utilisateur, spécifiez le `-privilege-user-name` paramètre.

   Le texte suivant fournit un exemple de création FPolicy :

   ```
   cluster1::> vserver fpolicy policy create -vserver vs1.example.com
   -policy-name vs1_pol -events cserver_evt,v1e1 -engine native -is
   -mandatory true -allow-privileged-access no -is-passthrough-read-enabled
   false
   ```

2. Une fois que vous avez créé la règle FPolicy, vous devez l'activer avec `vserver fpolicy enable` la commande. Cette commande définit également la priorité ou la séquence de l'entrée FPolicy.

   > La séquence FPolicy est importante car, si plusieurs règles ont souscrit au même événement d'accès aux fichiers, la séquence détermine l'ordre dans lequel l'accès est accordé ou refusé.

   Le texte suivant fournit un exemple de configuration pour l'activation de la règle FPolicy et la validation de la configuration avec la `vserver fpolicy show` commande :

```
cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
vs2_pol -sequence-number 5

cluster1::> vserver fpolicy show
Vserver                 Policy Name                  Sequence  Status
Engine
----------------------- ---------------------------- --------  -------
-------
vs1.example.com         vs1_pol
vs2.example.com         vs2_pol
 external
2 entries were displayed.
```

Améliorations de FPolicy

ONTAP 9 inclut les améliorations de FPolicy décrites dans les sections suivantes.

Filtrage des contrôles

De nouveaux filtres sont disponibles pour `SetAttr` et pour la suppression de notifications sur les activités d'annuaire.

Résilience asynchrone

Lorsqu'un serveur FPolicy fonctionnant en mode asynchrone est en panne du réseau, les notifications FPolicy générées lors de la panne sont stockées sur le nœud de stockage. Lorsque le serveur FPolicy est de nouveau en ligne, il est averti des notifications stockées et peut les récupérer du nœud de stockage. La durée pendant laquelle les notifications peuvent être stockées en cas de panne peut être configurée pendant 10 minutes.

Caractéristiques de sécurité des rôles LIF dans ONTAP

Une LIF est une adresse IP ou un nom de port mondial (WWPN) avec des caractéristiques associées, telles qu'un rôle, un port d'attache, un nœud d'attache, une liste de ports à basculer et une politique de pare-feu. Vous pouvez configurer les LIF sur les ports sur lesquels le cluster envoie et reçoit des communications sur le réseau. Il est essentiel de comprendre les caractéristiques de sécurité de chaque rôle de LIF.

Rôles LIF

Les rôles LIF peuvent être les suivants :

- **Data LIF** : une LIF associée à un SVM et utilisée pour communiquer avec les clients.
- **Cluster LIF** : une LIF utilisée pour transporter le trafic intracluster entre les nœuds d'un cluster.
- **Node management LIF** : une LIF qui fournit une adresse IP dédiée pour la gestion d'un nœud particulier dans un cluster.
- **Cluster management LIF** : une LIF qui fournit une interface de gestion unique pour l'ensemble du cluster.
- **Intercluster LIF** : une LIF utilisée pour la communication, la sauvegarde et la réplication entre clusters.

Caractéristiques de sécurité de chaque rôle de LIF

	LIF de données	LIF de cluster	FRV de gestion des nœuds	LIF de gestion de cluster	LIF intercluster
Nécessite un sous-réseau IP privé ?	Non	Oui	Non	Non	Non
Nécessite un réseau sécurisé ?	Non	Oui	Non	Non	Oui
Politique de pare-feu par défaut	Très restrictif	Entièrement ouvert	Moyen	Moyen	Très restrictif
Le pare-feu est-il personnalisable ?	Oui	Non	Oui	Oui	Oui

- La LIF de cluster étant complètement ouverte sans règle de pare-feu configurable, elle doit se trouver sur un sous-réseau IP privé sur un réseau isolé et sécurisé.
- Les rôles LIF ne doivent jamais être exposés à Internet.

Pour en savoir plus sur la sécurisation des LIF, consultez "Configuration des politiques de pare-feu pour les LIF". Cette page fournit également des détails sur les politiques de service LIF à partir d' ONTAP 9.10.1.

Pour en savoir plus sur la création d'une nouvelle politique de service, consultez la documentation. `network interface service-policy create` commande dans le "Référence des commandes."

Protocole et sécurité des ports

Outre les opérations et fonctions de sécurité intégrées, le renforcement d'une solution doit également inclure des mécanismes de sécurité externe. L'utilisation de dispositifs d'infrastructure supplémentaires, tels que des pare-feu, des systèmes de prévention des intrusions et d'autres dispositifs de sécurité, pour filtrer et limiter l'accès à ONTAP constitue un moyen efficace d'établir et de maintenir une stratégie de sécurité rigoureuse. Ces informations sont un élément clé pour filtrer et limiter l'accès à l'environnement et à ses ressources.

Protocoles et ports couramment utilisés

Service	Port/Protocole	Description
`SSH`	22/TCP	Connexion SSH
`telnet`	23/TCP	Connexion à distance
`Domain`	53/TCP	Serveur de noms de domaine
`HTTP`	80/TCP 80/UDP	HTTP
`rpcbind`	111/TCP 111/UDP	Appel de procédure à distance

Service	Port/Protocole	Description
NTP	123/UDP	Protocole de temps réseau
msrpc	135/TCP	Appel de procédure à distance Microsoft
Netbios-name	137/TCP 137/UDP	Service de noms NetBIOS
netbios-ssn	139/TCP	Session de service NetBIOS
SNMP	161/UDP	SNMP
HTTPS	443/TCP	Lien sécurisé :http
microsoft-ds	445/TCP	Services d'annuaire Microsoft
IPsec	500/UDP	Sécurité du protocole Internet
mount	635/UDP	Montage NFS
named	953/UDP	Nom démon
NFS	2049/UDP 2049/TCP	Démon du serveur NFS
nrv	2050/TCP	Protocole de volume distant NetApp
iscsi	3260/TCP	Port cible iSCSI
Lockd	4045/TCP 4045/UDP	Démon de verrouillage NFS
NFS	4046/TCP	Protocole de montage NFS
acp-proto	4046/UDP	Protocole de comptabilité
rquotad	4049/UDP	Protocole NFS rquotad
krb524	4444/UDP	Kerberos 524
IPsec	4500/UDP	Sécurité du protocole Internet
acp	5125/UDP 5133/UDP 5144/TCP	Autre port de contrôle pour le disque
Mdns	5353/UDP	DNS multicast
HTTPS	5986/UDP	Port HTTPS : protocole binaire d'écoute
TELNET	8023/TCP	Nœud-portée Telnet
HTTPS	8443/TCP	Outil 7MTT avec interface graphique via lien:HTTPS
RSH	8514/TCP	Portée du nœud RSH
KMIP	9877/TCP	Port client KMIP (hôte local interne uniquement)
ndmp	10000/TCP	NDMP
cifs port de témoin	40001/TCP	Port témoin CIFS
TLS	50000/TCP	Sécurité de la couche de transport

Service	Port/Protocole	Description
`Iscsi`	65200/TCP	Port iSCSI
`SSH`	65502/TCP	Coque sécurisée
`vsun`	65503/TCP	vsun

Ports internes NetApp

Port/Protocole	Description
900	RPC de cluster NetApp
902	RPC de cluster NetApp
904	RPC de cluster NetApp
905	RPC de cluster NetApp
910	RPC de cluster NetApp
911	RPC de cluster NetApp
913	RPC de cluster NetApp
914	RPC de cluster NetApp
915	RPC de cluster NetApp
918	RPC de cluster NetApp
920	RPC de cluster NetApp
921	RPC de cluster NetApp
924	RPC de cluster NetApp
925	RPC de cluster NetApp
927	RPC de cluster NetApp
928	RPC de cluster NetApp
929	RPC de cluster NetApp
931	RPC de cluster NetApp
932	RPC de cluster NetApp
933	RPC de cluster NetApp
934	RPC de cluster NetApp
935	RPC de cluster NetApp
936	RPC de cluster NetApp
937	RPC de cluster NetApp
939	RPC de cluster NetApp
940	RPC de cluster NetApp
951	RPC de cluster NetApp

Port/Protocole	Description
954	RPC de cluster NetApp
955	RPC de cluster NetApp
956	RPC de cluster NetApp
958	RPC de cluster NetApp
961	RPC de cluster NetApp
963	RPC de cluster NetApp
964	RPC de cluster NetApp
966	RPC de cluster NetApp
967	RPC de cluster NetApp
7810	RPC de cluster NetApp
7811	RPC de cluster NetApp
7812	RPC de cluster NetApp
7813	RPC de cluster NetApp
7814	RPC de cluster NetApp
7815	RPC de cluster NetApp
7816	RPC de cluster NetApp
7817	RPC de cluster NetApp
7818	RPC de cluster NetApp
7819	RPC de cluster NetApp
7820	RPC de cluster NetApp
7821	RPC de cluster NetApp
7822	RPC de cluster NetApp
7823	RPC de cluster NetApp
7824	RPC de cluster NetApp

Rapports techniques sur ONTAP SnapCenter

SnapCenter fournit une plateforme unifiée qui assure la cohérence de la protection des données et de la gestion des clones au niveau des applications. SnapCenter simplifie la sauvegarde, la restauration et la gestion du cycle de vie des clones avec des workflows intégrés aux applications. En outre, grâce à la gestion des données de stockage, SnapCenter améliore la performance et la disponibilité, tout en réduisant le temps consacré au développement et aux tests.

Ces rapports techniques sont détaillés dans "SnapCenter"la documentation produit.

SnapCenter pour Oracle

"Tr-4700 : plug-in SnapCenter pour les meilleures pratiques relatives aux bases de données Oracle"
NetApp SnapCenter est une plateforme unifiée et évolutive de protection des données cohérente avec Oracle qui automatise les opérations complexes grâce à un contrôle et une surveillance centralisés. Découvrez les pratiques recommandées pour le déploiement de bases de données Oracle avec SnapCenter.

"Tr-4964 : sauvegarde, restauration et clonage des bases de données Oracle avec les services SnapCenter"
Découvrez comment configurer les services SnapCenter pour sauvegarder, restaurer et cloner les bases de données Oracle déployées dans Amazon FSX pour le stockage ONTAP et les instances de calcul EC2. Bien qu'il soit beaucoup plus facile à configurer et à utiliser, les services SnapCenter fournissent des fonctionnalités clés via l'interface SnapCenter.

SnapCenter pour Microsoft SQL Server

"Tr-4714 : meilleures pratiques pour Microsoft SQL Server avec NetApp SnapCenter"
Découvrez comment déployer avec succès Microsoft SQL Server sur un système de stockage NetApp à l'aide de SnapCenter pour la protection des données.

SnapCenter pour Microsoft Exchange Server

"Tr-4681 : meilleures pratiques pour Microsoft Exchange Server utilisant NetApp SnapCenter"
Découvrez comment déployer Microsoft Exchange Server sur un système de stockage NetApp à l'aide de SnapCenter pour la protection des données.

SnapCenter pour SAP HANA

"Tr-4614 : sauvegarde et restauration SAP HANA avec SnapCenter" SnapCenter est une plateforme unifiée et évolutive de protection des données cohérente au niveau des applications pour SAP HANA et d'autres bases de données. SnapCenter offre un contrôle et une surveillance centralisés, tout en déléguant aux utilisateurs la possibilité de gérer les tâches de sauvegarde, de restauration et de clonage spécifiques aux applications. Avec SnapCenter, les administrateurs de bases de données et de stockage apprennent à utiliser un seul outil pour gérer les opérations de sauvegarde, de restauration et de clonage des différentes applications et bases de données.

"Tr-4926 : SAP HANA sur Amazon FSX pour NetApp ONTAP - sauvegarde et restauration avec SnapCenter"
Découvrez les pratiques recommandées pour la protection des données SAP HANA dans Amazon FSX pour NetApp ONTAP et SnapCenter. Il aborde les concepts SnapCenter, les recommandations relatives à la

configuration et les flux de production des opérations, notamment les opérations de configuration et de sauvegarde, pour les opérations de restauration et de reprise.

"Tr-4667 : automatisation des opérations de copie et de clonage du système SAP HANA avec SnapCenter" Le clonage du stockage SnapCenter et la possibilité de définir de manière flexible des opérations de préclonage et de post-clonage permettent aux administrateurs de base SAP d'accélérer et d'automatiser les opérations de copie, de clonage ou d'actualisation du système SAP. Découvrez maintenant la possibilité de choisir une sauvegarde Snapshot SnapCenter sur un système de stockage primaire ou secondaire vous permet de répondre à vos utilisations les plus importantes, notamment la corruption logique, les tests de reprise d'activité ou la mise à jour d'un système d'assurance qualité SAP.

"Tr-4719 : réplication du système SAP HANA, sauvegarde et restauration avec SnapCenter"
Découvrez comment la technologie SnapCenter et le plug-in SAP HANA peuvent être utilisés pour la sauvegarde et la restauration dans un environnement de réplication système SAP HANA.

"Tr-4667 : automatisation des opérations de copie et de clonage du système SAP HANA avec SnapCenter" La possibilité de créer des sauvegardes Snapshot NetApp cohérentes au niveau des applications sur la couche de stockage constitue la base des opérations de copie du système et de clonage du système. Les sauvegardes Snapshot basées sur le stockage sont créées à l'aide du plug-in NetApp SnapCenter pour SAP HANA et des interfaces fournies par la base de données SAP HANA. SnapCenter enregistre les sauvegardes Snapshot dans le catalogue de sauvegardes SAP HANA afin que les sauvegardes puissent être utilisées pour la restauration et la restauration, ainsi que pour les opérations de clonage.

Guide de renforcement SnapCenter

"Tr-4957 : guide sur le renforcement de la sécurité pour NetApp SnapCenter"
Découvrez comment configurer SnapCenter pour aider les entreprises à atteindre les objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité des systèmes d'information.

Rapports techniques sur le Tiering ONTAP

Grâce à la solution de Tiering des données FabricPool, l'expérience utilisateur globale des systèmes Flash est améliorée et l'architecture des applications n'est plus nécessaire pour optimiser l'efficacité du stockage. FabricPool réduit l'empreinte du stockage et les coûts associés à l'environnement d'un système. Les données actives restent sur les disques SSD haute performance. Les données inactives sont envoyées vers un stockage objet à faible coût tout en préservant les fonctionnalités d'efficacité du stockage.

Ces rapports techniques sont détaillés dans "ONTAP FabricPool"la documentation produit.

"Tr-4598 : meilleures pratiques de FabricPool"
Découvrez les fonctionnalités, les exigences, l'implémentation et les pratiques recommandées pour FabricPool.

"Tr-4826 : guide de recommandations NetApp FabricPool avec StorageGRID"
Découvrez les pratiques recommandées pour le déploiement et le dimensionnement de StorageGRID en tant que niveau de capacité pour le composant ONTAP FabricPool. Ce document présente également les principales fonctionnalités, les exigences, l'implémentation et les pratiques recommandées lors de l'utilisation de StorageGRID.

"Tr-4695 : hiérarchisation du stockage de base de données avec NetApp FabricPool"
Découvrez les avantages et les options de configuration de FabricPool avec diverses bases de données, notamment le système de gestion de bases de données relationnelles (SGBDR) d'Oracle.

Rapports techniques sur la virtualisation ONTAP

Les solutions de virtualisation NetApp vous aident à tirer le meilleur parti de vos serveurs. Grâce à une infrastructure de serveur virtuel réactive basée sur des systèmes Flash ONTAP haute performance révolutionnaires, vous pouvez accéder à vos données plus rapidement. Votre infrastructure virtuelle granulaire évolue sans interruption sur plusieurs pétaoctets de données et apporte les performances dont vous avez besoin pour faciliter l'accès partagé à plusieurs workloads. ONTAP vous aide à rationaliser et à réduire la complexité de votre déploiement d'infrastructure de serveurs virtuels grâce à des partenariats clés, des conseils de déploiement, une intégration d'applications et une conception supérieure. ONTAP fournit de nombreuses pratiques et solutions recommandées pour créer un environnement de virtualisation robuste à la fois sur site et dans le cloud.

Ces rapports techniques sont détaillés dans "Les outils ONTAP pour VMware vSphere"la documentation produit.

"Tr-4597 : VMware vSphere pour ONTAP" ONTAP est une solution de stockage leader pour les environnements VMware vSphere depuis près de vingt ans et continue d'ajouter des fonctionnalités innovantes pour simplifier la gestion tout en réduisant les coûts. Ce document présente la solution ONTAP pour vSphere, notamment les dernières informations sur les produits et les pratiques recommandées, afin de rationaliser le déploiement, de réduire les risques et de simplifier la gestion.

"Tr-4400 : volumes virtuels VMware vSphere (vVols) avec NetApp ONTAP" ONTAP est une solution de stockage leader pour les environnements VMware vSphere depuis plus de vingt ans et continue d'ajouter des fonctionnalités innovantes pour simplifier la gestion tout en réduisant les coûts. Ce document présente les fonctionnalités de ONTAP pour les volumes virtuels VMware vSphere (vVols), notamment les dernières informations sur les produits et les cas d'utilisation, ainsi que les pratiques recommandées et d'autres informations permettant de rationaliser le déploiement et de réduire les erreurs.

"Tr-4900 : VMware site Recovery Manager avec NetApp ONTAP" Depuis son introduction dans le data Center moderne en 2002, ONTAP est une solution de stockage leader pour les environnements VMware vSphere. De plus, il continue d'ajouter des fonctionnalités innovantes pour simplifier la gestion tout en réduisant les coûts. Ce document présente la solution ONTAP pour VMware site Recovery Manager (SRM), le logiciel de reprise après incident de pointe de VMware, qui inclut les dernières informations produit et les pratiques recommandées pour rationaliser le déploiement, réduire les risques et simplifier la gestion au quotidien.

"Introduction à l'automatisation pour ONTAP et vSphere" Depuis les premiers jours de VMware ESX, l'automatisation fait partie intégrante de la gestion des environnements VMware. La possibilité de déployer une infrastructure en tant que code et d'étendre les pratiques aux opérations de cloud privé permet de réduire les problèmes liés à l'évolutivité, à la flexibilité, au provisionnement automatique et à l'efficacité. Ce document présente la solution ONTAP pour l'automatisation de l'environnement ONTAP et VMware vSphere.

"WP-7353 : outils ONTAP pour VMware vSphere - sécurité des produits" Ce document décrit les techniques et la technologie utilisées pour sécuriser les outils ONTAP pour VMware vSphere 9.X contre les menaces existantes et émergentes dans les environnements produits.

"WP-7355 : plug-in SnapCenter VMware vSphere : sécurité des produits" Ce document décrit les techniques et la technologie utilisées pour sécuriser le plug-in NetApp SnapCenter pour VMware vSphere 4.X contre les menaces existantes et émergentes dans les environnements produits.

"Tr-4568 : instructions de déploiement de NetApp et meilleures pratiques de stockage pour Windows Server"

Microsoft Windows Server est un système d’exploitation professionnel qui couvre la mise en réseau, la sécurité, la virtualisation, le cloud, l’infrastructure de postes de travail virtuels, la protection des accès, la protection des informations, les services Web, l’infrastructure de plate-forme d’application, etc. Ce document est axé sur Microsoft Windows, en mettant particulièrement l’accent sur la technologie de virtualisation Hyper-V, y compris les dernières informations sur les produits et les pratiques recommandées, afin de rationaliser le déploiement, de réduire les risques et de simplifier la gestion.

Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d'auteur

"https://www.netapp.com/company/legal/copyright/"

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l'adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

Source ouverte

Les fichiers de notification fournissent des informations sur les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp.

ONTAP

"Avis pour ONTAP 9.16.1" "Avis pour ONTAP 9.16.0" "Avis pour ONTAP 9.15.1" "Avis pour ONTAP 9.15.0" "Avis pour ONTAP 9.14.1" "Avis pour ONTAP 9.14.0" "Avis pour ONTAP 9.13.1" "Notification relative à ONTAP 9.12.1" "Notification relative à ONTAP 9.12.0" "Notification relative à ONTAP 9.11.1" "Notification relative à ONTAP 9.10.1" "Avis pour ONTAP 9.10.0" "Notification relative à ONTAP 9.9.1" "Notification relative à ONTAP 9.8" "Avis pour ONTAP 9.7" "Avis pour ONTAP 9.6" "Avis pour ONTAP 9.5" "Avis pour ONTAP 9.4" "Avis pour ONTAP 9.3" "Avis pour ONTAP 9.2" "Avis pour ONTAP 9.1"

ONTAP Mediator pour les configurations IP MetroCluster

"9.9.1 Avis concernant le médiateur ONTAP pour les configurations IP MetroCluster" "9.8 Avis concernant le médiateur ONTAP pour les configurations IP MetroCluster" "9.7 Avis concernant le médiateur ONTAP pour les configurations IP MetroCluster"

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.