Documentation sur les outils ONTAP pour VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
February 20, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/ontap-tools-vmware-vsphere-10/index.html on February 20, 2026. Always check docs.netapp.com for the latest.

Sommaire

Documentation sur les outils ONTAP pour VMware vSphere . . . 1
Notes de mise à jour . . . 2
Notes de version pour ONTAP tools . . . 2
Nouveautés des ONTAP tools for VMware vSphere 10.5 . . . 2
Plateformes ONTAP et versions de vCenter Server prises en charge . . . 3
Comparaison des fonctionnalités des ONTAP tools for VMware vSphere 9 et 10 . . . 3
Concepts . . . 5
Découvrez les outils ONTAP . . . 5
Concepts et termes clés dans ONTAP tools . . . 5
Contrôle d’accès basé sur les rôles (RBAC) . . . 8
En savoir plus sur le RBAC des outils ONTAP . . . 8
RBAC avec VMware vSphere . . . 10
RBAC avec ONTAP . . . 17
Déployez les outils ONTAP pour VMware vSphere . . . 21
Démarrage rapide des outils ONTAP pour VMware vSphere . . . 21
Flux de travail de déploiement à haute disponibilité pour ONTAP tools . . . 23
Exigences et limites de configuration des outils ONTAP pour VMware vSphere . . . 23
Configuration minimale requise . . . 24
Exigences minimales en matière de stockage et d’applications . . . 24
Configuration requise pour les ports . . . 25
Limites de configuration pour déployer ONTAP tools for VMware vSphere pour les datastores vVols . . . 27
Limites de configuration pour le déploiement des ONTAP tools for VMware vSphere pour les datastores VMFS et NFS . . . 28
Outils ONTAP pour VMware vSphere - Storage Replication adapter (SRA) . . . 28
Exigences préalables au déploiement des ONTAP tools . . . 29
Fiche technique de déploiement . . . 30
Configuration du pare-feu réseau . . . 31
Paramètres de stockage ONTAP . . . 31
Déployer les outils ONTAP . . . 31
Dépanner les erreurs de déploiement des outils ONTAP . . . 36
Collectez les fichiers journaux . . . 36
Codes d’erreur de déploiement . . . 37
Configuration des outils ONTAP pour VMware vSphere . . . 40
Ajouter des instances vCenter Server aux outils ONTAP . . . 40
Enregistrez le fournisseur VASA auprès d’une instance de serveur vCenter dans ONTAP tools . . . 41
Installer le plug-in NFS VAAI à l’aide des outils ONTAP . . . 42
Configurer les paramètres de l’hôte ESXi dans ONTAP tools . . . 43
Configurer les paramètres de chemins d’accès multiples et de délai d’attente du serveur ESXi . . . 43
Définissez les valeurs de l’hôte ESXi . . . 43
Configurer les rôles et privilèges des utilisateurs ONTAP pour les outils ONTAP . . . 44
Exigences de mappage des agrégats du SVM . . . 45
Créez manuellement un utilisateur et un rôle ONTAP . . . 46
Mise à niveau des outils ONTAP pour VMware vSphere 10.1 utilisateur vers 10.3 utilisateurs . . . 54

Mise à niveau des outils ONTAP pour VMware vSphere 10.3 utilisateur vers 10.4 utilisateurs . . . 56
Ajouter un système de stockage dorsal aux ONTAP tools . . . 56
Associer un système de stockage principal à une instance de serveur vCenter dans ONTAP tools . . . 59
Configurer l'accès réseau dans ONTAP tools . . . 59
Créer un datastore dans ONTAP tools . . . 60
Protection des datastores et des machines virtuelles . . . 65
Protéger un cluster hôte dans ONTAP tools . . . 65
Protégez à l'aide de la protection SRA . . . 66
Configurez SRA dans ONTAP tools pour protéger les banques de données . . . 66
Configurer SRA dans ONTAP tools for VMware vSphere pour les environnements SAN et NAS . . . 67
Configurer SRA dans ONTAP tools pour les environnements à grande échelle . . . 68
Configurez SRA sur l'appliance VMware Live Site Recovery à l'aide des ONTAP tools. . . . 69
Mettre à jour les informations d'identification SRA dans ONTAP tools . . . 70
Configurer les sites protégés et de récupération dans ONTAP tools . . . 70
Configuration des ressources protégées et du site de reprise . . . 72
Vérifier les systèmes de stockage répliqués dans ONTAP tools . . . 76
Protection contre le fan-out dans ONTAP tools . . . 76
Gérez les outils ONTAP pour VMware vSphere . . . 80
Découvrez le tableau de bord des ONTAP tools . . . 80
Comment les ONTAP tools gèrent les igroups et les politiques d'exportation . . . 81
Export-policies . . . 85
Comment les ONTAP tools gèrent les igroups . . . 86
Découvrez l'interface utilisateur du gestionnaire d'outils ONTAP . . . 89
Gérer les paramètres du gestionnaire d'outils ONTAP . . . 91
Modifier les paramètres AutoSupport des outils ONTAP . . . 91
Ajouter des serveurs NTP aux outils ONTAP . . . 92
Réinitialiser les informations d'identification du VASA Provider et du SRA dans ONTAP tools . . . 93
Modifier les paramètres de sauvegarde des outils ONTAP . . . 93
Activer les services ONTAP tools . . . 93
Modifier les paramètres de l'appliance ONTAP tools . . . 94
Ajouter des hôtes VMware vSphere aux outils ONTAP . . . 95
Gérer les datastores . . . 96
Monter les datastores NFS et VMFS dans ONTAP tools . . . 96
Démontez les datastores NFS et VMFS dans ONTAP tools . . . 96
Monter un datastore vVols dans ONTAP tools . . . 97
Redimensionner les datastores NFS et VMFS dans ONTAP tools . . . 97
Développez les datastores vVols dans les outils ONTAP . . . 98
Réduire la taille d'un vVols datastore dans ONTAP tools . . . 98
Supprimer les banques de données dans ONTAP tools . . . 99
Vues de stockage ONTAP pour les banques de données dans ONTAP tools . . . 100
Vue du stockage des machines virtuelles dans ONTAP tools . . . 100
Gérer les seuils de stockage dans ONTAP tools . . . 101
Gérer les backends de stockage dans ONTAP tools . . . 101
Découverte du stockage . . . 101
Modification des systèmes back-end de stockage . . . 102

Suppression des systèmes back-end . . . 102
Vue détaillée du système back-end de stockage . . . 103
Gérer les instances vCenter Server dans les outils ONTAP . . . 103
Dissociez les systèmes back-end de stockage de l'instance vCenter Server . . . 103
Modifier une instance de vCenter Server . . . 104
Supprimer une instance de vCenter Server . . . 104
Renouveler le certificat du serveur vCenter . . . 105
Gérer les certificats des outils ONTAP . . . 107
Accès aux outils ONTAP pour la console de maintenance VMware vSphere . . . 109
Découvrez la console de maintenance des ONTAP tools . . . 109
Configurer l'accès de diagnostic à distance pour ONTAP tools . . . 110
Démarrer SSH sur les autres nœuds ONTAP tools . . . 111
Mettre à jour les informations d'identification du serveur vCenter dans ONTAP tools . . . 111
Modifier l'indicateur de validation du certificat dans ONTAP tools . . . 111
Rapports sur les outils ONTAP . . . 112
Gérer des machines virtuelles . . . 112
Considérations relatives à la migration et au clonage de machines virtuelles pour ONTAP tools . . . 112
Migrer des machines virtuelles vers des datastores vVols dans ONTAP tools . . . 113
Nettoyer les configurations VASA dans ONTAP tools . . . 114
Attacher ou détacher un disque de données d'une machine virtuelle dans ONTAP tools . . . 114
Découvrez les systèmes de stockage et les hôtes dans ONTAP tools . . . 115
Modifiez les paramètres de l'hôte VMware ESXi à l'aide des outils ONTAP . . . 116
Gérer les mots de passe . . . 117
Modifier le mot de passe du gestionnaire d'outils ONTAP . . . 117
Réinitialisez le mot de passe du gestionnaire d'outils ONTAP . . . 117
Réinitialiser le mot de passe utilisateur de l'application dans ONTAP tools . . . 117
Réinitialiser le mot de passe de la console de maintenance des ONTAP tools . . . 118
Gestion de la protection des clusters hôtes . . . 119
Modifier un cluster d'hôtes protégé dans ONTAP tools . . . 119
Supprimer la protection du cluster hôte dans ONTAP tools . . . 122
Récupérer la configuration des outils ONTAP . . . 123
Désinstaller les outils ONTAP . . . 124
Supprimez les volumes FlexVol après la désinstallation des ONTAP tools . . . 125
Mettez à niveau les outils ONTAP pour VMware vSphere . . . 126
Mise à niveau des ONTAP tools for VMware vSphere 10.x vers 10.5 . . . 126
Codes d'erreur de mise à niveau des ONTAP tools . . . 128
Migrer les ONTAP tools for VMware vSphere 9.xx vers 10.5 . . . 132
Migrer des ONTAP tools for VMware vSphere 9.xx vers 10.5 . . . 132
Migrez le fournisseur VASA et mettez à jour le SRA dans ONTAP tools . . . 132
Étapes pour migrer le fournisseur VASA . . . 132
Étapes pour mettre à jour l'adaptateur de réplication de stockage (SRA) . . . 137
Automatisation à l'aide de l'API REST . . . 139
Découvrez l'API REST des ONTAP tools . . . 139
Base de services Web REST . . . 139
Environnement ONTAP Tools Manager . . . 139

Détails d'implémentation de l'API REST des ONTAP tools . . . 140
Comment accéder à l'API REST . . . 140
Détails d'HTTP . . . 141
Authentification . . . 142
Demandes synchrones et asynchrones . . . 142
Effectuez votre premier appel API REST avec les ONTAP tools . . . 142
Avant de commencer . . . 143
Étape 1 : acquérir un jeton d'accès . . . 143
Étape 2 : lancez l'appel de l'API REST . . . 144
Référence de l'API REST des ONTAP tools . . . 144
Mentions légales . . . 145
Droits d'auteur . . . 145
Marques déposées . . . 145
Brevets . . . 145
Politique de confidentialité . . . 145
Source ouverte . . . 145

Documentation sur les outils ONTAP pour VMware vSphere

Notes de mise à jour

Notes de version pour ONTAP tools

Découvrez les fonctionnalités nouvelles et améliorées disponibles dans les ONTAP tools for VMware vSphere 10.5.

Pour une liste complète des nouvelles fonctionnalités et améliorations, reportez-vous àNouveautés des ONTAP tools for VMware vSphere 10.5 .

Pour obtenir les informations de compatibilité les plus récentes, reportez-vous à "Matrice d'interopérabilité NetApp" .

La migration est prise en charge à partir des ONTAP tools for VMware vSphere 9.12D1, 9.13D2 et 9.13P2 vers les ONTAP tools for VMware vSphere 10.5.

Pour plus d'informations, reportez-vous à la "Notes de publication des ONTAP tools for VMware vSphere 10.5" . Vous devez vous connecter avec votre compte NetApp ou créer un compte pour accéder aux notes de publication.

Nouveautés des ONTAP tools for VMware vSphere 10.5

Découvrez les nouvelles fonctionnalités disponibles dans les ONTAP tools for VMware vSphere 10.5.

- **Qualification de la plateforme**

Les ONTAP tools for VMware vSphere 10.5 ajoutent la prise en charge des systèmes ASA r2, offrant une compatibilité avec les dernières configurations matérielles et logicielles. Cette version inclut également l'intégration avec ONTAP 9.16.1 et 9.17.1, élargissant ainsi les environnements pris en charge.

- **Qualification et certifications VMware**

Les ONTAP tools for VMware vSphere 10.5 sont conformes aux normes de certification d'interopérabilité VMware actuelles, prenant en charge à la fois l'hôte ESXi et vCenter Server.

- * Prise en charge de MetroCluster *

Cette version introduit la prise en charge des configurations MetroCluster , améliorant ainsi les capacités de haute disponibilité et de reprise après sinistre.

- **Gestion de la sécurité et des certificats**

Cette version introduit une gestion simplifiée des certificats auto-signés, améliorant à la fois l'expérience utilisateur et le respect des normes de sécurité. Il fournit des flux de travail de validation de certificat améliorés pour sécuriser les outils ONTAP et ONTAP tools for VMware vSphere .

- **Améliorations de la réplication**

Cette version prend en charge la réplication VMFS avec un groupe de cohérence hiérarchique incluant SRA et SnapMirror Active Sync dans les systèmes ASA r2. Il prend en charge les sauvegardes RPO zéro pour améliorer la protection et la récupération des données.

- **Mise à niveau et migration**

Le processus de mise à niveau et de migration des versions précédentes des ONTAP tools for VMware vSphere vers les ONTAP tools for VMware vSphere 10.5 est conçu pour être transparent et efficace, minimisant les temps d'arrêt et garantissant une transition en douceur.

Plateformes ONTAP et versions de vCenter Server prises en charge

ONTAP tools for VMware vSphere 10.5 P1 prend en charge les configurations de haute disponibilité (HA) de vCenter pour les composants SRA et SnapMirror active sync. vVols n'est pas pris en charge dans cette configuration. Lors d'un basculement HA, vCenter peut être indisponible pendant plusieurs minutes. Dans les grands environnements ou en cas d'erreur, la durée du basculement peut dépasser 15 minutes.

Pour plus d'informations, consultez le "Documentation de haute disponibilité vCenter". Pour des questions concernant vCenter HA, contactez "Support Broadcom".

Pour les derniers détails sur la compatibilité des versions, reportez-vous à "Matrice d'interopérabilité NetApp" .

Comparaison des fonctionnalités des ONTAP tools for VMware vSphere 9 et 10

Découvrez si la migration des ONTAP tools for VMware vSphere 9 vers les ONTAP tools for VMware vSphere 10.2 ou versions ultérieures vous convient.

Pour obtenir les informations de compatibilité les plus récentes, reportez-vous à "Matrice d'interopérabilité NetApp" .

Fonctionnalité	Outils ONTAP 9.13	Outils ONTAP 10.2 et versions ultérieures
Proposition de valeur clé	Rationalisez et simplifiez les opérations du jour 0 au jour 2 grâce à des capacités de sécurité, de conformité et d'automatisation améliorées	Prise en charge étendue pour inclure FC pour VMFS et NVMe-oF pour VMFS uniquement. Facilité d'utilisation pour NetApp SnapMirror, configuration simple pour les clusters de stockage métropolitains vSphere et prise en charge de VMware Live Site Recovery sur trois sites
Qualification de la version ONTAP	ONTAP 9.9.1 à ONTAP 9.16.1	ONTAP 9.12.1 à 9.15.1 pour ONTAP tools 10.2. ONTAP 9.14.1, 9.15.1, 9.16.0 et 9.16.1 pour ONTAP tools 10.3. ONTAP 9.14.1, 9.15.1, 9.16.0 et 9.16.1 pour ONTAP tools 10.4. ONTAP 9.16.1P3 et versions ultérieures sont requis pour ONTAP tools 10.4 lors de l'utilisation de systèmes ASA r2. ONTAP 9.15.1, 9.16.1 et 9.17.0 pour ONTAP tools 10.5

Fonctionnalité	Outils ONTAP 9.13	Outils ONTAP 10.2 et versions ultérieures
Prise en charge des versions VMware	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.5 vers VMware Live Site Recovery 9.0	vSphere 7.x-8.x vSphere 9.0 à partir d' ONTAP tools 10.5 VMware Site Recovery Manager (SRM) 8.7 à VMware Live Site Recovery 9.0 **REMARQUE :** Dans ONTAP tools 10.x, SRM prend en charge les sites partagés, permettant une évolutivité accrue et des performances améliorées.
Prise en charge du protocole	Magasins de données NFS et VMFS : NFS (v3 et v4.1), VMFS (iSCSI et FCP)	Magasins de données NFS et VMFS : NFS (v3 et v4.1), VMFS (iSCSI/FCP/NVMe-oF)
Évolutivité	Hôtes et machines virtuelles : 300 hôtes, jusqu'à 10 000 machines virtuelles. Banques de données : 600 NFS, jusqu'à 50 VMFS.	Hôtes et machines virtuelles : 600 hôtes
Observabilité	Tableaux de bord des performances, de la capacité et de la conformité de l'hôte Rapports dynamiques sur les machines virtuelles et les banques de données	Tableaux de bord mis à jour sur les performances, la capacité et la conformité de l'hôte Rapports dynamiques sur les machines virtuelles et les banques de données
Protection des données	Réplication SRA pour VMFS et NFS. Intégration SCV et interopérabilité pour la sauvegarde.	Réplication SRA pour les banques de données iSCSI VMFS et NFS v3, protection sur trois sites combinant SMAS et VMware Live Site Recovery. Prise en charge SRA pour FCP avec VMFS.
Assistance aux fournisseurs VASA	VASA 4,0	VASA 3,0

Concepts

Découvrez les outils ONTAP

Les ONTAP tools for VMware vSphere sont un ensemble d'outils pour la gestion du cycle de vie des machines virtuelles. Il s'intègre à l'écosystème VMware pour simplifier le provisionnement des banques de données et fournir une protection de base aux machines virtuelles. Il s'agit d'un ensemble de microservices évolutifs horizontalement et pilotés par événements, déployés en tant qu'appliance virtuelle ouverte (OVA).

Les ONTAP tools for VMware vSphere prennent en charge :

- Fonctionnalités principales des machines virtuelles (VM) telles que la protection et la reprise après sinistre
- Fournisseur VASA pour la gestion basée sur les politiques de stockage
- Gestion du stockage basée sur des règles
- Storage Replication adapter (SRA)

Haute disponibilité des outils ONTAP pour VMware

Les ONTAP tools for VMware vSphere offrent une prise en charge de haute disponibilité (HA) pour aider à maintenir un fonctionnement ininterrompu en cas de panne.

La solution HA vous aide à récupérer rapidement des types de pannes suivants :

- Panne de l'hôte : seule une panne d'un seul nœud est prise en charge.
- Défaillance du réseau
- Panne de la machine virtuelle (système d'exploitation invité)
- Échec de l'application (outils ONTAP)

Vous n'avez pas besoin d'effectuer de configuration supplémentaire pour activer les ONTAP tools for VMware vSphere.

Les ONTAP tools for VMware vSphere ne prennent pas en charge vCenter HA.

Pour utiliser la fonctionnalité HA, assurez-vous que l'ajout à chaud du processeur et le branchement à chaud de la mémoire sont activés pendant le déploiement ou ultérieurement dans les paramètres de la machine virtuelle.

Concepts et termes clés dans ONTAP tools

La section suivante décrit les principaux concepts et termes utilisés dans le document.

Autorité de certification (CA)

CA est une entité de confiance qui émet des certificats SSL (Secure Sockets Layer).

Groupe de cohérence

Un groupe de cohérence est un ensemble de volumes gérés comme une seule unité. Les groupes de cohérence sont synchronisés pour assurer la cohérence des données entre les unités de stockage et les volumes. Dans ONTAP, ils offrent une gestion facile et une garantie de protection pour une charge de travail applicative couvrant plusieurs volumes. En savoir plus sur "groupes de cohérence" .

Double pile

Un réseau à double pile est un environnement réseau qui prend en charge l'utilisation simultanée des adresses IPv4 et IPv6.

Haute disponibilité (HA)

Les nœuds de cluster sont configurés en paires haute disponibilité pour assurer la continuité de l'activité.

Numéro d'unité logique (LUN)

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

Espace de noms et sous-système NVMe

Un namespace NVMe est une quantité de mémoire non volatile pouvant être formatée dans des blocs logiques. Les espaces de noms sont l'équivalent de LUN pour les protocoles FC et iSCSI, et un sous-système NVMe est similaire à un groupe initiateur. Un sous-système NVMe peut être associé à des initiateurs pour que les initiateurs associés puissent accéder aux espaces de noms dans le sous-système.

Gestionnaire d'outils ONTAP

ONTAP Tools Manager offre davantage de contrôle aux outils ONTAP pour les administrateurs VMware vSphere sur les instances vCenter Server gérées et les systèmes back-end de stockage intégrés. Il facilite la gestion des instances vCenter Server, des systèmes back-end de stockage, des certificats, des mots de passe et des téléchargements de bundles de journaux.

Appliance virtuelle ouverte (OVA)

OVA est une norme ouverte pour le packaging et la distribution d'appliances ou de logiciels virtuels devant être exécutés sur des machines virtuelles.

Objectif de point de récupération

Le RPO mesure la fréquence de sauvegarde ou de réplication des données. Il précise le moment exact où vous devez restaurer les données après une panne pour reprendre l'activité. Par exemple, si une entreprise a un objectif de point de récupération de 4 heures, elle peut tolérer la perte de 4 heures de données en cas d'incident.

Synchronisation active SnapMirror

La synchronisation active SnapMirror assure la continuité des services, même en cas de défaillance complète d'un site. Les applications peuvent ainsi basculer en toute transparence grâce à une copie secondaire. Il n'est pas nécessaire d'intervenir manuellement ou de créer des scripts personnalisés pour déclencher un basculement avec la synchronisation active SnapMirror. En savoir plus sur "Synchronisation active

SnapMirror".

Systèmes back-end

Les systèmes back-end de stockage constituent l'infrastructure de stockage sous-jacente utilisée par l'hôte ESXi pour stocker les fichiers, données et autres ressources des machines virtuelles. Ils permettent à l'hôte ESXi d'accéder aux données persistantes et de les gérer, offrant ainsi les capacités de stockage et les performances requises pour un environnement virtualisé.

Cluster global (back-end de stockage)

Les systèmes back-end de stockage global, disponibles uniquement avec des identifiants de cluster ONTAP, sont intégrés via l'interface ONTAP Tools Manager. Ils peuvent être ajoutés avec un Privileges minimal pour permettre la découverte des ressources de cluster essentielles nécessaires à la gestion des vVols. Les clusters globaux sont parfaits pour les scénarios de colocation dans lesquels un utilisateur SVM est ajouté localement pour la gestion des vVols.

Back-end du stockage local

Les systèmes back-end de stockage local dotés d'identifiants de cluster ou SVM sont ajoutés via l'interface utilisateur des outils ONTAP et limités à une instance vCenter. Lors de l'utilisation locale des identifiants de cluster, les SVM associés sont automatiquement mappés avec vCenter pour gérer les vVols ou VMFS. Pour la gestion VMFS, notamment SRA, les outils ONTAP prennent en charge les identifiants SVM sans avoir besoin d'un cluster global.

Storage Replication adapter (SRA)

SRA est le logiciel spécifique au fournisseur de stockage installé dans l'appliance VMware Live site Recovery. L'adaptateur permet la communication entre site Recovery Manager et un contrôleur de stockage au niveau du SVM (Storage Virtual machine) et la configuration au niveau du cluster.

SVM (Storage Virtual machine)

La SVM est l'unité de colocation dans ONTAP. Tout comme une machine virtuelle s'exécutant sur un hyperviseur, SVM est une entité logique qui extrait les ressources physiques. Le SVM contient des volumes de données et une ou plusieurs LIF via lesquelles il transmet des données aux clients.

Configuration uniforme et non uniforme

- **Accès hôte uniforme** signifie que les hôtes de deux sites sont connectés à tous les chemins vers les clusters de stockage sur les deux sites. Les chemins d'accès intersites sont étendus sur plusieurs distances.
- **Accès hôte non uniforme** signifie que les hôtes de chaque site sont connectés uniquement au cluster du même site. Les chemins intersites et les chemins étendus ne sont pas connectés.

> Un accès uniforme à l'hôte est pris en charge pour tout déploiement SnapMirror à synchronisation active. L'accès non uniforme à l'hôte n'est pris en charge que pour les déploiements actif-actif symétriques. En savoir plus sur "Présentation de la synchronisation active SnapMirror dans ONTAP".

VMFS (Virtual machine File System)

VMFS est un système de fichiers en cluster conçu pour stocker des fichiers de machines virtuelles dans des environnements VMware vSphere.

Volumes virtuels (vvols)

Les vVols fournissent une abstraction au niveau du volume pour le stockage utilisé par une machine virtuelle. Il comprend plusieurs avantages et offre une alternative à l'utilisation d'un LUN traditionnel. Une banque de données vVol est généralement associée à un seul LUN qui agit comme conteneur pour les vVols.

Stratégie de stockage de VM

Les stratégies de stockage VM sont créées dans vCenter Server sous stratégies et profils. Pour les vVols, créez un jeu de règles à l'aide de règles provenant du fournisseur de type de stockage NetApp vVols.

Restauration de site en direct VMware

VMware Live site Recovery, anciennement site Recovery Manager (SRM), assure la continuité de l'activité, la reprise après incident, la migration de sites et les fonctionnalités de test sans interruption pour les environnements virtuels VMware.

API VMware vSphere pour la sensibilisation du stockage (VASA)

Vasa est un ensemble d'API qui intègre les baies de stockage à vCenter Server pour la gestion et l'administration. L'architecture repose sur plusieurs composants, notamment le VASA Provider, qui gère les communications entre VMware vSphere et les systèmes de stockage.

API de stockage VMware vSphere - intégration de baies (VAAI)

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

Cluster de stockage vSphere Metro

VSphere Metro Storage Cluster (vMSC) est une architecture qui permet et prend en charge vSphere dans un déploiement de clusters étendus. Les solutions VMSC sont prises en charge avec NetApp MetroCluster et SnapMirror Active Sync (anciennement SMBC). Ces solutions assurent une meilleure continuité de l'activité en cas de défaillance de domaine. Le modèle de résilience est basé sur vos choix de configuration spécifiques. En savoir plus sur "Cluster de stockage VMware vSphere Metro".

Datastore vVols

Le datastore vVols est une représentation logique de datastore d'un conteneur vVols créé et géré par un fournisseur VASA.

RPO nul

RPO désigne l'objectif de point de récupération, la quantité de perte de données jugée acceptable au cours d'une période donnée. La valeur RPO de zéro signifie qu'aucune perte de données n'est acceptable.

Contrôle d'accès basé sur les rôles (RBAC)

En savoir plus sur le RBAC des outils ONTAP

Le contrôle d'accès basé sur des rôles (RBAC) est un framework de sécurité qui permet

de contrôler l'accès aux ressources au sein d'une entreprise. Le contrôle d'accès basé sur des rôles simplifie l'administration en définissant des rôles disposant de niveaux d'autorisation spécifiques pour effectuer des actions, au lieu d'attribuer des autorisations à des utilisateurs individuels. Les rôles définis sont attribués aux utilisateurs, ce qui permet de réduire le risque d'erreur et simplifie la gestion du contrôle d'accès dans l'ensemble de votre organisation.

Le modèle standard RBAC se compose de plusieurs technologies d'implémentation ou phases de plus en plus complexes. Il en résulte que les déploiements RBAC réels, basés sur les besoins des fournisseurs de logiciels et de leurs clients, peuvent différer et aller de relativement simple à très complexe.

Composants RBAC

À un niveau élevé, plusieurs composants sont généralement inclus dans chaque implémentation de RBAC. Ces composants sont liés de différentes manières dans le cadre de la définition des processus d'autorisation.

Privilèges

Un privilège est une action ou une capacité qui peut être autorisée ou refusée. Il peut s'agir d'une action simple, comme la possibilité de lire un fichier, ou d'une opération plus abstraite, spécifique à un système logiciel donné. Des Privileges peuvent également être définis pour restreindre l'accès aux points de terminaison de l'API REST et aux commandes CLI. Chaque implémentation RBAC inclut des privilèges prédéfinis et peut également permettre aux administrateurs de créer des privilèges personnalisés.

Rôles

Un *role* est un conteneur qui inclut un ou plusieurs Privileges. Les rôles sont généralement définis en fonction de tâches ou de fonctions particulières. Lorsqu'un rôle est attribué à un utilisateur, tous les Privileges contenus dans le rôle lui sont attribués. Comme avec Privileges, les implémentations incluent des rôles prédéfinis et permettent généralement de créer des rôles personnalisés.

Objets

Un *objet* représente une ressource réelle ou abstraite identifiée dans l'environnement RBAC. Les actions définies via la Privileges sont effectuées sur ou avec les objets associés. Selon l'implémentation, Privileges peut être accordé à un type d'objet ou à une instance d'objet spécifique.

Utilisateurs et groupes

Users sont affectés ou associés à un rôle appliqué après l'authentification. Certaines implémentations RBAC ne permettent d'attribuer qu'un seul rôle à un utilisateur, tandis que d'autres autorisent plusieurs rôles par utilisateur, peut-être avec un seul rôle actif à la fois. L'attribution de rôles à des *groupes* peut simplifier davantage l'administration de la sécurité.

Autorisations

Une *permission* est une définition qui lie un utilisateur ou un groupe avec un rôle à un objet. Les autorisations peuvent être utiles avec un modèle d'objet hiérarchique dans lequel elles peuvent éventuellement être héritées par les enfants de la hiérarchie.

Deux environnements RBAC

Il existe deux environnements RBAC distincts à prendre en compte lors de l'utilisation des ONTAP tools for VMware vSphere 10. Les ONTAP tools for VMware vSphere 10 nécessitent des privilèges spécifiques dans vCenter et ONTAP pour fonctionner. Bien que les outils ONTAP automatisent les tâches de gestion du stockage, ils ne créent pas de comptes d'utilisateurs ni dans vCenter ni dans ONTAP. Les comptes de service doivent être créés par un administrateur vSphere selon les besoins. Cette documentation fournit aux

administrateurs des instructions pour attribuer les rôles et les autorisations nécessaires à une gestion efficace des outils ONTAP .

Serveur VMware vCenter

L'implémentation RBAC dans VMware vCenter Server permet de restreindre l'accès aux objets exposés via l'interface utilisateur du client vSphere. Dans le cadre de l'installation des outils ONTAP pour VMware vSphere 10, l'environnement RBAC est étendu pour inclure des objets supplémentaires représentant les fonctionnalités des outils ONTAP. L'accès à ces objets est fourni via le plug-in distant. Pour plus d'informations, reportez-vous à la section."Environnement RBAC du serveur vCenter"

Groupe ONTAP

Les outils ONTAP pour VMware vSphere 10 se connectent à un cluster ONTAP via l'API REST ONTAP pour effectuer des opérations de stockage. L'accès aux ressources de stockage est contrôlé via un rôle ONTAP associé à l'utilisateur ONTAP lors de l'authentification. Voir "Environnement ONTAP RBAC" pour plus d'informations.

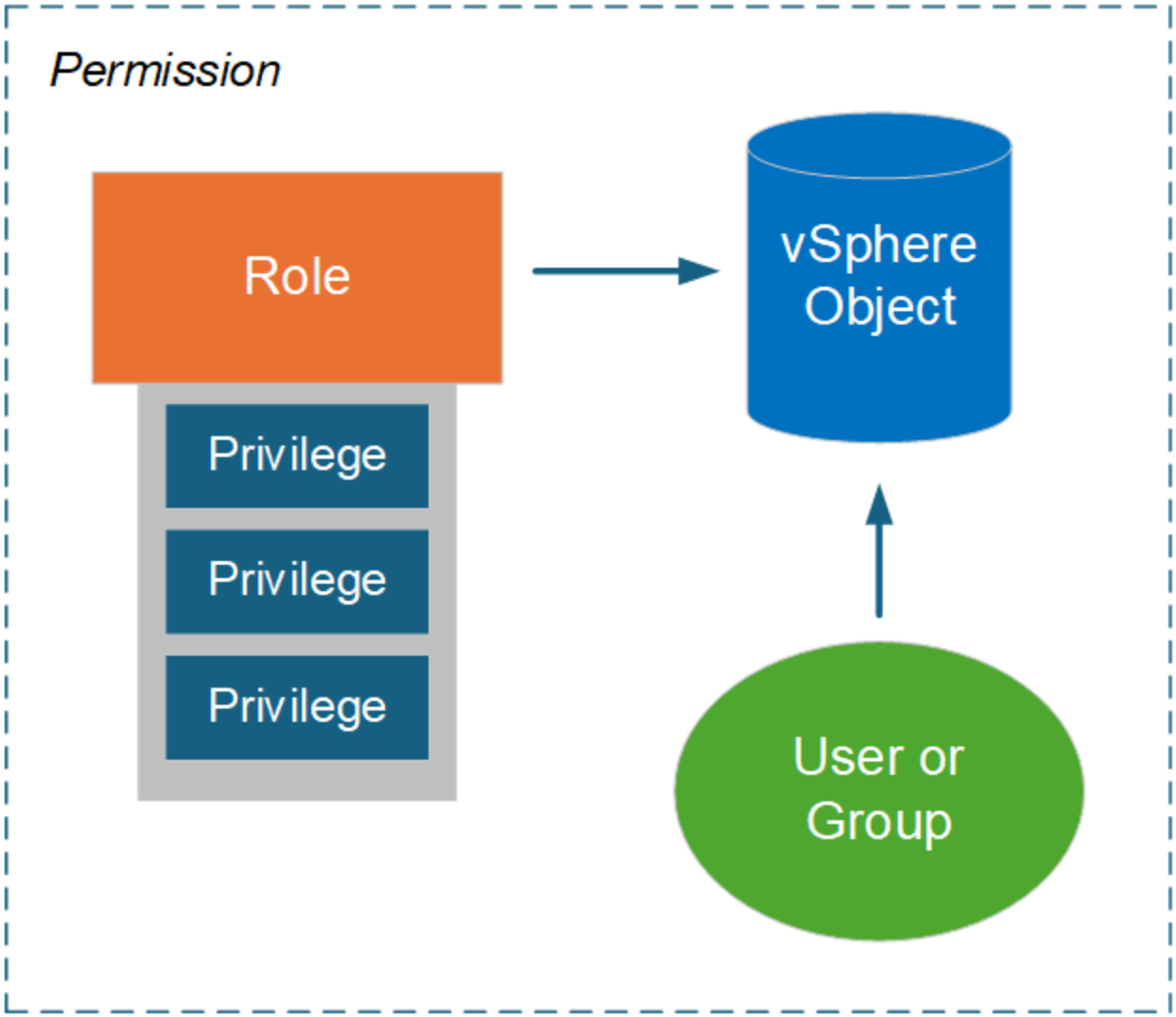
RBAC avec VMware vSphere

Comment le contrôle d'accès basé sur les rôles (RBAC) du serveur vCenter fonctionne avec les outils ONTAP

VMware vCenter Server propose une fonctionnalité RBAC qui vous permet de contrôler l'accès aux objets vSphere. Il s'agit d'une partie importante des services de sécurité d'authentification et d'autorisation centralisés vCenter.

Illustration d'une autorisation vCenter Server

Une autorisation est la base de l'application du contrôle d'accès dans l'environnement vCenter Server. Elle est appliquée à un objet vSphere avec un utilisateur ou un groupe inclus dans la définition des autorisations. Vous trouverez une illustration de haut niveau d'une autorisation vCenter dans la figure ci-dessous.



Composants d'une autorisation vCenter Server

Une autorisation vCenter Server est un ensemble de plusieurs composants qui sont liés ensemble lors de la création de l'autorisation.

Objets vSphere

Les autorisations sont associées aux objets vSphere, tels que vCenter Server, les hôtes ESXi, les machines virtuelles, les datastores, les data centers et les dossiers. En fonction des autorisations attribuées à l'objet, vCenter Server détermine les actions ou les tâches pouvant être effectuées sur l'objet par chaque utilisateur ou groupe. Pour les tâches spécifiques aux outils ONTAP pour VMware vSphere, toutes les autorisations sont attribuées et validées au niveau du dossier racine ou racine du serveur vCenter. Voir "Utilisez RBAC avec le serveur vCenter" pour plus d'informations.

Privileges et rôles

Deux types de vSphere Privileges sont utilisés avec les outils ONTAP pour VMware vSphere 10. Pour simplifier l'utilisation du contrôle d'accès basé sur des rôles dans cet environnement, les outils ONTAP fournissent les rôles contenant le Privileges natif et personnalisé requis. Le Privileges comprend :

- Privilèges de serveur vCenter natif

  Il s'agit du Privileges fourni par vCenter Server.

- Privilèges spécifiques aux outils ONTAP

  Il s'agit d'une solution Privileges personnalisée propre aux outils ONTAP pour VMware vSphere.

Utilisateurs et groupes

Vous pouvez définir des utilisateurs et des groupes via Active Directory ou l'instance locale de vCenter Server. En combinant un rôle, vous pouvez créer une autorisation sur un objet de la hiérarchie d'objets vSphere. L'autorisation accorde l'accès en fonction des privilèges du rôle associé. Notez que les rôles ne sont pas attribués directement aux utilisateurs. Les utilisateurs et les groupes accèdent à un objet via les privilèges de rôle, dans le cadre de l'autorisation globale de vCenter Server.

vCenter Server : considérations RBAC pour les ONTAP tools

Il existe plusieurs aspects des outils ONTAP pour l'implémentation de VMware vSphere 10 RBAC avec vCenter Server que vous devez prendre en compte avant de l'utiliser dans un environnement de production.

Rôles vCenter et compte administrateur

Vous n'avez besoin de définir et d'utiliser les rôles de serveur vCenter personnalisés que si vous souhaitez limiter l'accès aux objets vSphere et aux tâches administratives associées. Si la limitation de l'accès n'est pas nécessaire, vous pouvez utiliser un compte d'administrateur. Chaque compte administrateur est défini avec le rôle Administrateur au niveau supérieur de la hiérarchie des objets. Vous bénéficiez ainsi d'un accès complet aux objets vSphere, y compris ceux ajoutés par les outils ONTAP pour VMware vSphere 10.

Hiérarchie des objets vSphere

L'inventaire des objets vSphere est organisé dans une hiérarchie. Par exemple, vous pouvez déplacer la hiérarchie vers le bas comme suit :

`vCenter Server --> Datacenter --> Cluster --> - Virtual Machine--> ESXi host`

Toutes les autorisations sont validées dans la hiérarchie des objets vSphere, à l'exception des opérations du plug-in VAAI, qui sont validées par rapport à l'hôte ESXi cible.

Rôles inclus avec les outils ONTAP pour VMware vSphere 10

Pour simplifier l'utilisation du RBAC de vCenter Server, les outils ONTAP pour VMware vSphere fournissent des rôles prédéfinis adaptés à diverses tâches d'administration.

> Vous pouvez créer de nouveaux rôles personnalisés si nécessaire. Dans ce cas, vous devez cloner l'un des rôles d'outils ONTAP existants et le modifier si nécessaire. Après avoir modifié la configuration, les utilisateurs du client vSphere concernés doivent se déconnecter et se reconnecter pour activer les modifications.

Pour afficher les ONTAP tools for VMware vSphere , sélectionnez **Menu** en haut du client vSphere, puis cliquez sur **Administration** et enfin sur **Rôles** à gauche. Les privilèges suivants doivent être inclus dans le rôle attribué à l'utilisateur vCenter responsable du déploiement ou de l'intégration de vCenter. Assurez-vous

que ces privilèges sont configurés comme condition préalable au déploiement ou au processus d'intégration.

- Alarmes
  - Accuser réception de l'alarme
- Bibliothèque de contenu
  - Ajouter un élément de bibliothèque
  - Vérifier dans un modèle
  - Consultez un modèle
  - Télécharger les fichiers
  - Stockage d'importation
  - Stockage de lecture
  - Élément de bibliothèque synchroniser
  - Bibliothèque synchronisée par abonnement
  - Afficher les paramètres de configuration
- Datastore
  - Allouer de l'espace
  - Parcourir le magasin de données
  - Opérations de fichiers de bas niveau
  - Supprimer le fichier
  - Mettre à jour les fichiers de la machine virtuelle
  - Mettre à jour les métadonnées de la machine virtuelle
- Gestionnaire d'agents ESX
  - View
- Dossier
  - Créer un dossier
- Hôte
  - Configuration
    - Paramètres avancés
    - Modifier les paramètres
    - Configuration du réseau
    - Ressources système
    - configuration du démarrage automatique de la machine virtuelle
  - Opérations locales
    - Créer une machine virtuelle
    - Supprimer la machine virtuelle
    - Reconfigurer la machine virtuelle
- Réseau
  - Attribuer un réseau

    - Configure
- Gestionnaire Ovf
    - Accès consommateur Ovf
- Profil de l’hôte
    - View
- Ressource
    - Affecter une machine virtuelle au pool de ressources
- Tâche planifiée
    - Créer des tâches
    - Modifier la tâche
    - Exécuter la tâche
- Tâches
    - Créer une tâche
    - Tâche de mise à jour
- vApp
    - Ajouter une machine virtuelle
    - Affecter un pool de ressources
    - Attribuer une vApp
    - Créer
    - Importer
    - Se déplacer
    - Mise hors tension
    - Mise sous tension
    - Récupérer depuis l’URL
    - Afficher l’environnement OVF
- Ordinateur virtuel
    - Modifier la configuration
        - Ajouter un disque existant
        - Ajouter un nouveau disque
        - Ajouter ou supprimer un appareil
        - Configuration avancée
        - Modifier le nombre de cœurs du processeur
        - Changer la mémoire
        - Modifier les paramètres
        - Modifier la ressource
        - Étendre le disque virtuel
        - Modifier les paramètres de l’appareil

        - Retirer le disque
        - Réinitialiser les informations des invités
        - Mise à niveau de la compatibilité des machines virtuelles
    - Modifier l'inventaire
        - Créer à partir d'un existant
        - Créer un nouveau
        - Se déplacer
        - Registre
        - Retirer
        - Désinscription
    - Interaction
        - Opération de sauvegarde sur machine virtuelle
        - Configurer le support CD
        - Configurer le lecteur de disquettes
        - Appareils de connexion
        - Interaction avec la console
        - Gestion du système d'exploitation invité par l'API VIX
        - Mise hors tension
        - Mise sous tension
        - Réinitialiser
        - Suspendre
    - Provisionnement
        - Autoriser l'accès au disque
        - Modèle clone
        - Personnaliser l'expérience invité
        - Modèle de déploiement
        - Modifier les spécifications de personnalisation
        - Lire les spécifications de personnalisation
    - Gestion des instantanés
        - Créer un instantané
        - Supprimer l'instantané
        - Renommer l'instantané
        - Rétablir l'instantané

Il existe trois rôles prédéfinis comme décrit ci-dessous.

Outils NetApp ONTAP pour VMware vSphere Administrator

Fournit tous les outils vCenter Server Privileges natifs et ONTAP spécifiques Privileges requis pour effectuer les tâches d'administration des principaux outils ONTAP pour VMware vSphere.

Outils NetApp ONTAP pour VMware vSphere en lecture seule

Accès en lecture seule aux outils ONTAP. Ces utilisateurs ne peuvent pas exécuter d'actions ONTAP Tools for VMware vSphere contrôlées par accès.

Outils NetApp ONTAP pour le provisionnement VMware vSphere

Fournit certains privilèges vCenter Server natifs et certains privilèges spécifiques aux outils ONTAP requis pour provisionner le stockage. Vous pouvez effectuer les tâches suivantes :

- Créer de nouveaux datastores
- Gérer les datastores

Objets vSphere et systèmes back-end de stockage ONTAP

Les deux environnements RBAC fonctionnent ensemble. Lors de l'exécution d'une tâche dans l'interface client vSphere, les rôles des outils ONTAP définis pour vCenter Server sont vérifiés en premier. Si l'opération est autorisée par vSphere, le Privileges de rôle ONTAP est examiné. Cette deuxième étape est effectuée en fonction du rôle ONTAP attribué à l'utilisateur au moment de la création et de la configuration du back-end de stockage.

Utilisation de vCenter Server RBAC

Vous devez tenir compte de quelques éléments lorsque vous travaillez avec vCenter Server Privileges et les autorisations.

Privilèges requis

Pour accéder à l'interface utilisateur des outils ONTAP pour VMware vSphere 10, vous devez disposer du privilège *View* spécifique aux outils ONTAP. Si vous vous connectez à vSphere sans ce privilège et que vous cliquez sur l'icône NetApp, ONTAP Tools for VMware vSphere affiche un message d'erreur et vous empêche d'accéder à l'interface utilisateur.

Le niveau d'affectation dans la hiérarchie des objets vSphere détermine les parties de l'interface utilisateur auxquelles vous pouvez accéder. L'attribution du privilège d'affichage à l'objet racine vous permet d'accéder aux outils ONTAP pour VMware vSphere en cliquant sur l'icône NetApp.

Vous pouvez à la place attribuer le privilège d'affichage à un autre niveau d'objet vSphere inférieur. Toutefois, cela limite les menus des outils ONTAP pour VMware vSphere auxquels vous pouvez accéder et utiliser.

Attribution d'autorisations

Vous devez utiliser les autorisations vCenter Server si vous souhaitez limiter l'accès aux objets et aux tâches vSphere. Lorsque vous attribuez des autorisations dans la hiérarchie d'objets vSphere, les outils ONTAP pour les tâches VMware vSphere 10 peuvent être utilisés par les utilisateurs.

À moins que vous n'ayez besoin de définir un accès plus restrictif, il est généralement recommandé d'attribuer des autorisations au niveau de l'objet racine ou du dossier racine.

Les autorisations disponibles avec les outils ONTAP pour VMware vSphere 10 s'appliquent aux objets non vSphere personnalisés, tels que les systèmes de stockage. Si possible, vous devez attribuer ces autorisations aux outils ONTAP pour l'objet racine VMware vSphere car il n'y a pas d'objet vSphere auquel vous pouvez l'affecter. Par exemple, toute autorisation qui inclut un privilège « Ajout/modification/Suppression de systèmes de stockage » des outils ONTAP pour VMware vSphere doit être attribuée au niveau de l'objet racine.

Lors de la définition d'une autorisation à un niveau supérieur dans la hiérarchie d'objets, vous pouvez configurer l'autorisation de sorte qu'elle soit transmise et héritée par les objets enfants. Si nécessaire, vous pouvez attribuer des autorisations supplémentaires aux objets enfants qui remplacent les autorisations héritées du parent.

Vous pouvez modifier une autorisation à tout moment. Si vous modifiez l'une des Privileges dans le cadre d'une autorisation, les utilisateurs associés à cette autorisation doivent se déconnecter de vSphere et se reconnecter pour activer la modification.

RBAC avec ONTAP

Fonctionnement du contrôle d'accès basé sur les rôles (RBAC) ONTAP avec les ONTAP tools

ONTAP fournit un environnement RBAC robuste et extensible. Vous pouvez utiliser la fonctionnalité RBAC pour contrôler l'accès aux opérations du système et du stockage comme exposées via l'API REST et l'interface de ligne de commande. Il est utile de se familiariser avec l'environnement avant de l'utiliser avec les outils ONTAP pour le déploiement de VMware vSphere 10.

Présentation des options administratives

Plusieurs options sont disponibles lorsque vous utilisez ONTAP RBAC, en fonction de votre environnement et de vos objectifs. Un aperçu des principales décisions administratives est présenté ci-dessous. Voir également "Automatisation ONTAP : présentation de la sécurité RBAC" pour plus d'informations.

> ONTAP RBAC est adapté à un environnement de stockage et est plus simple que l'implémentation RBAC fournie avec vCenter Server. Avec ONTAP, vous attribuez un rôle directement à l'utilisateur. La configuration d'autorisations explicites, telles que celles utilisées avec vCenter Server, n'est pas nécessaire avec ONTAP RBAC.

Types de rôles et de Privileges

Un rôle ONTAP est requis lors de la définition d'un utilisateur ONTAP. Il existe deux types de rôles ONTAP :

- REPOS

  Les rôles REST ont été introduits avec ONTAP 9.6 et sont généralement appliqués aux utilisateurs qui accèdent à ONTAP via l'API REST. Les Privileges incluses dans ces rôles sont définies en termes d'accès aux terminaux de l'API REST ONTAP et aux actions associées.

- Traditionnel

  Il s'agit des rôles hérités inclus avant ONTAP 9.6. Elles continuent d'être un aspect fondamental du RBAC. Les Privileges sont définies en termes d'accès aux commandes de l'interface de ligne de commandes ONTAP.

Alors que les AUTRES rôles ont été introduits plus récemment, les rôles traditionnels ont quelques avantages. Par exemple, des paramètres de requête supplémentaires peuvent être inclus de manière à ce que Privileges définisse plus précisément les objets auxquels ils sont appliqués.

Portée

Les rôles ONTAP peuvent être définis avec l'une des deux étendues différentes. Elles peuvent être appliquées à un SVM de données spécifique (niveau SVM) ou à l'ensemble du cluster ONTAP (niveau cluster).

Définitions de rôle

ONTAP fournit un ensemble de rôles prédéfinis au niveau du cluster et du SVM. Vous pouvez également définir des rôles personnalisés.

Utilisation des rôles REST ONTAP

Plusieurs considérations sont à prendre en compte lors de l'utilisation des rôles REST ONTAP inclus dans les outils ONTAP pour VMware vSphere 10.

Mappage de rôles

Que vous utilisiez un rôle classique ou REST, toutes les décisions d'accès à ONTAP sont basées sur la commande de l'interface de ligne de commande sous-jacente. Mais comme le Privileges dans un rôle REST est défini en termes de terminaux d'API REST, ONTAP doit créer un rôle *mappé* traditionnel pour chacun des rôles REST. Par conséquent, chaque rôle REST est associé à un rôle traditionnel sous-jacent. ONTAP peut ainsi prendre des décisions de contrôle d'accès de manière cohérente, quel que soit le type de rôle. Vous ne pouvez pas modifier les rôles mappés en parallèle.

Définition d'un rôle REST à l'aide de l'interface de ligne de commande Privileges

Comme ONTAP utilise toujours les commandes de l'interface de ligne de commande pour déterminer l'accès au niveau de base, il est possible d'exprimer un rôle REST en utilisant la commande de l'interface de ligne de commande Privileges à la place des terminaux REST. L'un des avantages de cette approche est la granularité supplémentaire disponible avec les rôles traditionnels.

Interface d'administration lors de la définition des rôles ONTAP

Vous pouvez créer des utilisateurs et des rôles à l'aide de l'interface de ligne de commandes et de l'API REST de ONTAP. Cependant, il est plus pratique d'utiliser l'interface System Manager et le fichier JSON disponible via le gestionnaire d'outils ONTAP. Voir "Utilisez ONTAP RBAC avec les outils ONTAP pour VMware vSphere 10" pour plus d'informations.

Considérations RBAC ONTAP pour les outils ONTAP

Il existe plusieurs aspects des outils ONTAP pour l'implémentation de VMware vSphere 10 RBAC avec ONTAP que vous devez prendre en compte avant de l'utiliser dans un environnement de production.

Présentation du processus de configuration

Les ONTAP tools for VMware vSphere incluent la prise en charge de la création d'un utilisateur ONTAP avec un rôle personnalisé. Les définitions sont regroupées dans un fichier JSON que vous pouvez télécharger sur le cluster ONTAP . Vous pouvez créer l'utilisateur et personnaliser le rôle en fonction de votre environnement et de vos besoins de sécurité.

Les principales étapes de configuration sont décrites ci-dessous à un niveau élevé. Voir "Configurer les rôles et privilèges des utilisateurs ONTAP"pour plus de détails.

1. Préparation

Vous devez disposer d'informations d'identification d'administration pour le gestionnaire d'outils ONTAP et le cluster ONTAP.

2. Téléchargez le fichier de définition JSON

Une fois connecté à l'interface utilisateur du Gestionnaire d'outils ONTAP, vous pouvez télécharger le fichier JSON contenant les définitions RBAC.

3. Créez un utilisateur ONTAP avec un rôle

Une fois connecté à System Manager, vous pouvez créer l'utilisateur et le rôle :

1. Sélectionnez **Cluster** sur la gauche, puis **Settings**.
2. Faites défiler jusqu'à **utilisateurs et rôles** et cliquez sur →.
3. Sélectionnez **Ajouter** sous **utilisateurs** et sélectionnez **produits de virtualisation**.
4. Sélectionnez le fichier JSON sur votre poste de travail local et chargez-le.

4. Configurez le rôle

Dans le cadre de la définition du rôle, vous devez prendre plusieurs décisions administratives. Voir Configurez le rôle à l'aide de System Manager pour plus de détails.

Configurez le rôle à l'aide de System Manager

Une fois que vous avez commencé à créer un utilisateur et un rôle avec System Manager et que vous avez téléchargé le fichier JSON, vous pouvez personnaliser le rôle en fonction de votre environnement et de vos besoins.

Configuration de l'utilisateur principal et du rôle

Les définitions RBAC sont packagées sous la forme de plusieurs fonctionnalités, dont une combinaison de VSC, VASA Provider et SRA. Vous devez sélectionner l'environnement ou les environnements dans lesquels vous avez besoin de la prise en charge de RBAC. Par exemple, si vous souhaitez que les rôles prennent en charge la fonctionnalité de plug-in à distance, sélectionnez VSC. Vous devez également choisir le nom d'utilisateur et le mot de passe associé.

Privilèges

Les Privileges de rôle sont organisés en quatre ensembles en fonction du niveau d'accès requis au stockage ONTAP. Le Privileges sur lequel sont basés les rôles comprend :

- Détection

  Il permet donc d'ajouter des systèmes de stockage.

- Créer du stockage

  Grâce à ce rôle, vous pouvez créer du stockage. Il inclut également toutes les Privileges associées au rôle de découverte.

- Modifier le stockage

  Ce rôle vous permet de modifier le stockage. Il inclut également toutes les Privileges associées à la détection et crée des rôles de stockage.

- Détruire le stockage

  Vous pouvez ainsi détruire le stockage. Elle inclut également toutes les Privileges associées à la détection, la création du stockage et la modification des rôles de stockage.

Générer l’utilisateur avec un rôle

Après avoir sélectionné les options de configuration pour votre environnement, cliquez sur **Ajouter** et ONTAP crée l’utilisateur et le rôle. Le nom du rôle généré est une concaténation des valeurs suivantes :

- Valeur de préfixe constante définie dans le fichier JSON (par exemple « OTV_10 »)
- Fonctionnalité de produit que vous avez sélectionnée
- Liste des jeux de privilèges.

Exemple

```
OTV_10_VSC_Discovery_Create
```

Le nouvel utilisateur sera ajouté à la liste de la page "utilisateurs et rôles". Notez que les méthodes de connexion utilisateur HTTP et ONTAPI sont prises en charge.

Déployez les outils ONTAP pour VMware vSphere

Démarrage rapide des outils ONTAP pour VMware vSphere

Configurez les ONTAP tools for VMware vSphere avec cette section de démarrage rapide.

Dans un premier temps, vous déploierez les ONTAP tools for VMware vSphere sous la forme d'une configuration de nœud unique de petite taille qui fournit des services de base pour prendre en charge les banques de données NFS et VMFS. Pour étendre votre configuration pour des conteneurs supplémentaires par service, une résilience améliorée ou pour utiliser des banques de données vVols et une haute disponibilité (HA), effectuez d'abord ce workflow, puis passez aux étapes d'extension. Pour plus d'informations, reportez-vous à la "Workflow de déploiement de la HAUTE DISPONIBILITÉ" .

Planification du déploiement

Vérifiez que vos versions d'hôte vSphere, ONTAP et ESXi sont compatibles avec la version des outils ONTAP . Allouez suffisamment d'espace CPU, de mémoire et de disque. Selon vos règles de sécurité, vous devrez peut-être configurer des pare-feu ou d'autres outils de sécurité pour autoriser le trafic réseau.

Assurez-vous que vCenter Server est installé et accessible.

- "Matrice d'interopérabilité"
- "Exigences et limites de configuration des outils ONTAP pour VMware vSphere"
- "Avant de commencer"

Déployez les outils ONTAP pour VMware vSphere

Dans un premier temps, vous déploierez les ONTAP tools for VMware vSphere sous forme de configuration à nœud unique de petite taille, fournissant les services de base nécessaires à la prise en charge des banques de données NFS et VMFS. Si vous envisagez d'étendre votre configuration pour utiliser les banques de données vVols et la haute disponibilité (HA), vous le ferez après avoir terminé ce workflow. Pour étendre votre configuration à une haute disponibilité, assurez-vous que l'ajout à chaud de processeur et le remplacement à chaud de mémoire sont activés.

- "Déployez les outils ONTAP pour VMware vSphere"

Ajouter des instances vCenter Server

Ajoutez des instances vCenter Server aux ONTAP tools for VMware vSphere pour configurer, gérer et protéger les banques de données virtuelles dans l'environnement vCenter Server.

- "Ajouter des instances vCenter Server"

Configurez les rôles d'utilisateur ONTAP et Privileges

Configurez de nouveaux rôles utilisateur et Privileges pour la gestion des systèmes back-end de stockage à l'aide du fichier JSON fourni avec les outils ONTAP pour VMware vSphere.

- "Configurer les rôles et privilèges des utilisateurs ONTAP"

5 **Configuration des systèmes back-end**

Ajout d'un système back-end de stockage à un cluster ONTAP Pour les configurations de colocation dans lesquelles vCenter agit en tant que locataire avec un SVM associé, utilisez ONTAP Tools Manager pour ajouter le cluster. Associez le système back-end de stockage au serveur vCenter pour le mapper globalement à l'instance du serveur vCenter intégré.

Ajoutez les systèmes back-end de stockage local avec des identifiants de cluster ou de SVM à l'aide de l'interface utilisateur des outils ONTAP. Ces systèmes de stockage back-end sont limités à une seule instance vCenter. Lors de l'utilisation locale des identifiants de cluster, les SVM associés sont automatiquement mappés sur vCenter pour gérer les vVols ou VMFS. Pour la gestion VMFS, notamment SRA, les outils ONTAP prennent en charge les identifiants SVM sans avoir besoin d'un cluster global.

- "Ajout d'un système back-end"
- "Associez le back-end de stockage à une instance vCenter Server"

6 **Mettez à niveau les certificats si vous travaillez avec plusieurs instances de vCenter Server**

Lorsque vous travaillez avec plusieurs instances de vCenter Server, mettez à niveau le certificat auto-signé vers un certificat signé par une autorité de certification (CA).

- "Gérer les certificats"

7 **(Facultatif) Configurer la protection SRA**

Utilisez la fonctionnalité SRA pour configurer la reprise après incident et protéger les datastores NFS ou VMFS.

- "Activez les outils ONTAP pour les services VMware vSphere"
- "Configurez SRA sur l'appliance VMware Live site Recovery"

8 **(Facultatif) Activer la protection de synchronisation active SnapMirror**

Configurez les outils ONTAP pour VMware vSphere afin de gérer la protection des clusters hôtes pour la synchronisation active SnapMirror. Effectuez le cluster ONTAP et le peering SVM dans les systèmes ONTAP pour utiliser la synchronisation active SnapMirror. Cela s'applique uniquement aux datastores VMFS.

- "Protégez à l'aide de la protection de cluster hôte"

9 **Configurez la sauvegarde et la restauration pour vos outils ONTAP pour le déploiement de VMware vSphere**

La sauvegarde est activée par défaut dans les ONTAP tools for VMware vSphere 10.5 et se produit toutes les 10 minutes. Planifiez des sauvegardes de vos ONTAP tools for VMware vSphere que vous pouvez utiliser pour récupérer la configuration en cas de panne.

- "Modifier les paramètres de sauvegarde"
- "Récupérer la configuration des outils ONTAP"

Flux de travail de déploiement à haute disponibilité pour ONTAP tools

Pour augmenter la résilience et prendre en charge davantage de conteneurs par service, étendez votre déploiement initial d'outils ONTAP à une configuration haute disponibilité (HA). L'activation du service VASA Provider est requise pour les banques de données vVols dans une configuration HA.

1. **Scale-up du déploiement**

Vous pouvez faire évoluer verticalement les outils ONTAP de la configuration VMware vSphere pour augmenter le nombre de nœuds utilisés pour le déploiement et remplacer la configuration par une configuration haute disponibilité.

- "Modification des outils ONTAP pour la configuration de VMware vSphere"

2. **Activation des services**

Pour configurer les magasins de données vVols , vous devez activer le service VASA Provider. Enregistrez le fournisseur VASA auprès de vCenter et assurez-vous que vos politiques de stockage répondent aux exigences HA, y compris les configurations de réseau et de stockage appropriées.

Utilisez les services SRA (ONTAP Tools Storage Replication adapter) pour VMware site Recovery Manager (SRM) ou VMware Live site Recovery (VLSR).

- "Activation des services VASA Provider et SRA"

3. **Mettre à niveau les certificats**

Si vous utilisez des datastores vVol avec plusieurs instances de vCenter Server, mettez à niveau le certificat auto-signé vers un certificat signé par une autorité de certification.

- "Gérer les certificats"

Exigences et limites de configuration des outils ONTAP pour VMware vSphere

Avant de déployer les outils ONTAP pour VMware vSphere, vous devez connaître les besoins en espace requis pour le package de déploiement et la configuration système hôte de base requise.

Vous pouvez utiliser les outils ONTAP pour VMware vSphere avec VMware vCenter Server Virtual Appliance (vCSA). Vous devez déployer les outils ONTAP pour VMware vSphere sur un client vSphere pris en charge qui inclut le système ESXi.

Configuration minimale requise

- **Espace requis pour le package d'installation par nœud**
  - 15 Go pour les installations à provisionnement fin
  - 348 Go pour les installations à provisionnement lourd
- **Dimensionnement requis du système hôte** Le tableau ci-dessous indique la mémoire recommandée pour chaque taille de déploiement. Pour les déploiements haute disponibilité (HA), vous avez besoin de trois fois la taille de l'appliance indiquée.

Type de déploiement	CPU par nœud	Mémoire (Go) par nœud	Espace disque (Go) thick provisionné par nœud
Petit	9	18	350
Moyen	13	26	350
REMARQUE importante : le déploiement de grande envergure concerne uniquement la configuration haute disponibilité.	17	34	350

Lorsque la sauvegarde est activée, chaque cluster d'outils ONTAP a besoin d'un espace supplémentaire de 50 Go sur le datastore où les machines virtuelles sont déployées. Par conséquent, une configuration non HA requiert 400 Go et la haute disponibilité requiert au total 1100 Go d'espace.

Exigences minimales en matière de stockage et d'applications

Stockage, hôte et applications	Exigences de version
ONTAP	9.15.1, 9.16.1, et 9.17.0
Les outils ONTAP prennent en charge les hôtes ESXi	à partir de 7.0.3
Les outils ONTAP prennent en charge vCenter Server	7.0U3 à partir de
Vasa Provider	3.0
Application OVA	10,5
Hôte VMware ESXi pour déployer la machine virtuelle des outils ONTAP	7.0U3 et 8.0U3
VCenter Server pour déployer la machine virtuelle des outils ONTAP	7.0 et 8.0

À partir des outils ONTAP pour VMware vSphere 10.4, le matériel de la machine virtuelle passe de la version 10 à la version 17.

La matrice d'interopérabilité (IMT) contient les dernières informations sur les versions prises en charge de ONTAP, de vCenter Server, d'hôtes ESXi et d'applications de plug-in.

"Matrice d’interopérabilité"

Configuration requise pour les ports

Le tableau suivant présente les ports réseau utilisés par NetApp et leurs fonctions. Il existe trois types de ports différents :

- Ports externes : ces ports sont accessibles depuis l’extérieur du cluster ou du nœud Kubernetes. Ils permettent aux services de communiquer avec des réseaux ou des utilisateurs externes, permettant ainsi l’intégration avec des systèmes situés en dehors de l’environnement du cluster.
- Ports inter-nœuds : ces ports permettent la communication entre les nœuds au sein du cluster Kubernetes. Ils sont nécessaires pour les tâches en cluster telles que le partage de données et le travail collaboratif. Pour les déploiements à nœud unique, les ports inter-nœuds sont utilisés uniquement au sein du nœud et n’ont pas besoin d’accès externe. Les ports inter-nœuds peuvent accepter le trafic provenant de l’extérieur du cluster. Bloquez l’accès Internet aux ports inter-nœuds à l’aide de règles de pare-feu.
- Ports internes : ces ports communiquent au sein du cluster Kubernetes à l’aide d’adresses ClusterIP. Elles ne sont pas exposées de l’extérieur et n’ont pas besoin d’être ajoutées aux règles du pare-feu.

Assurez-vous que tous les nœuds des outils ONTAP résident sur le même sous-réseau pour maintenir une communication ininterrompue entre eux.

Cliquez pour développer ou réduire le tableau des exigences relatives aux ports.

Nom du service/composant	Port	Protocole	Type de port	Description
ntv-gateway-svc (LB)	443, 8443	TCP	Externe	Port de transit pour les communications entrantes du service fournisseur VASA. Le certificat auto-signé du fournisseur VASA et le certificat CA personnalisé sont hébergés sur ce port.
SSH	22	TCP	Externe	Secure Shell pour la connexion à un serveur distant et l'exécution de commandes.
serveur rke2	9345	TCP	Inter-nœud	API de supervision RKE2 (Restriction aux réseaux de confiance).
kube-apiserver	6443	TCP	Inter-nœud	Port du serveur API Kubernetes (à limiter aux réseaux de confiance).
rpcbind/portmapper	111	TCP/UDP	Inter-nœud	Utilisé pour la communication RPC entre les services.
coredns (DNS)	53	TCP/UDP	Inter-nœud	Service DNS (Domain Name System) pour la résolution de noms au sein du cluster.
NTP	123	UDP	Inter-nœud	Protocole NTP (Network Time Protocol) pour la synchronisation de l'heure.
etcd	2379, 2380, 2381	TCP	Inter-nœud	Système de stockage clé-valeur pour les données de cluster.
kube-vip	2112	TCP	Inter-nœud	Port du serveur API Kubernetes.

Nom du service/composant	Port	Protocole	Type de port	Description
kubelet	10248, 10250	TCP	Inter-nœud	Composant Kubernetes
contrôleur kube	10257	TCP	Inter-nœud	Composant Kubernetes
contrôleur cloud	10258	TCP	Inter-nœud	Composant Kubernetes
kube-scheduler	10259	TCP	Inter-nœud	Composant Kubernetes
kube-proxy	10249, 10256	TCP	Inter-nœud	Composant Kubernetes
nœud calico	9091, 9099	TCP	Inter-nœud	Composant réseau Calico.
conteneur	10010	TCP	Inter-nœud	Service démon du conteneur.
VXLAN (Flannel)	8472	UDP	Inter-nœud	Réseau superposé pour la communication entre les pods.

Pour les déploiements HA, assurez-vous que le port UDP 8472 est ouvert entre tous les nœuds. Ce port permet la communication entre les pods au sein des nœuds ; son blocage interrompra la mise en réseau entre les nœuds.

Limites de configuration pour déployer ONTAP tools for VMware vSphere pour les datastores vVols

Vous pouvez utiliser le tableau suivant comme guide pour configurer les ONTAP tools for VMware vSphere.

Déploiement	Type	Nombre de vVols	Nombre d'hôtes
Non HA	Petit (S)	jusqu'à 12K	32
Non HA	Moyen (M)	jusqu'à 24K	64
Haute-disponibilité	Petit (S)	jusqu'à 24K	64
Haute-disponibilité	Moyen (M)	jusqu'à 50k	128
Haute-disponibilité	Grand (L)	jusqu'à 100k	256

Le nombre d'hôtes indiqué dans le tableau représente le total combiné pour tous les vCenters connectés.

Limites de configuration pour le déploiement des ONTAP tools for VMware vSphere pour les datastores VMFS et NFS

Les limites de configuration indiquées dans cette section sont validées et prises en charge par NetApp. Les limites réelles peuvent varier en fonction de votre environnement et de votre charge de travail. Le dépassement de ces limites peut impacter les performances ou la prise en charge et est déconseillé. Tenez compte des éléments suivants lors de l'examen du tableau :

- La reprise après sinistre (DR) des machines virtuelles est configurée à l'aide de stratégies synchrones, asynchrones ou de synchronisation stricte. DR n'est pas pris en charge pour le protocole NVMe.
- La protection des clusters hôtes ESXi utilise SnapMirror Active Sync, qui ne prend pas en charge les déploiements multi-vCenter.
- ONTAP tools limite uniquement le nombre d'hôtes ESXi et de banques de données en fonction de la taille du déploiement. Il n'y a aucune restriction sur le nombre de vCenter Servers pouvant être connectés à ONTAP tools.
- ONTAP tools effectue une découverte parallèle de tous les objets de stockage. Les limites de configuration des objets de stockage ONTAP s'appliquent quel que soit le nombre d'objets utilisés.
- ONTAP tools n'impose aucune limite quant au nombre de serveurs vCenter pouvant être intégrés. Les limites de configuration sont déterminées par le nombre d'hôtes et de banques de données pris en charge, comme indiqué dans le tableau suivant.

Déploiement	Nombre de banques de données VMFS et NFS	Nombre de banques de données VMFS activées pour la reprise après sinistre	Nombre d'hôtes
Non HA petit	200	80	32
Non HA Moyen	250	100	32
HA petit	350	200	64
HA Moyen	600	200	128
HAUTE disponibilité	1024	250	256

Outils ONTAP pour VMware vSphere - Storage Replication adapter (SRA)

Le tableau suivant indique les chiffres pris en charge par instance VMware Live site Recovery à l'aide des outils ONTAP pour VMware vSphere.

Taille du déploiement vCenter	Petit	Moyen
Nombre total de machines virtuelles configurées pour la protection à l'aide de la réplication basée sur les baies	2000	5000
Nombre total de groupes de protection de réplication basés sur les baies	250	250
Nombre total de groupes de protection par plan de reprise d'activité	50	50

Taille du déploiement vCenter	Petit	Moyen
Nombre de datastores répliqués	255	255
Nombre de VM	4000	7000

Le tableau suivant indique le nombre de VMware Live site Recovery et les outils ONTAP correspondants pour la taille du déploiement de VMware vSphere.

Nombre d'instances de VMware Live site Recovery	Déploiement des outils ONTAP taille
Jusqu'à 4	Petit
4 à 8	Moyen
Plus de 8	Grand

Pour plus d'informations, reportez-vous "Limites opérationnelles de la restauration VMware Live site"à .

Exigences préalables au déploiement des ONTAP tools

Assurez-vous que les conditions suivantes sont remplies avant de poursuivre le déploiement :

De formation	Votre statut
La version vSphere, la version ONTAP et la version hôte ESXi sont compatibles avec la version des outils ONTAP.	□ Oui □ non
L'environnement vCenter Server est configuré et configuré	□ Oui □ non
Le cache du navigateur est supprimé	□ Oui □ non
Vous disposez des informations d'identification du serveur vCenter parent	□ Oui □ non
Vous disposez des informations d'identification de connexion pour l'instance vCenter Server, à laquelle les outils ONTAP pour VMware vSphere connecteront le post-déploiement pour l'enregistrement	□ Oui □ non
Le nom de domaine sur lequel le certificat est émis est mappé à l'adresse IP virtuelle dans un déploiement multi-vCenter où les certificats d'autorité de certification personnalisés sont obligatoires.	□ Oui □ non
Vous avez exécuté la vérification nslookup sur le nom de domaine pour vérifier si le domaine est résolu à l'adresse IP prévue.	□ Oui □ non
Le certificat est créé avec le nom de domaine et l'adresse IP des outils ONTAP.	□ Oui □ non
L'application des outils ONTAP et les services internes sont accessibles depuis le serveur vCenter.	□ Oui □ non

De formation	Votre statut
Lorsque vous utilisez des SVM mutualisés, vous disposez d'une LIF de gestion de SVM sur chaque SVM.	□ Oui □ non

Fiche technique de déploiement

Pour le déploiement d'un seul nœud

Utilisez la feuille de calcul suivante pour rassembler les informations requises pour les outils ONTAP pour le déploiement initial de VMware vSphere :

Conditions requises	Votre valeur
Adresse IP de l'application ONTAP tools. Il s'agit de l'adresse IP permettant d'accéder à l'interface web du gestionnaire ONTAP tools (load balancer) à `https://<ip>:8443/virtualization/ui/`	
Adresse IP virtuelle des outils ONTAP pour la communication interne. Cette adresse IP est utilisée pour la communication interne dans une configuration avec plusieurs instances d'outils ONTAP . Cette adresse IP ne doit pas être la même que l'adresse IP de l'application des outils ONTAP . (Le plan de contrôle Kubernetes)	
Nom d'hôte DNS pour le nœud de gestion des outils ONTAP	
Serveur DNS principal	
Serveur DNS secondaire	
Domaine de recherche DNS	
Adresse IPv4 pour le nœud de gestion des outils ONTAP. Il s'agit d'une adresse IPv4 unique pour l'interface de gestion du nœud sur le réseau de gestion. Ceci est utilisé pour se connecter à l'appliance des outils ONTAP pour un accès de diagnostic à distance via SSH.	
Masque de sous-réseau de l'adresse IPv4	
Passerelle par défaut pour l'adresse IPv4	
Adresse IPv6 (facultatif)	
Longueur du préfixe IPv6 (facultatif)	
Passerelle pour l'adresse IPv6 (facultatif)	

Créez des enregistrements DNS pour toutes les adresses IP ci-dessus. Avant d'attribuer des noms d'hôte, mappez-les aux adresses IP libres sur le DNS. Toutes les adresses IP doivent se trouver sur le même VLAN sélectionné pour le déploiement.

Pour les déploiements haute disponibilité (HA)

Outre les exigences de déploiement d'un seul nœud, vous aurez besoin des informations suivantes pour les déploiements HA :

Conditions requises	Votre valeur
Serveur DNS principal	
Serveur DNS secondaire	
Domaine de recherche DNS	
Nom d'hôte DNS du second nœud	
Adresse IP du second nœud	
Nom d'hôte DNS du troisième nœud	
Adresse IP du troisième nœud	

Configuration du pare-feu réseau

Assurez-vous que les ports de pare-feu nécessaires sont ouverts pour toutes les adresses IP concernées. Les outils ONTAP nécessitent un accès au LIF via le port 443. Pour une liste complète des ports requis, consultez la section relative aux exigences de port à l'adresse"Exigences et limites de configuration des outils ONTAP pour VMware vSphere" .

Paramètres de stockage ONTAP

Pour assurer une intégration transparente du stockage ONTAP avec les outils ONTAP pour VMware vSphere, tenez compte des paramètres suivants :

- Si vous utilisez Fibre Channel (FC) pour la connectivité de stockage, configurez le zonage sur vos commutateurs FC pour connecter les hôtes ESXi aux LIF FC du SVM. "En savoir plus sur le zoning FC et FCoE avec les systèmes ONTAP"
- Pour utiliser la réplication SnapMirror gérée par les outils ONTAP, l'administrateur du stockage ONTAP doit créer "Relations entre clusters ONTAP" et "Relations entre les pairs du SVM intercluster ONTAP" dans ONTAP avant d'utiliser SnapMirror.

Déployer les outils ONTAP

Les ONTAP tools for VMware vSphere sont déployés sous la forme d'un nœud unique de petite taille avec des services principaux pour prendre en charge les banques de données NFS et VMFS. Le déploiement des outils ONTAP peut prendre jusqu'à 45 minutes.

Avant de commencer

Si vous déployez un petit nœud unique, une bibliothèque de contenu est facultative. Pour les déploiements multi-nœuds ou HA, une bibliothèque de contenu est requise. Dans VMware, une bibliothèque de contenu stocke des modèles de machine virtuelle, des modèles vApp et d'autres fichiers. Le déploiement avec une bibliothèque de contenu offre une expérience transparente car elle ne dépend pas de la connectivité réseau.

Tenez compte des éléments suivants avant de créer une bibliothèque de contenu :

- Créez la bibliothèque de contenu sur une banque de données partagée afin que tous les hôtes du cluster puissent y accéder.
- Configurez la bibliothèque de contenu avant de déployer les ONTAP tools for VMware vSphere OVA.
- Assurez-vous que la bibliothèque de contenu est créée avant de configurer l'appliance pour HA.

Ne supprimez pas le modèle OVA de la bibliothèque de contenu après le déploiement.

Pour activer le déploiement HA à l'avenir, évitez de déployer la machine virtuelle des outils ONTAP directement sur un hôte ESXi. Déployez-le plutôt dans un cluster hôte ou un pool de ressources ESXi.

Suivez ces étapes pour créer une bibliothèque de contenu :

1. Téléchargez le fichier contenant les binaires (*.ova*) et les certificats signés pour les ONTAP tools for VMware vSphere à partir du "Site de support NetApp" .
2. Connectez-vous au client vSphere
3. Sélectionnez le menu du client vSphere et sélectionnez **bibliothèques de contenu**.
4. Sélectionnez **Créer** à droite de la page.
5. Indiquez un nom pour la bibliothèque et créez la bibliothèque de contenu.
6. Accédez à la bibliothèque de contenu que vous avez créée.
7. Sélectionnez **actions** à droite de la page et sélectionnez **Importer élément** et importez le fichier OVA.

Pour plus d'informations, consultez "Création et utilisation de la bibliothèque de contenu" le blog.

Avant de procéder au déploiement, définissez le planificateur de ressources distribuées (DRS) du cluster sur l'inventaire sur « Conservateur ». Cela garantit que les machines virtuelles ne sont pas migrées pendant l'installation.

Les ONTAP tools for VMware vSphere sont initialement déployés en tant que configuration non HA. Pour un déploiement haute disponibilité, vous devrez activer le branchement à chaud du processeur et de la mémoire. Vous pouvez effectuer cette étape lors du déploiement ou modifier les paramètres de la machine virtuelle après le déploiement.

Étapes

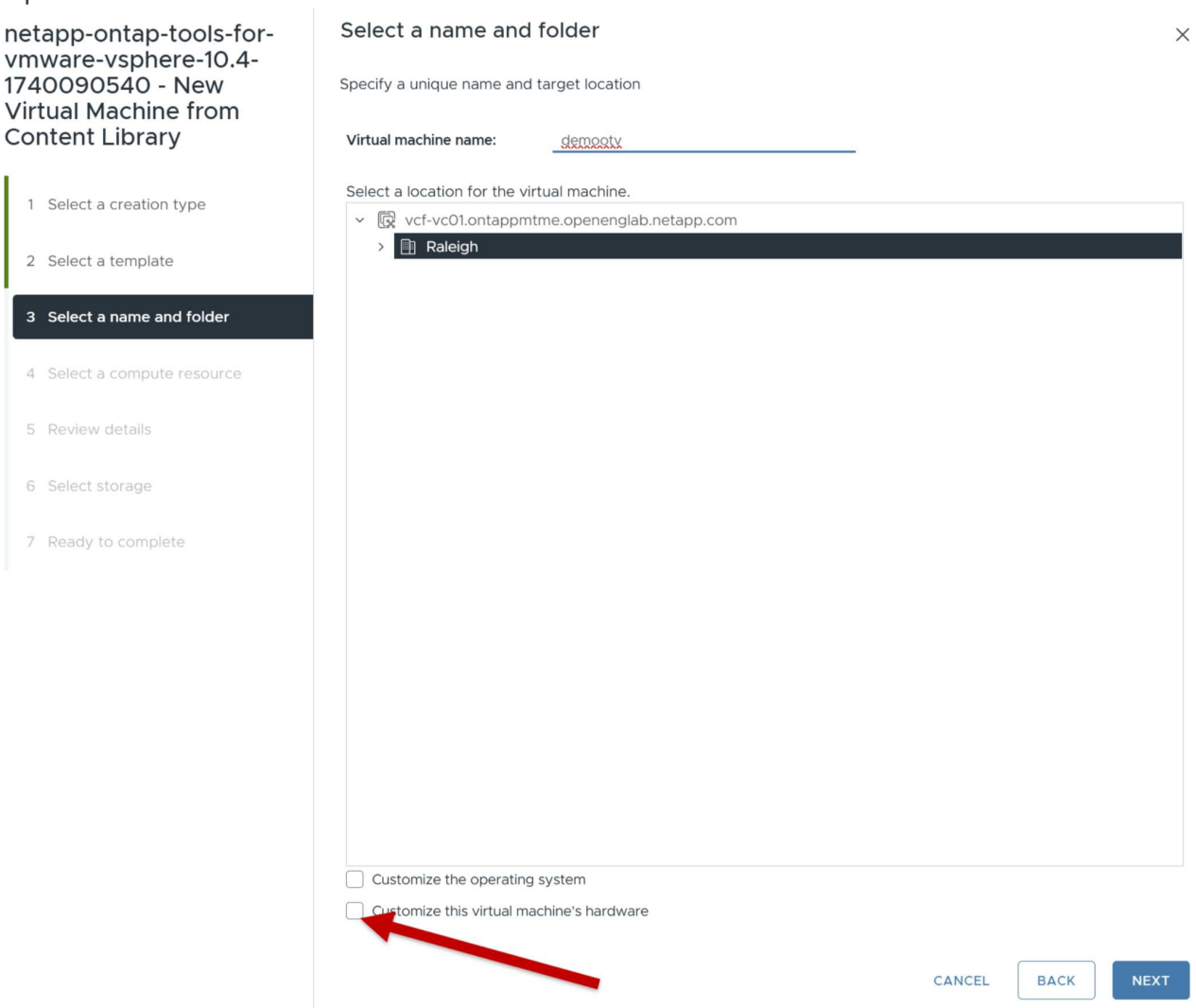
1. Téléchargez le fichier contenant les binaires (*.ova*) et les certificats signés pour les ONTAP tools for VMware vSphere à partir du "Site de support NetApp" . Si vous avez importé l'OVA dans la bibliothèque de contenu, vous pouvez ignorer cette étape et passer à l'étape suivante.
2. Connectez-vous au serveur vSphere.
3. Accédez au pool de ressources, au cluster ou à l'hôte sur lequel vous souhaitez déployer l'OVA.

Ne stockez jamais d'outils ONTAP pour la machine virtuelle VMware vSphere sur les datastores vVols qu'il gère.

4. Vous pouvez déployer l'OVA à partir de la bibliothèque de contenu ou du système local.

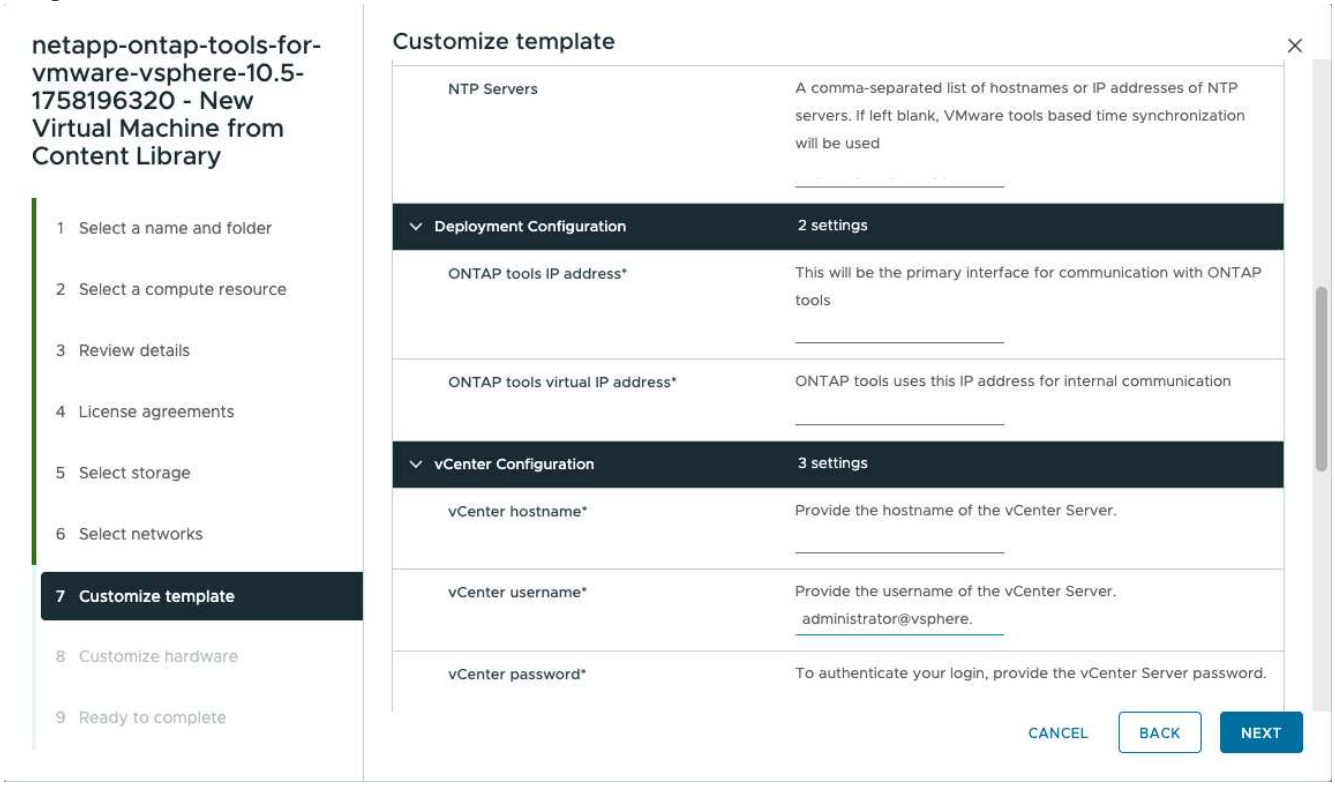
À partir du système local	À partir de la bibliothèque de contenu
a. cliquez avec le bouton droit de la souris et sélectionnez **déployer le modèle OVF….** b. Choisissez le fichier OVA à partir de l'URL ou naviguez jusqu'à son emplacement, puis sélectionnez **Suivant**.	a. accédez à votre bibliothèque de contenu et sélectionnez l'élément de bibliothèque que vous souhaitez déployer. b. sélectionnez **actions** > **Nouveau VM à partir de ce modèle**

5. Dans le champ **Sélectionner un nom et un dossier**, entrez le nom de la machine virtuelle et choisissez son emplacement.
   - Si vous utilisez la version de vCenter Server 8.0.3, sélectionnez l'option **Personnaliser le matériel de cette machine virtuelle**, qui activera une étape supplémentaire appelée **Personnaliser le matériel** avant de passer à la fenêtre **prêt à terminer**.
   - Si vous utilisez la version vCenter Server 7.0.3, suivez les étapes de la section **Quelle est la prochaine étape ?** à la fin du déploiement.



6. Sélectionnez une ressource d'ordinateur et sélectionnez **Suivant**. Si vous le souhaitez, cochez la case **mettre automatiquement sous tension la machine virtuelle déployée**.
7. Passez en revue les détails du modèle et sélectionnez **Suivant**.
8. Lisez et acceptez le contrat de licence et sélectionnez **Suivant**.

9. Sélectionnez le stockage pour la configuration et le format du disque, puis sélectionnez **Suivant**.
10. Sélectionnez le réseau de destination pour chaque réseau source et sélectionnez **Suivant**.
11. Dans la fenêtre **Personnaliser le modèle**, remplissez les champs obligatoires.



Le nom d'hôte vCenter correspond au nom de l'instance vCenter Server sur laquelle l'appliance ONTAP Tools est déployée.

Si vous déployez des outils ONTAP dans une topologie à deux serveurs vCenter (où l'appliance est hébergée dans une instance vCenter et en gère une autre), vous pouvez attribuer un rôle restreint à l'instance vCenter hébergeant les outils ONTAP . Vous pouvez créer un utilisateur et un rôle vCenter dédiés, disposant uniquement des autorisations requises pour le déploiement du modèle OVF. Pour plus de détails, consultez les rôles énumérés dans "Rôles inclus avec les outils ONTAP pour VMware vSphere 10".

Pour l'instance vCenter qui sera gérée par les outils ONTAP , assurez-vous que le compte utilisateur vCenter dispose des privilèges d'administrateur.

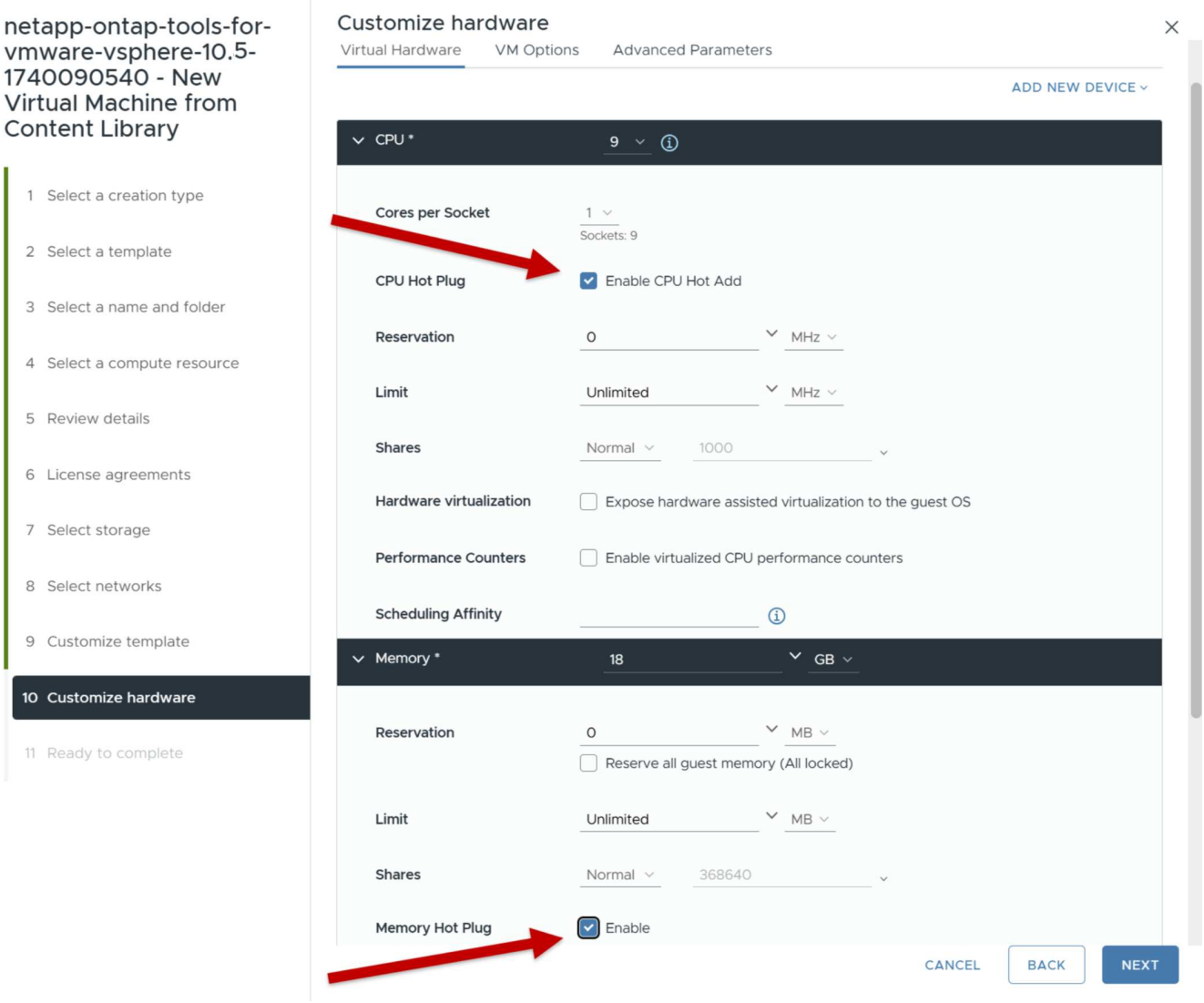
- Les noms d'hôte doivent comporter des lettres (A-Z, a-z), des chiffres (0-9) et des tirets (-). Pour configurer la double pile, spécifiez le nom d'hôte mappé sur l'adresse IPv6.

  Le PROTOCOLE IPv6 pur n'est pas pris en charge. Le mode mixte est pris en charge avec un VLAN contenant à la fois des adresses IPv6 et IPv4.

- L'adresse IP des outils ONTAP est l'interface principale de communication avec les outils ONTAP.
- IPv4 est le composant d'adresse IP de la configuration du nœud, qui peut être utilisé pour activer le shell de diagnostic et l'accès SSH sur le nœud à des fins de débogage et de maintenance.

12. Lors de l'utilisation de la version 8.0.3 de vCenter Server, dans la fenêtre **Personnaliser le matériel**, activez les options **Ajout à chaud du processeur** et **Pont à chaud de la mémoire** pour permettre la

fonctionnalité
HA.



13. Consultez les détails dans la fenêtre **prêt à terminer**, sélectionnez **Terminer**.

    Au fur et à mesure de la création de la tâche de déploiement, la progression s'affiche dans la barre des tâches vSphere.

14. Mettez la machine virtuelle sous tension après avoir terminé la tâche si l'option de mise sous tension automatique de la machine virtuelle n'a pas été sélectionnée.

Vous pouvez suivre la progression de l'installation au sein de la console Web de la machine virtuelle.

S'il y a des divergences dans le formulaire OVF, une boîte de dialogue demandera une action corrective. Utilisez le bouton Tab pour naviguer, effectuez les modifications nécessaires et sélectionnez **OK**. Vous disposez de trois tentatives pour résoudre les problèmes. Si les problèmes persistent après trois tentatives, le processus d'installation s'arrêtera et il est conseillé de réessayer l'installation sur une nouvelle machine virtuelle.

Et la suite ?

Si vous avez déployé des outils ONTAP pour VMware vSphere avec vCenter Server 7.0.3, suivez ces étapes après le déploiement.

1. Connectez-vous au client vCenter
2. Mettez le nœud ONTAP Tools hors tension.
3. Accédez aux ONTAP tools for VMware vSphere sous **Inventaires** et sélectionnez l'option **Modifier les paramètres**.
4. Sous les options **CPU**, cochez la case **Activer l'ajout à chaud de CPU**
5. Sous les options **Memory**, cochez la case **Enable** par rapport à **Memory hot plug**.

Dépanner les erreurs de déploiement des outils ONTAP

Si vous rencontrez des problèmes de déploiement, consultez les journaux et les codes d'erreur pour diagnostiquer et résoudre les problèmes. À partir des ONTAP tools for VMware vSphere 10.5, les groupes de journaux collectés à partir des pods incluent les journaux de MongoDB, RabbitMQ et Vault, ainsi que l'état et les descriptions de tous les pods. Ils sont fournis en plus des journaux de service des outils ONTAP existants, améliorant ainsi la prise en charge et le dépannage.

Collectez les fichiers journaux

Vous pouvez collecter les fichiers journaux des outils ONTAP pour VMware vSphere à partir des options disponibles dans l'interface utilisateur de ONTAP Tools Manager. Le support technique peut vous demander de collecter les fichiers journaux afin de résoudre un problème.

> La génération de journaux à partir du Gestionnaire d'outils ONTAP inclut tous les journaux de toutes les instances de vCenter Server. La génération des journaux à partir de l'interface utilisateur du client vCenter est étendue pour le serveur vCenter sélectionné.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **Log Bundles** dans la barre latérale.

   Cette opération peut prendre plusieurs minutes.
4. Sélectionnez **générer** pour générer les fichiers journaux.
5. Saisissez le libellé du lot de journaux et sélectionnez **Generate**.

   Téléchargez le fichier tar.gz et envoyez-le au support technique.

Pour générer un bundle de journaux à l'aide de l'interface utilisateur du client vCenter, procédez comme suit :

Étapes

1. Connectez-vous au client vSphere.
2. Depuis la page d'accueil de vSphere client, accédez à **support** > **Log bundle** > **Generate**.
3. Indiquez l'étiquette du fichier journal et générez-le. L'option de téléchargement s'affiche une fois les fichiers générés. Le téléchargement peut prendre un certain temps.

L'ensemble de journaux généré remplace l'ensemble de journaux généré au cours des 3 derniers jours ou des 72 dernières heures.

Codes d'erreur de déploiement

Des codes d'erreur peuvent s'afficher lors du déploiement, du redémarrage et des opérations de restauration des outils ONTAP pour VMware vSphere.
Les codes d'erreur sont composés de cinq chiffres, les deux premiers chiffres représentant le script qui a rencontré le problème, et les trois derniers chiffres représentent le flux de travail spécifique de ce script.

Tous les journaux d'erreurs sont enregistrés dans le fichier ansible-perl-errors.log sous le répertoire /var/log pour faciliter le suivi et la résolution des problèmes. Ce fichier journal contient le code d'erreur et la tâche Ansible ayant échoué.

Les codes d'erreur fournis sur cette page sont fournis à titre de référence uniquement. Contactez l'équipe d'assistance si l'erreur persiste ou si aucune résolution n'est mentionnée.

Le tableau suivant répertorie les codes d'erreur et les noms de fichier correspondants.

Code d'erreur	Nom du script
00	firstboot-network-config.pl, mode deploy
01	firstboot-network-config.pl, mise à niveau du mode
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, déploiement, haute disponibilité
04	firstboot-deploy-otv-ng.pl, déploiement, non HA
05	firstboot-deploy-otv-ng.pl, redémarrer
06	firstboot-deploy-otv-ng.pl, mise à niveau, haute disponibilité
07	firstboot-deploy-otv-ng.pl, mise à niveau, non HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Les trois derniers chiffres du code d'erreur indiquent l'erreur de flux de travail spécifique dans le script :

Code d'erreur de déploiement	Workflow	Résolution
049	Pour le réseau et la validation, le script perl les attribuera également sous peu	-
050	Échec de la génération de la clé SSH	Redémarrez la machine virtuelle (VM) principale.

053	Echec de l’installation de RKE2	Exécutez les opérations suivantes et redémarrez la machine virtuelle principale ou redéployez : Sudo rke2-killall.sh (toutes les VM) Sudo rke2-uninstall.sh (toutes les VM).
054	Échec du paramétrage kubeconfig	Redéploiement
055	Échec du déploiement du registre	Si le pod de registre est présent, attendez que le pod soit prêt, puis redémarrez la machine virtuelle principale ou redéployez-la.
059	Échec du déploiement KubeVip	Vérifiez que l’adresse IP virtuelle du plan de contrôle Kubernetes et l’adresse IP des outils ONTAP fournies lors du déploiement appartiennent au même VLAN et sont des adresses IP libres. Redémarrez si tous les points précédents sont corrects. Sinon, redéployer.
060	Le déploiement de l’opérateur a échoué	Redémarrer
061	Le déploiement des services a échoué	Effectuez des opérations de débogage Kubernetes de base comme GET pods, GET RS, GET svc, etc. Dans l’espace de noms du système ntv pour plus de détails et des journaux d’erreurs dans /var/log/ansible-perl-errors.log et /var/log/ansible-run.log et redéployez.
062	Le déploiement des services d’outils ONTAP a échoué	Reportez-vous aux journaux d’erreurs à l’adresse /var/log/ansible-perl-errors.log pour plus de détails et redéployez.
065	L’URL de la page swagger est inaccessible	Redéploiement
066	Les étapes de post-déploiement du certificat de passerelle ont échoué	Procédez comme suit pour récupérer/terminer la mise à niveau : * Activer le shell de diagnostic. * Exécutez la commande 'sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy'. * Consultez les journaux dans /var/log/post-deploy-upgrade.log.

088	La configuration de la rotation du journal pour journald a échoué	Vérifiez les paramètres réseau de la machine virtuelle compatibles avec l'hôte sur lequel la machine virtuelle est hébergée. Vous pouvez essayer de migrer vers un autre hôte et redémarrer la machine virtuelle.
089	La modification de la propriété du fichier de configuration de rotation du journal de synthèse a échoué	Redémarrez la machine virtuelle principale.
096	Installer le provisionneur de stockage dynamique	-
108	Echec du script d'amorçage	-

Redémarrez le code d'erreur	Workflow	Résolution
067	Délai d'attente du serveur rke2 dépassé.	-
101	Echec de la réinitialisation du mot de passe utilisateur maint/Console.	-
102	Échec de la suppression du fichier de mot de passe lors de la réinitialisation du mot de passe utilisateur maint/Console.	-
103	Échec de la mise à jour du nouveau mot de passe utilisateur maint/Console dans le coffre-fort.	-
088	La configuration de la rotation du journal pour journald a échoué.	Vérifiez les paramètres réseau de la machine virtuelle compatibles avec l'hôte sur lequel la machine virtuelle est hébergée. Vous pouvez essayer de migrer vers un autre hôte et redémarrer la machine virtuelle.
089	La modification de la propriété du fichier de configuration de rotation du journal de synthèse a échoué.	Redémarrez l'unité VM.

Configuration des outils ONTAP pour VMware vSphere

Ajouter des instances vCenter Server aux outils ONTAP

Ajoutez des instances de vCenter Server aux outils ONTAP pour VMware vSphere pour configurer, gérer et protéger vos datastores virtuels dans votre environnement vCenter Server. Lorsque vous ajoutez plusieurs instances de vCenter Server, des certificats d'autorité de certification personnalisés sont requis pour une communication sécurisée entre les outils ONTAP et chaque vCenter Server.

Description de la tâche

Les outils ONTAP s'intègrent à vCenter Server pour effectuer des tâches de stockage telles que le provisionnement, les instantanés et la protection des données directement à partir du client vSphere.

Avant de commencer

- Assurez-vous que le certificat du serveur vCenter inclut une extension SAN (Subject Alternative Name) valide avec des entrées DNS et d'adresse IP. Par exemple :

```
X509v3 extensions:
    X509v3 Subject Alternative Name:
        DNS: vcenter.example.com, DNS: vcenter, IP Address: 192.168.0.50
```

  Si le certificat ne comporte pas d'extension SAN, ou si l'extension SAN ne contient pas les valeurs DNS ou d'adresse IP correctes, les opérations des ONTAP tools peuvent échouer en raison d'erreurs de validation du certificat.

- L'identifiant réseau principal (PNID) du vCenter Server doit figurer dans les détails du SAN. Le PNID et le nom DNS doivent être identiques et résolvables dans le DNS.
- Il est recommandé de déployer vCenter Server en utilisant son nom de domaine complet (FQDN), et de s'assurer que le SAN dans le certificat inclut DNS Name=machine_FQDN pour une compatibilité et un support optimaux.
- Pour plus d'informations, consultez la documentation VMware :
  - "vSphere Exigences de certification pour les différents chemins de solution"
  - "Remplacez le certificat SSL de la machine vCenter par un certificat signé par une autorité de certification personnalisée"
  - "Erreur : Le champ Subject Alternate Name (SAN) ne contient pas le PNID. Veuillez fournir un certificat valide"

> Si le FQDN n'est pas disponible, vous pouvez définir le PNID sur l'adresse IP et inclure l'adresse IP dans le SAN. Cependant, cela n'est pas recommandé par VMware.

Étapes

1. Ouvrez un navigateur Web et accédez à l'URL :
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`

2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **vCenters** > **Add** pour intégrer les instances de vCenter Server. Indiquez l'adresse IP ou le nom d'hôte, le nom d'utilisateur, le mot de passe et les informations de port de vCenter.
4. Dans les options avancées, récupérez automatiquement le certificat vCenter Server (autorisez-le) ou téléchargez-le manuellement.

> Vous n'avez pas besoin d'un compte d'administrateur pour ajouter des instances vCenter aux outils ONTAP. Vous pouvez créer un rôle personnalisé sans le compte admin avec des autorisations limitées. Voir "Utilisez vCenter Server RBAC avec les outils ONTAP pour VMware vSphere 10" pour plus de détails.

L'ajout d'une instance de serveur vCenter aux outils ONTAP déclenche automatiquement les actions suivantes :

- Les outils ONTAP enregistrent le plug-in client vCenter en tant que plug-in distant.
- Les Privileges personnalisés pour les plug-ins et les API sont appliqués à l'instance de vCenter Server.
- Des rôles personnalisés sont créés pour gérer les utilisateurs.
- Le plug-in apparaît sous la forme d'un raccourci dans l'interface utilisateur vSphere.

Enregistrez le fournisseur VASA auprès d'une instance de serveur vCenter dans ONTAP tools

Utilisez les ONTAP tools for VMware vSphere pour enregistrer le fournisseur VASA auprès d'une instance de vCenter Server. Cela permet une gestion basée sur des politiques de stockage, la prise en charge de vVols et l'intégration avec les appliances VMware Live Site Recovery sur les systèmes ONTAP .

Les paramètres du fournisseur VASA affichent l'état d'enregistrement du serveur vCenter sélectionné.

Étapes

1. Connectez-vous au client vSphere.
2. Sélectionnez **raccourcis** > **Outils NetApp ONTAP** dans la section modules externes.
3. Sélectionnez **Paramètres** > **Paramètres du fournisseur VASA**. Les outils ONTAP affichent le statut d'enregistrement du fournisseur VASA comme non enregistré.
4. Sélectionnez le bouton **Register** pour enregistrer le fournisseur VASA.
5. Saisissez un nom et des informations d'identification pour le fournisseur VASA. Le nom d'utilisateur ne peut contenir que des lettres, des chiffres et des traits de soulignement. Définissez la longueur du mot de passe entre 8 et 256 caractères.
6. Sélectionnez **Enregistrer**.
7. Après une inscription et une actualisation de la page réussies, les outils ONTAP affichent le statut, le nom et la version du fournisseur VASA enregistré.

Et la suite

Vérifiez que le fournisseur VASA intégré est répertorié sous VASA Provider du client vCenter :

Étapes

1. Accédez à l'instance vCenter Server.
2. Connectez-vous avec les informations d'identification de l'administrateur.
3. Sélectionnez **fournisseurs de stockage** > **configurer**. Vérifiez que le fournisseur VASA intégré est correctement répertorié.

Installer le plug-in NFS VAAI à l'aide des outils ONTAP

Le plug-in NFS vStorage API for Array Integration (NFS VAAI) connecte VMware vSphere aux baies de stockage NFS. Utilisez les ONTAP tools for VMware vSphere pour installer le plug-in VAAI. Cela permet à la baie de stockage NFS de gérer certaines opérations de stockage à la place des hôtes ESXi.

Avant de commencer

- Téléchargez le "Plug-in NetApp NFS pour VMware VAAI" package d'installation.
- Assurez-vous que vous disposez de l'hôte VMware ESXi et du dernier correctif ou des versions ultérieures de vSphere 7.0U3 et de ONTAP 9.14.1 ou versions ultérieures.
- Monter un datastore NFS.

Étapes

1. Connectez-vous au client vSphere.
2. Sélectionnez **raccourcis** > **Outils NetApp ONTAP** dans la section modules externes.
3. Sélectionnez **Paramètres** > **Outils NFS VAAI**.
4. Si vous avez déjà téléchargé le plug-in VAAI sur vCenter Server, sélectionnez **Modifier** dans **Version existante**. Si vous ne l'avez pas encore fait, sélectionnez **Télécharger**.
5. Parcourez et sélectionnez le `.vib` fichier et sélectionnez **Télécharger** pour télécharger le fichier vers les outils ONTAP.
6. Sélectionnez **installer sur l'hôte ESXI**, sélectionnez l'hôte ESXi sur lequel vous souhaitez installer le plug-in NFS VAAI, puis sélectionnez **installer**.

   Le client Web vSphere affiche uniquement les hôtes ESXi pouvant installer le plug-in. Vous pouvez suivre la progression de l'installation dans la section « Tâches récentes ».

7. Redémarrez l'hôte ESXi manuellement après l'installation.

   Après avoir redémarré l'hôte ESXi, les ONTAP tools for VMware vSphere détectent et activent automatiquement le plug-in NFS VAAI.

Et la suite ?

Après avoir installé le plug-in NFS VAAI et redémarré votre hôte ESXi, configurez les stratégies d'exportation NFS pour le déchargement de copie VAAI. Assurez-vous que les règles de la politique d'exportation répondent à ces exigences :

- Le volume ONTAP concerné autorise les appels NFSv4.
- L'utilisateur root reste root et NFSv4 est autorisé dans tous les volumes parents de jonction.
- L'option de prise en charge VAAI est définie sur le serveur NFS concerné.

Pour plus d'informations, reportez-vous à "Configurez les règles d'exportation NFS appropriées pour le déchargement des copies VAAI" Article de la base de connaissances.

Informations associées

"Prise en charge de VMware vStorage over NFS"

"Activer ou désactiver NFSv4.0"

"Prise en charge de ONTAP pour NFSv4.2"

Configurer les paramètres de l'hôte ESXi dans ONTAP tools

La configuration des paramètres de délai d'expiration et de multi-chemin du serveur ESXi permet de maintenir la disponibilité et l'intégrité des données. Il permet le basculement automatique vers un chemin de stockage de sauvegarde si le chemin principal devient indisponible.

Configurer les paramètres de chemins d'accès multiples et de délai d'attente du serveur ESXi

Les outils ONTAP pour VMware vSphere vérifient et définissent les paramètres des chemins d'accès multiples de l'hôte ESXi ainsi que les paramètres de délai d'expiration de l'adaptateur HBA qui fonctionnent mieux avec les systèmes de stockage NetApp.

Description de la tâche

Ce processus peut prendre du temps, en fonction de votre configuration et de la charge du système. Vous pouvez afficher la progression dans le panneau Tâches récentes.

Étapes

1. Sur la page d'accueil du client Web VMware vSphere, sélectionnez **hosts and clusters**.
2. Sur la page des raccourcis du client Web VMware vSphere, sélectionnez **NetApp ONTAP Tools** dans la section des plug-ins.
3. Accédez à la carte **ESXi Host Compliance** dans la présentation (tableau de bord) du plug-in ONTAP Tools for VMware vSphere.
4. Sélectionnez le lien **appliquer les paramètres recommandés**.
5. Dans la fenêtre **Appliquer les paramètres d'hôte recommandés**, sélectionnez les hôtes que vous souhaitez mettre à jour pour utiliser les paramètres recommandés par NetApp et sélectionnez **Suivant**.

   Vous pouvez développer l'hôte ESXi pour voir les valeurs actuelles.

6. Dans la page des paramètres, sélectionnez les valeurs recommandées.
7. Dans le volet récapitulatif, vérifiez les valeurs et sélectionnez **Terminer**. Vous pouvez suivre la progression dans le panneau des tâches récentes.

Définissez les valeurs de l'hôte ESXi

Utilisez les ONTAP tools for VMware vSphere pour définir des délais d'expiration et d'autres valeurs sur les hôtes ESXi pour des performances et un basculement optimaux. Il définit ces valeurs en fonction des tests NetApp .

Vous pouvez définir les valeurs suivantes sur un hôte ESXi :

Paramètres de l'adaptateur HBA/CNA

Définit les paramètres suivants sur les valeurs par défaut :

- Disk.QFullSampleSize
- Disk.QFullThreshold
- Délais d'expiration de la carte HBA FC Emulex
- Délais de connexion HBA FC QLogic

Paramètres MPIO

Les paramètres MPIO sélectionnent les meilleurs chemins pour les systèmes de stockage NetApp . Les paramètres MPIO sélectionnent le meilleur chemin et l'utilisent.

Pour les environnements hautes performances ou lors de tests avec une seule banque de données LUN, ajustez le paramètre d'équilibrage de charge de la stratégie de sélection de chemin (PSP) à tour de rôle (VMW_PSP_RR) pour améliorer les performances. Définissez la valeur IOPS par défaut de 1 000 à 1.

Les paramètres MPIO ne s'appliquent pas aux protocoles NVMe, NVMe/FC et NVMe/TCP.

Paramètres NFS

Paramètre	Définir cette valeur sur…
Net.TcpipeHeapSize	32
Net.TcpipeHeapMax	1024 MO
NFS.MaxVolumes	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128 ou plus
NFS.HeartbeatMaxFailures	10
NFS.HeartbeatFrequency	12
NFS.HeartbeatTimeout	5

Configurer les rôles et privilèges des utilisateurs ONTAP pour les outils ONTAP

Utilisez cette section pour configurer les rôles et privilèges des utilisateurs ONTAP pour les systèmes de stockage avec les ONTAP tools for VMware vSphere et ONTAP System Manager. Vous pouvez attribuer des rôles à l'aide des fichiers JSON fournis, créer manuellement des utilisateurs et des rôles, et appliquer les privilèges minimaux requis aux comptes non administrateurs.

Avant de commencer

- Téléchargez le fichier ONTAP Privileges à partir des ONTAP tools for VMware vSphere à l'aide de *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip*. Après avoir téléchargé le fichier zip, vous trouverez deux fichiers JSON. Utilisez le fichier JSON spécifique à ASA r2 lors de la configuration d'un système ASA r2.

> Vous pouvez créer des utilisateurs au niveau du cluster ou directement au niveau des machines virtuelles de stockage (SVM). Si vous n'utilisez pas le fichier user_roles.json, assurez-vous que l'utilisateur dispose des autorisations SVM minimales requises.

- Connectez-vous avec les privilèges d'administrateur pour le backend de stockage.

Étapes

1. Extrayez le fichier *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* que vous avez téléchargé.
2. Accédez à ONTAP System Manager à l'aide de l'adresse IP de gestion du cluster.
3. Connectez-vous au cluster avec des privilèges d'administrateur. Pour configurer un utilisateur :
   a. Pour configurer un utilisateur des outils Cluster ONTAP , sélectionnez le volet **Cluster** > **Paramètres** > **Utilisateurs et rôles**.
   b. Pour configurer un utilisateur des outils SVM ONTAP , sélectionnez le volet **Stockage SVM** > **Paramètres** > **Utilisateurs et rôles**.
   c. Sélectionnez **Ajouter** sous utilisateurs.
   d. Dans la boîte de dialogue **Ajouter un utilisateur**, sélectionnez **produits de virtualisation**.
   e. **Parcourir** pour sélectionner et télécharger le fichier JSON des Privileges ONTAP . Pour les systèmes non ASA r2, sélectionnez le fichier users_roles.json et pour les systèmes ASA r2, sélectionnez le fichier users_roles_ASAr2.json.

      Les outils ONTAP remplissent automatiquement le champ Produit.

   f. Sélectionnez la capacité du produit comme **VSC, VASA Provider et SRA** dans la liste déroulante.

      Les outils ONTAP remplissent automatiquement le champ **Rôle** en fonction de la fonctionnalité du produit que vous sélectionnez.

   g. Saisissez le nom d'utilisateur et le mot de passe requis.
   h. Sélectionnez les privilèges (Découverte, Créer un stockage, Modifier un stockage, Détruire un stockage, Rôle NAS/SAN) dont l'utilisateur a besoin, puis sélectionnez **Ajouter**.

Les outils ONTAP ajoutent le nouveau rôle et le nouveau utilisateur. Vous pouvez afficher les privilèges sous le rôle que vous avez configuré.

Exigences de mappage des agrégats du SVM

Lors du provisionnement de banques de données à l'aide des informations d'identification de l'utilisateur SVM, les ONTAP tools for VMware vSphere créent des volumes sur l'agrégat spécifié dans l'API POST des banques de données. ONTAP empêche les utilisateurs SVM de créer des volumes sur des agrégats non mappés au SVM. Mappez le SVM aux agrégats requis à l'aide de l'API REST ONTAP ou de la CLI avant de créer des volumes.

API REST :

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

Interface de ligne de commande ONTAP :

```
sti115_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver        Aggregate      State         Size Type    SnapLock
Type-------------- -------------- ------- ---------- -------
--------------svm_test       sti115_vsim_ucs630f_aggr1
online     10.11GB vmdisk  non-snaplock
```

Créez manuellement un utilisateur et un rôle ONTAP

Créez des utilisateurs et des rôles manuellement sans le fichier JSON.

1. Accédez à ONTAP System Manager à l'aide de l'adresse IP de gestion du cluster.
2. Connectez-vous au cluster avec admin Privileges.
   a. Pour configurer les rôles des outils Cluster ONTAP , sélectionnez **Cluster** > **Paramètres** > **Utilisateurs et rôles**.
   b. Pour configurer les rôles des outils SVM ONTAP du cluster, sélectionnez **Stockage SVM** > **Paramètres** > **Utilisateurs et rôles**.
3. Créer des rôles :
   a. Sélectionnez **Ajouter** dans la table **rôles**.
   b. Entrez les détails **nom de rôle** et **attributs de rôle**.

      Ajoutez le **chemin d'accès à l'API REST** et choisissez l'accès dans la liste déroulante.

   c. Ajoutez toutes les API nécessaires et enregistrez les modifications.
4. Créer des utilisateurs :
   a. Sélectionnez **Ajouter** dans la table **utilisateurs**.
   b. Dans la boîte de dialogue **Ajouter un utilisateur**, sélectionnez **System Manager**.
   c. Entrez le **Nom d'utilisateur**.
   d. Sélectionnez **role** parmi les options créées à l'étape **Create Roles** ci-dessus.
   e. Entrez les applications à laquelle vous souhaitez accorder l'accès et la méthode d'authentification. ONTAPI et HTTP sont les applications requises et le type d'authentification est **Password**.
   f. Définissez le **Mot de passe pour l'utilisateur** et le **Enregistrer** pour l'utilisateur.

Liste des privilèges minimaux requis pour les utilisateurs du cluster dont le périmètre global n'est pas défini sur admin

Cette page répertorie les privilèges minimaux requis pour un utilisateur de cluster global non administrateur sans fichier JSON. Si un cluster est dans la portée locale, utilisez le fichier JSON pour créer des utilisateurs, car les ONTAP tools for VMware vSphere nécessitent plus que de simples privilèges de lecture pour le provisionnement sur ONTAP.

Vous pouvez accéder aux fonctionnalités en utilisant les API :

API	Niveau d'accès	Utilisé pour
/api/cluster	Lecture seule	Découverte de la configuration du cluster
/api/cluster/licences/licences	Lecture seule	Vérification des licences pour les licences spécifiques au protocole
/api/cluster/nœuds	Lecture seule	Découverte du type de plate-forme
/api/sécurité/comptes	Lecture seule	Découverte de privilèges
/api/sécurité/rôles	Lecture seule	Découverte de privilèges
/api/stockage/agrégats	Lecture seule	Vérification de l'espace agrégé lors de l'approvisionnement du magasin de données/volume
/api/stockage/cluster	Lecture seule	Pour obtenir les données d'espace et d'efficacité au niveau du cluster
/api/stockage/disques	Lecture seule	Pour obtenir les disques associés dans un agrégat
/api/stockage/qos/politiques	Lire/Créer/Modifier	Gestion des politiques QoS et VM
/api/svm/svm	Lecture seule	Pour obtenir la configuration SVM lorsque le cluster est ajouté localement.
/api/network/ip/interfaces	Lecture seule	Ajouter un backend de stockage - Pour identifier la portée du LIF de gestion en cluster/SVM
/api/stockage/zones de disponibilité	Lecture seule	Découverte de la SAZ. Applicable aux versions ONTAP 9.16.1 et ultérieures et aux systèmes ASA r2.
/api/cluster/metrocluster	Lecture seule	Obtient l'état et les détails de configuration de MetroCluster .

Créez les outils ONTAP pour l'utilisateur avec périmètre de cluster basé sur l'API VMware vSphere ONTAP

Les privilèges de découverte, de création, de modification et de destruction sont requis pour les opérations PATCH et la restauration automatique sur les banques de données. Les autorisations manquantes peuvent entraîner des problèmes de flux de travail et de nettoyage.

Un utilisateur basé sur l'API ONTAP avec des privilèges de découverte, de création, de modification et de destruction peut gérer les flux de travail des outils ONTAP .

Pour créer un utilisateur avec toutes les Privileges mentionnées ci-dessus, exécuter les commandes suivantes :

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all
```

```
security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all

security login rest-role create -role <role-name> -api /api/storage/luns
-access all

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all

security login rest-role create -role <role-name> -api
/api/storage/qos/policies -access all

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create

security login rest-role create -role <role-name> -api
```

```
/api/storage/file/clone -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify

security login rest-role create -role <role-name> -api /api/cluster
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/licensing/licenses -access readonly

security login rest-role create -role <role-name> -api /api/cluster/nodes
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly
```

```
security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly

security login rest-role create -role <role-name> -api
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/metrocluster -access readonly
```

En outre, pour ONTAP versions 9.16.0 et supérieures, exécutez la commande suivante :

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all
```

Pour les systèmes ASA r2 sous ONTAP versions 9.16.1 et supérieures, exécutez la commande suivante :

```
security login rest-role create -role <role-name> -api
/api/storage/availability-zones -access readonly
```

Créez les outils ONTAP pour l'utilisateur avec périmètre du SVM basé sur l'API VMware vSphere ONTAP

Exécutez les commandes suivantes pour créer un utilisateur de portée SVM avec tous les privilèges :

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
```

```
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/luns
-access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>
```

En outre, pour ONTAP versions 9.16.0 et supérieures, exécutez la commande suivante :

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all -vserver <vserver-name>
```

Pour créer un utilisateur basé sur une API à l'aide des rôles basés sur une API créés ci-dessus, exécutez la commande suivante :

```
security login create -user-or-group-name <user-name> -application http
-authentication-method password -role <role-name> -vserver <cluster-or-
vserver-name>
```

Exemple :

```
security login create -user-or-group-name testvpsraall -application http
-authentication-method password -role
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_sti160-cluster_
```

Exécutez la commande suivante pour déverrouiller le compte et activer l'accès à l'interface de gestion :

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

Exemple :

```
security login unlock -username testvpsraall -vserver C1_sti160-cluster
```

Mise à niveau des outils ONTAP pour VMware vSphere 10.1 utilisateur vers 10.3 utilisateurs

Pour les outils ONTAP pour les utilisateurs de VMware vSphere 10.1 avec un utilisateur dont la portée est définie par le cluster et créé à l'aide du fichier JSON, utilisez les commandes CLI ONTAP suivantes avec Privileges d'administration utilisateur pour effectuer la mise à niveau vers la version 10.3.

Pour les fonctionnalités du produit :

- VSC
- Fournisseur VSC et VASA
- VSC et SRA
- Fournisseur VSC, VASA et SRA.

Cluster Privileges :

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all

Pour les outils ONTAP pour un utilisateur VMware vSphere 10.1 avec un utilisateur dont le périmètre SVM a été créé à l'aide du fichier json, utiliser les commandes de l'interface de ligne de commande ONTAP avec l'utilisateur admin Privileges pour effectuer la mise à niveau vers la version 10.3.

SVM Privileges :

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all -vserver <vserver-name>

Pour activer les commandes suivantes, ajoutez les commandes *vserver nvme namespace show* et *vserver nvme subsystem show* au rôle existant.

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

Mise à niveau des outils ONTAP pour VMware vSphere 10.3 utilisateur vers 10.4 utilisateurs

À partir d' ONTAP 9.16.1, mettez à niveau les ONTAP tools for VMware vSphere 10.3 vers l'utilisateur 10.4.

Pour les outils ONTAP pour un utilisateur VMware vSphere 10.3 avec un utilisateur dont le périmètre de cluster a été créé à l'aide du fichier JSON et de ONTAP version 9.16.1 ou ultérieure, utilisez la commande de ligne de commande ONTAP avec l'utilisateur admin Privileges pour effectuer la mise à niveau vers la version 10.4.

Pour les fonctionnalités du produit :

- VSC
- Fournisseur VSC et VASA
- VSC et SRA
- Fournisseur VSC, VASA et SRA.

Cluster Privileges :

```
security login role create -role <existing-role-name> -cmddirname "storage
availability-zone show" -access all
```

Ajouter un système de stockage dorsal aux ONTAP tools

Utilisez les ONTAP tools for VMware vSphere afin d'ajouter et de gérer les systèmes de stockage pour vos hôtes ESXi. Vous pouvez intégrer des clusters ou des SVM, activer la prise en charge de MetroCluster et valider les certificats pour une connectivité sécurisée. Vous pouvez configurer les systèmes de stockage à l'aide ONTAP Tools Manager ou du client vSphere, surveiller l'état des certificats et redécouvrir manuellement les ressources après des modifications du cluster.

Pour ajouter un système de stockage local, utilisez les informations d'identification du cluster ou de la SVM dans l'interface des outils ONTAP . Les systèmes de stockage local sont disponibles uniquement pour le serveur vCenter sélectionné. Les outils ONTAP mappent les SVM au serveur vCenter pour la gestion des banques de données vVols ou VMFS. Pour les banques de données VMFS et les flux de travail SRA, vous pouvez utiliser les informations d'identification SVM sans mapper un cluster globalement.

Pour ajouter un système de stockage global, utilisez les informations d'identification du cluster ONTAP dans ONTAP Tools Manager. Les systèmes de stockage globaux permettent aux flux de travail de découverte d'identifier les ressources du cluster nécessaires à la gestion des vVol. Dans les environnements mutualisés, vous pouvez ajouter localement un utilisateur SVM pour gérer les banques de données vVols .

Si la prise en charge de MetroCluster est activée dans ONTAP, intégrez les clusters source et de destination en tant que backends de stockage locaux ou globaux.

Avant de commencer

Vérifiez que le certificat inclut un champ Nom alternatif du sujet (SAN) valide. Les systèmes ONTAP utilisent le champ SAN pour identifier les LIF de gestion des clusters et des SVM.

Utilisation du Gestionnaire d'outils ONTAP

Dans une configuration mutualisée, vous pouvez ajouter un cluster back-end de stockage globalement et un SVM localement pour utiliser les identifiants utilisateur de SVM.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **systèmes back-end de stockage** dans la barre latérale.
4. Ajoutez le back-end de stockage et fournissez l'adresse IP ou le nom de domaine complet du serveur, le nom d'utilisateur et le mot de passe.

   Les LIF de gestion d'adresses IPv4 et IPv6 sont prises en charge.

5. Récupérez automatiquement les certificats du cluster ONTAP et autorisez le certificat, ou téléchargez-le manuellement en accédant à son emplacement.

   Si nécessaire, vous pouvez désactiver la validation du nom alternatif du sujet (SAN) à partir de la console de maintenance. Pour les instructions, voir"Modifier l'indicateur de validation du certificat" .

6. Si le backend de stockage que vous ajoutez fait partie d'une configuration MetroCluster , ONTAP Tools Manager affiche un message contextuel pour ajouter le cluster appairé. Sélectionnez **Ajouter** et fournissez les détails du backend de stockage homologue MetroCluster .

   Une fois que le système ONTAP a effectué un basculement et un retour en arrière, exécutez la découverte des outils ONTAP manuellement.

À l'aide de l'interface utilisateur du client vSphere

Les banques de données vVols ne prennent pas en charge l'ajout direct d'un utilisateur SVM via l'interface utilisateur du client vSphere.

1. Connectez-vous au client vSphere.
2. Dans la page raccourcis, sélectionnez **NetApp ONTAP Tools** dans la section modules externes.
3. Sélectionnez **systèmes back-end de stockage** dans la barre latérale.
4. Ajoutez le back-end de stockage et fournissez l'adresse IP du serveur, le nom d'utilisateur, le mot de passe et les détails du port.

   Vous pouvez ajouter un backend de stockage à l'aide d'informations d'identification basées sur un cluster avec des LIF de gestion IPv4 ou IPv6. Pour ajouter directement un utilisateur SVM, fournissez les informations d'identification basées sur SVM ainsi qu'un LIF de gestion SVM. Si un cluster est déjà intégré, vous ne pouvez pas intégrer à nouveau un utilisateur SVM à partir de ce cluster.

5. Récupérez automatiquement les certificats du cluster ONTAP et autorisez le certificat, ou téléchargez-

le manuellement en accédant à son emplacement.

6. Si le backend de stockage ajouté fait partie de la configuration MetroCluster , les outils ONTAP affichent l'écran **Ajouter un homologue MetroCluster *. Sélectionnez *Ajouter un pair** pour ajouter le backend de stockage pair.

> Une fois que le système ONTAP a effectué un basculement et un retour en arrière, exécutez la découverte des outils ONTAP manuellement.

Et la suite ?

Les outils ONTAP mettent à jour la liste pour afficher le nouveau backend de stockage.

Les outils ONTAP répertorient le backend de stockage nouvellement ajouté sur la page **Backends de stockage**. Si un certificat expire dans 30 jours ou moins, les outils ONTAP affichent un avertissement dans la colonne de date d'expiration du certificat. Après expiration, les outils ONTAP marquent le backend de stockage comme inconnu car il ne peut pas se connecter au système de stockage.

Informations associées

"Configuration des clusters dans une configuration MetroCluster"

Associer un système de stockage principal à une instance de serveur vCenter dans ONTAP tools

Associez un backend de stockage à une instance de vCenter Server pour activer l'accès à toutes les instances de vCenter Server. Pour la configuration de MetroCluster , lorsque vous associez un cluster backend de stockage, assurez-vous d'associer également son cluster homologue au vCenter Server.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez vCenter dans la barre latérale.
4. Sélectionnez les points de suspension verticaux en regard de l'instance vCenter Server à laquelle vous souhaitez connecter les backends de stockage.
5. Dans le menu déroulant, choisissez le backend de stockage que vous souhaitez associer à l'instance vCenter Server sélectionnée.

Configurer l'accès réseau dans ONTAP tools

Par défaut, toutes les adresses IP détectées depuis l'hôte ESXi sont automatiquement ajoutées à la stratégie d'exportation, sauf si vous configurez l'accès réseau. Vous pouvez modifier la politique d'exportation pour autoriser l'accès uniquement à partir d'adresses IP spécifiques. Si un hôte ESXi exclu tente une opération de montage, l'opération échoue.

Étapes

1. Connectez-vous au client vSphere.
2. Sélectionnez **NetApp ONTAP Tools** dans la page des raccourcis sous la section des modules externes.
3. Dans le volet gauche des outils ONTAP , accédez à **Paramètres** > **Gérer l'accès au réseau** > **Modifier**.

   Pour ajouter plusieurs adresses IP, séparez la liste par des virgules, une plage, un routage CIDR (Classless Inter-Domain Routing) ou une combinaison des trois.

4. Sélectionnez **Enregistrer**.

Créer un datastore dans ONTAP tools

Lorsque vous créez une banque de données au niveau du cluster hôte, les outils ONTAP la montent sur tous les hôtes de destination et activent l'action uniquement si vous disposez des privilèges requis.

Interopérabilité entre les banques de données natives avec les banques de données gérées par vCenter Server et les outils ONTAP

À partir des ONTAP tools for VMware vSphere 10.4, les outils ONTAP créent des igroups imbriqués pour les banques de données, avec des igroups parents spécifiques aux banques de données et des igroups enfants mappés aux hôtes. Vous pouvez créer des groupes i plats à partir d' ONTAP System Manager et les utiliser pour créer des banques de données VMFS sans utiliser les outils ONTAP . Se référer à "Gérer les initiateurs et les groupes SAN" pour plus d'informations.

Une fois que vous avez intégré le stockage et exécuté la découverte de la banque de données, les outils ONTAP modifient les groupes i plats dans les banques de données VMFS en groupes i imbriqués. Vous ne pouvez pas utiliser d'anciens groupes i plats pour créer de nouveaux magasins de données. Utilisez l'interface des outils ONTAP ou l'API REST pour réutiliser les igroups imbriqués.

Créer un datastore vVols

À partir des ONTAP tools for VMware vSphere 10.3, vous pouvez créer une banque de données vVols sur des systèmes ASA r2 avec une efficacité spatiale telle que thin.vVol. Le fournisseur VASA crée un conteneur et les points de terminaison de protocole souhaités lors de la création de la banque de données vVol. Le fournisseur VASA n'attribue aucun volume de sauvegarde à ce conteneur.

Avant de commencer

- Assurez-vous que les agrégats racines ne sont pas mappés à SVM.
- Assurez-vous que le fournisseur VASA est enregistré avec le vCenter sélectionné.
- Dans le système de stockage ASA r2, le SVM doit être mappé à l'agrégat pour l'utilisateur SVM.

Étapes

1. Connectez-vous au client vSphere.
2. Cliquez avec le bouton droit sur un système hôte, un cluster hôte ou un centre de données et sélectionnez * Outils NetApp ONTAP * > * Créer une banque de données *.
3. Sélectionnez vVols **type de datastore**.
4. Entrez les informations **nom du datastore** et **Protocole**.

   Le système ASA r2 prend en charge les protocoles iSCSI et FC pour les vVols.

5. Sélectionnez la VM de stockage où vous souhaitez créer le datastore.
6. Sous Options avancées :
   - Si vous sélectionnez la **politique d'exportation personnalisée**, assurez-vous d'exécuter la découverte dans vCenter pour tous les objets. Il est recommandé de ne pas utiliser cette option.
   - Vous pouvez sélectionner **Nom du groupe initiateur** personnalisé pour les protocoles iSCSI et FC.

   Dans le type de système de stockage ASA r2 SVM, les unités de stockage (LUN/espace de noms) ne sont pas créées car la banque de données n'est qu'un conteneur logique.

7. Dans le volet **attributs de stockage**, vous pouvez créer de nouveaux volumes ou utiliser les volumes existants. Toutefois, vous ne pouvez pas combiner ces deux types de volumes pour créer un datastore vVols.

   Lors de la création d'un nouveau volume, vous pouvez activer la QoS sur la banque de données. Par défaut, un volume est créé pour chaque demande de création de LUN. Ignorez cette étape pour les banques de données vVols sur les systèmes de stockage ASA r2.

8. Vérifiez votre sélection dans le volet **Résumé** et sélectionnez **Terminer**.

Créer un datastore NFS

Une banque de données NFS connecte les hôtes ESXi au stockage partagé à l'aide du protocole NFS. Ils sont simples et flexibles et sont utilisés dans les environnements VMware vSphere.

Étapes

1. Connectez-vous au client vSphere.

2. Cliquez avec le bouton droit sur un système hôte, un cluster hôte ou un centre de données et sélectionnez * Outils NetApp ONTAP * > * Créer une banque de données *.
3. Sélectionnez NFS dans le champ **type de datastore**.
4. Entrez le nom, la taille et les informations de protocole du datastore dans le volet **Nom et protocole**. Sélectionnez **datastore cluster** et **Kerberos Authentication** dans les options avancées.

   L'authentification Kerberos n'est disponible que lorsque le protocole NFS 4.1 est sélectionné.

5. Sélectionnez **Platform** et **Storage VM** dans le volet **Storage**.
6. Si vous sélectionnez **Politique d'exportation personnalisée** sous les options avancées, exécutez la découverte dans vCenter pour tous les objets. Il est recommandé de ne pas utiliser cette option.

   Vous ne pouvez pas créer une banque de données NFS à l'aide de la stratégie de volume racine ou par défaut de la SVM.

   - Dans les options avancées, le bouton bascule **asymétrique** n'est visible que si la performance ou la capacité est sélectionnée dans la liste déroulante plate-forme.
   - Lorsque vous choisissez l'option **Tout** dans la liste déroulante de la plate-forme, vous pouvez voir tous les SVM dans vCenter. La plate-forme et le drapeau asymétrique n'affectent pas la visibilité.
7. Sélectionnez l'agrégat pour la création du volume dans le volet **Storage Attributes**. Dans les options avancées, choisissez **Réserve d'espace** et **Activer QoS** selon les besoins.
8. Vérifiez les sélections dans le volet **Résumé** et sélectionnez **Terminer**.

Les outils ONTAP créent le magasin de données NFS et le montent sur tous les hôtes.

Créer un datastore VMFS

VMFS est un système de fichiers en cluster pour stocker les fichiers de machines virtuelles. Plusieurs hôtes ESXi peuvent accéder simultanément aux mêmes fichiers VM pour les fonctionnalités vMotion et haute disponibilité.

Sur un cluster protégé :

- Vous ne pouvez créer que des banques de données VMFS. L'ajout d'une banque de données VMFS à un cluster protégé le protège automatiquement.
- Vous ne pouvez pas créer de datastore sur un data Center avec un ou plusieurs clusters hôtes protégés.
- Vous ne pouvez pas créer de banque de données sur un hôte ESXi si le cluster d'hôte parent est protégé par une « stratégie de duplex de basculement automatisé » (configuration uniforme ou non uniforme).
- Vous pouvez créer un datastore VMFS uniquement sur un hôte ESXi protégé par une relation asynchrone. Vous ne pouvez pas créer et monter un datastore sur un hôte ESXi faisant partie d'un cluster hôte protégé par la règle « Automated Failover Duplex ».

Avant de commencer

- Activez les services et les LIF pour chaque protocole côté stockage ONTAP.
- Mapper SVM à l'agrégat pour l'utilisateur SVM dans le système de stockage ASA r2
- Configurez l'hôte ESXi si vous utilisez le protocole NVMe/TCP :

a. Examinez le "Guide de compatibilité VMware"

> VMware vSphere 7.0 U3 et versions ultérieures prennent en charge le protocole NVMe/TCP. Toutefois, VMware vSphere 8.0 et versions ultérieures sont recommandés.

b. Vérifiez si le fournisseur de la carte d'interface réseau (NIC) prend en charge la carte réseau ESXi avec le protocole NVMe/TCP.

c. Configurez la carte réseau ESXi pour NVMe/TCP conformément aux spécifications du fournisseur de la carte réseau.

d. Si vous utilisez VMware vSphere 7, suivez les instructions qui s'affichent sur le site VMware "Configurez la liaison VMkernel pour l'adaptateur NVMe over TCP" pour configurer la liaison du port NVMe/TCP. Si vous utilisez VMware vSphere 8, suivez "Configuration de NVMe over TCP sur ESXi"la procédure pour configurer la liaison du port NVMe/TCP.

e. Pour VMware vSphere 7, suivez les instructions à la page "Activez NVMe over RDMA ou les adaptateurs logiciels NVMe over TCP" pour configurer les adaptateurs logiciels NVMe/TCP. Pour la version VMware vSphere 8, reportez-vous à la section "Ajout de NVMe over RDMA Software ou de NVMe over TCP Adapters" pour configurer les adaptateurs logiciels NVMe/TCP.

f. Exécutez "Découverte des systèmes et des hôtes de stockage" l'action sur l'hôte ESXi. Pour plus d'informations, reportez-vous "Comment configurer NVMe/TCP avec vSphere 8.0 Update 1 et ONTAP 9.13.1 pour les datastores VMFS"à .

- Si vous utilisez le protocole NVME/FC, procédez comme suit pour configurer l'hôte ESXi :

a. Si ce n'est pas déjà fait, activez NVMe over Fabrics (NVMe-of) sur vos hôtes ESXi.

b. Segmentation SCSI complète.

c. Assurez-vous que les hôtes ESXi et le système ONTAP sont connectés au niveau d'une couche physique et logique.

Pour configurer un SVM ONTAP pour le protocole FC, reportez-vous à "Configuration d'un SVM pour FC"la .

Pour plus d'informations sur l'utilisation du protocole NVMe/FC avec VMware vSphere 8.0, reportez-vous à "Configuration d'hôte NVMe-of pour ESXi 8.x avec ONTAP"la .

Pour plus d'informations sur l'utilisation de NVMe/FC avec VMware vSphere 7.0, reportez-vous aux sections "Guide de configuration d'hôte NVMe/FC de ONTAP" et "TR-4684".

Étapes

1. Connectez-vous au client vSphere.
2. Cliquez avec le bouton droit sur un système hôte, un cluster hôte ou un centre de données et sélectionnez * Outils NetApp ONTAP * > * Créer une banque de données *.
3. Sélectionnez le type de datastore VMFS.
4. Saisissez le nom, la taille et les informations de protocole du magasin de données dans le volet **Nom et protocole**. Pour ajouter le nouveau magasin de données à un cluster VMFS existant, sélectionnez le cluster de magasin de données dans les Options avancées.
5. Sélectionnez Storage VM dans le volet **Storage**. Indiquez le **Nom du groupe d'initiateurs personnalisé** dans la section **Options avancées**, si nécessaire. Vous pouvez choisir un groupe initiateur existant pour le datastore ou créer un nouveau groupe initiateur avec un nom personnalisé.

Lorsque le protocole NVMe/FC ou NVMe/TCP est sélectionné, un nouveau sous-système d'espace de noms est créé et utilisé pour le mappage d'espace de noms. Les outils ONTAP créent le sous-système d'espace de noms à l'aide du nom généré automatiquement qui inclut le nom de la banque de données. Vous pouvez renommer le sous-système d'espace de noms dans le champ **nom du sous-système d'espace de noms personnalisé** dans les options avancées du volet **Stockage**.

6. Dans le volet **Storage Attributes** :

   a. Sélectionnez **aggregate** dans les options de la liste déroulante.

   Pour les systèmes de stockage ASA r2, l'option **Aggregate** n'est pas affichée car le stockage est désagrégé. Lorsque vous choisissez un système de stockage ASA r2 de type SVM, la page des attributs de stockage affiche les options d'activation de la qualité de service.

   b. Les outils ONTAP créent une unité de stockage (LUN/Namespace) avec une réserve d'espace mince en fonction du protocole sélectionné.

   À partir de ONTAP 9.16.1, les systèmes de stockage ASA r2 prennent en charge jusqu'à 12 nœuds par cluster.

   c. Sélectionner le **niveau de service Performance** pour les systèmes de stockage ASA r2 avec un SVM à 12 nœuds qui est un cluster hétérogène. Cette option n'est pas disponible si le SVM sélectionné est un cluster homogène ou utilise un utilisateur SVM.

   'Any' est la valeur par défaut du niveau de service de performance (PSL). Ce paramètre crée l'unité de stockage à l'aide de l'algorithme de placement équilibré ONTAP. Toutefois, vous pouvez sélectionner l'option performance ou Extreme selon vos besoins.

   d. Sélectionnez **utiliser le volume existant**, **Activer les options QoS** selon les besoins et fournissez les détails.

   Dans le type de stockage ASA r2, la création ou la sélection de volume ne s'applique pas à la création d'unité de stockage (LUN/espace de noms). Par conséquent, ces options ne sont pas affichées.

   Vous ne pouvez pas utiliser le volume existant pour créer une banque de données VMFS avec le protocole NVMe/FC ou NVMe/TCP. Créez un nouveau volume pour la banque de données VMFS.

7. Vérifiez les détails du datastore dans le volet **Summary** et sélectionnez **Finish**.

   Si vous créez le datastore sur un cluster protégé, un message en lecture seule s'affiche : « le datastore est en cours de montage sur un cluster protégé ».

Résultat

Les outils ONTAP créent le magasin de données VMFS et le montent sur tous les hôtes.

Protection des datastores et des machines virtuelles

Protéger un cluster hôte dans ONTAP tools

Les outils ONTAP pour VMware vSphere gèrent la protection des clusters hôtes. Tous les datastores appartenant au SVM sélectionné et montés sur un ou plusieurs hôtes du cluster sont protégés sous un cluster hôte.

Avant de commencer

Assurez-vous de répondre à ces exigences avant de protéger un cluster hôte :

- Le cluster hôte contient des banques de données provenant d'une seule SVM uniquement.
- Les banques de données sur le cluster hôte ne sont pas montées sur des hôtes extérieurs au cluster.
- Les banques de données montées sur le cluster hôte sont des banques de données VMFS avec protocole iSCSI ou FC. Vous ne pouvez pas utiliser les banques de données vVols, NFS ou VMFS avec les protocoles NVMe/FC et NVMe/TCP.
- Les banques de données basées sur des volumes FlexVol/LUN montés sur un hôte ne font partie d'aucun groupe de cohérence.
- Les banques de données basées sur des volumes FlexVol/LUN montés sur un hôte ne font partie d'aucune relation SnapMirror .
- Le cluster hôte contient au moins une banque de données.

Étapes

1. Connectez-vous au client vSphere.
2. Cliquez avec le bouton droit sur un cluster hôte et sélectionnez * Outils NetApp ONTAP * > * Protéger le cluster *.
3. Dans la fenêtre de protection du cluster, le système renseigne automatiquement le type de banque de données et les détails de la machine virtuelle (VM) de stockage source. Sélectionnez le lien des magasins de données pour afficher les magasins de données protégés.
4. Sélectionnez **Ajouter une relation**.
5. Dans la fenêtre **Ajouter une relation SnapMirror**, sélectionnez **VM de stockage cible** et le type **Stratégie**.

   Le type de règle peut être asynchrone ou automatique FailOverDuplex.

   Lorsque vous ajoutez la relation SnapMirror en tant que stratégie de type AutomatedFailOverDuplex, vous devez ajouter la machine virtuelle de stockage cible en tant que back-end de stockage au serveur vCenter sur lequel les outils ONTAP pour VMware vSphere sont déployés.

   Dans le type de stratégie AutomatedFailOverDuplex, il existe des configurations d'hôte uniformes et non uniformes. Lorsque vous sélectionnez le bouton bascule **configuration uniforme de l'hôte**, la configuration du groupe d'initiateurs de l'hôte est implicitement répliquée sur le site cible. Pour plus d'informations, reportez-vous à "Concepts et termes clés" .

6. Si vous choisissez d'avoir une configuration hôte non uniforme, sélectionnez l'accès hôte (source/cible) pour chaque hôte à l'intérieur de ce cluster.

7. Sélectionnez **Ajouter**.
8. Vous pouvez modifier la protection du cluster hôte à l'aide de l'opération **Modifier la protection du cluster hôte**. Vous pouvez modifier ou supprimer les relations à l'aide des options du menu à points de suspension.
9. Sélectionnez le bouton **protéger**.

   Le système crée une tâche vCenter avec les détails de l'ID de tâche et affiche sa progression dans le panneau des tâches récentes. Il s'agit d'une tâche asynchrone ; l'interface utilisateur affiche uniquement l'état de soumission de la demande et n'attend pas la fin de la tâche.

10. Pour afficher les clusters d'hôtes protégés, accédez à * Outils NetApp ONTAP * > **Protection** > **Relations entre les clusters d'hôtes**. Sélectionnez un groupe de cohérence pour afficher sa capacité, les banques de données associées et les groupes de cohérence enfants.

> Si vous devez supprimer la protection dans l'heure suivant sa création, exécutez d'abord la découverte de stockage.

Informations associées

"Cluster de stockage VMware vSphere Metro (vMSC)"

Protégez à l'aide de la protection SRA

Configurez SRA dans ONTAP tools pour protéger les banques de données

Les outils ONTAP pour VMware vSphere permettent d'activer la fonctionnalité SRA pour configurer la reprise après incident.

Avant de commencer

- Vous devez avoir configuré votre instance vCenter Server et votre hôte ESXi.
- Vous devez avoir déployé des outils ONTAP pour VMware vSphere.
- Vous devez avoir téléchargé le `.tar.gz` fichier de l'adaptateur SRA à partir du "Site de support NetApp".
- Vous devez disposer des mêmes planifications SnapMirror personnalisées sur les clusters ONTAP source et de destination avant d'exécuter les workflows SRA.
- "Activez les outils ONTAP pour les services VMware vSphere" pour activer la capacité SRA.

Étapes

1. Connectez-vous à l'interface de gestion de l'appliance VMware Live site Recovery à l'aide de `https://:<srm_ip>:5480` l'URL :, puis accédez à Storage Replication Adapters dans l'interface de gestion de l'appliance VMware VMware Live site Recovery.
2. Sélectionnez **nouvel adaptateur**.
3. Téléchargez le programme d'installation *.tar.gz* du plug-in SRA vers VMware Live site Recovery.
4. Relancez la recherche des adaptateurs pour vérifier que les détails sont mis à jour sur la page adaptateurs de réplication de stockage de VMware Live site Recovery.

> Après un basculement, des actions telles que l'extension, le montage et la suppression peuvent ne pas être disponibles pour les banques de données. Effectuez la découverte du magasin de données pour actualiser et afficher les actions du menu contextuel appropriées.

Après chaque opération de reprotection, vous devez effectuer une découverte de stockage sur les deux sites.

Dans une nouvelle configuration avec protection SRA, exécutez toujours un test de basculement. L'omission du test de basculement peut entraîner l'échec de l'opération de reprotection.

Dans une configuration de distribution, après un basculement de SnapMirror Active Sync où la source SnapMirror passe au site B pour le basculement automatique duplex et SnapMirror asynchrone, exécutez un basculement de test entre les sites B et C. L'omission de cette étape peut entraîner l'échec d'une opération de reprotection.

Informations associées

"Configurer la reprise après sinistre pour les banques de données NFS à l'aide de VMware Site Recovery Manager"

Configurer SRA dans ONTAP tools for VMware vSphere pour les environnements SAN et NAS

Vous devez configurer les systèmes de stockage avant d'exécuter Storage Replication adapter (SRA) pour VMware Live site Recovery.

Configurez SRA pour les environnements SAN

Avant de commencer

Les programmes suivants doivent être installés sur le site protégé et le site de reprise :

- VMware Live Site Recovery : le site VMware fournit une documentation d'installation pour VMware Live Site Recovery.

  "À propos de VMware Live site Recovery"

- SRA : installez l'adaptateur sur VMware Live Site Recovery.

Étapes

1. Vérifiez que les hôtes ESXi principaux sont connectés aux LUN du système de stockage principal du site protégé.
2. Vérifiez que LES LUN sont dans des igroups qui ont `ostype` Option définie sur *VMware* sur le système de stockage principal.
3. Vérifiez que les hôtes ESXi sur le site de récupération disposent d'une connectivité iSCSI et Fibre Channel appropriée à la machine virtuelle de stockage (SVM). Les hôtes ESXi du site secondaire doivent avoir accès au stockage du site secondaire et les hôtes ESXi du site principal doivent avoir accès au stockage du site principal.

   Vous pouvez le faire en vérifiant que les hôtes ESXi disposent de LUN locales connectées au SVM ou au `iscsi show initiators` Commande sur les SVM.
   Vérifiez l'accès aux LUN mappées sur l'hôte ESXi pour vérifier la connectivité iSCSI.

Configurez SRA pour les environnements NAS

Avant de commencer

Les programmes suivants doivent être installés sur le site protégé et le site de reprise :

- VMware Live Site Recovery : vous pouvez trouver la documentation d'installation de VMware Live Site Recovery sur le site VMware - "À propos de VMware Live site Recovery"
- SRA : installez l'adaptateur sur VMware Live Site Recovery et le serveur SRA.

Étapes

1. Vérifiez que les datastores du site protégé contiennent des machines virtuelles enregistrées auprès de vCenter Server.
2. Vérifier que les hôtes ESXi du site protégé ont monté les volumes NFS exportés depuis la machine virtuelle de stockage (SVM).
3. Vérifiez que des adresses valides, telles que l'adresse IP ou le nom de domaine complet (FQDN) sur lesquels les exportations NFS sont présentes, sont spécifiées dans le champ « Adresses NFS » lorsque vous utilisez l'assistant Gestionnaire de baies pour ajouter des baies à VMware Live Site Recovery. N'utilisez pas le nom d'hôte NFS dans le champ « Adresses NFS ».
4. Utilisez le `ping` Commande sur chaque hôte ESXi du site de reprise pour vérifier que l'hôte dispose d'un port VMkernel qui peut accéder aux adresses IP utilisées pour servir les exportations NFS à partir du SVM.

Configurer SRA dans ONTAP tools pour les environnements à grande échelle

Vous devez configurer les intervalles de délai d'expiration du stockage conformément aux paramètres recommandés pour Storage Replication adapter (SRA) afin de garantir des performances optimales dans des environnements hautement évolutifs.

Paramètres du fournisseur de stockage

Vous devez définir les valeurs de temporisation suivantes sur VMware Live site Recovery pour un environnement évolutif :

Paramètres avancés	Valeurs de temporisation
`StorageProvider.resignatureTimeout`	Augmentez la valeur du réglage de 900 à 12000 secondes.
`storageProvider.hostRescanDelaySec`	60
`storageProvider.hostRescanRepeatCnt`	20
`storageProvider.hostRescanTimeoutSec`	Définir une valeur élevée (par exemple : 99999)

Vous devez également activer le `StorageProvider.autoResignatureMode` option.

Pour plus d'informations sur la modification des paramètres du fournisseur de stockage, reportez-vous à la section "Modifier les paramètres du fournisseur de stockage".

Paramètres de stockage

Lorsque vous appuyez sur une temporisation, augmentez les valeurs de `storage.commandTimeout` et `storage.maxConcurrentCommandCnt` à une valeur supérieure.

L'intervalle de délai d'expiration spécifié est la valeur maximale. Vous n'avez pas besoin d'attendre que le délai d'expiration maximal soit atteint. La plupart des commandes se terminent dans l'intervalle de délai d'expiration maximal défini.

Pour modifier les paramètres du fournisseur SAN, reportez-vous à la section "Modifier les paramètres de stockage".

Configurez SRA sur l'appliance VMware Live Site Recovery à l'aide des ONTAP tools.

Après avoir déployé le dispositif VMware Live Site Recovery, configurez l'adaptateur de réplication de stockage (SRA) pour activer la gestion de la reprise après sinistre.

La configuration de SRA sur l'appliance VMware Live Site Recovery enregistre les ONTAP tools for VMware vSphere au sein de l'appliance, permettant ainsi la communication entre VMware Live Site Recovery et SRA.

Avant de commencer

- Téléchargez le fichier *.tar.gz* depuis le "Site de support NetApp" .
- Activez les services SRA dans le gestionnaire d'outils ONTAP . Pour plus d'informations, consultez le "Activer les services" section.
- Ajoutez des serveurs vCenter aux outils ONTATP pour l'appliance VMware vSphere. Pour plus d'informations, consultez le "Ajouter des serveurs vCenter" section.
- Ajoutez des backends de stockage aux ONTAP tools for VMware vSphere. Pour plus d'informations, consultez le "Ajouter des backends de stockage" section.

Si vous avez appliqué le correctif de certificat vCenter à partir des outils ONTAP , mettez à jour la configuration vCenter dans le dispositif VMware Live Site Recovery à l'aide du port (:5480). Pour les instructions, reportez-vous à "Reconfigurer l'appliance Site Recovery Manager" .

Étapes

1. Sur l'écran de l'appliance VMware Live site Recovery, sélectionnez **Storage Replication adapter** > **New adapter**.
2. Chargez le fichier *.tar.gz* dans VMware Live site Recovery.
3. Connectez-vous au dispositif VMware Live Site Recovery à l'aide d'un compte administrateur via un client SSH tel que PuTTY.
4. Basculer vers l'utilisateur root à l'aide de la commande : `su root`
5. Exécutez la commande `cd /var/log/vmware/srm` pour accéder au répertoire des journaux.
6. À l'emplacement du journal, entrez la commande pour obtenir l'ID Docker utilisé par SRA : `docker ps -l`
7. Pour vous connecter à l'ID de conteneur, entrez la commande : `docker exec -it -u srm <container id> sh`
8. Configurez VMware Live Site Recovery avec les ONTAP tools for VMware vSphere à l'aide de la commande : `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
   - Fournissez le mot de passe entre guillemets simples afin que le script Perl traite les caractères spéciaux comme faisant partie du mot de passe, et non comme des délimiteurs.

- Vous pouvez définir le nom d'utilisateur et le mot de passe de l'application (fournisseur VASA/SRA) dans ONTAP Tools Manager lors de la première activation de ces services. Utilisez ces informations d'identification pour enregistrer SRA auprès de VMware Live Site Recovery.
- Pour localiser le GUID vCenter, accédez à la page vCenter Server dans ONTAP Tools Manager après avoir ajouté votre instance vCenter. Se référer à"Ajouter des serveurs vCenter" section.

9. Analysez à nouveau les adaptateurs pour confirmer que les détails mis à jour apparaissent sur la page Adaptateurs de réplication de stockage VMware Live Site Recovery.

Résultats Un message de confirmation apparaît indiquant que les informations d'identification de stockage ont été enregistrées. Vous pouvez désormais utiliser SRA pour communiquer avec le serveur SRA à l'aide de l'adresse IP, du port et des informations d'identification spécifiés.

Mettre à jour les informations d'identification SRA dans ONTAP tools

Pour que VMware Live site Recovery puisse communiquer avec SRA, vous devez mettre à jour les informations d'identification SRA sur le serveur VMware Live site Recovery si vous avez modifié les informations d'identification.

Avant de commencer

Vous devez avoir exécuté les étapes mentionnées dans la rubrique "Configuration de SRA sur l'appliance VMware Live site Recovery".

Étapes

1. Exécutez les commandes suivantes pour supprimer le dossier de la machine de restauration de site direct VMware Outils ONTAP mis en cache nom d'utilisateur mot de passe :
   a. `sudo su <enter root password>`
   b. `docker ps`
   c. `docker exec -it <container_id> sh`
   d. `cd conf/`
   e. `rm -rf *`
2. Exécutez la commande Perl pour configurer SRA avec les nouvelles informations d'identification :
   a. `cd ..`
   b. `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>` Vous devez avoir un devis unique autour de la valeur du mot de passe.

      Un message de confirmation de la mémorisation des identifiants de stockage s'affiche. SRA peut communiquer avec le serveur SRA à l'aide de l'adresse IP, du port et des informations d'identification fournis.

Configurer les sites protégés et de récupération dans ONTAP tools

Vous devez créer des groupes de protection pour protéger un groupe de machines virtuelles sur le site protégé.

Lorsque vous ajoutez une nouvelle banque de données, vous pouvez l'inclure dans le groupe de banques de

données existant ou en ajouter une nouvelle et créer un volume ou un groupe de cohérence à protéger. Après avoir ajouté une nouvelle banque de données à un groupe de cohérence ou à un volume protégé, mettez à jour SnapMirror et effectuez la découverte du stockage sur les sites protégé et de récupération. Vous pouvez exécuter la découverte manuellement ou selon un calendrier pour garantir la détection et la protection de la nouvelle banque de données.

Protection par paires et sites de reprise après incident

Vous devez coupler les sites protégés et de reprise créés à l'aide de votre client vSphere pour permettre à Storage Replication adapter (SRA) de détecter les systèmes de stockage.

> L'adaptateur de réplication de stockage (SRA) prend en charge la distribution avec une relation de synchronisation de type Duplex de basculement automatisé et une relation asynchrone SnapMirror sur le groupe de cohérence. Cependant, la distribution en éventail avec deux SnapMirror asynchrones sur un groupe de cohérence ou la distribution en éventail avec deux SnapMirrors sur un volume n'est pas prise en charge. Les relations SnapMirror de type Vault ne sont pas prises en compte dans ces restrictions de diffusion.

Avant de commencer

- VMware Live site Recovery doit être installé sur les sites protégés et de reprise.
- SRA doit être installée sur les sites protégés et de reprise.

Étapes

1. Sur la page d'accueil de vSphere Client, double-cliquez sur l'icône **Site Recovery**, puis sélectionnez **Sites**.
2. Sélectionnez **objets** > **actions** > **associer sites**.
3. Dans la boîte de dialogue **pair site Recovery Manager Servers**, entrez l'adresse du Platform Services Controller du site protégé, puis sélectionnez **Next**.
4. Dans la section Select vCenter Server, procédez comme suit :
   a. Vérifiez que le serveur vCenter du site protégé apparaît comme candidat correspondant au couplage.
   b. Entrez les informations d'identification d'administration SSO, puis sélectionnez **Terminer**.
5. Si vous y êtes invité, sélectionnez **Oui** pour accepter les certificats de sécurité.

Résultat

La boîte de dialogue **Objets** affiche les sites protégés et de récupération.

Configuration des groupes de protection

Avant de commencer

Vous devez vous assurer que les sites source et cible sont configurés pour les sites suivants :

- La même version de VMware Live site Recovery est installée
- Ordinateurs virtuels
- Sites protégés et de reprise par paires
- Les datastores source et de destination doivent être montés sur les sites respectifs

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **Site Recovery** > **Groupes de protection**.
2. Dans le volet **groupes de protection**, sélectionnez **Nouveau**.

3. Spécifiez un nom et une description pour le groupe de protection, Direction et sélectionnez **Suivant**.
4. Dans le champ **Type**, sélectionnez l'option **Type** comme groupes de banques de données (réplication basée sur une baie) pour les banques de données NFS et VMFS. Le domaine d'erreur ne comprend que les SVM avec réplication activée. Les SVM pour lesquelles seul le peering est implémenté et qui ne présentent aucun problème sont affichées.
5. Dans l'onglet Replication Groups, sélectionnez la paire de matrices activée ou les groupes de réplication sur lesquels la machine virtuelle est configurée, puis sélectionnez **Next**.

   Toutes les machines virtuelles du groupe de réplication sont ajoutées au groupe de protection.
6. Vous pouvez sélectionner le plan de récupération existant ou en créer un nouveau en sélectionnant **Ajouter au nouveau plan de récupération**.
7. Dans l'onglet prêt à terminer, vérifiez les détails du groupe de protection que vous avez créé, puis sélectionnez **Terminer**.

Configuration des ressources protégées et du site de reprise

Configurer les mappages réseau dans ONTAP tools

Vous devez configurer vos mappages de ressources tels que les réseaux de machines virtuelles, les hôtes ESXi et les dossiers sur les deux sites afin de pouvoir mapper chaque ressource du site protégé à la ressource appropriée sur le site de reprise.

Vous devez effectuer les configurations de ressources suivantes :

- Mappages de réseau
- Mappages de dossiers
- Mappages de ressources
- Datastores à espace réservé

Avant de commencer

Vous devez avoir connecté les sites protégés et de reprise.

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **site Recovery** > **sites**.
2. Sélectionnez votre site protégé et sélectionnez **gérer**.
3. Sélectionnez **mappages réseau** > **Nouveau** dans l'onglet gérer pour créer un nouveau mappage réseau.
4. Dans l'assistant Créer un mappage réseau, procédez comme suit :
   a. Sélectionnez **préparer automatiquement les mappages pour les réseaux avec des noms correspondants** et sélectionnez **Suivant**.
   b. Sélectionnez les objets de centre de données requis pour les sites protégés et de récupération, puis sélectionnez **Ajouter des mappages**.
   c. Sélectionnez **Suivant** une fois les mappages créés.
   d. Sélectionnez l'objet utilisé précédemment pour créer le mappage inverse, puis sélectionnez **Terminer**.

Résultat

La page Network mappings affiche les ressources du site protégé et les ressources du site de reprise. Vous

pouvez suivre les mêmes étapes pour les autres réseaux de votre environnement.

Configurer les mappages de dossiers dans ONTAP tools

Vous devez mapper vos dossiers sur le site protégé et le site de reprise pour permettre la communication entre eux.

Avant de commencer

Vous devez avoir connecté les sites protégés et de reprise.

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **site Recovery** > **sites**.
2. Sélectionnez votre site protégé et sélectionnez **gérer**.
3. Sélectionnez **mappages de dossiers** > icône **dossier** dans l'onglet gérer pour créer un nouveau mappage de dossiers.
4. Dans l'assistant Créer un mappage de dossier, effectuez les opérations suivantes :
   a. Sélectionnez **préparer automatiquement les mappages pour les dossiers avec des noms correspondants** et sélectionnez **Suivant**.
   b. Sélectionnez les objets de centre de données requis pour les sites protégés et de récupération, puis sélectionnez **Ajouter des mappages**.
   c. Sélectionnez **Suivant** une fois les mappages créés.
   d. Sélectionnez l'objet utilisé précédemment pour créer le mappage inverse, puis sélectionnez **Terminer**.

Résultat

La page mappages des dossiers affiche les ressources du site protégé et les ressources du site de reprise. Vous pouvez suivre les mêmes étapes pour les autres réseaux de votre environnement.

Configurer les mappages de ressources dans ONTAP tools

Vous devez mapper vos ressources sur le site protégé et le site de reprise de manière à ce que les machines virtuelles soient configurées pour basculer vers un groupe d'hôtes ou vers un autre.

Avant de commencer

Vous devez avoir connecté les sites protégés et de reprise.

> Dans VMware Live site Recovery, les ressources peuvent être des pools de ressources, des hôtes ESXi ou des clusters vSphere.

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **site Recovery** > **sites**.
2. Sélectionnez votre site protégé et sélectionnez **gérer**.
3. Sélectionnez **mappages de ressources** > **Nouveau** dans l'onglet gérer pour créer un mappage de ressources.
4. Dans l'assistant Créer un mappage de ressources, effectuez les opérations suivantes :
   a. Sélectionnez **préparer automatiquement les mappages pour la ressource avec les noms correspondants** et sélectionnez **Suivant**.

b. Sélectionnez les objets de centre de données requis pour les sites protégés et de récupération, puis sélectionnez **Ajouter des mappages**.

c. Sélectionnez **Suivant** une fois les mappages créés.

d. Sélectionnez l'objet utilisé précédemment pour créer le mappage inverse, puis sélectionnez **Terminer**.

Résultat

La page mappages des ressources affiche les ressources protégées du site et les ressources du site de reprise. Vous pouvez suivre les mêmes étapes pour les autres réseaux de votre environnement.

Configurer les magasins de données de substitution dans ONTAP tools

Configurez une banque de données d'espace réservé pour réserver de l'espace dans l'inventaire vCenter sur le site de récupération pour les machines virtuelles (VM) protégées. Les magasins de données d'espace réservé nécessitent une capacité minimale, car les machines virtuelles d'espace réservé sont petites et n'utilisent généralement que quelques centaines de kilo-octets.

Avant de commencer

- Assurez-vous que les sites protégés et de récupération sont connectés.
- Vérifiez que les mappages de ressources ont été configurés.

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **site Recovery** > **sites**.
2. Sélectionnez votre site protégé et sélectionnez **gérer**.
3. Sélectionnez **Placeholder datastores** > **New** dans l'onglet gérer pour créer un nouveau datastore de marque de réservation.
4. Sélectionnez le datastore approprié et sélectionnez **OK**.

> Les magasins de données d'espace réservé peuvent résider sur un stockage local ou distant, mais ils ne nécessitent pas de réplication.

5. Répétez les étapes 3 à 5 pour configurer un datastore de marque de réservation pour le site de reprise.

Configurez SRA à l'aide du gestionnaire de baies dans ONTAP tools

Vous pouvez configurer Storage Replication adapter (SRA) à l'aide de l'assistant Array Manager de VMware Live site Recovery pour activer les interactions entre VMware Live site Recovery et les machines virtuelles de stockage (SVM).

Avant de commencer

- Vous devez avoir couplé les sites protégés et les sites de reprise dans VMware Live site Recovery.
- Vous devez avoir configuré votre stockage intégré avant de configurer le gestionnaire de baie.
- Vous devez avoir configuré et répliqué les relations SnapMirror entre les sites protégés et les sites de reprise.
- Vous devez avoir activé les LIF de gestion du SVM pour permettre la colocation.

SRA prend en charge la gestion au niveau du cluster et de la SVM. Si vous ajoutez du stockage au niveau du

cluster, vous pouvez détecter et exécuter des opérations sur tous les SVM du cluster. Si vous ajoutez du stockage au niveau d'un SVM, vous ne pouvez gérer que ce SVM spécifique.

Étapes

1. Dans VMware Live site Recovery, sélectionnez **Array Managers** > **Add Array Manager**.
2. Entrez les informations suivantes pour décrire la baie dans VMware Live site Recovery :

   a. Entrez un nom pour identifier le gestionnaire de matrice dans le champ **Nom d'affichage**.

   b. Dans le champ **SRA Type**, sélectionnez **NetApp Storage Replication adapter pour ONTAP**.

   c. Entrer les informations pour se connecter au cluster ou au SVM :

      - Si vous vous connectez à un cluster, vous devez saisir le LIF de gestion du cluster.
      - Si vous vous connectez directement à un SVM, vous devez saisir l'adresse IP du LIF de gestion du SVM.

      Lors de la configuration du gestionnaire de baies, vous devez utiliser la même connexion (adresse IP) pour le système de stockage utilisé pour intégrer le système de stockage dans les outils ONTAP pour VMware vSphere. Par exemple, si la configuration de Array Manager est étendue au SVM, le stockage sous ONTAP Tools for VMware vSphere doit être ajouté au niveau du SVM.

   d. Si vous vous connectez à un cluster, spécifiez le nom de la SVM dans le champ **Nom de la SVM** ou laissez-le vide pour gérer toutes les SVM du cluster.

   e. Entrez les volumes à découvrir dans le champ **liste d'inclure le volume**.

      Vous pouvez saisir le volume source sur le site protégé et le volume de destination répliqué sur le site de reprise.

      Par exemple, si vous voulez découvrir le volume src_vol1 qui se trouve dans une relation SnapMirror avec le volume dst_vol1, vous devez spécifier src_vol1 dans le champ site protégé et dst_vol1 dans le champ site de reprise.

   f. **(Facultatif)** Entrez les volumes à exclure de la découverte dans le champ **liste d'exclusion de volume**.

      Vous pouvez saisir le volume source sur le site protégé et le volume de destination répliqué sur le site de reprise.

   Par exemple, si vous voulez exclure le volume *src_vol1* qui se trouve dans une relation SnapMirror avec le volume *dst_vol1*, vous devez spécifier *src_vol1* dans le champ site protégé et *dst_vol1* dans le champ site de reprise.

3. Sélectionnez **Suivant**.
4. Vérifiez que la matrice est découverte et affichée en bas de la fenêtre Ajouter un gestionnaire de matrice et sélectionnez **Terminer**.

Vous pouvez suivre les mêmes étapes pour le site de reprise à l'aide des adresses IP et des identifiants de gestion des SVM appropriés. Dans l'écran Activer les paires de matrices de l'assistant Ajouter un gestionnaire de matrice, vérifiez que la paire de matrices correcte est sélectionnée et qu'elle indique prête à être activée.

Vérifier les systèmes de stockage répliqués dans ONTAP tools

Vous devez vérifier que le site protégé et le site de reprise sont correctement couplés après avoir configuré Storage Replication adapter (SRA). Le système de stockage répliqué doit être détectable par le site protégé et le site de reprise.

Avant de commencer

- Vous devez avoir configuré votre système de stockage.
- Vous devez avoir couplé le site protégé et le site de reprise à l'aide du gestionnaire de baie VMware Live site Recovery.
- Vous devez avoir activé la licence FlexClone et la licence SnapMirror avant d'effectuer l'opération de basculement et l'opération de basculement pour SRA.
- Vous devez disposer des mêmes stratégies et plannings SnapMirror sur les sites source et de destination.

Étapes

1. Connectez-vous à votre serveur vCenter.
2. Accédez à **Site Recovery** > **Réplication basée sur la baie**.
3. Sélectionnez la paire de matrices requise et vérifiez les détails correspondants.

   Les systèmes de stockage doivent être découverts sur le site protégé et le site de reprise dont le statut est « activé ».

Protection contre le fan-out dans ONTAP tools

Dans un scénario de protection en éventail, le groupe de cohérence est doublement protégé avec une relation synchrone sur le premier cluster ONTAP de destination et avec une relation asynchrone sur le deuxième cluster ONTAP de destination. Les flux de travail de création, de modification et de suppression de la protection de synchronisation active SnapMirror maintiennent la protection synchrone. Les flux de travail de basculement et de reprotection des appliances VMware Live Site Recovery maintiennent la protection asynchrone.

Le déploiement n'est pas pris en charge pour l'utilisateur SVM.

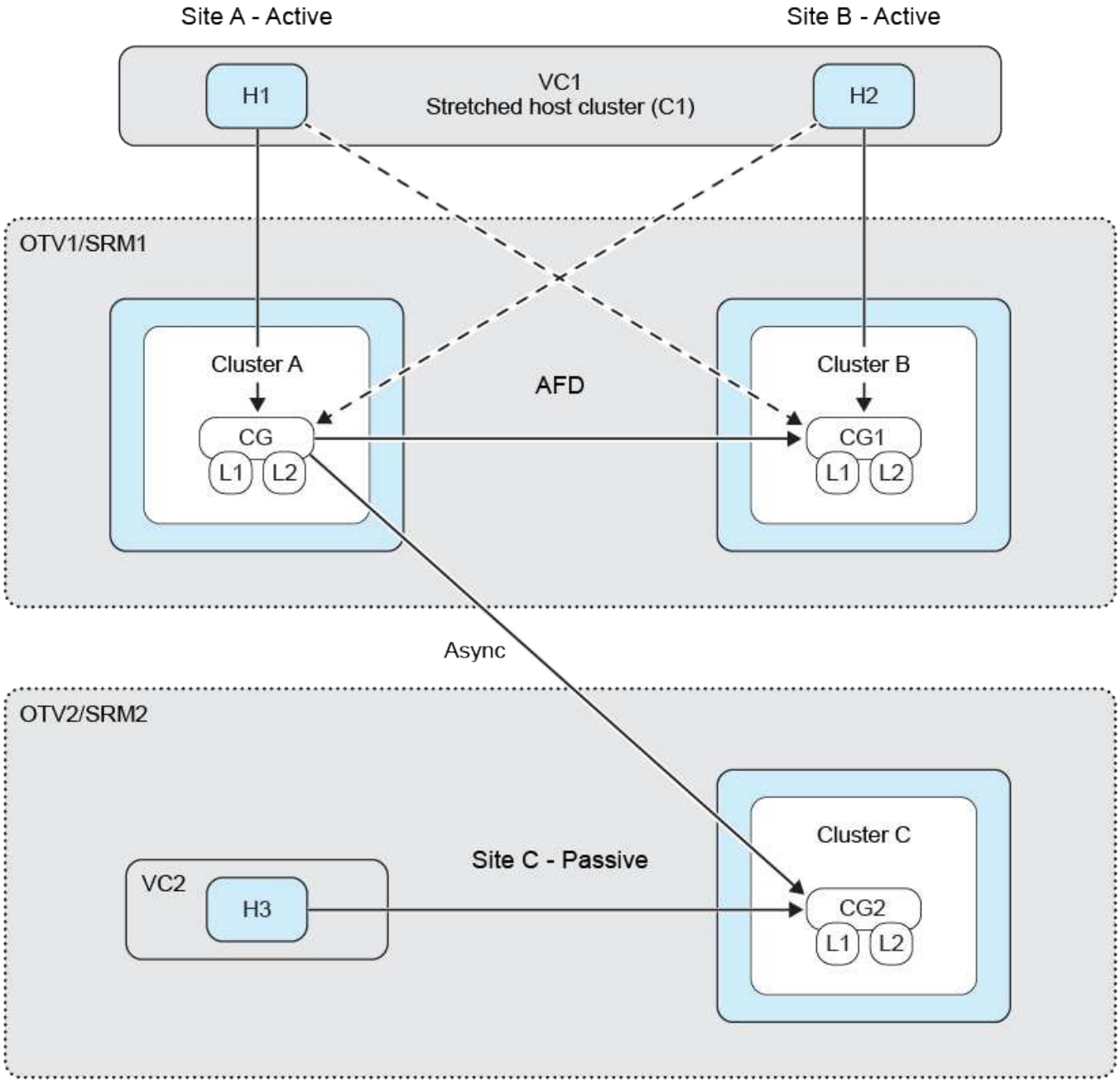
Pour configurer la protection en éventail, associez les trois clusters de sites et les SVM.

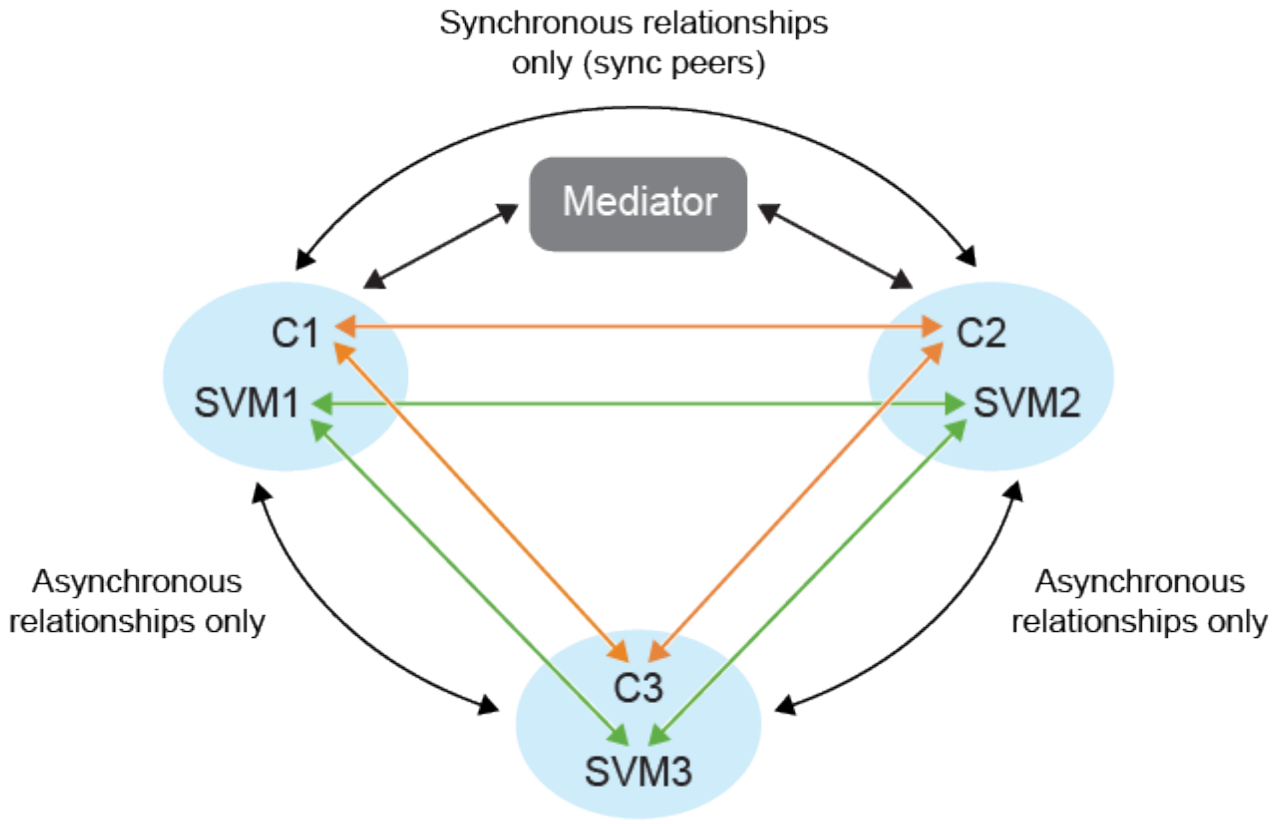
Exemple :

Si	ensuite

• Le groupe de cohérence source se trouve sur le cluster c1 et le SVM svm1 • Le premier groupe de cohérence de destination se trouve sur le cluster c2 et le SVM svm2 et • Le second groupe de cohérence de destination se trouve sur le cluster c3 et le SVM svm3	• Le cluster peering sur le cluster ONTAP source sera (C1, C2) et (C1, C3). • Le cluster peering sur le premier cluster ONTAP de destination sera (C2, C1) et (C2, C3) et • Le cluster peering sur le second cluster ONTAP de destination sera (C3, C1) et (C3, C2). • Le peering de SVM sur la SVM source sera (svm1, svm2) et (svm1, svm3). • Le peering de SVM sur la première SVM de destination sera (svm2, svm1) et (svm2, svm3) et • Le peering de SVM sur la deuxième svm de destination sera (svm3, svm1) et (svm3, svm2).

Le schéma suivant montre la configuration de la protection en éventail :


Site A - Active
Site B - Active
VC1
Stretched host cluster (C1)
H1
H2
OTV1/SRM1
Cluster A
AFD
Cluster B
CG
L1
L2
CG1
L1
L2
Async
OTV2/SRM2
Cluster C
Site C - Passive
VC2
H3
CG2
L1
L2



Étapes

1. Sélectionnez un nouveau magasin de données d'espace réservé. Les critères de sélection du magasin de données d'espace réservé pour la protection par phases sont :
   - Ne placez pas le magasin de données d'espace réservé dans le cluster hôte que vous protégez.
   - Si vous devez inclure la banque de données d'espace réservé dans le cluster hôte, ajoutez-la à l'appliance VMware Live Site Recovery avant de configurer la protection de synchronisation active SnapMirror . Avec cette configuration, vous pouvez laisser le magasin de données d'espace réservé hors de protection.

     Pour plus d'informations, reportez-vous à "Sélectionnez un datastore de placeholder"

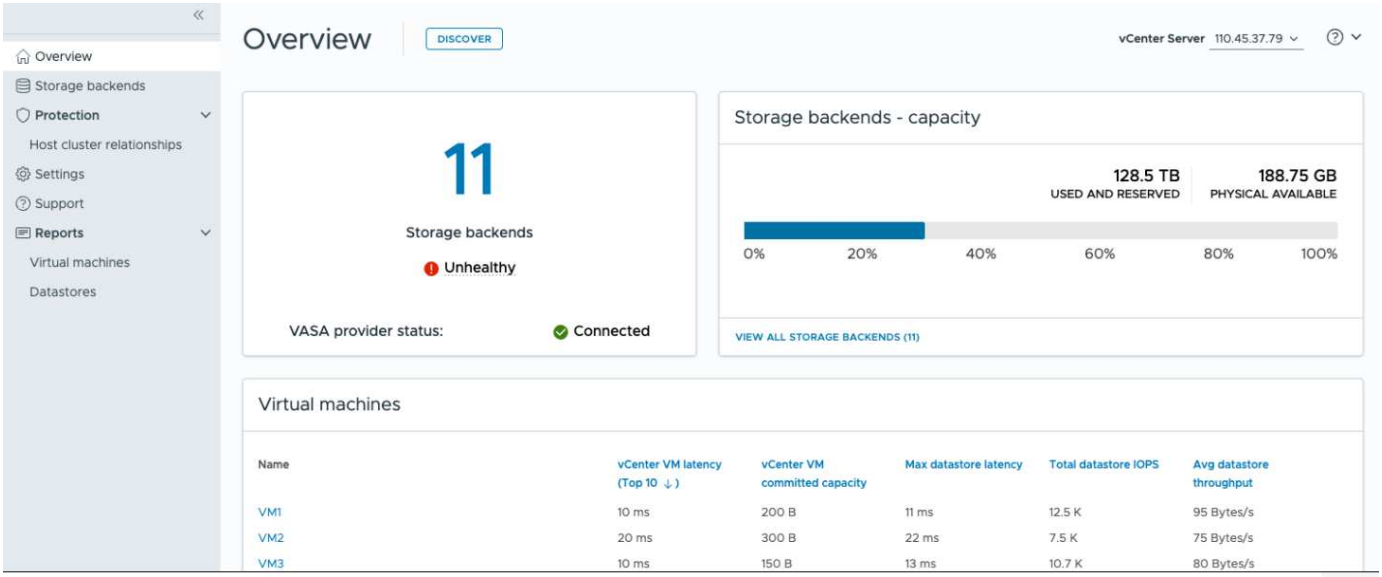
2. Ajoutez une banque de données à la protection du cluster hôte en suivant"Modifier le cluster hôte protégé" . Ajoutez des types de politiques asynchrones et synchrones.

Gérez les outils ONTAP pour VMware vSphere

Découvrez le tableau de bord des ONTAP tools

La sélection de l'icône du plug-in ONTAP tools for VMware vSphere dans la section Raccourcis du client vCenter ouvre la page de présentation. Ce tableau de bord fournit un résumé des ONTAP tools for VMware vSphere .

En mode lié amélioré (ELM), la liste déroulante vCenter Server apparaît. Choisissez un serveur vCenter pour afficher ses données. La liste déroulante est disponible dans toutes les vues de liste du plug-in. Lorsque vous sélectionnez un serveur vCenter sur une page, il reste identique lorsque vous changez d'onglet dans le plug-in.



Depuis la page d'aperçu, vous pouvez exécuter l'action **Découverte**. L'action de découverte détecte les backends de stockage, les hôtes, les banques de données et l'état ou les relations de protection nouvellement ajoutés ou mis à jour au niveau de vCenter. Exécutez la découverte à la demande sans attendre la découverte planifiée.

Le bouton d'action **Découverte** est activé uniquement si vous disposez du privilège requis pour effectuer l'action de découverte.

Une fois la demande de découverte soumise, vous pouvez suivre la progression de l'action dans le panneau des tâches récentes.

Le tableau de bord comporte plusieurs cartes montrant différents éléments du système. Le tableau suivant montre les différentes cartes et ce qu'elles représentent.

Carte	Description

État	La carte d'état indique le nombre de systèmes back-end de stockage et l'état global de santé des systèmes back-end de stockage et du fournisseur VASA. L'état des systèmes back-end de stockage affiche **Healthy** lorsque l'état de tous les systèmes back-end de stockage est normal et indique **malsain** si l'un des systèmes back-end de stockage présente un problème (état Inconnu/inaccessible/dégradé). Sélectionnez l'info-bulle pour ouvrir les détails sur le statut des systèmes back-end de stockage. Pour plus de détails, vous pouvez sélectionner n'importe quel système back-end. **Other VASA Provider States** link indique l'état actuel du VASA Provider enregistré dans vCenter Server.
Systèmes back-end de stockage - capacité	Cette carte affiche la capacité totale utilisée et disponible de tous les backends de stockage pour l'instance vCenter Server sélectionnée. Pour les systèmes de stockage ASA r2, les données de capacité ne sont pas affichées, car il s'agit d'un système désagrégé.
Ordinateurs virtuels	Cette fiche présente les 10 principales machines virtuelles classées par mesure de performance. Vous pouvez sélectionner l'en-tête pour obtenir les 10 premières machines virtuelles de la mesure sélectionnée, triées par ordre croissant ou décroissant. Les modifications de tri et de filtrage effectuées sur la carte persistent jusqu'à ce que vous changiez ou effacez le cache du navigateur.
Datastore	Cette carte présente les 10 principaux datastores classés par mesure de performance. Vous pouvez sélectionner l'en-tête pour obtenir les 10 principaux datastores de la mesure sélectionnée triés par ordre croissant ou décroissant. Les modifications de tri et de filtrage effectuées sur la carte persistent jusqu'à ce que vous changiez ou effacez le cache du navigateur. Une liste déroulante Type de datastore permet de sélectionner le type de datastores : NFS, VMFS ou vVols.
Carte de conformité de l'hôte ESXi	Cette carte indique si tous les hôtes ESXi (pour le vCenter sélectionné) suivent les paramètres d'hôte NetApp recommandés par groupe ou catégorie. Vous pouvez sélectionner le lien **Appliquer les paramètres recommandés** pour appliquer les paramètres recommandés. Vous pouvez sélectionner l'état de conformité des hôtes pour voir la liste des hôtes.

Comment les ONTAP tools gèrent les igroups et les politiques d'exportation

Les groupes d'initiateurs (igroups) sont des tables de noms de port mondiaux (WWPN)

d'hôte de protocole FC ou de noms de nœuds qualifiés d'hôte iSCSI. Vous pouvez définir des groupes initiateurs et les mapper sur des LUN pour contrôler l'accès des initiateurs aux LUN.

Dans les ONTAP tools for VMware vSphere 9.x, les igroups étaient créés et gérés dans une structure plate, où chaque banque de données dans vCenter était associée à un seul igroup. Ce modèle limitait la flexibilité et la réutilisation des igroups sur plusieurs banques de données. Les ONTAP tools for VMware vSphere introduisent des igroups imbriqués, où chaque banque de données de vCenter est associée à un igroup parent, tandis que chaque hôte est lié à un igroup enfant sous ce parent. Vous pouvez définir des groupes parents personnalisés avec des noms définis par l'utilisateur pour les réutiliser dans les banques de données afin de faciliter la gestion des groupes. Comprendre le flux de travail igroup pour gérer les LUN et les banques de données dans les ONTAP tools for VMware vSphere. Différents flux de travail génèrent des configurations igroup variables, comme illustré dans les exemples suivants :

Les noms mentionnés sont uniquement à des fins d'illustration et ne font pas référence aux vrais noms de groupes i. Les groupes gérés par les outils ONTAP utilisent le préfixe « otv_ ». Les groupes i personnalisés peuvent recevoir n'importe quel nom.

Terme	Description
DS<numéro>	Datastore
iqn<nombre>	IQN initiateur
hôte<numéro>	Hébergeur MoRef
lun<numéro>	IDENTIFIANT DE LUN
<DSName>Igroup<numéro>	Groupe parent par défaut (géré par les outils ONTAP)
<Host-Moref>Igroup<numéro>	Groupe d'enfants
CustomIgroup<numéro>	Groupe parent personnalisé défini par l'utilisateur
ClassicIgroup<numéro>	Igroup utilisé dans les versions 9.x des outils ONTAP.

Exemple 1 :

Créer une banque de données sur un seul hôte avec un seul initiateur

Workflow : [Créer] DS1 (lun1) : host1 (iqn1)

Résultat:

- DS1Igroup :
  - hôte1Igroupe → (iqn1: lun1)

ONTAP crée le groupe parent DS1Igroup pour DS1 et mappe le groupe enfant host1Igroup à lun1. Le système mappe toujours les LUN aux groupes enfants.

Exemple 2 :

Monter le magasin de données existant sur un hôte supplémentaire

Workflow : [Montage] DS1 (lun1) : host2 (iqn2)

Résultat:

- DS1Igroup :
  - hôte1Igroupe → (iqn1: lun1)
  - host2Igroup → (iqn2: lun1)

Les ONTAP tools for VMware vSphere créent un groupe i enfant host2Igroup et l'ajoutent au groupe i parent existant DS1Igroup.

Exemple 3 :

Démonter une banque de données d'un hôte

Workflow : [Démonter] DS1 (lun1) : hôte1 (iqn1)

Résultat:

- DS1Igroup :
  - host2Igroup → (iqn2: lun1)

Les ONTAP tools for VMware vSphere suppriment host1Igroup de la hiérarchie. Le système ne supprime pas explicitement les groupes enfants. Il les supprime sous ces deux conditions :

- Si aucun LUN n'est mappé, le système ONTAP supprime le groupe i enfant.
- Une tâche de nettoyage planifiée supprime les groupes enfants suspendus sans mappages LUN. Ces scénarios s'appliquent uniquement aux groupes gérés par les outils ONTAP, et non à ceux créés sur mesure.

Exemple 4 :

Supprimer le magasin de données

Workflow : [Supprimer] DS1 (lun1) : host2 (iqn2)

Résultat:

- DS1Igroup :
  - host2Igroup → (iqn2: lun1)

Les groupes i parents et enfants sont supprimés, sauf si une autre banque de données réutilise le groupe i parent. Les groupes enfants ne sont pas explicitement supprimés

Exemple 5 :

Créer plusieurs banques de données sous un groupe parent personnalisé

Flux de travail:

- [Créer] DS2 (lun2) : host1 (iqn1), host2 (iqn2)
- [Créer] DS3 (lun3) : host1 (iqn1), host3 (iqn3)

Résultat:

- CustomIgroup1 :
  - hôte1Igroup → (iqn1 : lun2, lun3)
  - host2Igroup → (iqn2: lun2)

    - host3Igroup → (iqn3: lun3)

CustomIgroup1 est créé pour DS2 et réutilisé pour DS3. Les groupes d'applications enfants sont créés ou mis à jour sous le parent partagé, chaque groupe d'applications enfant étant mappé à ses LUN respectifs.

Exemple 6 :
Supprimez un magasin de données sous un groupe parent personnalisé.

Workflow : [Supprimer] DS2 (lun2) : host1 (iqn1), host2 (iqn2)

Résultat:

- CustomIgroup1 :
    - hôte1Igroupe → (iqn1 : lun3)
    - host3Igroup → (iqn3: lun3)
- Même si CustomIgroup1 n'est pas réutilisé, il n'est pas supprimé.
- Si aucun LUN n'est mappé, le système ONTAP supprime host2Igroup.
- Le groupe hôte1 n'est pas supprimé, car il est mappé sur lun3 de DS3. Les groupes personnalisés ne sont jamais supprimés, quel que soit leur statut de réutilisation.

Exemple 7 :
Développer la banque de données vVols (ajouter un volume)

Flux de travail:

Avant l'extension :

[Développer] DS4 (lun4) : host4 (iqn4)

- DS4Igroup : host4Igroup → (iqn4 : lun4)

Après l'extension :

[Développer] DS4 (lun4, lun5) : host4 (iqn4)

- DS4Igroup : host4Igroup → (iqn4 : lun4, lun5)

Un nouveau LUN est créé et mappé au groupe enfant existant host4Igroup.

Exemple 8 :
Réduire le volume de la banque de données vVols (Supprimer le volume)

Flux de travail:

Avant rétrécissement :

[Rétrécir] DS4 (lun4, lun5) : host4 (iqn4)

- DS4Igroup : host4Igroup → (iqn4 : lun4, lun5)

Après rétrécissement :

[Rétrécir] DS4 (lun4) : host4 (iqn4)

- DS4Igroup : host4Igroup → (iqn4 : lun4)

Le LUN spécifié (lun5) est dissocié du groupe d'objets enfant. Ce groupe reste actif tant qu'il possède au moins un LUN mappé.

Exemple 9 :

Migration des outils ONTAP 9 vers 10 (normalisation igroup)

Workflow

Les outils ONTAP pour les versions VMware vSPhere 9.x ne prennent pas en charge les groupes hiérarchiques. Lors de la migration vers les versions 10.3 ou supérieures, les igroups doivent être normalisés dans la structure hiérarchique.

Avant la migration :

[Migration] DS6 (lun6, lun7) : host6 (iqn6), host7 (iqn7) → ClassicIgroup1 (iqn6 et iqn7 : lun6, lun7)

La logique des outils ONTAP 9.x autorise plusieurs initiateurs par igroup sans imposer de mappage d'hôte un à un.

Après la migration :

[Migration] DS6 (lun6, lun7) : host6 (iqn6), host7 (iqn7) → ClassicIgroup1 : otv_ClassicIgroup1 (iqn6 et iqn7 : lun6, lun7)

Pendant la migration :

- Un nouveau groupe parent (ClassicIgroup1) est créé.
- L'igroup d'origine est renommé avec le préfixe otv_ et devient un igroup enfant.

Cela garantit le respect du modèle hiérarchique.

Sections connexes

"À propos des igroups"

Export-policies

Les politiques d'exportation contrôlent l'accès à la banque de données NFS et les autorisations client dans les ONTAP tools for VMware vSphere. Les politiques d'exportation sont créées et gérées dans les systèmes ONTAP et peuvent être utilisées avec les banques de données NFS pour appliquer le contrôle d'accès. Chaque politique d'exportation se compose de règles qui spécifient les clients (adresses IP ou sous-réseaux) autorisés à accéder et les autorisations accordées (lecture seule ou lecture-écriture).

Lorsque vous créez une banque de données NFS dans les outils ONTAP pour VMware vSphere, vous pouvez sélectionner une politique d'exportation existante ou en créer une nouvelle. Cette politique est ensuite appliquée à la banque de données, garantissant ainsi que seuls les clients autorisés y ont accès.

Lorsque vous montez une banque de données NFS sur un nouvel hôte ESXi, les outils ONTAP pour VMware vSphere ajoutent l'adresse IP de l'hôte à la stratégie d'exportation existante associée à la banque de données. Cela permet au nouvel hôte d'accéder à la banque de données sans créer de nouvelle stratégie d'exportation.

Lorsque vous supprimez ou démontez une banque de données NFS d'un hôte ESXi, les ONTAP tools for VMware vSphere suppriment l'adresse IP de l'hôte de la stratégie d'exportation. Si aucun autre hôte n'utilise

cette politique d'exportation, elle sera supprimée. Lorsque vous supprimez une banque de données NFS, les ONTAP tools for VMware vSphere suppriment la stratégie d'exportation associée à cette banque de données si elle n'est pas réutilisée par d'autres banques de données. Si la politique d'exportation est réutilisée, elle conserve l'adresse IP de l'hôte et ne change pas. Lorsque vous supprimez les banques de données, la politique d'exportation annule l'attribution de l'adresse IP de l'hôte et attribue une politique d'exportation par défaut, afin que les systèmes ONTAP puissent y accéder si nécessaire.

L'attribution de la stratégie d'exportation diffère selon la réutilisation entre différents magasins de données. Lorsque vous réutilisez la stratégie d'exportation, vous pouvez lui ajouter la nouvelle adresse IP de l'hôte. Lorsque vous supprimez ou démontez un magasin de données utilisant une stratégie d'exportation partagée, celle-ci n'est pas supprimée. Elle reste inchangée et l'adresse IP de l'hôte n'est pas supprimée, car elle est partagée avec les autres magasins de données. La réutilisation des stratégies d'exportation est déconseillée, car elle peut entraîner des problèmes d'accès et de latence.

Sections connexes

"Créer une export-policy"

Comment les ONTAP tools gèrent les igroups

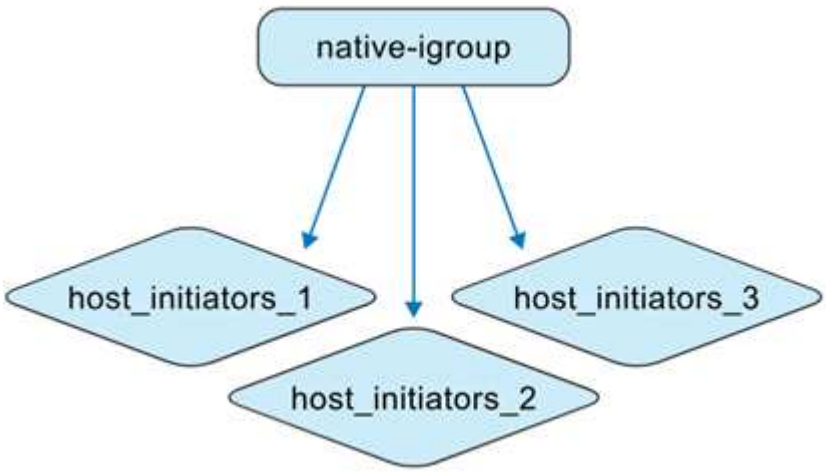
Si vous gérez à la fois des machines virtuelles ONTAP et des systèmes de stockage ONTAP , il est important de comprendre le comportement des igroups, en particulier lors du déplacement de banques de données d'environnements non gérés par les outils ONTAP vers ceux qui le sont. Cette page explique comment les igroups sont mis à jour au cours de ce processus.

Les ONTAP tools for VMware vSphere 10.4 et versions ultérieures créent et maintiennent automatiquement les objets ONTAP et vCenter pour simplifier la gestion des banques de données dans les environnements de centre de données VMware.

Les ONTAP tools for VMware vSphere interprètent les igroups dans deux contextes différents :

igroups gérés par des outils non ONTAP

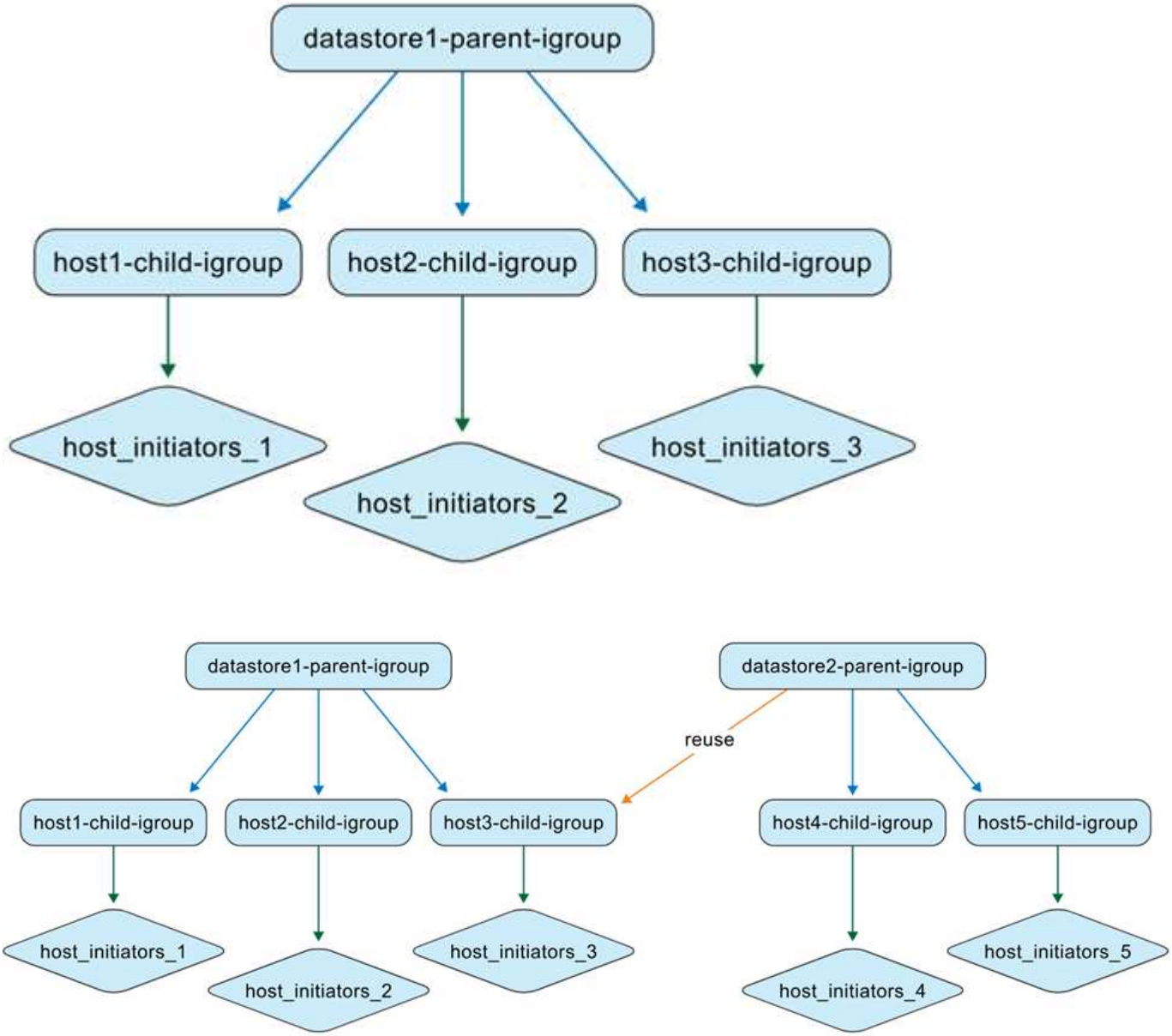
En tant qu'administrateur de stockage, vous pouvez créer des igroups sur le système ONTAP sous forme de structures plates ou imbriquées. L'illustration montre un igroup plat créé dans le système ONTAP .



igroups gérés par les outils ONTAP

Lorsque vous créez des banques de données, les ONTAP tools for VMware vSphere créent automatiquement des igroups à l'aide d'une structure imbriquée pour faciliter le mappage LUN.

Par exemple, lorsque datastore1 est créé et monté sur les hôtes 1, 2 et 3, et qu'un nouveau datastore (datastore2) est créé et monté sur les hôtes 3, 4 et 5, les outils ONTAP réutilisent le groupe i au niveau de l'hôte pour une gestion efficace.



Voici quelques cas d' ONTAP tools for VMware vSphere .

Lorsque vous créez une banque de données avec les paramètres igroup par défaut

Lorsque vous créez une banque de données et laissez le champ igroup vide (paramètre par défaut), les outils ONTAP génèrent automatiquement une structure igroup imbriquée pour cette banque de données. Le groupe parent au niveau du magasin de données est nommé à l'aide du modèle : otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name>. Chaque groupe enfant au niveau de l'hôte suit le modèle : otv_<hostMoref>_<vcguid>. Vous pouvez afficher l'association entre les groupes parents (au niveau du magasin de données) et enfants (au niveau de l'hôte) dans la section **Groupe d'initiateurs parents** de l'interface de stockage ONTAP .

Avec l'approche igroup imbriquée, les LUN sont mappés uniquement aux igroups enfants. L'inventaire vCenter Server affiche ensuite la nouvelle banque de données.

Lorsque vous créez une banque de données avec un nom de groupe i personnalisé

Lors de la création d'une banque de données dans les outils ONTAP , vous pouvez saisir un nom de groupe d'applications personnalisé au lieu de le sélectionner dans la liste déroulante. Les outils ONTAP créent ensuite un groupe parent au niveau du magasin de données en utilisant le nom que vous avez spécifié. Si le même hôte est utilisé pour plusieurs banques de données, le groupe i existant au niveau de l'hôte (enfant) est réutilisé. Par conséquent, le LUN du nouveau magasin de données est mappé à ce groupe i enfant existant, qui peut désormais être associé à plusieurs groupes i parents (un pour chaque magasin de données). Vous pouvez voir le nouveau magasin de données avec le nom igroup personnalisé dans l'interface vCenter Server.

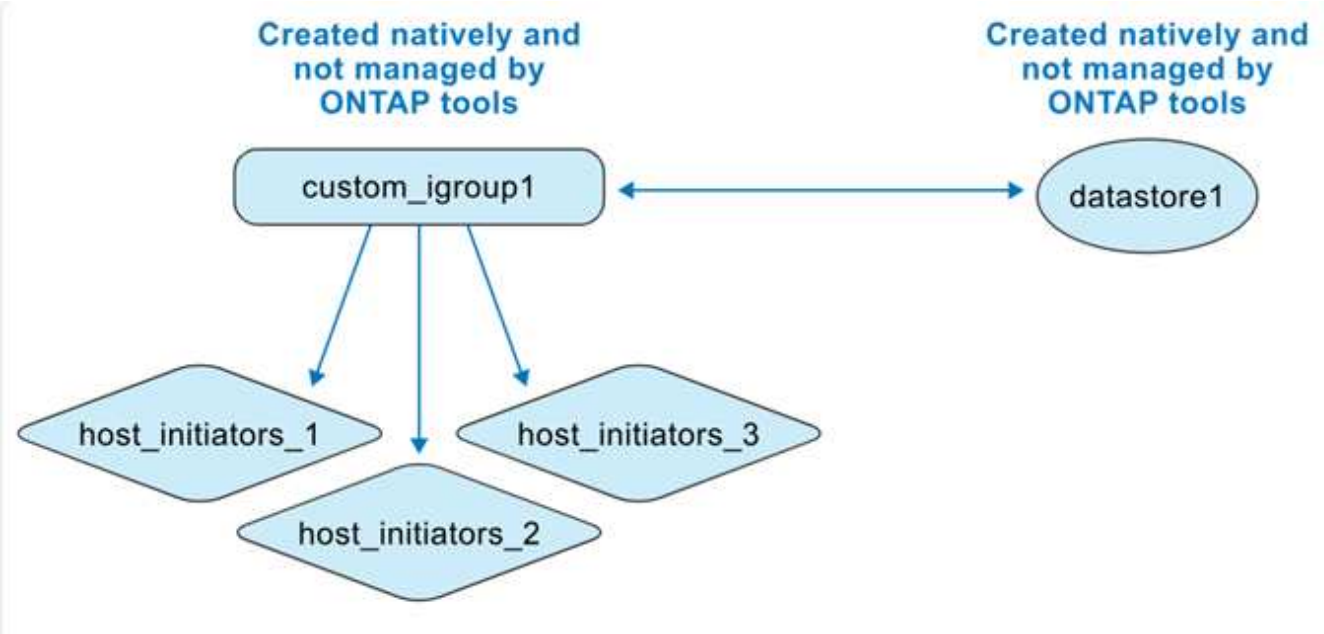
Lorsque vous réutilisez le nom du groupe i lors de la création du magasin de données

Lors de la création d'une banque de données à l'aide de l'interface utilisateur des outils ONTAP , vous pouvez choisir un groupe parent personnalisé existant dans la liste déroulante. Après avoir réutilisé le groupe parent pour créer une autre banque de données, l'interface utilisateur des systèmes ONTAP affiche cette association. Le nouveau magasin de données apparaît également dans l'interface utilisateur de vCenter Server.

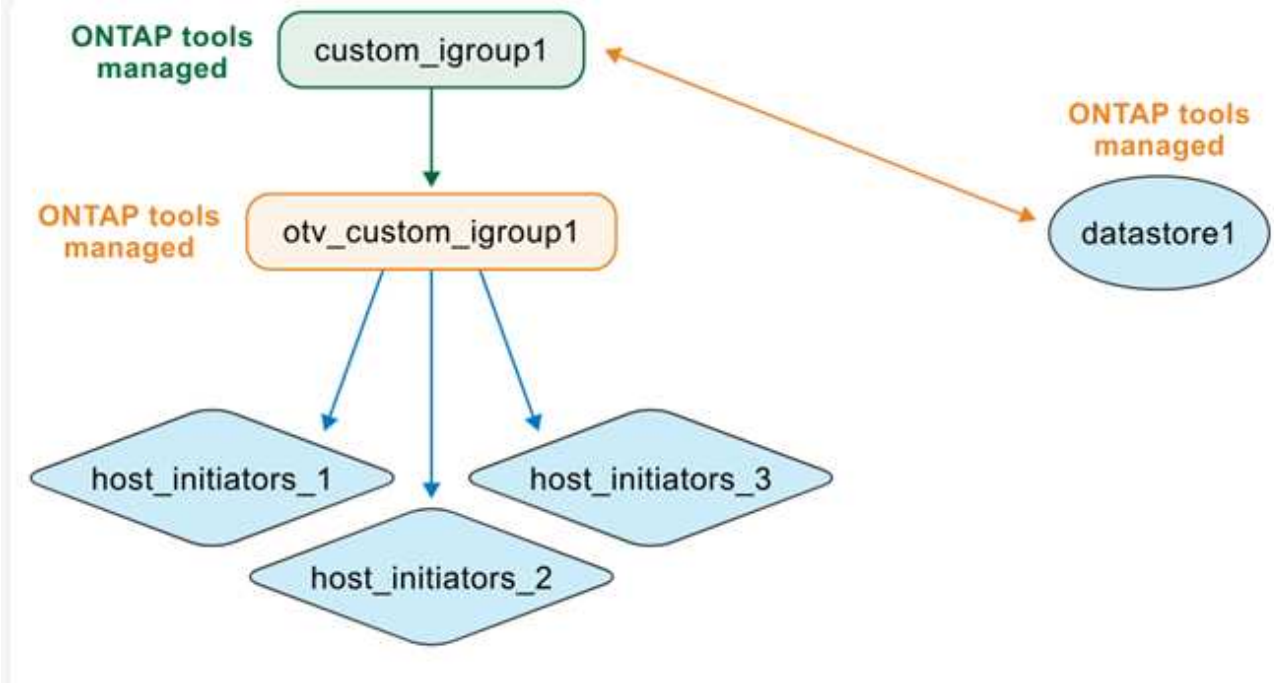
Cette opération peut également être effectuée à l'aide de l'API. Pour réutiliser un igroup existant lors de la création d'une banque de données, spécifiez l'UUID igroup dans la charge utile de la demande d'API.

Lorsque vous créez un datastore et un igroup nativement à partir ONTAP et de vCenter

Si vous créez l'igroup et le datastore directement dans les systèmes ONTAP et les environnements VMware, les outils ONTAP ne gèrent pas ces objets dans un premier temps. Cela crée une structure igroup plate.



Pour gérer une banque de données et un groupe d'applications existants avec les outils ONTAP , vous devez effectuer une découverte de banque de données. Les outils ONTAP identifient et enregistrent le magasin de données et l'igroup, et les convertissent en une structure imbriquée dans sa base de données. Un nouveau groupe parent est créé en utilisant le nom personnalisé, tandis que le groupe existant est renommé avec le préfixe « otv_ » et devient le groupe enfant. Les mappages d'initiateurs restent inchangés. Seuls les igroups mappés aux banques de données sont convertis lors de la découverte. Après cela, la structure igroup ressemble à l'illustration ci-dessous.



Une fois la découverte de banque de données exécutée dans les outils ONTAP , ONTAP derniers convertissent le groupe d'extension plat en une structure imbriquée. Les outils ONTAP gèrent ensuite l'igroup, en le renommant avec le préfixe « otv_ ». Le LUN reste mappé au même igroup tout au long de ce processus.

Comment les outils ONTAP réutilisent les igroups créés nativement

Vous pouvez créer une banque de données dans les outils ONTAP à l'aide d'un igroup qui a d'abord été créé dans les systèmes ONTAP , une fois que les outils ONTAP l'ont géré. Ces groupes i apparaissent dans la liste déroulante des noms de groupe d'initiateurs personnalisés. Le nouveau LUN pour le magasin de données est ensuite mappé au groupe enfant normalisé correspondant, tel que « otv_NativeIgroup1 ».

Les ONTAP tools for VMware vSphere ne détectent ni n'utilisent les igroups créés dans le système ONTAP qui ne sont pas gérés par les outils ONTAP ou liés à une banque de données.

Découvrez l'interface utilisateur du gestionnaire d'outils ONTAP

Les ONTAP tools for VMware vSphere prennent en charge la multilocation, permettant la gestion de plusieurs instances de vCenter Server.

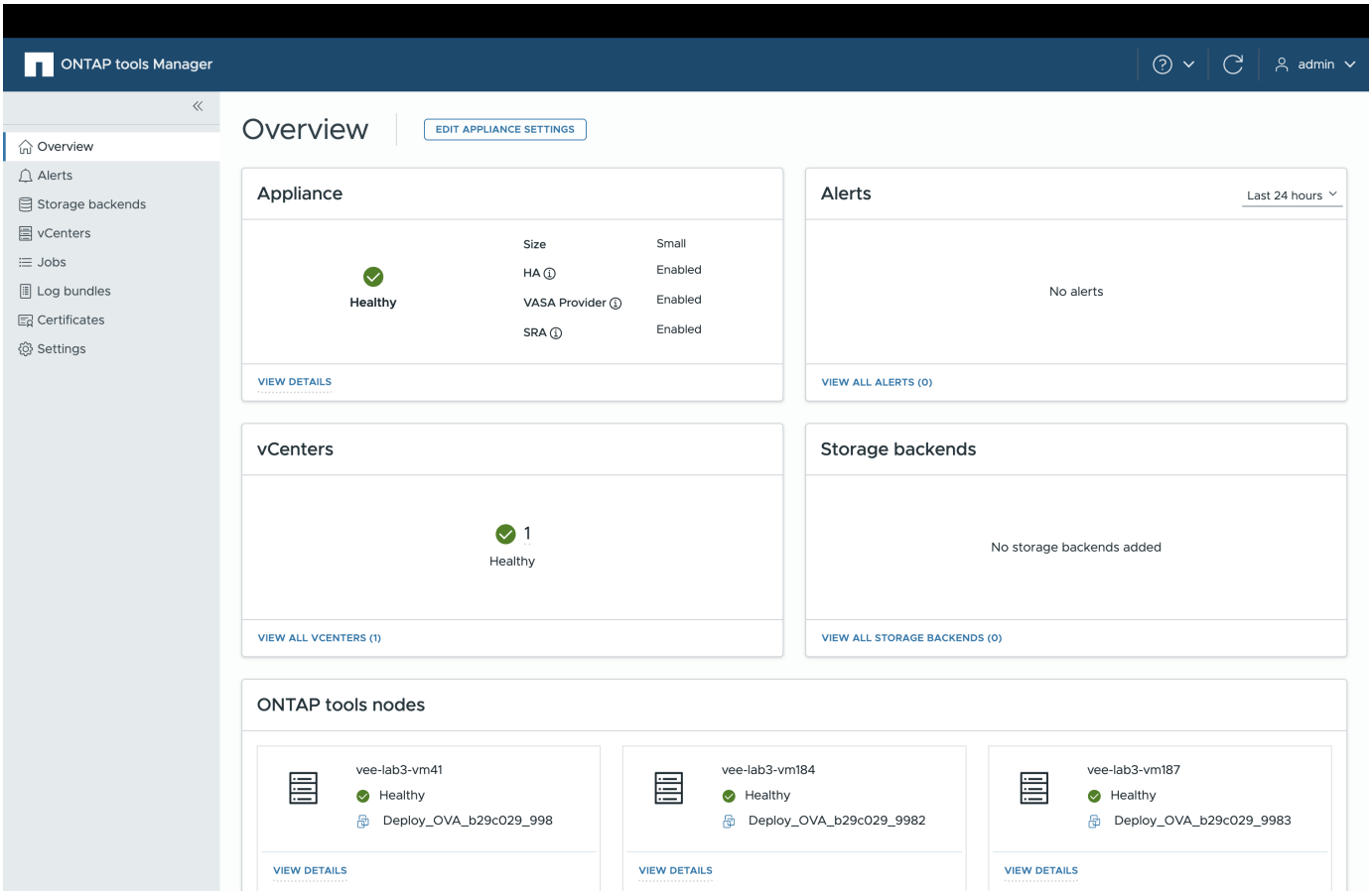
ONTAP Tools Manager est une console Web permettant de gérer les ONTAP tools for VMware vSphere, les instances vCenter Server, les backends de stockage et la configuration des appliances telles que la haute disponibilité (HA) et la mise à l'échelle des nœuds.

ONTAP Tools Manager offre les fonctionnalités suivantes :

- Gérer les alertes - Affichez et filtrez les alertes générées par les ONTAP tools for VMware vSphere.
- Gérer les backends de stockage - Ajoutez et gérez les clusters de stockage ONTAP et mappez-les aux instances vCenter Server à l'échelle mondiale.
- Gérer les instances vCenter Server - Ajoutez et gérez les instances vCenter Server dans les outils ONTAP .

- Surveiller les tâches - Surveiller et déboguer les tâches asynchrones lancées à partir de l'interface du plug-in des outils ONTAP et de l'interface du gestionnaire des outils ONTAP . Vous pouvez filtrer les tâches par période, ajuster la taille de la page et afficher les détails des tâches, y compris les erreurs et les sous-tâches. Cliquez sur un statut d'échec pour obtenir les détails de l'erreur. Pour les tâches comportant des sous-tâches, développez la ligne pour afficher les descriptions et les statuts. Pour les sous-tâches, utilisez la vue détaillée de la tâche pour afficher les détails.
- Télécharger des bundles de journaux - Collectez des fichiers journaux pour dépanner les ONTAP tools for VMware vSphere.
- Gérer les certificats - Remplacez le certificat auto-signé par un certificat d'autorité de certification personnalisé et renouvelez ou actualisez les certificats pour les outils VASA Provider et ONTAP .
- Réinitialiser les mots de passe - Modifiez le mot de passe du fournisseur VASA et du SRA.
- Gérer les paramètres de l'appliance - Configurez l'appliance des outils ONTAP , y compris l'activation de la haute disponibilité et l'augmentation de la taille des nœuds.

Pour accéder au gestionnaire d'outils ONTAP, lancez `https://<ONTAPtoolsIP>:8443/virtualization/ui/`-le à partir du navigateur et connectez-vous à l'aide des informations d'identification d'administrateur ONTAP Tools for VMware vSphere que vous avez fournies lors du déploiement.



Carte	Description
Carte d’appareil	La carte Appliance affiche l’état général de l’appliance des outils ONTAP , les détails de configuration et l’état des services activés. Pour afficher plus d’informations, sélectionnez le lien **Afficher les détails**. Si vous modifiez un paramètre d’appareil, la carte affiche l’état et les détails de la tâche jusqu’à ce que la modification soit terminée.
Carte d’alertes	La carte Alertes affiche les alertes des outils ONTAP classées par type, y compris les alertes au niveau du nœud HA. Vous pouvez afficher les alertes détaillées en cliquant sur le lien hypertexte de comptage, qui vous amène à la page des alertes filtrées par le type d’alerte sélectionné.
Carte vCenters	La carte vCenter affiche l’état de santé de toutes les instances de vCenter Server gérées par les outils ONTAP . Vous pouvez afficher les détails de chaque vCenter en sélectionnant le lien correspondant, qui accède à une page contenant plus d’informations sur l’instance sélectionnée.
Carte des backends de stockage	La carte Backends de stockage affiche l’état de santé et de connectivité de tous les clusters de stockage ONTAP configurés dans les outils ONTAP . Vous pouvez afficher les détails de chaque backend de stockage en sélectionnant le lien correspondant, qui accède à une page contenant plus d’informations sur le cluster sélectionné.
Carte des nœuds des outils ONTAP	La carte des nœuds des outils ONTAP affiche tous les nœuds de l’appliance, y compris le nom du nœud, le nom de la machine virtuelle, l’état et les informations réseau. Sélectionnez **Afficher les détails** pour voir plus de détails sur un nœud spécifique. [REMARQUE] Dans une configuration non HA, un seul nœud apparaît. Dans une configuration HA, trois nœuds sont affichés.

Gérer les paramètres du gestionnaire d’outils ONTAP

Modifier les paramètres AutoSupport des outils ONTAP

Lors de la première configuration des ONTAP tools for VMware vSphere , AutoSupport est activé par défaut. Il envoie des messages au support technique 24 heures après son activation.

Désactivez AutoSupport

Lorsque vous désactivez AutoSupport, vous ne recevez plus d’assistance ni de surveillance proactives.

Il est recommandé de garder AutoSupport activé, car cela permet d'accélérer la détection et la résolution des problèmes. Même lorsque AutoSupport est désactivé, le système continue de collecter et de stocker des informations localement, mais il n'envoie pas de rapports sur le réseau.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez l'option **Paramètres** > **télémétrie** > **Modifier**.
4. Désélectionnez l'option **AutoSupport** et enregistrez les modifications.

Mettre à jour l'URL du proxy AutoSupport

Mettez à jour l'URL du proxy AutoSupport afin que la fonction AutoSupport achemine les données via le serveur proxy pour une transmission sécurisée.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **Paramètres** dans la barre latérale.
4. Sélectionnez l'option **Paramètres** > **télémétrie** > **Modifier**.
5. Entrez une **URL proxy** valide et enregistrez les modifications.

   Si vous désactivez AutoSupport, l'URL du proxy est également désactivée.

Ajouter des serveurs NTP aux outils ONTAP

Entrez les détails du serveur NTP pour synchroniser les horloges de l'appliance ONTAP Tools.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez l'option **Paramètres** > **serveur NTP** > **Modifier**.
4. Entrez le nom de domaine complet (FQDN) séparé par des virgules, IPv4 ou adresses IPv6.

   Actualisez l'écran pour afficher les valeurs mises à jour.

Réinitialiser les informations d'identification du VASA Provider et du SRA dans ONTAP tools

Si vous oubliez vos informations d'identification VASA Provider ou SRA, vous pouvez les réinitialiser avec un nouveau mot de passe à l'aide de l'interface du gestionnaire d'outils ONTAP . Le nouveau mot de passe doit comporter entre 8 et 256 caractères.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez l'option **Paramètres** > **Informations d'identification du fournisseur VASA / SRA** > **Réinitialiser le mot de passe**.
4. Entrez le nouveau mot de passe et confirmez-le.
5. Sélectionnez **Enregistrer** pour appliquer les modifications.

Modifier les paramètres de sauvegarde des outils ONTAP

À partir des ONTAP tools for VMware vSphere 10.5, la fonction de sauvegarde est activée par défaut et une sauvegarde est créée toutes les 10 minutes. Vous pouvez désactiver la sauvegarde ou modifier la fréquence de la sauvegarde.

Ne désactivez pas la sauvegarde car elle empêche les outils ONTAP de maintenir un RPO faible. La désactivation de la sauvegarde ne supprime pas les fichiers de sauvegarde existants. Vous pouvez modifier la fréquence de la sauvegarde à une valeur comprise entre 10 et 60 minutes.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez l'option **Paramètres** > **Sauvegarde** > **Modifier**.
4. Dans la fenêtre d'édition, vous pouvez désactiver la sauvegarde ou modifier la fréquence de sauvegarde.

Activer les services ONTAP tools

Vous pouvez modifier le mot de passe de l'administrateur à l'aide du gestionnaire d'outils ONTAP pour activer des services tels que le fournisseur VASA, l'importation de la configuration vVols et la reprise après incident (SRA) à l'aide du gestionnaire d'outils ONTAP.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.

3. Sélectionnez **Modifier les paramètres de l'appareil** dans la section Présentation.
4. Dans la section **Services**, vous pouvez activer, selon vos besoins, des services optionnels tels que VASA Provider, l'importation de la configuration vVols et la reprise après sinistre (SRA).

   Lors de la première activation des services, vous devez créer les informations d'identification du fournisseur VASA et SRA. Ils permettent d'enregistrer ou d'activer les services VASA Provider et SRA sur le serveur vCenter. Le nom d'utilisateur ne peut contenir que des lettres, des chiffres et des traits de soulignement. La longueur du mot de passe doit être comprise entre 8 et 256 caractères.

   Avant de désactiver des services facultatifs, assurez-vous que les serveurs vCenter gérés par les outils ONTAP ne les utilisent pas.

   L'option *Autoriser l'importation de la configuration vVols * s'affiche uniquement lorsque le service VASA Provider est activé. Cette option permet la migration des données vVols des outils ONTAP 9.xx vers les outils ONTAP 10.5.

Modifier les paramètres de l'appliance ONTAP tools

Utilisez ONTAP Tools Manager pour faire évoluer les ONTAP tools for VMware vSphere , soit en augmentant le nombre de nœuds, soit en activant la haute disponibilité (HA). Par défaut, les ONTAP tools for VMware vSphere sont déployés en tant que configuration à nœud unique, non HA.

Avant de commencer

- Assurez-vous que votre modèle OVA possède la même version OVA que le nœud 1. Le nœud 1 est le nœud par défaut sur lequel les outils ONTAP pour VMware vSphere OVA sont initialement déployés.
- Assurez-vous que l'ajout à chaud du processeur et la connexion à chaud de la mémoire sont activés.
- Dans vCenter Server, définissez le niveau d'automatisation du service de reprise après sinistre (DRS) sur partiellement automatisé. Après le déploiement de la haute disponibilité, rétablissez le niveau d'automatisation complet.
- Les noms d'hôtes des nœuds dans la configuration HA doivent être en minuscules.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web :
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **Modifier les paramètres de l'appareil** dans la section Présentation.
4. Dans la section **Configuration**, augmentez la taille du nœud et activez la configuration HA. Utilisez les identifiants du serveur vCenter pour effectuer les modifications.

   Dans la configuration HA, vous pouvez modifier les détails de la bibliothèque de contenu. Veuillez indiquer le mot de passe pour chaque modification.

   Dans les ONTAP tools for VMware vSphere, vous êtes uniquement autorisé à augmenter la taille du nœud ; vous ne pouvez pas la réduire. Dans une configuration non HA, seule une configuration de taille moyenne est prise en charge. Dans une configuration HA, les configurations moyennes et grandes sont prises en charge.

5. Utilisez le bouton bascule HA pour activer la configuration HA. Sur la page **HA settings**, assurez-vous que :
   - La bibliothèque de contenu appartient au même serveur vCenter sur lequel s'exécutent les machines virtuelles du nœud des outils ONTAP. Les informations d'identification du serveur vCenter sont utilisées pour valider et télécharger le modèle OVA pour les modifications de l'appliance.
   - La machine virtuelle hébergeant les outils ONTAP n'est pas directement déployée sur un hôte VMware ESXi. La machine virtuelle doit être déployée sur un cluster ou un pool de ressources.

   > Une fois la configuration HA activée, vous ne pouvez pas revenir à une configuration à nœud unique non HA.

6. Dans la section **HA settings** de la fenêtre **Edit Appliance Settings**, vous pouvez entrer les détails des nœuds 2 et 3. Les outils ONTAP pour VMware vSphere prennent en charge trois nœuds lors de la configuration haute disponibilité.

   > Les outils ONTAP pré-remplissent la plupart des options d'entrée avec les détails du réseau Node 1 afin de simplifier le flux de travail. Vous pouvez modifier les données saisies avant d'accéder à la dernière page de l'assistant. Vous pouvez saisir les détails de l'adresse IPv6 pour les deux autres nœuds uniquement lorsque l'adresse IPv6 est activée sur le nœud de gestion des outils ONTAP .

   Assurez-vous qu'un hôte ESXi ne contient qu'une seule machine virtuelle d'outils ONTAP. Les entrées sont validées chaque fois que vous passez à la fenêtre suivante.

7. Passez en revue les détails dans la section **Résumé** et **Enregistrer** les modifications.

Et la suite ?

La page **Aperçu** affiche l'état du déploiement. Vous pouvez également suivre l'état de la tâche de modification des paramètres de l'appareil depuis la vue des tâches en utilisant l'ID de la tâche.

Si le déploiement HA échoue et que le statut du nouveau nœud est « Nouveau », supprimez la nouvelle machine virtuelle dans vCenter avant de tenter à nouveau d'activer HA.

L'onglet **alertes** du panneau de gauche répertorie les alertes des outils ONTAP pour VMware vSphere.

Ajouter des hôtes VMware vSphere aux outils ONTAP

Ajoutez de nouveaux hôtes VMware vSphere aux ONTAP tools for VMware vSphere afin de gérer et de protéger les banques de données sur les hôtes.

Étapes

1. Ajoutez un hôte à votre cluster VMware vSphere en suivant le flux de travail décrit à la page : "Comment ajouter un hôte ESX à votre cluster vSphere à l'aide du flux de travail de démarrage rapide"
2. Après avoir ajouté l'hôte, accédez au menu principal des outils ONTAP et sélectionnez **Découvrir** dans le panneau d'aperçu. Attendez la fin de la phase de découverte. Vous pouvez également attendre la fin de la découverte de l'hôte planifiée.

Résultat

Le nouvel hôte est désormais détecté et géré par les ONTAP tools for VMware vSphere. Vous pouvez maintenant procéder à la gestion du datastore sur le nouvel hôte.

Sections connexes

- "Montez un datastore vvols"sur de nouveaux hôtes.
- "Montez les datastores NFS et VMFS"sur de nouveaux hôtes.

Gérer les datastores

Monter les datastores NFS et VMFS dans ONTAP tools

Le montage d'un datastore permet d'accéder au stockage à des hôtes supplémentaires. Après avoir ajouté les hôtes à votre environnement VMware, vous pouvez monter le datastore sur les hôtes supplémentaires.

> Lorsque vous ajoutez un nouvel hôte ESXi à l'aide de "Ajouter un hôte ESX à votre flux de travail de cluster vSphere" Veuillez attendre que la découverte planifiée de l'hôte soit terminée avant qu'elle n'apparaisse dans les outils ONTAP . Vous pouvez également lancer manuellement la découverte à partir de l'écran de présentation des outils NetApp ONTAP .

Description de la tâche

- Certaines actions du clic droit sont désactivées ou indisponibles selon la version du client vSphere et le type de datastore sélectionné.
  - Si vous utilisez vSphere client 8.0 ou une version ultérieure, certaines options du clic droit sont masquées.
  - De vSphere 7.0U3 à vSphere 8.0, même si les options apparaissent, l'action est désactivée.
- vSphere désactive l'option de montage de la banque de données lorsque le cluster hôte est protégé par des configurations uniformes.

Étapes

1. Sur la page d'accueil de vSphere client, sélectionnez **hosts and clusters**.
2. Dans le volet de navigation de gauche, sélectionnez les centres de données contenant les hôtes.
3. Pour monter des banques de données NFS/VMFS sur un hôte ou un cluster d'hôtes, cliquez avec le bouton droit et sélectionnez * Outils NetApp ONTAP * > *Monter les banques de données *.
4. Sélectionnez les datastores à monter et sélectionnez **Mount**.

Et la suite ?

Vous pouvez suivre la progression dans le panneau des tâches récentes.

Sujet connexe

"Ajouter de nouveaux hôtes VMware vSphere"

Démontez les datastores NFS et VMFS dans ONTAP tools

L'action « Démonter le datastore » supprime un datastore NFS ou VMFS des hôtes ESXi. Il est disponible pour les banques de données découvertes ou gérées par les ONTAP tools for VMware vSphere.

Étapes

1. Connectez-vous au client vSphere.

2. Cliquez avec le bouton droit sur un objet de banque de données NFS ou VMFS et sélectionnez **Démonter la banque de données**.

   Le client vSphere ouvre une boîte de dialogue et liste les hôtes ESXi qui montent la banque de données. Lorsque l'opération est effectuée sur une banque de données protégée, un message d'avertissement s'affiche à l'écran.

3. Sélectionnez un ou plusieurs hôtes ESXi pour démonter le datastore.

   Vous ne pouvez pas démonter le datastore de tous les hôtes. L'interface utilisateur suggère d'utiliser l'opération de suppression de datastore.

4. Sélectionnez le bouton **Unmount**.

   Si le datastore fait partie d'un cluster hôte protégé, un message d'avertissement s'affiche.

> Si la banque de données protégée est démontée, le paramètre de protection existant peut entraîner une protection partielle. Consultez "Modifier le cluster hôte protégé" pour permettre une protection complète.

Et la suite ?

Vous pouvez suivre la progression dans le panneau tâches récentes.

Monter un datastore vVols dans ONTAP tools

Vous pouvez monter un datastore VMware Virtual volumes (vVols) sur un ou plusieurs hôtes supplémentaires pour fournir un accès au stockage à des hôtes supplémentaires. Vous pouvez démonter le datastore vVols uniquement à l'aide des API.

> Lorsque vous ajoutez un nouvel hôte ESXi à l'aide de "Ajouter un hôte ESX à votre flux de travail de cluster vSphere" Veuillez attendre que la découverte planifiée de l'hôte soit terminée avant qu'elle n'apparaisse dans les outils ONTAP . Vous pouvez également lancer manuellement la découverte à partir de l'écran de présentation des outils NetApp ONTAP .

Étapes

1. Sur la page d'accueil de vSphere client, sélectionnez **hosts and clusters**.
2. Dans le volet de navigation, sélectionnez le centre de données qui contient le datastore.
3. Cliquez avec le bouton droit de la souris sur le datastore et sélectionnez **NetApp ONTAP Tools** > **Mount datastore**.
4. Dans la boîte de dialogue **Mount datastores on hosts**, sélectionnez les hôtes sur lesquels vous souhaitez monter le datastore, puis sélectionnez **Mount**.

Le panneau des tâches récentes affiche la progression.

Sujet connexe

"Ajouter de nouveaux hôtes VMware vSphere"

Redimensionner les datastores NFS et VMFS dans ONTAP tools

Le redimensionnement d'un datastore vous permet d'augmenter le stockage des fichiers

de votre machine virtuelle. Vous pouvez modifier la taille d'un datastore en fonction de l'évolution des exigences de votre infrastructure.

Description de la tâche

Vous pouvez augmenter la taille des banques de données NFS et VMFS. Un FlexVol volume dans ces datastores ne peut pas diminuer en dessous de sa taille actuelle, mais peut croître jusqu'à 120 %.

Étapes

1. Sur la page d'accueil de vSphere client, sélectionnez **hosts and clusters**.
2. Dans le volet de navigation, sélectionnez le centre de données qui contient le datastore.
3. Cliquez avec le bouton droit de la souris sur le datastore NFS ou VMFS et sélectionnez **NetApp ONTAP Tools** > **Redimensionner le datastore**.
4. Dans la boîte de dialogue Redimensionner, saisissez une nouvelle taille pour le magasin de données et sélectionnez **OK**.

Développez les datastores vVols dans les outils ONTAP

Lorsque vous cliquez avec le bouton droit sur l'objet datastore dans la vue d'objet vCenter, la section des plug-ins affiche les actions prises en charge pour les ONTAP tools for VMware vSphere. Des actions spécifiques sont activées en fonction du type de banque de données et des privilèges utilisateur actuels.

L'opération étendre le datastore vVols ne s'applique pas aux datastores vVols système ASA r2.

Étapes

1. Sur la page d'accueil de vSphere client, sélectionnez **hosts and clusters**.
2. Dans le volet de navigation, sélectionnez le centre de données qui contient le datastore.
3. Cliquez avec le bouton droit de la souris sur le datastore et sélectionnez **NetApp ONTAP Tools** > **Add Storage to datastore**.
4. Dans la fenêtre **Créer ou sélectionner des volumes**, vous pouvez soit créer de nouveaux volumes, soit choisir parmi les volumes existants. Suivez les instructions à l'écran pour effectuer votre sélection.
5. Dans la fenêtre **Résumé**, examinez les sélections et sélectionnez **développer**. Vous pouvez suivre la progression dans le panneau tâches récentes.

Réduire la taille d'un vVols datastore dans ONTAP tools

Cette page explique comment supprimer des volumes d'un datastore vVols .

Utilisez l'action « Supprimer le stockage de la banque de données » sur toute banque de données vVols gérée par les outils ONTAP dans vCenter Server.

Vous ne pouvez pas supprimer le stockage d'un volume s'il contient des vVols; l'option de suppression sera désactivée pour ces volumes. Lors de la suppression de volumes de la banque de données, vous avez également la possibilité de supprimer les volumes sélectionnés du stockage ONTAP .

L'opération de réduction de la banque de données vVols n'est pas prise en charge pour les banques de données vVols basées sur les systèmes ASA r2.

Étapes

1. Sur la page d'accueil de vSphere client, sélectionnez **hosts and clusters**.
2. Dans le volet de navigation, sélectionnez le centre de données qui contient le datastore.
3. Cliquez avec le bouton droit de la souris sur le datastore vVol et sélectionnez **NetApp ONTAP Tools** > **Remove Storage from datastore**.
4. Sélectionnez les volumes qui ne possèdent pas de vVols et sélectionnez **Supprimer**.

   L'option permettant de sélectionner le volume sur lequel réside vVols est désactivée.

5. Dans la fenêtre contextuelle **Supprimer le stockage**, cochez la case **Supprimer les volumes du cluster ONTAP** pour supprimer les volumes du datastore et du stockage ONTAP, puis sélectionnez **Supprimer**.

Supprimer les banques de données dans ONTAP tools

Cette page explique comment supprimer des banques de données NFS, VMFS ou vVols à l'aide des outils ONTAP dans vCenter Server.

Lorsque vous supprimez une banque de données, les actions suivantes sont effectuées en fonction du type de banque de données :

- Le conteneur vVol est démonté.
- Si l'igroup n'est pas utilisé, iqn est supprimé de l'igroup.
- Le conteneur vVol est supprimé.
- Les volumes flexibles sont laissés sur la baie de stockage.

Vous ne pouvez supprimer le magasin de données que si aucun vVols n'est présent sur le magasin de données sélectionné.

Étapes

1. Connectez-vous au client vSphere.
2. Cliquez avec le bouton droit sur un système hôte, un cluster hôte ou un centre de données et sélectionnez * Outils NetApp ONTAP * > * Supprimer la banque de données *.

   Vous ne pouvez pas supprimer une banque de données utilisée par des machines virtuelles. Déplacez les machines virtuelles vers un autre magasin de données avant de les supprimer. Vous ne pouvez pas supprimer le volume s'il fait partie d'un cluster hôte protégé.

   a. Dans le cas d'une banque de données NFS ou VMFS, une boîte de dialogue apparaît avec la liste des machines virtuelles utilisant la banque de données.
   b. Si aucune machine virtuelle n'est associée à une banque de données VMFS, une boîte de dialogue de confirmation s'affiche. Si la protection du cluster hôte est activée et qu'une relation AFD existe, vous pouvez nettoyer les éléments de stockage secondaires.
   c. Pour les banques de données VMFS protégées sur les systèmes ASA r2, supprimez la protection avant de les supprimer. À partir d' ONTAP 9.17.1 et des ONTAP tools for VMware vSphere 10.5, vous pouvez supprimer une banque de données protégée. S'il s'agit du seul datastore du groupe de protection, la protection du cluster hôte est automatiquement supprimée.
   d. Pour les magasins de données vVols , vous ne pouvez supprimer le magasin de données que s'il n'y a aucun vVols présent. La boîte de dialogue **Supprimer la banque de données** inclut une option

permettant de supprimer des volumes du cluster ONTAP .

e. Pour les banques de données vVols sur les systèmes ASA r2, vous ne pouvez pas supprimer les volumes de sauvegarde d' ONTAP à l'aide de l'option **Supprimer la banque de données**.

3. Pour supprimer les volumes de sauvegarde sur le stockage ONTAP, sélectionnez **Supprimer les volumes sur le cluster ONTAP**.

> Pour les banques de données VMFS sur un stockage ONTAP unifié qui font partie d'un cluster hôte protégé, vous ne pouvez pas supprimer le volume du cluster ONTAP .

Lorsque vous supprimez une banque de données NFS, VMFS ou vVols , les groupes parents restent sur le système ONTAP . Les groupes enfants qui ne sont mappés à aucun LUN sont supprimés automatiquement. Les outils ONTAP effectuent un nettoyage quotidien pour supprimer les groupes parents par défaut non mappés. Supprimez manuellement les igroups parents personnalisés dans ONTAP. Les outils ONTAP ne peuvent pas réutiliser les igroups parents obsolètes.

Vues de stockage ONTAP pour les banques de données dans ONTAP tools

Les outils ONTAP pour VMware vSphere affichent la vue côté stockage ONTAP des datastores et de leurs volumes dans l'onglet configurer.

Étapes

1. Depuis le client vSphere, accédez au magasin de données.
2. Sélectionnez l'onglet **configurer** dans le volet de droite.
3. Sélectionnez * Outils NetApp ONTAP * > * Stockage ONTAP *. L'affichage varie selon le type de base de données. Voir le tableau ci-dessous :

Type de datastore	Information disponible
Datastore NFS	La page **Détails du stockage** contient des informations sur les systèmes back-end de stockage, les agrégats et les volumes. La page **NFS details** contient des données relatives au datastore NFS.
Datastores VMFS	La page **Détails du stockage** contient les détails du back-end de stockage, de l'agrégat, du volume et de la zone de disponibilité du stockage (SAZ). La page **Détails de l'unité de stockage** contient des détails sur l'unité de stockage.
Datastores vVols	Répertorie tous les volumes. Vous pouvez étendre ou supprimer du stockage à partir du volet de stockage ONTAP . Les outils ONTAP ne prennent pas en charge cette vue pour les datastores vVols basés sur le système ASA r2.

Vue du stockage des machines virtuelles dans ONTAP tools

La vue de stockage affiche la liste des vVols créés par la machine virtuelle.

Cette vue s'applique aux machines virtuelles disposant d'au moins un disque provenant d'un datastore vVols géré par les ONTAP tools for VMware vSphere .

Étapes

1. Depuis le client vSphere, accédez à la machine virtuelle.
2. Sélectionnez l'onglet **Monitor** dans le volet de droite.
3. Sélectionnez **NetApp ONTAP Tools** > **Storage**. Les détails **Storage** apparaissent dans le volet de droite. Vous pouvez voir la liste des vVols présents sur la machine virtuelle.

   Vous pouvez utiliser l'option « gérer les colonnes » pour masquer ou afficher différentes colonnes.

Gérer les seuils de stockage dans ONTAP tools

Vous pouvez définir le seuil de réception des notifications dans vCenter Server lorsque le volume et la capacité globale atteignent certains niveaux.

Étapes :

1. Connectez-vous au client vSphere.
2. Dans la page raccourcis, sélectionnez **NetApp ONTAP Tools** dans la section modules externes.
3. Dans le volet gauche des outils ONTAP , accédez à **Paramètres** > **Paramètres de seuil** > **Modifier**.
4. Dans la fenêtre **Modifier le seuil**, indiquez les valeurs souhaitées dans les champs **Presque plein** et **Plein** et sélectionnez **Enregistrer**. Vous pouvez rétablir les valeurs seuils aux valeurs par défaut recommandées : 80 pour Presque plein et 90 pour Plein.

Gérer les backends de stockage dans ONTAP tools

Les systèmes back-end de stockage sont des systèmes que les hôtes ESXi utilisent pour le stockage des données.

Découverte du stockage

Vous pouvez exécuter la découverte d'un backend de stockage à la demande sans attendre qu'une découverte planifiée mette à jour immédiatement les détails de stockage. Pour les configurations MetroCluster , exécutez la découverte des outils ONTAP manuellement après un basculement.

Suivez les étapes ci-dessous pour découvrir les systèmes back-end.

Étapes

1. Connectez-vous au client vSphere.
2. Dans la page raccourcis, sélectionnez **NetApp ONTAP Tools** dans la section modules externes.
3. Dans le volet gauche des outils ONTAP , accédez à **Backends de stockage** et sélectionnez un backend de stockage.
4. Sélectionnez le menu des ellipses verticales et sélectionnez **découvrir le stockage**

Vous pouvez suivre la progression dans le panneau tâches récentes.

Modification des systèmes back-end de stockage

Vous pouvez modifier les informations d'identification du backend de stockage ou le nom du port. Vous pouvez également modifier le backend de stockage pour les clusters ONTAP globaux à l'aide du gestionnaire d'outils ONTAP . Si le certificat expire dans 30 jours ou moins, les outils ONTAP affichent un avertissement. Modifiez le backend de stockage et téléchargez le nouveau certificat depuis l'administrateur ONTAP .

Lorsque vous modifiez le backend de stockage, les ONTAP tools for VMware vSphere effectuent une découverte du backend de stockage pour mettre à jour les détails de stockage.

Suivez les étapes de cette section pour modifier un système back-end de stockage.

1. Connectez-vous au client vSphere.
2. Dans la page raccourcis, sélectionnez **NetApp ONTAP Tools** dans la section modules externes.
3. Dans le volet gauche des outils ONTAP , accédez à **Backends de stockage** et sélectionnez un backend de stockage.
4. Sélectionnez le menu des ellipses verticales et sélectionnez **Modifier** pour modifier les informations d'identification ou le nom du port. Vous pouvez suivre la progression dans le panneau tâches récentes.

Modifiez les clusters ONTAP globaux avec le gestionnaire d'outils ONTAP comme suit.

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez les systèmes back-end de stockage dans la barre latérale.
4. Sélectionnez le back-end de stockage à modifier.
5. Sélectionnez le menu ellipses verticales et sélectionnez **Modifier**.
6. Vous pouvez modifier les informations d'identification ou le port. Entrez **Nom d'utilisateur** et **Mot de passe** pour modifier le backend de stockage.

Suppression des systèmes back-end

Vous devez supprimer tous les magasins de données attachés au backend de stockage avant de le supprimer. Suivez les étapes ci-dessous pour supprimer un backend de stockage.

1. Connectez-vous au client vSphere.
2. Dans la page raccourcis, sélectionnez **NetApp ONTAP Tools** dans la section modules externes.
3. Dans le volet gauche des outils ONTAP , accédez à **Backends de stockage** et sélectionnez un backend de stockage.
4. Sélectionnez le menu des ellipses verticales et sélectionnez **Supprimer**. Assurez-vous que le backend de stockage ne contient aucun magasin de données. Vous pouvez suivre la progression dans le panneau des tâches récentes.

Vous pouvez effectuer l'opération de suppression pour les clusters ONTAP globaux à l'aide du gestionnaire d'outils ONTAP.

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`

2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **systèmes back-end de stockage** dans la barre latérale.
4. Sélectionnez le système back-end de stockage à supprimer
5. Sélectionnez le menu ellipses verticales et sélectionnez **Supprimer**.

Vue détaillée du système back-end de stockage

La page backend de stockage répertorie tous les backends de stockage. Vous pouvez effectuer des opérations de découverte, de modification et de suppression de stockage sur les backends de stockage que vous avez ajoutés, mais pas sur le SVM enfant individuel sous le cluster.

Sélectionnez le cluster parent ou l'enfant pour afficher le résumé du composant. Pour le cluster parent, utilisez la liste déroulante des actions pour découvrir le stockage, modifier ou supprimer le backend de stockage.

La page de résumé fournit les détails suivants :

- État du système back-end de stockage
- Informations sur la capacité
- Informations de base sur la machine virtuelle
- Détails du certificat tels que le statut du certificat et la date d'expiration.
- Informations réseau telles que l'adresse IP et le port du réseau. Pour le SVM enfant, les informations sont les mêmes que celles du backend de stockage parent.
- Privileges autorisés et restreints pour le backend de stockage. Pour le SVM enfant, les informations sont les mêmes que celles du backend de stockage parent. Les outils ONTAP affichent les privilèges uniquement sur les backends de stockage basés sur des clusters. Si vous ajoutez SVM comme backend de stockage, les informations sur les privilèges ne sont pas affichées.
- La vue détaillée du cluster système ASA r2 n'inclut pas l'onglet des niveaux locaux lorsque la propriété désagrégée est définie sur « vrai » pour le SVM ou le cluster.
- Pour les systèmes SVM ASA r2, le portlet capacité n'est pas affiché. Le portail de capacité n'est requis que lorsque la propriété désagrégée est définie comme « true » pour le SVM ou le cluster.
- Pour les systèmes ASA r2 SVM, la section informations de base présente le type de plateforme.

L'onglet interface fournit des informations détaillées sur l'interface.

L'onglet niveaux locaux fournit des informations détaillées sur la liste des agrégats.

Gérer les instances vCenter Server dans les outils ONTAP

Les instances vCenter Server sont des plateformes de gestion centralisée qui vous permettent de contrôler les hôtes, les machines virtuelles et les systèmes back-end de stockage.

Dissociez les systèmes back-end de stockage de l'instance vCenter Server

La page de liste vCenter Server affiche le nombre de systèmes back-end de stockage associés. Chaque instance de vCenter Server peut être associée ou dissociée à un système back-end de stockage.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web :
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez l'instance vCenter Server requise dans la barre latérale.
4. Sélectionnez les ellipses verticales par rapport au serveur vCenter que vous souhaitez associer ou dissocier avec les systèmes back-end de stockage.
5. Sélectionnez **dissocier le backend de stockage**.

Modifier une instance de vCenter Server

Suivez les étapes ci-dessous pour modifier des instances de vCenter Server.

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web :
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez l'instance de vCenter Server appropriée dans la barre latérale
4. Sélectionnez les ellipses verticales par rapport au serveur vCenter que vous souhaitez modifier et sélectionnez **Modifier**.
5. Dans la fenêtre **Modifier vCenter**, saisissez le nom d'utilisateur, le mot de passe et les détails du port.
6. Téléchargez le certificat et sélectionnez **Modifier**.

Supprimer une instance de vCenter Server

Supprimez tous les backends de stockage du vCenter Server avant de le supprimer.

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web :
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez les instances vCenter Server applicables dans la barre latérale
4. Sélectionnez les points de suspension verticaux en regard du serveur vCenter que vous souhaitez supprimer et sélectionnez **Supprimer**.

> Une fois les instances de vCenter Server supprimées, elles ne seront plus gérées par l'application.

Lorsque vous supprimez des instances de vCenter Server dans les outils ONTAP, les actions suivantes sont effectuées automatiquement :

- Le plug-in n'est pas enregistré.
- Les privilèges de plug-in et les rôles de plug-in sont supprimés.

Renouveler le certificat du serveur vCenter

Les outils ONTAP vous avertissent lorsque le certificat vCenter approche de son expiration ou a expiré. Après avoir renouvelé le certificat vCenter, téléchargez le nouveau certificat sur les outils ONTAP en suivant les étapes suivantes :

1. Connectez-vous à l'interface de diagnostic à distance des outils ONTAP .
2. Obtenez le certificat vCenter renouvelé depuis l'interface de diagnostic :

```
echo | openssl s_client connect <vcenter>:443 2>&1 | sed -n '/-BEGIN
CERTIFICATE/,/END CERTIFICATE/p'
```

3. Assurez-vous que le certificat est au format ASCII Base 64 et qu'il comprend les lignes de début et de fin, par exemple :

```
---{}BEGIN CERTIFICATE{}---
MIIFUzCCA7ugAwIBAgIJANOgLapcl5oSMA0GCSqGSIb3DQEBCwUAMIGJMQwwCgYD
VQQDDAN2YzExFDASBgoJkiaJk/IsZAEZFgRkZW1vMRUwEwYKCZImiZPyLGQBGRYF
bG9jYWwxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRwwGgYDVQQK
DBN2YzEuZGVtby5uZXRhcHAuY29tMQwwCgYDVQQLDANMT0QwHhcNMjQwNDA1MTgw
NTE4WhcNMjYwNDA1MTgwNTE4WjBzMRwwGgYDVQQDDBN2YzEuZGVtby5uZXRhcHAu
Y29tMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTESMBAGA1UEBwwJ
UGFsbyBBbHRvMQ8wDQYDVQQKDAZOZXRBcHAxDDAKBgNVBAsMA0xPRDCCAaIwDQYJ
KoZIhvcNAQEBBQADggGPADCCAYoCggGBALU8OCWMtA2gvIC/OTw/7xucvPVuM+b8
DhzvNpQ2phjfr6ctEhbntPpqPdu+t2CKK7l0mzg3D9cJ/rvMvdDDXr0tgaD1oi2u
ZDW0CaF0QhLOpNfRXMoogBZ66csEhViAy3CHTcOse770mA/PyoHgrCPZngVlZIiQ
TIWpdQMbEEzFIkrLfC70UW2MzfublrsH7Dn/kOu/iCSlVJWixKf7SmZtVQ5ZxBTD
UlJSiqoX1eRXGyunArEvrIpOY9kkKXUElm3hGnk/ZmiuBJ+HqUYqYW+H+7vE3lKa
6NEqDX+tZotxTx2bXMjeiIWU30ZbshgeXlIG9qc49clBoC9iGjavhctOcaXg/W3h
dLKK5ds3rpRERgMg6VMkrfiqAJuiq+b3sTvXMAul/3hL7hz5QABAE/hP4ZvIHV02
WWDQRLiuVFAcDAyvCrO9Irx0Gk1RyRShKYakdWxZ3hhMdLuGq0yvRXqo1Ib94zwO
JfBJHjFToA/GqwromZgiTzJkKq5xbN8MFwIDAQABo4HSMIHPMAsGA1UdDwQEAwIF
4DA7BgNVHREENDAygRVlbWFpbEBkZW1vLm5ldGFwcC5jb22HBMCoAB+CE3ZjMS5k
ZW1vLm5ldGFwcC5jb20wHQYDVR0OBBYEFJ0V0zY+JRpFrEt31ovAY4BLFXmAMB8G
A1UdIwQYMBaAFENf6fRxWF3OJQNTPIdUpK6kjA78MEMGCCsGAQUFBwEBBDcwNTAz
BggrBgEFBQcwAoYnaHR0cHM6Ly92YzEuZGVtby5uZXRhcHAuY29tL2FmZC92ZWNz
L2NhMA0GCSqGSIb3DQEBCwUAA4IBgQBaDfk7GBM4vmhzYCqGrr6KB+h3qeTJ+Y0Y
5nIPRP1HucawDQ8QTay605ddJ8gFGoxkOQDn9tdXWXGjnTRFOT8R+Hw/nUfVSiDP
sYienb16copzUNwtqh+m9Ifow74Gf+ulRzEC0EAVO1X/nTEYH6NKM6Wy7y7F8g5J
lrpM3JY90ZChMqHO3Av/88rbErfQ/gU1brJ3u9Gks4e20Z7Ff312ZKhWRuJDlN2Z
0tc/gp90N9GxaVvELovq/pdjaZ8xiXCxa6piicrJd9WnqMH1gmxP2PIBDxMDBWBG
gwsfs5H7VG9MJYks6lViNsGclo0EwEdF0MfoB3JtsWpPWq6+jBua0Jm7/aFCU+Ht
mykr0gaV7muegoiBQuDma4EkAI31D7ZlUgJQaw157NTk4RW3TFcbtViBHJkM54Hr
iVm0cl+2BZNi/QTMh/MkWV2dYXJ3NuNlqqfzFY+bUfkzkR4SneMk0HX3joNNYDJv
siO7bL+k/Pxql27NVIhuCoVJAlcI7ak=
---{}END CERTIFICATE{}---
```

4. Copiez le résultat et enregistrez-le dans un fichier texte avec un `.pem` extension sur votre bureau.
5. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
6. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
7. Sélectionnez l'instance de vCenter Server appropriée dans la barre latérale
8. Sélectionnez les ellipses verticales par rapport au serveur vCenter que vous souhaitez modifier et sélectionnez **Modifier**.
9. Dans la fenêtre **Modifier vCenter**, saisissez le nom d'utilisateur, le mot de passe et les détails du port.
10. Téléchargez le certificat et sélectionnez **Modifier**.

Informations associées

"Configurer l’accès aux diagnostics à distance"

Gérer les certificats des outils ONTAP

Un certificat auto-signé est généré par défaut pour les outils ONTAP et le fournisseur VASA lors du déploiement. Vous pouvez utiliser l’interface du gestionnaire d’outils ONTAP pour renouveler ce certificat ou le remplacer par un certificat d’autorité de certification personnalisé. Dans les déploiements multi-vCenter, l’utilisation de certificats d’autorité de certification personnalisés est requise.

Avant de commencer

Vous devriez avoir les éléments suivants avant de commencer :

- Le nom de domaine correspond à l’adresse IP virtuelle.
- Résolution réussie du nom de domaine par nslookup, confirmant qu’il correspond à l’adresse IP correcte.
- Certificats créés avec le nom de domaine et l’adresse IP des outils ONTAP .

Une adresse IP des outils ONTAP doit correspondre à un nom de domaine complet (FQDN). Les certificats doivent contenir le même nom de domaine complet mappé à l’adresse IP des outils ONTAP dans les autres noms d’objet ou d’objet.

Vous ne pouvez pas passer d’un certificat signé par une autorité de certification à un certificat auto-signé.

Certificat de mise à niveau des outils ONTAP

L'onglet Outils ONTAP affiche des détails tels que le type de certificat (auto-signé/CA signé) et le nom de domaine. Pendant le déploiement, le certificat auto-signé est généré par défaut. Vous pouvez renouveler le certificat ou le mettre à niveau vers une autorité de certification.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **certificats** > **ONTAP Tools** > **Renew** pour renouveler les certificats.

   Vous pouvez renouveler le certificat s'il a expiré ou s'il approche de sa date d'expiration. L'option renouveler est disponible lorsque le type de certificat est signé par une autorité de certification. Dans la fenêtre contextuelle, indiquez le certificat du serveur, la clé privée, l'autorité de certification racine et le certificat intermédiaire.

   Le système sera hors ligne jusqu'à ce que le certificat soit renouvelé et vous serez déconnecté de l'interface du Gestionnaire d'outils ONTAP.

4. Pour mettre à niveau le certificat auto-signé vers un certificat CA personnalisé, sélectionnez **certificats** > **ONTAP Tools** > **mettre à niveau vers CA** option.
   a. Dans la fenêtre contextuelle, téléchargez le certificat du serveur, la clé privée du certificat du serveur, le certificat de l'autorité de certification racine et les fichiers de certificat intermédiaires.
   b. Saisissez le nom de domaine complet (FQDN) de l'adresse IP de l'équilibreur de charge pour lequel vous avez généré ce certificat et mettez-le à jour.

      Le système sera hors ligne jusqu'à la fin de la mise à niveau et vous serez déconnecté de l'interface du Gestionnaire d'outils ONTAP.

Mettre à niveau le certificat VASA Provider

Les outils ONTAP pour VMware vSphere sont déployés avec un certificat auto-signé pour VASA Provider. Avec cela, une seule instance vCenter Server peut être gérée pour les datastores vVols. Lorsque vous gérez plusieurs instances de vCenter Server et que vous souhaitez activer la fonctionnalité vVols sur celles-ci, vous devez remplacer le certificat auto-signé par un certificat d'autorité de certification personnalisé.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **certificats** > **VASA Provider** ou **ONTAP Tools** > **Renew** pour renouveler les certificats.
4. Sélectionnez **certificats** > **VASA Provider** ou **ONTAP Tools** > **mettre à niveau vers CA** pour mettre à niveau le certificat auto-signé vers un certificat CA personnalisé.
   a. Dans la fenêtre contextuelle, téléchargez le certificat du serveur, la clé privée du certificat du serveur, le certificat de l'autorité de certification racine et les fichiers de certificat intermédiaires.

b. Saisissez le nom de domaine complet (FQDN) de l'adresse IP de l'équilibreur de charge pour lequel vous avez généré ce certificat et mettez-le à jour.

Le système sera hors ligne jusqu'à la fin de la mise à niveau et vous serez déconnecté de l'interface du Gestionnaire d'outils ONTAP.

Accès aux outils ONTAP pour la console de maintenance VMware vSphere

Découvrez la console de maintenance des ONTAP tools

La console de maintenance des ONTAP tools for VMware vSphere vous permet de gérer les paramètres des applications, du système et du réseau. Vous pouvez mettre à jour les mots de passe d'administrateur et de maintenance, générer des packages de support, configurer les niveaux de journalisation, gérer les paramètres TLS et activer les diagnostics à distance.

Après le déploiement des ONTAP tools for VMware vSphere, si la console de maintenance n'est pas accessible, installez les outils VMware à partir du serveur vCenter. Connectez-vous en utilisant le `maint` Nom d'utilisateur et mot de passe définis lors du déploiement. Utilisez **nano** pour modifier les fichiers dans la console de maintenance ou la console de connexion root.

Vous devez définir un mot de passe pour le `diag` utilisateur lors de l'activation des diagnostics à distance.

Vous devez utiliser l'onglet **Summary** de vos outils ONTAP déployés pour VMware vSphere pour accéder à la console de maintenance. Lorsque vous sélectionnez , la console de maintenance démarre.

Menu Console	Options
Configuration de l'application	1. Afficher le récapitulatif de l'état du serveur 2. Modifier le niveau LOG pour les services des outils ONTAP 3. Modifier l'indicateur de validation du certificat
Configuration du système	1. Redémarrez la machine virtuelle 2. Arrêter la machine virtuelle 3. Modifier le mot de passe utilisateur « familiariser » 4. Modifier le fuseau horaire 5. Augmentation de la taille des disques de prison (/prison) 6. Mise à niveau 7. Installez VMware Tools

Configuration du réseau	1. Afficher les paramètres d'adresse IP 2. Afficher les paramètres de recherche du nom de domaine 3. Modifier les paramètres de recherche du nom de domaine 4. Afficher les routes statiques 5. Modifier les routes statiques 6. Valider les modifications 7. Envoyez une requête ping à un hôte 8. Restaurez les paramètres par défaut
Support et diagnostics	1. Accéder au shell de diagnostic 2. Activer l'accès aux diagnostics à distance 3. Fournir les informations d'identification vCenter pour la sauvegarde 4. Effectuer des sauvegardes

Configurer l'accès de diagnostic à distance pour ONTAP tools

Vous pouvez configurer les outils ONTAP pour VMware vSphere afin d'activer l'accès SSH pour l'utilisateur diag.

Avant de commencer

Activez l'extension VASA Provider pour votre instance vCenter Server.

Description de la tâche

L'utilisation de SSH pour accéder au compte utilisateur diag présente les limites suivantes :

- vous n'êtes autorisé qu'à un seul compte de connexion par activation de SSH.
- L'accès SSH au compte utilisateur diag est désactivé lorsque l'une des conditions suivantes se produit :
  - Le délai expire.

    La session de connexion expire à minuit le lendemain.
  - Vous vous connectez à nouveau en tant qu'utilisateur diag à l'aide de SSH.

Étapes

1. Depuis vCenter Server, ouvrez une console vers VASA Provider.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrez `4` pour sélectionner **support et diagnostic**.
4. Entrer `2` pour sélectionner **Activer l'accès au diagnostic à distance**.
5. Entrez `y` Dans la boîte de dialogue Confirmation pour activer l'accès au diagnostic à distance.
6. Saisissez un mot de passe pour l'accès au diagnostic à distance.

Démarrer SSH sur les autres nœuds ONTAP tools

Vous devez démarrer SSH sur les autres nœuds avant la mise à niveau.

Avant de commencer

Activez l'extension VASA Provider pour votre instance vCenter Server.

Description de la tâche

Répétez cette procédure sur chaque nœud avant la mise à niveau.

Étapes

1. Depuis vCenter Server, ouvrez une console vers VASA Provider.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrez `4` Pour sélectionner support et Diagnostics.
4. Entrez `1` Pour sélectionner accès au shell de diagnostic.
5. Entrez `y` pour continuer.
6. Exécutez la commande *sudo systemctl restart ssh*.

Mettre à jour les informations d'identification du serveur vCenter dans ONTAP tools

Vous pouvez mettre à jour les informations d'identification de l'instance vCenter Server à l'aide de la console de maintenance.

Avant de commencer

Vous devez disposer des informations d'identification de l'utilisateur de maintenance.

Description de la tâche

Si vous avez modifié les informations d'identification de vCenter Server après le déploiement, mettez-les à jour en suivant cette procédure.

Étapes

1. Depuis vCenter Server, ouvrez une console vers VASA Provider.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrez `2` pour sélectionner le menu de configuration du système.
4. Entrer `8` modifier les informations d'identification vCenter.

Modifier l'indicateur de validation du certificat dans ONTAP tools

Par défaut, l'indicateur de validation du certificat est activé (défini sur vrai). Vous pouvez définir l'indicateur de validation du certificat backend de stockage ONTAP sur false si vous devez contourner les vérifications de certificat SAN. Ce paramètre ne s'applique pas aux certificats vCenter Server.

Avant de commencer

Vous devez disposer des informations d'identification de l'utilisateur de maintenance.

Étapes

1. À partir du serveur vCenter, ouvrez une console pour accéder aux outils ONTAP.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrer `1` pour sélectionner le menu **Configuration de l'application**.
4. Entrer `3` pour modifier l'indicateur de validation du certificat.

   La console de maintenance affiche l'état de l'indicateur de validation du certificat et vous invite à le modifier.

5. Entrez « y » pour basculer le drapeau ou « n » pour annuler.

Lorsque vous activez l'indicateur de validation du certificat (défini sur vrai), les outils ONTAP vérifient que tous les systèmes de stockage utilisent des certificats avec un nom alternatif de sujet (SAN). Si un système dorsal utilise un certificat sans SAN, la validation du certificat ne peut pas être activée. Avant d'activer cette option, vérifiez que tous les systèmes de stockage utilisent des certificats basés sur SAN. Si vous désactivez l'indicateur de validation du certificat (défini sur false), les outils ONTAP contournent la validation du certificat pour tous les systèmes de stockage configurés.

Rapports sur les outils ONTAP

Le plug-in ONTAP Tools for VMware vSphere fournit des rapports pour les machines virtuelles et les datastores. Lorsque vous sélectionnez l'icône du plug-in NetApp ONTAP Tools for VMware vSphere dans la section des raccourcis du client vCenter, l'interface utilisateur accède à la page Présentation. Sélectionnez l'onglet Rapports pour afficher la machine virtuelle et le rapport datastores.

Le rapport Machines virtuelles affiche la liste des machines virtuelles découvertes (doivent avoir au moins un disque provenant de banques de données basées sur le stockage ONTAP) avec des mesures de performances. Lorsque vous développez l'enregistrement de la machine virtuelle, l'interface affiche toutes les informations relatives au disque et à la banque de données.

Le rapport sur les banques de données répertorie les banques de données découvertes ou reconnues par les ONTAP tools for VMware vSphere qui utilisent un stockage ONTAP , avec des indicateurs de performance.

Vous pouvez utiliser l'option gérer les colonnes pour masquer ou afficher différentes colonnes.

Gérer des machines virtuelles

Considérations relatives à la migration et au clonage de machines virtuelles pour ONTAP tools

Lors de la migration de machines virtuelles existantes dans votre data Center, vous devez prendre en compte certaines considérations.

Migrer des machines virtuelles protégées

Vous pouvez migrer les machines virtuelles protégées vers :

- Même datastore vVvols dans un autre hôte ESXi

- Il existe un autre datastore compatible vVvols dans le même hôte ESXi
- Il existe un autre datastore compatible vVvols dans un hôte VMware ESXi différent

Si vous migrez la machine virtuelle vers un autre FlexVol volume, le système met à jour le fichier de métadonnées de ce volume avec les informations de la machine virtuelle. Si une machine virtuelle est migrée vers un autre hôte ESXi mais avec le même stockage, le fichier de métadonnées du FlexVol volume sous-jacent ne sera pas modifié.

Machines virtuelles protégées par des clones

Vous pouvez cloner des machines virtuelles protégées à plusieurs méthodes :

- Même conteneur du même volume FlexVol à l'aide du groupe de réplication

  Le fichier de métadonnées du volume FlexVol est mis à jour avec les détails de la machine virtuelle clonée.

- Même conteneur d'un autre volume FlexVol utilisant le groupe de réplication

  Volume FlexVol où la machine virtuelle clonée est placée, le fichier de métadonnées est mis à jour avec les détails de la machine virtuelle clonée.

- Il existe un autre conteneur ou datastore vvols

  Volume FlexVol sur lequel la machine virtuelle clonée est placée, le fichier de métadonnées est mis à jour les informations relatives à la machine virtuelle.

VMware ne prend actuellement pas en charge les machines virtuelles clonées sur un modèle de machine virtuelle.

Le clonage d'une machine virtuelle protégée est pris en charge.

Voir "Création d'une machine virtuelle pour le clonage" pour plus de détails.

Snapshots de machine virtuelle

Actuellement, seuls les snapshots de machine virtuelle sans mémoire sont pris en charge. Si la machine virtuelle possède une copie Snapshot de la mémoire, la machine virtuelle n'est pas prise en compte pour sa protection.

Vous ne pouvez pas non plus protéger les machines virtuelles non protégées qui disposent d'un instantané de mémoire. Pour cette version, vous devez supprimer l'instantané de mémoire avant d'activer la protection de la machine virtuelle.

Pour une machine virtuelle Windows avec le type de stockage ASA r2, un instantané de la machine virtuelle est en lecture seule. Lorsque vous mettez la VM sous tension, le fournisseur VASA crée un LUN à partir de l'instantané en lecture seule et active les IOPS. Lorsque vous mettez la machine virtuelle hors tension, le fournisseur VASA supprime le LUN et désactive les IOPS.

Migrer des machines virtuelles vers des datastores vVols dans ONTAP tools

Vous pouvez migrer des machines virtuelles des datastores NFS et VMFS vers des datastores Virtual volumes (vVols) pour tirer parti de la gestion des machines virtuelles basée sur des règles et d'autres fonctionnalités vVols. Les datastores vvols vous

permettent de répondre à de plus en plus de besoins de charge de travail.

Avant de commencer

Assurez-vous que VASA Provider ne s'exécute sur aucune des machines virtuelles que vous prévoyez de migrer. Si vous migrez une machine virtuelle qui exécute VASA Provider dans un datastore vvols, vous ne pouvez pas effectuer d'opérations de gestion, y compris la mise sous tension des machines virtuelles qui se trouvent sur des datastores vvols.

Description de la tâche

Lorsque vous migrez d'un datastore NFS et VMFS vers un datastore vVols, vCenter Server utilise les API vStorage APIs for Array Integration (VAAI) pour décharger les données lors du déplacement de datastores VMFS, mais pas à partir d'un fichier VMDK NFS. VAAI réduit généralement la charge sur l'hôte.

Étapes

1. Cliquez avec le bouton droit de la souris sur la machine virtuelle à migrer et sélectionnez **migrer**.
2. Sélectionnez **changer stockage uniquement**, puis **Suivant**.
3. Sélectionnez un format de disque virtuel, une stratégie de stockage de machine virtuelle et une banque de données vVol qui correspondent aux fonctionnalités de la banque de données que vous migrez.
4. Vérifiez les paramètres et sélectionnez **Terminer**.

Nettoyer les configurations VASA dans ONTAP tools

Pour mener à bien le processus de nettoyage VASA, suivez ces étapes.

Il est recommandé de supprimer tous les datastores vVols avant de commencer le nettoyage VASA.

Étapes

1. Annulez l'enregistrement du plug-in en accédant à https://OTV_IP:8143/Register.html
2. Vérifiez que le plug-in n'est plus disponible sur vCenter Server.
3. Fermez les outils ONTAP pour VMware vSphere VM.
4. Supprimez les outils ONTAP pour VMware vSphere VM.

Attacher ou détacher un disque de données d'une machine virtuelle dans ONTAP tools

Suivez ces étapes pour attacher ou détacher des disques de données de machines virtuelles dans vSphere et gérer leurs ressources de stockage.

Reliez un disque de données à une machine virtuelle

Connectez un disque de données à une machine virtuelle pour augmenter son espace de stockage.

Étapes

1. Connectez-vous au client vSphere.
2. Cliquez avec le bouton droit sur une machine virtuelle dans l'inventaire et sélectionnez **Modifier les paramètres**.
3. Dans l'onglet **matériel virtuel**, sélectionnez **disque dur existant**.

4. Sélectionnez la machine virtuelle sur laquelle le disque existe.
5. Sélectionnez le disque que vous souhaitez connecter et sélectionnez le bouton **OK**.

Résultat

Le disque dur apparaît dans la liste périphériques matériels virtuels.

Détacher un disque de données de la machine virtuelle

Détachez un disque de données d'une machine virtuelle lorsque vous n'en avez plus besoin. Le disque n'est pas supprimé ; il reste sur le système de stockage ONTAP .

Étapes

1. Connectez-vous au client vSphere.
2. Cliquez avec le bouton droit sur une machine virtuelle dans l'inventaire et sélectionnez **Modifier les paramètres**.
3. Déplacez votre pointeur sur le disque et sélectionnez **Supprimer**.

> Le disque est supprimé de la machine virtuelle. Si d'autres machines virtuelles partagent le disque, les fichiers du disque ne sont pas supprimés.

Informations associées

"Ajouter un nouveau disque dur à une machine virtuelle"

"Ajouter un disque dur existant à une machine virtuelle"

Découvrez les systèmes de stockage et les hôtes dans ONTAP tools

Lors du premier lancement ONTAP tools for VMware vSphere dans le client vSphere, celui-ci détecte automatiquement les hôtes ESXi, leurs LUN et exportations NFS associés, ainsi que les systèmes de stockage NetApp qui possèdent ces ressources.

Avant de commencer

- Assurez-vous que tous les hôtes ESXi sont allumés et connectés.
- Assurez-vous que toutes les machines virtuelles de stockage (SVM) à découvrir sont en cours d'exécution et que chaque nœud du cluster dispose d'au moins une interface logique de données (LIF) configurée pour le protocole de stockage utilisé (NFS ou iSCSI).

Description de la tâche

Vous pouvez découvrir de nouveaux systèmes de stockage ou mettre à jour ceux existants pour obtenir les dernières informations sur leur capacité et leur configuration. Vous pouvez également modifier les ONTAP tools for VMware vSphere afin d'accéder au système de stockage.

Lors de la découverte des systèmes de stockage, les outils ONTAP pour VMware vSphere collectent des informations à partir des hôtes ESXi gérés par l'instance vCenter Server.

Étapes

1. Sur la page d'accueil de vSphere client, sélectionnez **hosts and clusters**.

2. Cliquez avec le bouton droit sur le centre de données requis et sélectionnez * Outils NetApp ONTAP * > * Mettre à jour les données de l'hôte * .

   Dans la boîte de dialogue **confirmer**, confirmez votre choix.

3. Sélectionnez les contrôleurs de stockage détectés qui ont l'état `Authentication Failure` et sélectionnez **actions** > **Modifier**.
4. Renseignez les informations requises dans la boîte de dialogue **Modifier le système de stockage**.
5. Répétez les étapes 4 et 5 pour tous les contrôleurs de stockage avec `Authentication Failure` état.

Une fois le processus de détection terminé, effectuez les actions suivantes :

- Utilisez les outils ONTAP pour VMware vSphere pour configurer les paramètres de l'hôte VMware ESXi pour les hôtes qui affichent l'icône d'alerte dans la colonne des paramètres de l'adaptateur, dans la colonne des paramètres MPIO ou dans la colonne des paramètres NFS.
- Indiquez les informations d'identification du système de stockage.

Modifiez les paramètres de l'hôte VMware ESXi à l'aide des outils ONTAP

Utilisez le tableau de bord des outils ONTAP dans VMware vSphere pour identifier les problèmes de configuration, sélectionner les hôtes ESXi, consulter les paramètres recommandés par NetApp et les appliquer.

Avant de commencer

Le portlet des systèmes hôtes ESXi affiche les problèmes liés aux paramètres de l'hôte ESXi. Sélectionnez un problème pour afficher le nom d'hôte ou l'adresse IP.

Étapes

1. Connectez-vous au client vSphere.
2. Dans la page raccourcis, sélectionnez **NetApp ONTAP Tools** dans la section modules externes.
3. Accédez au portlet **ESXi Host Compliance** dans la Présentation (tableau de bord) du plug-in ONTAP Tools for VMware vSphere.
4. Sélectionnez le lien **appliquer les paramètres recommandés**.
5. Dans la fenêtre **Appliquer les paramètres d'hôte recommandés**, sélectionnez les hôtes pour lesquels vous souhaitez utiliser les paramètres d'hôte recommandés par NetApp , puis sélectionnez **Suivant**.

   Vous pouvez développer l'hôte ESXi pour voir les valeurs actuelles.

6. Dans la page des paramètres, sélectionnez les valeurs recommandées.
7. Dans le volet récapitulatif, vérifiez les valeurs et sélectionnez **Terminer**. Vous pouvez suivre la progression dans le panneau des tâches récentes.

Informations associées

"Configurer les paramètres de l'hôte ESXi"

Gérer les mots de passe

Modifier le mot de passe du gestionnaire d'outils ONTAP

Vous pouvez modifier le mot de passe administrateur à l'aide du Gestionnaire d'outils ONTAP.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec vos identifiants d'administrateur ONTAP tools for VMware vSphere .
3. Sélectionnez l'icône **Administrator** dans le coin supérieur droit de l'écran et sélectionnez **Modifier le mot de passe**.
4. Dans la fenêtre contextuelle de changement de mot de passe, saisissez l'ancien et le nouveau mot de passe. L'écran de l'interface utilisateur affiche les exigences relatives au mot de passe.
5. Sélectionnez **Modifier** pour appliquer les modifications.

Réinitialisez le mot de passe du gestionnaire d'outils ONTAP

Si vous oubliez le mot de passe du gestionnaire d'outils ONTAP , vous pouvez rétablir l'accès administrateur à l'aide d'un jeton de réinitialisation généré à partir de la console de maintenance des ONTAP tools for VMware vSphere .

Étapes

1. Ouvrez un navigateur web et accédez à `https://<ONTAPtoolsIP>:8443/virtualization/ui/` pour accéder au gestionnaire d'outils ONTAP .
2. Sur la page de connexion, sélectionnez **Réinitialiser le mot de passe**.
3. Générez un jeton de réinitialisation de mot de passe à l'aide des ONTAP tools for VMware vSphere :
   a. Connectez-vous au serveur vCenter et ouvrez la console de maintenance.
   b. Entrer `2` pour sélectionner **Configuration système**.
   c. Entrer `3` pour sélectionner **Modifier le mot de passe de l'utilisateur 'maintenance'**.
4. Dans la boîte de dialogue de réinitialisation du mot de passe, saisissez le jeton de réinitialisation, le nom d'utilisateur et le nouveau mot de passe.
5. Sélectionnez **Réinitialiser** pour mettre à jour les informations d'identification.
6. Connectez-vous à ONTAP Tools Manager avec le nouveau mot de passe.

Réinitialiser le mot de passe utilisateur de l'application dans ONTAP tools

Suivez ces étapes pour réinitialiser le mot de passe utilisateur de l'application nécessaire à l'enregistrement du fournisseur SRA et VASA auprès de vCenter Server à l'aide des ONTAP tools for VMware vSphere.

Étapes

1. Ouvrez un navigateur web et accédez à : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`

2. Connectez-vous en utilisant les identifiants d'administrateur configurés lors du déploiement des outils ONTAP .
3. Dans la barre latérale, sélectionnez **Paramètres**.
4. Sur la page **identifiants VASA/SRA**, sélectionnez **Réinitialiser le mot de passe**.
5. Saisissez et confirmez le nouveau mot de passe.
6. Sélectionnez **Réinitialiser** pour appliquer le nouveau mot de passe.

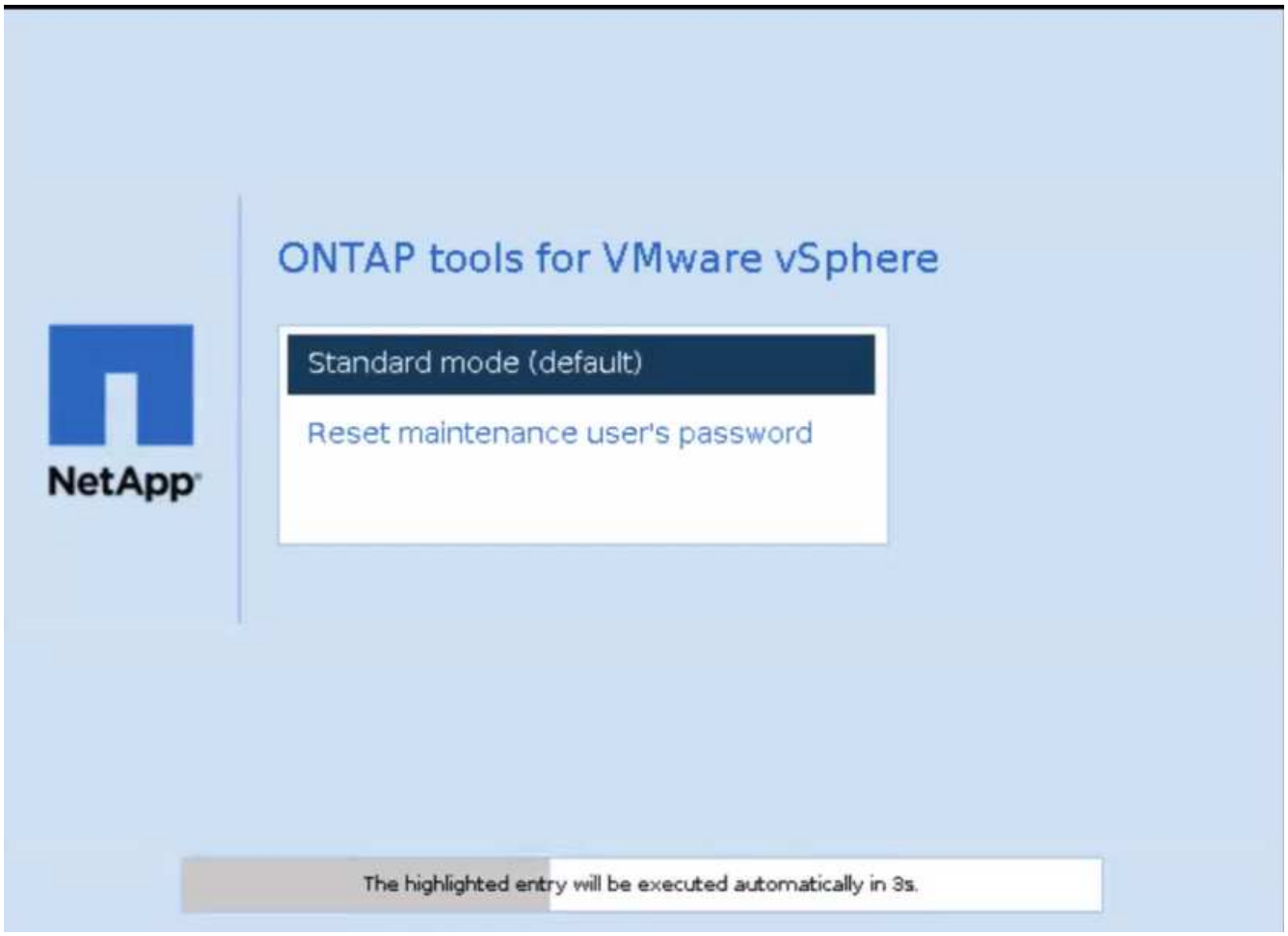
Réinitialiser le mot de passe de la console de maintenance des ONTAP tools

Lors du redémarrage du système d'exploitation invité, le menu GRUB affiche une option permettant de réinitialiser le mot de passe de l'utilisateur de la console de maintenance. Utilisez cette option pour mettre à jour le mot de passe utilisateur de la console de maintenance sur la machine virtuelle. Après avoir réinitialisé le mot de passe, la machine virtuelle redémarre pour définir le nouveau mot de passe. Dans un scénario de déploiement haute disponibilité, après le redémarrage de la machine virtuelle, le mot de passe est automatiquement mis à jour sur les deux autres machines virtuelles.

Pour les ONTAP tools for VMware vSphere HA, vous devez modifier le mot de passe utilisateur de la console de maintenance sur le nœud de gestion des outils ONTAP , qui est node1.

Étapes

1. Connectez-vous à votre serveur vCenter
2. Cliquez avec le bouton droit de la souris sur la machine virtuelle et sélectionnez **Power** > **Restart Guest OS**
   Pendant le redémarrage du système, l'écran suivant s'affiche :



Vous avez 5 secondes pour choisir votre option. Appuyez sur n'importe quelle touche pour arrêter la progression et geler le menu GRUB.

3. Sélectionnez l'option **Réinitialiser le mot de passe de l'utilisateur de maintenance**. La console de maintenance s'ouvre.
4. Dans la console, saisissez et confirmez le nouveau mot de passe. Vous avez trois tentatives. Le système redémarre après la saisie correcte du nouveau mot de passe.
5. Appuyez sur **Entrée** pour continuer. Le système met à jour le mot de passe sur la machine virtuelle.

Le même menu GRUB apparaît également lors de la mise sous tension de la VM. Toutefois, vous ne devez utiliser l'option de réinitialisation du mot de passe qu'avec l'option **Redémarrer le système d'exploitation invité**.

Gestion de la protection des clusters hôtes

Modifier un cluster d'hôtes protégé dans ONTAP tools

Vous pouvez modifier les paramètres de protection d'un cluster hôte dans un seul workflow. Les modifications suivantes sont prises en charge :

- Ajoutez de nouveaux datastores ou hôtes au cluster protégé.
- Ajoutez de nouvelles relations SnapMirror aux paramètres de protection.

- Supprimez les relations SnapMirror existantes des paramètres de protection.
- Modifier une relation SnapMirror existante.

> Vous devez effectuer la découverte de stockage après avoir créé, modifié ou supprimé la protection d'un cluster hôte afin de refléter les modifications. Si vous n'effectuez pas la découverte de stockage, les modifications sont reflétées après le déclenchement de la découverte de stockage périodique.

Surveillez la protection des clusters hôtes

Surveillez l'état de protection, les relations SnapMirror , les banques de données et l'état SnapMirror pour chaque cluster d'hôtes protégé.

Étapes

1. Connectez-vous au client vSphere.
2. Accédez à * Outils NetApp ONTAP * > **Protection** > **Relations entre clusters d'hôtes**.

   La colonne de protection affiche une icône qui indique l'état de protection.

3. Passez la souris sur l'icône pour afficher plus de détails.

Ajoutez de nouveaux datastores ou hôtes

Ajoutez des hôtes ou créez des banques de données sur le cluster protégé à l'aide de l'interface utilisateur vCenter.

Étapes

1. Connectez-vous au client vSphere.
2. Pour modifier les propriétés d'un cluster protégé, vous pouvez l'un ou l'autre
   a. Accédez à * Outils NetApp ONTAP * > * Protection * > * Relations entre clusters d'hôtes *, sélectionnez le menu à points de suspension à côté du cluster et sélectionnez * Modifier * ou
   b. Cliquez avec le bouton droit sur un cluster hôte et sélectionnez * Outils NetApp ONTAP * > * Protéger le cluster *.
3. Si vous créez une banque de données dans l'interface utilisateur de vCenter, elle apparaît comme non protégée. Vous pouvez afficher tous les magasins de données du cluster et leur état de protection dans une boîte de dialogue. Sélectionnez le bouton **Protéger** pour activer la protection.

   > Après avoir créé une banque de données dans l'interface utilisateur de vCenter Server, sélectionnez **Découvrir** sur la page de présentation pour afficher la banque de données comme candidate à la protection dans le cluster hôte. L'état de protection est mis à jour sur protégé après la prochaine découverte de protection périodique.

4. Si vous ajoutez un nouvel hôte ESXi, l'état de protection est affiché comme partiellement protégé. Sélectionnez le menu points de suspension sous les paramètres SnapMirror et sélectionnez **Modifier** pour définir la proximité de l'hôte ESXi nouvellement ajouté.

   > Pour les relations asynchrones, la modification n'est pas prise en charge dans les outils ONTAP car le SVM cible d'un site tertiaire ne peut pas être ajouté à la même instance. Pour modifier la configuration de la relation, utilisez le Gestionnaire système ou l'interface de ligne de commande sur la SVM cible.

5. Après avoir effectué les modifications, sélectionnez **Enregistrer**.
6. Vous pouvez voir les modifications dans la fenêtre **Protect Cluster**.

Les outils ONTAP créent une tâche vCenter et vous pouvez suivre sa progression dans le panneau **Tâche récente**.

Ajouter une nouvelle relation SnapMirror

Étapes

1. Connectez-vous au client vSphere.
2. Pour modifier les propriétés d'un cluster protégé, vous pouvez l'un ou l'autre
   a. Accédez à * Outils NetApp ONTAP * > * Protection * > * Relations entre clusters d'hôtes *, sélectionnez le menu à points de suspension en regard du cluster et sélectionnez * Modifier * ou
   b. Cliquez avec le bouton droit sur un cluster hôte et sélectionnez * Outils NetApp ONTAP * > * Protéger le cluster *.
3. Sélectionnez **Ajouter une relation**.
4. Ajoutez une nouvelle relation en tant que type de stratégie **Asynchronous** ou **AutomatedFailOverDuplex**.
5. Sélectionnez **protéger**.

   Vous pouvez voir les modifications dans la fenêtre **Protect Cluster**.

Les outils ONTAP créent une tâche vCenter et vous pouvez suivre sa progression dans le panneau **Tâche récente**.

Supprimez une relation SnapMirror existante

Pour supprimer une relation asynchrone SnapMirror , assurez-vous que le SVM ou le cluster du site secondaire est ajouté en tant que backend de stockage dans les ONTAP tools for VMware vSphere. Vous ne pouvez pas supprimer toutes les relations SnapMirror à la fois. La suppression d'une relation supprime également la relation correspondante du cluster ONTAP . Lorsque vous supprimez une relation SnapMirror Duplex de basculement automatisé, le système démappe les banques de données de destination et supprime le groupe de cohérence, les LUN, les volumes et les igroups du cluster ONTAP de destination.

Lorsque vous supprimez la relation, le système réanalyse le site secondaire pour supprimer le LUN non mappé en tant que chemin actif des hôtes.

Étapes

1. Connectez-vous au client vSphere.
2. Pour modifier les propriétés d'un cluster protégé, vous pouvez l'un ou l'autre
   a. Accédez à * Outils NetApp ONTAP * > * Protection * > * Relations entre clusters d'hôtes *, sélectionnez le menu à points de suspension en regard du cluster et sélectionnez * Modifier * ou
   b. Cliquez avec le bouton droit sur un cluster hôte et sélectionnez * Outils NetApp ONTAP * > * Protéger le cluster *.
3. Sélectionnez le menu points de suspension sous les paramètres SnapMirror et sélectionnez **Supprimer**.
   - Si vous supprimez une relation basée sur un type de stratégie asynchrone d'un cluster d'hôtes protégé, vous devez supprimer manuellement les éléments de stockage du cluster de stockage tertiaire. Les éléments de stockage incluent des groupes de cohérence, des volumes (pour les systèmes ONTAP),

des unités de stockage (LUN/espaces de noms) et des instantanés.

- Si vous supprimez une relation basée sur une stratégie de basculement automatique duplex (AFD) d'un cluster d'hôtes protégé, vous pouvez choisir de supprimer les éléments de stockage associés sur le stockage secondaire directement à partir de l'interface.
- Si vous supprimez une relation basée sur une stratégie de duplex de basculement automatisé (AFD) et que le groupe de cohérence est désormais hiérarchique pour les sauvegardes au niveau de l'application, un avertissement s'affiche concernant l'impact de la sauvegarde. Confirmez pour continuer. Après confirmation, supprimez les éléments de stockage associés sur le stockage secondaire. Si vous ne les supprimez pas, ils restent sur le site secondaire.

Les outils ONTAP créent une tâche vCenter et vous pouvez suivre sa progression dans le panneau **Tâche récente**.

Modifier une relation SnapMirror existante

Pour modifier une relation asynchrone SnapMirror , assurez-vous que le SVM ou le cluster du site secondaire est ajouté en tant que backend de stockage dans les ONTAP tools for VMware vSphere. Pour les relations SnapMirror Duplex de basculement automatisé, vous pouvez mettre à jour la proximité de l'hôte pour les configurations uniformes ou l'accès à l'hôte pour les configurations non uniformes. Le changement entre les types de stratégie Duplex de basculement asynchrone et automatisé n'est pas pris en charge. Vous pouvez configurer les paramètres de proximité ou d'accès pour les hôtes nouvellement découverts dans le cluster.

Vous ne pouvez pas modifier une relation asynchrone SnapMirror existante.

Étapes

1. Connectez-vous au client vSphere.
2. Pour modifier les propriétés d'un cluster protégé, vous pouvez l'un ou l'autre
   a. Accédez à * Outils NetApp ONTAP * > * Protection * > * Relations entre clusters d'hôtes *, sélectionnez le menu à points de suspension en regard du cluster et sélectionnez * Modifier * ou
   b. Cliquez avec le bouton droit sur un cluster hôte et sélectionnez * Outils NetApp ONTAP * > * Protéger le cluster *.
3. Si le type de stratégie AutomatedFailOverDuplex est sélectionné, ajoutez les détails de proximité ou d'accès à l'hôte.
4. Sélectionnez le bouton **protéger**.

Les outils ONTAP créent une tâche vCenter. Suivez sa progression dans le panneau **Tâche récente**.

Supprimer la protection du cluster hôte dans ONTAP tools

Lorsque vous supprimez la protection du cluster hôte, les datastores deviennent non protégés.

Étapes

1. Pour afficher la liste des clusters d'hôtes protégés, accédez à * Outils NetApp ONTAP * > **Protection** > **Relations entre les clusters d'hôtes**.

   Sur cette page, surveillez les clusters d'hôtes protégés, l'état de protection, la relation SnapMirror et le statut. Sélectionnez des groupes de cohérence pour afficher la capacité, les banques de données associées et les groupes enfants.

2. Dans la fenêtre **Protection du cluster hôte**, sélectionnez le menu à points de suspension à côté du cluster et sélectionnez **Supprimer la protection**.
    - Si vous supprimez la protection d'un cluster hôte avec uniquement une relation asynchrone SnapMirror , vous devez supprimer manuellement les éléments de stockage. Les éléments de stockage incluent des groupes de cohérence, des volumes (pour le système ONTAP), des unités de stockage (LUN) et des instantanés.
    - Si vous supprimez la protection d'un cluster hôte avec uniquement une relation de stratégie SnapMirror basée sur un duplex de basculement automatisé et un groupe de cohérence non hiérarchique, vous pouvez supprimer les éléments de stockage associés sur le stockage secondaire directement à partir du même écran.
    - Si vous supprimez la protection d'un cluster hôte avec à la fois des stratégies SnapMirror et un groupe de cohérence hiérarchique pour les sauvegardes, un avertissement s'affiche concernant les impacts de la sauvegarde. Confirmez pour continuer. Après confirmation, supprimez les éléments de stockage associés sur le stockage secondaire. Si vous ne nettoyez pas, les éléments de stockage restent sur le site secondaire.

Récupérer la configuration des outils ONTAP

À partir des ONTAP tools for VMware vSphere 10.5, la fonction de sauvegarde est activée par défaut.

La banque de données dans laquelle vous déployez les ONTAP tools for VMware vSphere stocke les fichiers de sauvegarde. Un dossier nommé d'après l'adresse IP des outils ONTAP (points remplacés par des traits de soulignement et suffixés par *OTV_backup*) conserve les deux fichiers de sauvegarde les plus récents (*OTV_backup_1.tar.enc* et *OTV_backup_2.tar.enc*) et un fichier d'informations (*OTV_backup_info.txt*) qui contient le nom de la dernière sauvegarde.

Assurez-vous que la nouvelle machine virtuelle utilise la même adresse IP des outils ONTAP et correspond à la configuration initiale du système, y compris les services activés, la taille du nœud et le mode HA.

Étapes

1. Téléchargez les fichiers de sauvegarde du magasin de données de la machine virtuelle d'origine sur votre système local.
    a. Accédez à la section Stockage et choisissez le magasin de données qui contient les fichiers de sauvegarde de la machine virtuelle.
    b. Sélectionnez la section **fichiers**.
    c. Téléchargez le répertoire de sauvegarde requis.
2. Mettez hors tension la machine virtuelle existante. Ensuite, déployez une nouvelle machine virtuelle en utilisant le même fichier OVA que le déploiement d'origine.
3. Dans vCenter Server, ouvrez la console de maintenance.
4. Connectez-vous en tant qu'utilisateur de maintenance.
5. Entrez `4` pour sélectionner **support et diagnostic**.
6. Entrez `2` pour sélectionner l'option **Activer l'accès au diagnostic à distance** et créer un nouveau mot de passe pour l'accès au diagnostic.
7. Choisissez un fichier de sauvegarde dans le répertoire téléchargé. Reportez-vous au fichier *OTV_backup_info.txt* pour identifier la dernière sauvegarde.
8. Utilisez la commande suivante pour transférer le fichier de sauvegarde vers la nouvelle machine virtuelle.

Lorsque vous y êtes invité, saisissez le mot de passe de diagnostic.

```
scp <OTV_backup_X.tar.enc>
diag@<node_ip>:/home/diag/system_recovery.tar.enc
```

ne modifiez pas le chemin de destination et le nom du fichier (/home/diag/system_recovery.tar.enc) mentionnés dans la commande.

9. Une fois le fichier de sauvegarde transféré, connectez-vous au shell de diagnostic et exécutez la commande suivante :

```
sudo perl /home/maint/scripts/post-deploy-upgrade.pl -recovery
```

Les journaux sont enregistrés dans le fichier */var/log/post-deploy-upgrade.log*.

Une fois la récupération terminée, les outils ONTAP restaurent les services et les objets vCenter.

Désinstaller les outils ONTAP

La désinstallation des outils ONTAP pour VMware vSphere supprime toutes les données contenues dans les outils.

Étapes

1. Supprimez ou déplacez toutes les machines virtuelles des outils ONTAP pour les datastores gérés VMware vSphere.
   - Pour supprimer les machines virtuelles, reportez-vous à la section "Supprimez et réenregistrez les machines virtuelles et les modèles de machines virtuelles"
   - Pour les déplacer vers un magasin de données non géré, reportez-vous à "Comment migrer votre machine virtuelle avec Storage vMotion"
2. "Supprimer les datastores" Créé sur les outils ONTAP pour VMware vSphere.
3. Si vous avez activé le fournisseur VASA, sélectionnez **Paramètres** > **VASA Provider settings** > **Unregister** dans les outils ONTAP pour désenregistrer les fournisseurs VASA de tous les serveurs vCenter.
4. Dissociez tous les systèmes back-end de l'instance vCenter Server. Reportez-vous à la "Dissociez les systèmes back-end de stockage de l'instance vCenter Server".
5. Suppression de tous les systèmes back-end Reportez-vous à la "Gestion des systèmes back-end".
6. Supprimez l'adaptateur SRA de VMware Live site Recovery :
   a. Connectez-vous en tant qu'administrateur à l'interface de gestion de l'appliance VMware Live site Recovery à l'aide du port 5480.
   b. Sélectionnez **Storage Replication Adapters**.
   c. Sélectionnez la carte SRA appropriée et, dans le menu déroulant, sélectionnez **Supprimer**.
   d. Confirmez que vous connaissez les résultats de la suppression de la carte et sélectionnez **Supprimer**.
7. Supprimez les instances de serveur vCenter intégrées aux outils ONTAP pour VMware vSphere. Reportez-

vous à la "Gestion des instances vCenter Server".

8. Mettez hors tension les outils ONTAP pour les machines virtuelles VMware vSphere à partir du serveur vCenter et supprimez les machines virtuelles.

Et la suite ?

"Supprimez les volumes FlexVol"

Supprimez les volumes FlexVol après la désinstallation des ONTAP tools

L'utilisation d'un cluster ONTAP dédié aux outils ONTAP pour le déploiement VMware crée de nombreux volumes FlexVol inutilisés. Après avoir supprimé les outils ONTAP pour VMware vSphere, vous devez supprimer les volumes FlexVol afin d'éviter tout impact sur les performances.

Étapes

1. Découvrez les ONTAP tools for VMware vSphere à partir de la machine virtuelle du nœud de gestion des outils ONTAP . Exécutez la commande suivante pour vérifier le type de déploiement : *cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocol*

   S'il s'agit d'un déploiement iSCSI, supprimez également les igroups.

2. Obtenez la liste des volumes FlexVol . *kubectl décrit les volumes persistants | grep internalName | awk -F'=' '{print $2}'*
3. Supprimez les machines virtuelles du serveur vCenter. Reportez-vous à la "Supprimez et réenregistrez les machines virtuelles et les modèles de machines virtuelles".
4. Supprimer les volumes FlexVol . Se référer à "Supprime un volume FlexVol" . Saisissez le nom exact du FlexVol volume dans la commande CLI pour supprimer un volume.
5. Supprimez les igroups SAN du système de stockage ONTAP en cas de déploiement iSCSI. Reportez-vous à la "Affichez et gérez les initiateurs SAN et igroups".

Mettez à niveau les outils ONTAP pour VMware vSphere

Mise à niveau des ONTAP tools for VMware vSphere 10.x vers 10.5

Vous pouvez effectuer une mise à niveau des ONTAP tools for VMware vSphere 10.3 ou 10.4 vers 10.5. Cependant, pour effectuer une mise à niveau des outils ONTAP 10.0, 10.1 ou 10.2 vers 10.5, vous devez d'abord effectuer une mise à niveau vers 10.3 ou 10.4 avant de passer à 10.5.

- Pour les systèmes ASA r2, assurez-vous de mettre à niveau les ONTAP tools for VMware vSphere vers 10.5 et ONTAP vers 9.16.1, avant de configurer davantage de zones de disponibilité de stockage (SAZ).
- Si la mise à niveau des ONTAP tools for VMware vSphere 10.3 ou 10.4 vers 10.5 échoue, vous ne pouvez pas revenir en arrière. Utilisez un RPO faible ou une récupération de snapshot pour restaurer la configuration. Pour les ONTAP tools for VMware vSphere 10.2 et versions antérieures, utilisez le RPO zéro pour restaurer la configuration.

Avant de commencer

- Assurez-vous que tous les nœuds sont actifs.
- Assurez-vous que le certificat système ONTAP et les certificats vCenter intégrés sont valides pendant au moins 5 jours. Si les certificats expirent plus tôt, la mise à niveau échoue.
- Assurez-vous d'avoir un cinquième disque d'une capacité de 100 Go sur tous les nœuds.
- Vérifiez que la configuration du nœud correspond aux spécifications du tableau ci-dessous.

Type de déploiement	CPU (Core) par nœud	Mémoire (Go) par nœud	Espace disque (Go) par nœud	Total CPU (cœur)	Mémoire (Go)	Espace disque total (Go)
Non HA petit	9	18	350	9	18	350
Non HA Moyen	13	26	350	13	26	350
HA petit	9	18	350	27	54	1050
HA Moyen	13	26	350	39	78	1050
HAUTE disponibilité	17	34	350	51	102	1050

- Assurez-vous que le branchement à chaud pour le processeur et la RAM est activé.
- Activez la sauvegarde à faible RPO et assurez-vous qu'une sauvegarde soit visible dans l'interface du client vCenter. Téléchargez le dossier de sauvegarde avant la mise à niveau.
- Une sauvegarde avec un RPO faible est recommandée. Toutefois, dans un déploiement non HA, vous pouvez prendre un instantané mis au repos de la machine virtuelle des outils ONTAP avant la mise à niveau.

Se référer à "Modifier les paramètres de sauvegarde" et "Récupérer la configuration des outils ONTAP" pour plus d'informations sur la sauvegarde et la restauration.

Étapes

1. Télécharger les outils ONTAP pour VMware vSphere, mettez à niveau ISO vers la bibliothèque de contenu.
2. Sur la page principale de la VM, sélectionnez **Actions** > **Modifier les paramètres**. Pour identifier le nom de la machine virtuelle principale :
   a. Activer le shell de diagnostic sur n'importe quel nœud
   b. Exécutez la commande suivante :
   `grep sourceHost /opt/netapp/meta/ansible_vars.yaml`
3. Sélectionnez le **fichier ISO de la bibliothèque de contenu** dans la fenêtre des paramètres d'édition sous le champ **lecteur CD/DVD**.
4. Sélectionnez le fichier ISO, cochez la case **Connecté** pour le champ **lecteur CD/DVD** et cliquez sur **OK**.
5. À partir du serveur vCenter, ouvrez une console pour accéder aux outils ONTAP.
6. Connectez-vous en tant qu'utilisateur de maintenance.
7. Entrez **2** pour sélectionner le menu **Configuration système**.
8. Entrez **7** pour sélectionner l'option **Mise à niveau**.
9. Fournissez les informations d'identification vCenter lorsque vous y êtes invité. Il s'agit de l'instance vCenter sur laquelle sont hébergés les outils ONTAP .

   Si vous utilisez les outils ONTAP dans une topologie à deux serveurs vCenter (où l'appliance est hébergée dans une instance vCenter et en gère une autre), vous pouvez attribuer un rôle restreint à l'instance vCenter hébergeant les outils ONTAP . Vous pouvez créer un utilisateur et un rôle vCenter dédiés, disposant uniquement des autorisations requises pour le déploiement du modèle OVF. Pour plus de détails, consultez les rôles énumérés dans "Rôles inclus avec les outils ONTAP pour VMware vSphere 10".

   Pour l'instance vCenter qui sera gérée par les outils ONTAP , assurez-vous que le compte utilisateur vCenter dispose des privilèges d'administrateur.

   Pendant la mise à niveau, si des certificats backend de stockage intégrés manquent d'entrées de nom alternatif du sujet (SAN), vous recevrez une invite indiquant le SAN manquant. Si vous choisissez de continuer sans valider le SAN, la mise à niveau se poursuivra, mais cela n'est pas recommandé en raison de risques de sécurité potentiels.

10. Lorsque vous effectuez une mise à niveau, les actions suivantes sont automatiquement exécutées :
    a. Le certificat de passerelle est renouvelé avec une durée de validité d'un an. Lorsque vous supprimez l'adaptateur SRA précédent et téléchargez le nouvel adaptateur 10.5, la validité du certificat SRA passe de 10 ans à 1 an.
    b. Le plug-in distant est mis à niveau
    c. Les certificats ONTAP et vCenter Server sont validés et ajoutés aux outils ONTAP
    d. La sauvegarde est activée

Et la suite

Après la mise à niveau vers les ONTAP tools for VMware vSphere 10.5 :

- Surveillez les alertes système et prévoyez de renouveler le certificat de passerelle avant son expiration dans un an.

- Supprimez l'adaptateur SRA 10.4 ou 10.3 des outils ONTAP et téléchargez le fichier tar de l'adaptateur SRA 10.5.
- Exécutez la commande d'installation après avoir téléchargé l'archive tar de l'adaptateur SRA. Ensuite, analysez à nouveau les adaptateurs SRA pour mettre à jour la page des adaptateurs de réplication de stockage VMware Site Recovery.

Après la mise à niveau, vous pouvez :

- Désactivez les services à partir de l'interface utilisateur Manager
- Passez d'une configuration non HA à une configuration haute disponibilité
- Faites évoluer une petite configuration non HA vers une configuration moyenne non HA, ou vers une configuration moyenne ou grande HA.

Informations associées

"Migrer des ONTAP tools for VMware vSphere 9.xx vers 10.5"

Codes d'erreur de mise à niveau des ONTAP tools

Des codes d'erreur peuvent s'afficher lors de la mise à niveau des outils ONTAP pour VMware vSphere.
Les codes d'erreur sont composés de cinq chiffres, les deux premiers chiffres représentant le script qui a rencontré le problème, et les trois derniers chiffres représentent le flux de travail spécifique de ce script.

Tous les journaux d'erreurs sont enregistrés dans le fichier ansible-perl-errors.log pour faciliter le suivi et la résolution des problèmes. Ce fichier journal contient le code d'erreur et la tâche Ansible qui a échoué.

Les codes d'erreur fournis sur cette page sont fournis à titre de référence uniquement. Contactez l'équipe d'assistance si l'erreur persiste ou si aucune résolution n'est mentionnée.

Le tableau suivant répertorie les codes d'erreur et les noms de fichier correspondants.

Code d'erreur	Nom du script
00	firstboot-network-config.pl, mode deploy
01	firstboot-network-config.pl, mise à niveau du mode
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, déploiement, haute disponibilité
04	firstboot-deploy-otv-ng.pl, déploiement, non HA
05	firstboot-deploy-otv-ng.pl, redémarrer
06	firstboot-deploy-otv-ng.pl, mise à niveau, haute disponibilité
07	firstboot-deploy-otv-ng.pl, mise à niveau, non HA
08	firstboot-otv-recovery.pl

09	post-deploy-upgrade.pl

Les trois derniers chiffres du code d'erreur indiquent l'erreur de flux de travail spécifique dans le script :

Mettre à niveau le code d'erreur	Workflow	Résolution
052	L'ISO peut être la même que la version actuelle ou deux versions au-dessus de la version actuelle.	Utilisez une version ISO compatible pour effectuer une mise à niveau à partir de votre version actuelle.
068	Échec de la restauration des paquets Debian	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
069	Échec de la restauration des fichiers	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
070	Échec de la suppression de la sauvegarde	-
071	Cluster Kubernetes défectueux	-
074	Echec du montage ISO	Vérifiez le fichier /var/log/upgrade-run.log et réessayez la mise à niveau.
075	Échec des pré-vérifications de mise à niveau	Réessayez la mise à niveau.
076	Échec de la mise à niveau du Registre	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
077	Échec de la restauration du registre	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
078	La mise à niveau de l'opérateur a échoué	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
079	Echec du retour arrière de l'opérateur	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
080	La mise à niveau des services a échoué	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
081	Échec de la restauration des services	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
082	Échec de la suppression des anciennes images du conteneur	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.

Mettre à niveau le code d'erreur	Workflow	Résolution
083	La suppression de la sauvegarde a échoué	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
084	Echec de la remise en production du JobManager	Suivez les étapes ci-dessous pour récupérer/terminer la mise à niveau. 1. Activer le shell de diagnostic 2. Exécutez la commande : *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 3. Vérifiez les journaux dans /var/log/post-deploy-upgrade.log
087	Échec des étapes post-mise à niveau.	Procédez comme suit pour récupérer/terminer la mise à niveau. 1. Activer le shell de diagnostic 2. Exécutez *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* command 3. Vérifiez les journaux dans /var/log/post-deploy-upgrade.log
088	La configuration de la rotation du journal pour journald a échoué	Vérifiez les paramètres réseau de la machine virtuelle compatibles avec l'hôte sur lequel la machine virtuelle est hébergée. Vous pouvez essayer de migrer la machine virtuelle vers un autre hôte et redémarrer.
089	La modification de la propriété du fichier de configuration de rotation du journal de synthèse a échoué	Réessayez la mise à niveau.
095	Échec de la mise à niveau du se	Aucune récupération pour la mise à niveau du système d'exploitation. Les services d'outils ONTAP sont mis à niveau et de nouveaux pods seront en cours d'exécution.
096	Installer le provisionneur de stockage dynamique	Consultez les journaux de mise à niveau et réessayez la mise à niveau.
097	La désinstallation des services pour la mise à niveau a échoué	Utilisez un RPO nul ou une restauration basée sur des snapshots et réessayez la mise à niveau.

Mettre à niveau le code d'erreur	Workflow	Résolution
098	échec de la copie du secret dockercred du système ntv vers l'espace de noms du mécanisme de provisionnement de stockage dynamique	Consultez les journaux de mise à niveau et réessayez la mise à niveau.
099	Impossible de valider l'ajout de nouveau disque dur	Ajout du nouveau disque dur à tous les nœuds en cas de haute disponibilité et à un nœud en cas de déploiement non HA
109	la sauvegarde des données du volume persistant a échoué	Consultez les journaux de mise à niveau et réessayez la mise à niveau.
110	échec de la restauration des données du volume persistant	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
111	Échec de la mise à jour des paramètres de délai d'attente d'ETCD pour le RKE2	Consultez les journaux de mise à niveau et réessayez la mise à niveau.
112	La désinstallation du provisionnement de stockage dynamique a échoué	-
113	L'actualisation des ressources sur les nœuds secondaires a échoué	Consultez les journaux de mise à niveau et réessayez la mise à niveau.
104	Le redémarrage du nœud secondaire a échoué	Redémarrez les nœuds manuellement un par un
100	échec de la restauration du noyau	-
051	la mise à niveau du provisionnement de stockage dynamique a échoué	Consultez les journaux de mise à niveau et réessayez la mise à niveau.
056	échec de la suppression de la sauvegarde de migration	NA
090	la validation du certificat pour les backends de stockage et vCenter a échoué	Vérifiez les journaux de mise à niveau et le fichier journal dans /var/log/cert_validation_error.log et réessayez la mise à niveau.

À partir des outils ONTAP pour VMware vSphere 10.3, le RPO nul n'est pas pris en charge.

En savoir plus sur "Restauration des outils ONTAP pour VMware vSphere en cas d'échec de la mise à niveau de la version 10.0 vers la version 10.1"

Migrer les ONTAP tools for VMware vSphere 9.xx vers 10.5

Migrer des ONTAP tools for VMware vSphere 9.xx vers 10.5

Le déplacement des outils NetApp ONTAP tools for VMware vSphere de la version 9.xx vers la version 10.5 nécessite un processus de migration en raison des mises à jour et des améliorations importantes du produit entre les versions.

Vous pouvez migrer des ONTAP tools for VMware vSphere 9.12D1, 9.13D2 et 9.13P2 vers les ONTAP tools for VMware vSphere 10.5.

Si vous disposez de banques de données NFS et VMFS et d'aucune banque de données vVols dans votre configuration, désinstallez simplement les outils ONTAP 9.xx et déployez les outils ONTAP 10.5. Cependant, si votre configuration contient des magasins de données vVols , vous devrez suivre un processus de migration du fournisseur VASA et du SRA.

Le tableau suivant décrit le processus de migration dans ces deux scénarios différents.

Si la configuration dispose de magasins de données vVols	Si la configuration contient uniquement des banques de données NFS et VMFS
Étapes : 1. "Migrer le fournisseur VASA" 2. "Créer des politiques de stockage de machines virtuelles"	Étapes : 1. Supprimez les outils ONTAP 9.xx de votre environnement. Se référer à "Comment supprimer OTV 9.xx de votre environnement" Article de la base de connaissances NetApp . 2. "Déployer et configurer les ONTAP tools for VMware vSphere 10.5" 3. "Mettre à jour le SRA" 4. "Créer des politiques de stockage de machines virtuelles"

Après la migration des ONTAP tools for VMware vSphere 9.xx vers 10.5, les banques de données vVols utilisant le protocole NVMe/FC deviennent non opérationnelles car les outils ONTAP 10.5 prennent en charge le protocole NVMe-oF uniquement avec les banques de données VMFS.

Migrez le fournisseur VASA et mettez à jour le SRA dans ONTAP tools

Suivez les étapes de cette section pour migrer le fournisseur VASA des ONTAP tools for VMware vSphere 9.xx vers les ONTAP tools for VMware vSphere 10.5 et mettre à jour l'adaptateur de réplication de stockage (SRA) sur l'appliance VMware Live Site Recovery.

Étapes pour migrer le fournisseur VASA

1. Pour activer LE PORT Derby 1527 sur les outils ONTAP existants pour VMware vSphere, activez l'utilisateur root et connectez-vous à l'interface de ligne de commande via SSH. Exécutez ensuite la commande suivante :

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. Déployez les ONTAP tools for VMware vSphere 10.5.
3. Ajoutez l'instance vCenter Server que vous souhaitez migrer vers les ONTAP tools for VMware vSphere 10.5. Consultez "Ajoutez une instance de vCenter Server" pour plus d'informations.
4. "Activez VASA Provider"service sur les ONTAP tools for VMware vSphere 10.5.
5. Intégrez localement le système de stockage à partir des API du serveur vCenter pour le plug-in ONTAP Tools. Voir"Ajoutez un système de stockage dorsal à l'aide de l'interface client vSphere." pour plus d'informations.
6. Obtenez un jeton d'accès pour authentifier les requêtes API REST. Utilisez l'exemple suivant en remplaçant les variables par des valeurs spécifiques à votre environnement.

```
curl --request POST \
  --location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/vcenter-
login" \
  --header "Content-Type: application/json" \
  --header "Accept: */*" \
  -d '{"username": "$MYUSER", "password": "$MYPASSWORD"}'
```

Copiez et enregistrez le jeton d'accès renvoyé dans la réponse.

7. Exécutez l'API suivante depuis swagger ou dans Postman pour effectuer la migration.

```
curl -X POST
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migra
tion-jobs`
```

Vous pouvez accéder à Swagger via cette URL : `https://$FQDN_IP_PORT/` , Par exemple: `https://10.67.25.33:8443/` .

Méthode HTTP et noeud final

Cet appel d'API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
POST	/api/v1

Type de traitement

Asynchrone

Exemple Curl

```
curl -X POST 'https://<OTV-NG-
IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-jobs' \
  --header 'x-auth: <auth_token>' \
  --header 'Content-Type: application/json' \
  --data '{
    "otv_ip": "xx.xx.xx.xx",
    "vasa_provider_credentials": {
      "username": "xxxxx",
      "password": "******"
    },
    "database_password": "******"
  }'
```

Corps de la demande pour une autre migration de version :

```
{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxx",
    "password": "*******"
  }
}
```

Exemple de sortie JSON

Le système renvoie un objet de travail. Enregistrez l'identifiant du travail pour l'utiliser à l'étape suivante.

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```

8. Utilisez l'URI suivant dans swagger pour vérifier l'état :

```
curl
`\https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobId
>?includeSubJobsAndTasks=true`
```

   Utilisez la valeur 'id' renvoyée par le travail de migration de l'étape précédente. Après la fin du travail, consultez le rapport de migration dans la réponse du travail.

9. Ajoutez les ONTAP tools for VMware vSphere au serveur vCenter.
10. Enregistrez le fournisseur VASA auprès des ONTAP tools for VMware vSphere. Pour les instructions, voir"Enregistrez le fournisseur VASA" .
11. Vérifiez l'inscription du fournisseur VASA :
    a. Dans le vSphere Client, accédez au vCenter Server.
    b. Sélectionnez **Configurer** > **Storage Providers**.
    c. Confirmez que le VASA Provider enregistré à l'étape précédente apparaît en ligne.
12. Arrêtez les ONTAP tools for VMware vSphere 9.10/9.11/9.12/9.13 (service VASA Provider) en suivant ces étapes :
    a. Dans ONTAP tools 9.x, ouvrez la console web.
    b. Accéder à la console de maintenance.
    c. Entrer `1` pour sélectionner le menu **Configuration de l'application**.
    d. Entrer `5` pour mettre fin aux services VASA Provider et SRA.
    e. Dans le vSphere Client, accédez au vCenter Server et sélectionnez **Configurer** > **Fournisseurs de stockage**.
    f. Sélectionnez le fournisseur VASA hors ligne pour les outils ONTAP 9.x et sélectionnez **Supprimer**.

       Après l'arrêt de l'ancien fournisseur VASA, vCenter Server bascule vers les ONTAP tools for VMware vSphere. Tous les datastores et machines virtuelles deviennent accessibles et sont gérés par les ONTAP tools for VMware vSphere.

13. Les banques de données NFS et VMFS migrées apparaissent dans les ONTAP tools for VMware vSphere 10.5 après la tâche de découverte de banque de données, ce qui peut prendre jusqu'à 30 minutes. Vérifiez leur visibilité sur la page d'aperçu.
14. Effectuez la migration des correctifs à l'aide de l'API suivante dans swagger ou dans Postman :

Méthode HTTP et noeud final

Cet appel d'API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
CORRECTIF	/api/v1

Type de traitement

Asynchrone

Utilisez l'URI suivant dans Swagger :

```
curl  -X PATCH
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_i
d>/migration-jobs/<migration_id>`
```

Méthode HTTP et noeud final

Cet appel d'API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
CORRECTIF	/api/v1

Type de traitement

Asynchrone

Utilisez l'URI suivant dans Swagger :

```
curl  -X PATCH
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_i
d>/migration-jobs/<migration_id>`
```

Exemple Curl

```
curl  -X PATCH
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-
4163-44f9-a872-9adabb008ca9/migration-jobs/d50073ce-35b4-4c51-9d2e-
4ce66f802c35`
```

Exemple de sortie JSON

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```

Utilisez la valeur 'migration_id' renvoyée à l'étape 7 comme <migration_id> dans l'appel API PATCH. Le corps de la requête est vide pour une opération PATCH.

UUID est l'UUID de migration renvoyé en réponse à l'API post-migration.

Après avoir exécuté l'API de migration des correctifs, toutes les machines virtuelles respectent la stratégie de stockage.

Et la suite

Après avoir terminé la migration et enregistré les outils ONTAP 10.5 sur vCenter Server, suivez ces étapes :

- Attendez que **Discovery** soit terminé et le système actualise automatiquement les certificats sur tous les hôtes.
- Attendez avant de démarrer les opérations de la banque de données et de la machine virtuelle. Le temps d'attente dépend du nombre d'hôtes, de banques de données et de machines virtuelles. Si vous n'attendez pas, vous risquez de voir des échecs occasionnels.

Après la mise à niveau, si l'état de conformité de la machine virtuelle est obsolète, réappliquez la stratégie de stockage en procédant comme suit :

1. Accédez au magasin de données et sélectionnez **Résumé** > **Stratégies de stockage VM**.
2. Le système affiche l'état de conformité sous **Conformité à la politique de stockage VM** comme **Obsolète**.
3. Sélectionnez la politique de machine virtuelle de stockage et la machine virtuelle correspondante.
4. Sélectionnez **Appliquer**.
5. L'état de conformité sous **Conformité à la politique de stockage VM** indique qu'il est conforme.

Informations associées

- "Découvrez les outils ONTAP pour VMware vSphere 10 RBAC"
- "Mise à niveau des ONTAP tools for VMware vSphere 10.x vers 10.5"

Étapes pour mettre à jour l'adaptateur de réplication de stockage (SRA)

Avant de commencer

Dans le plan de récupération, le site protégé désigne l'emplacement où les machines virtuelles sont actuellement exécutées, tandis que le site de récupération désigne l'emplacement où elles seront restaurées. L'interface du dispositif VMware Live Site Recovery affiche l'état du plan de récupération avec des détails sur les sites protégés et de récupération. Dans le plan de récupération, les boutons NETTOYER et REPROTÉGER sont désactivés, tandis que les boutons TESTER et EXÉCUTER restent activés. Cela indique que le site est prêt pour la récupération des données. Avant de migrer le SRA, vérifiez qu'un site est en état

protégé et l'autre en état de récupération.

> Ne commencez pas la migration si le basculement a été effectué mais que la reprotection est en attente. Assurez-vous que le processus de reprotection est terminé avant de procéder à la migration. Si un basculement de test est en cours, nettoyez le basculement de test et démarrez la migration.

1. Procédez comme suit pour supprimer l'adaptateur ONTAP Tools SRA pour VMware vSphere 9.xx dans VMware site Recovery :
   a. Accédez à la page de gestion de la configuration de VMware Live site Recovery
   b. Accédez à la section **Storage Replication adapter**.
   c. Dans le menu points de suspension, sélectionnez **Réinitialiser la configuration**.
   d. Dans le menu points de suspension, sélectionnez **Supprimer**.
2. Effectuez ces étapes sur les sites de protection et de reprise d'activité.
   a. "Activez les outils ONTAP pour les services VMware vSphere"
   b. Configurez les ONTAP tools for VMware vSphere 10.5 SRA en suivant les étapes décrites dans"Configurez SRA sur l'appliance VMware Live site Recovery" .
   c. Sur l'interface VMware Live Site Recovery, exécutez **Discover Arrays** et **Discover Devices**. Confirmez que les appareils s'affichent comme avant la migration.

Automatisation à l’aide de l’API REST

Découvrez l’API REST des ONTAP tools

Les outils ONTAP pour VMware vSphere 10 sont un ensemble d’outils destinés à la gestion du cycle de vie des machines virtuelles. Elle comprend une API REST robuste que vous pouvez utiliser dans le cadre de vos processus d’automatisation.

Base de services Web REST

Representational State Transfer (REST) est un style permettant de créer des applications Web distribuées, y compris la conception d’API de services Web. Il établit un ensemble de technologies permettant d’exposer les ressources basées sur les serveurs et de gérer leur état.

Ressources et représentation d’état

Les ressources sont les composants de base d’une application de services Web REST. Lors de la conception d’une API REST, deux tâches initiales sont importantes :

- Identifier les ressources système ou serveur
- Définissez les États de ressource et les opérations de transition d’état associées

Les applications client peuvent afficher et modifier les États de ressources via des flux de messages bien définis.

Messages HTTP

HTTP (HyperText Transfer Protocol) est le protocole utilisé par le client et le serveur de services Web pour échanger des messages sur les ressources. Il suit le modèle CRUD basé sur les opérations génériques de création, lecture, mise à jour et suppression. Le protocole HTTP comprend des en-têtes de requête et de réponse ainsi que des codes d’état de réponse.

Formatage des données JSON

Bien qu’il existe plusieurs formats de message disponibles, l’option la plus populaire est JavaScript Object notation (JSON). JSON est une norme industrielle pour la représentation de structures de données simples en texte brut et sert à transférer des informations d’état décrivant les ressources et les actions souhaitées.

Sécurité

La sécurité est un aspect important des API REST. Outre le protocole TLS (transport Layer Security) utilisé pour protéger le trafic HTTP sur le réseau, les outils ONTAP pour l’API REST VMware vSphere 10 utilisent également des jetons d’accès pour l’authentification. Vous devez acquérir un jeton d’accès et l’utiliser lors des appels API suivants.

Prise en charge des requêtes asynchrones

Les outils ONTAP pour l’API REST VMware vSphere 10 effectuent la plupart des requêtes de manière synchrone, en renvoyant un code d’état une fois l’opération terminée. Il prend également en charge le traitement asynchrone pour les tâches qui nécessitent plus de temps.

Environnement ONTAP Tools Manager

L’environnement ONTAP Tools Manager comporte plusieurs aspects à prendre en compte.

Ordinateur virtuel

Les ONTAP tools for VMware vSphere 10 sont déployés à l'aide de l'architecture de plug-in distant vSphere. Le logiciel, y compris la prise en charge de l'API REST, s'exécute sur une machine virtuelle distincte.

Adresse IP des outils ONTAP

Les outils ONTAP pour VMware vSphere 10 exposent une adresse IP unique qui fournit une passerelle vers les fonctionnalités de la machine virtuelle. Vous devez fournir cette adresse lors de la configuration initiale et l'attribuer à un composant d'équilibrage de charge interne. L'adresse est utilisée par l'interface utilisateur du Gestionnaire d'outils ONTAP ainsi que pour accéder directement à la page de documentation swagger et à l'API REST.

Deux API REST

Outre les outils ONTAP pour l'API REST de VMware vSphere 10, le cluster ONTAP dispose de sa propre API REST. Le gestionnaire d'outils ONTAP utilise l'API REST ONTAP en tant que client pour effectuer des tâches liées au stockage. Il est important de garder à l'esprit que ces deux API sont distinctes. Pour plus d'informations, reportez-vous "Automatisation ONTAP"à .

Détails d'implémentation de l'API REST des ONTAP tools

Même si REST établit un ensemble commun de technologies et de bonnes pratiques, l'implémentation exacte de chaque API peut varier en fonction des choix de conception. Vous devez vous familiariser avec la conception préalable des outils ONTAP pour l'API REST VMware vSphere 10.

L'API REST comprend plusieurs catégories de ressources telles que les instances vCenter et les agrégats. Consultez le "Référence API" pour plus d'informations.

Comment accéder à l'API REST

Vous pouvez accéder aux outils ONTAP pour l'API REST VMware vSphere 10 via l'adresse IP et le port de l'outil ONTAP. L'URL complète comprend plusieurs parties, notamment :

- Adresse IP et port des outils ONTAP
- Version API
- Catégorie de ressource
- Ressource spécifique

Vous devez configurer l'adresse IP lors de la configuration initiale, tandis que le port reste fixe à 8443. La première partie de l'URL est cohérente pour chaque instance des ONTAP tools for VMware vSphere 10 ; seules la catégorie de ressource et la ressource spécifique changent entre les points de terminaison.

> Les valeurs d'adresse IP et de port indiquées dans les exemples ci-dessous sont fournies à titre d'illustration uniquement. Vous devez modifier ces valeurs pour votre environnement.

Exemple d'accès aux services d'authentification

```
https://10.61.25.34:8443/virtualization/api/v1/auth/login
```

Cette URL peut être utilisée pour demander un jeton d'accès à l'aide de la méthode POST.

Exemple de liste des serveurs vCenter

```
https://10.61.25.34:8443/virtualization/api/v1/vcenters
```

Cette URL peut être utilisée pour demander une liste des instances de serveur vCenter définies à l'aide de LA méthode GET.

Détails d'HTTP

Les outils ONTAP pour l'API REST VMware vSphere 10 utilisent le protocole HTTP et les paramètres associés pour agir sur les instances et les collections de ressources. Les détails de l'implémentation HTTP sont présentés ci-dessous.

Méthodes HTTP

Les méthodes HTTP ou verbes pris en charge par l'API REST sont présentées dans le tableau ci-dessous.

Méthode	CRUD	Description
OBTENEZ	Lecture	Récupère les propriétés d'un objet pour une instance ou une collection de ressources. Cette opération est considérée comme une opération de liste lorsqu'elle est utilisée avec une collection.
POST	Créer	Crée une nouvelle instance de ressource basée sur les paramètres d'entrée.
EN	Mise à jour	Met à jour une instance de ressource entière avec le corps de requête JSON fourni. Les valeurs clés non modifiables par l'utilisateur sont conservées.
CORRECTIF	Mise à jour	Demande l'application d'un ensemble de modifications sélectionnées dans la demande à l'instance de ressource.
SUPPRIMER	Supprimer	Supprime une instance de ressource existante.

En-têtes de demande et de réponse

Le tableau suivant récapitule les en-têtes HTTP les plus importants utilisés avec l'API REST.

En-tête	Type	Remarques sur l'utilisation
Accepter	Demande	Il s'agit du type de contenu que l'application client peut accepter. Les valeurs valides incluent '*/*' ou `application/json`.
x-auth	Demande	Contient un jeton d'accès identifiant l'utilisateur qui émet la demande via l'application client.
Type de contenu	Réponse	Renvoyé par le serveur en fonction de l' `Accept`en-tête de la requête.

Codes d'état HTTP

Les codes d'état HTTP utilisés par l'API REST sont décrits ci-dessous.

Code	Signification	Description
200	OK	Indique le succès des appels qui ne créent pas de nouvelle instance de ressource.
201	Créé	Un objet a été créé avec succès avec un identifiant unique pour l'instance de ressource.

Code	Signification	Description
202	Accepté	La demande a été acceptée et un travail en arrière-plan a été créé pour exécuter la demande.
204	Aucun contenu	La demande a réussi bien qu'aucun contenu n'ait été renvoyé.
400	Demande incorrecte	L'entrée de la demande n'est pas reconnue ou est inappropriée.
401	Non autorisé	L'utilisateur n'est pas autorisé et doit s'authentifier.
403	Interdit	L'accès est refusé en raison d'une erreur d'autorisation.
404	Introuvable	La ressource référencée dans la demande n'existe pas.
409	Conflit	La tentative de création d'un objet a échoué car celui-ci existe déjà.
500	Erreur interne	Une erreur interne générale s'est produite sur le serveur.

Authentification

L'authentification d'un client sur l'API REST s'effectue à l'aide d'un jeton d'accès. Les caractéristiques pertinentes du token et du processus d'authentification sont les suivantes :

- Le client doit demander un jeton à l'aide des informations d'identification de l'administrateur du Gestionnaire d'outils ONTAP (nom d'utilisateur et mot de passe).
- Les tokens sont formatés en tant que jeton Web JSON (JWT).
- Chaque jeton expire au bout de 60 minutes.
- Les requêtes API d'un client doivent inclure le token dans l' `x-auth`en-tête de la requête.

Reportez-vous à la "Votre premier appel de l'API REST" pour un exemple de demande et d'utilisation d'un jeton d'accès.

Demandes synchrones et asynchrones

La plupart des appels d'API REST s'effectuent rapidement et s'exécutent donc de manière synchrone. C'est-à-dire qu'ils renvoient un code d'état (tel que 200) après qu'une demande a été traitée. Les requêtes qui prennent plus de temps à effectuer s'exécutent de manière asynchrone à l'aide d'une tâche en arrière-plan.

Après avoir émis un appel API qui s'exécute de manière asynchrone, le serveur renvoie un code d'état HTTP 202. Cela indique que la demande a été acceptée mais pas encore terminée. Vous pouvez interroger le travail en arrière-plan pour déterminer son état, y compris sa réussite ou son échec.

Le traitement asynchrone est utilisé pour plusieurs types d'opérations longues à réaliser, notamment les opérations de datastore et vVol. Pour plus d'informations, reportez-vous à la catégorie Gestionnaire de travaux de l'API REST à la page swagger.

Effectuez votre premier appel API REST avec les ONTAP tools

Vous pouvez émettre un appel d'API à l'aide de CURL pour commencer à utiliser les outils ONTAP pour l'API REST VMware vSphere 10.

Avant de commencer

Vous devez consulter les informations et les paramètres requis dans les exemples de boucles.

Informations requises

Il faut les éléments suivants :

- Outils ONTAP pour l'adresse IP ou le nom de domaine complet de VMware vSphere 10 ainsi que le port
- Informations d'identification de l'administrateur du Gestionnaire d'outils ONTAP (nom d'utilisateur et mot de passe)

Paramètres et variables

Les exemples de boucles présentés ci-dessous incluent des variables de style Bash. Vous pouvez définir ces variables dans l'environnement Bash ou les mettre à jour manuellement avant d'exécuter les commandes. Si vous définissez les variables, le shell substituera les valeurs dans chaque commande avant de l'exécuter. Les variables sont décrites dans le tableau ci-dessous.

Variable	Description
$FQDN_IP_PORT	Nom de domaine complet ou adresse IP du gestionnaire d'outils ONTAP avec le numéro de port.
$MONUTILISATEUR	Nom d'utilisateur du compte Gestionnaire d'outils ONTAP.
$MYPASSWORD	Mot de passe associé au nom d'utilisateur du Gestionnaire d'outils ONTAP.
$ACCESS_TOKEN	Jeton d'accès émis par le gestionnaire d'outils ONTAP.

Les commandes et résultats suivants au niveau de l'interface de ligne de commande Linux illustrent comment une variable peut être définie et affichée :

```
FQDN_IP_PORT=172.14.31.224:8443
echo $FQDN_IP
172.14.31.224:8443
```

Étape 1 : acquérir un jeton d'accès

Vous devez acquérir un jeton d'accès pour utiliser l'API REST. Un exemple de demande de jeton d'accès est présenté ci-dessous. Vous devez remplacer les valeurs appropriées pour votre environnement.

```
curl --request POST \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/login" \
--header "Content-Type: application/json" \
--header "Accept: */*" \
-d "{"username": "$MYUSER", "password": "$MYPASSWORD"}"
```

Copiez et enregistrez le jeton d'accès fourni dans la réponse.

Étape 2 : lancez l'appel de l'API REST

Après avoir un jeton d'accès, vous pouvez utiliser curl pour émettre un appel API REST. Incluez le jeton d'accès acquis dans la première étape.

Exemple de boucle

```
curl --request GET \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/vcenters" \
--header "Accept: */*" \
--header "x-auth: $ACCESS_TOKEN"
```

La réponse JSON inclut une liste des instances VMware vCenter configurées pour le gestionnaire d'outils ONTAP.

Référence de l'API REST des ONTAP tools

La référence des outils ONTAP pour l'API REST VMware vSphere 10 contient des détails sur tous les appels d'API. Cette référence est utile lors du développement d'applications d'automatisation.

Vous pouvez accéder à la documentation en ligne des outils ONTAP pour l'API REST de VMware vSphere 10 via l'interface utilisateur swagger. Vous avez besoin de l'adresse IP ou du nom de domaine complet des outils ONTAP pour le service de passerelle VMware vSphere 10 ainsi que du port.

Étapes

1. Tapez l'URL suivante dans votre navigateur en remplaçant l'adresse IP et la combinaison de ports appropriés par la variable et appuyez sur **entrée**.

   `https://$FQDN_IP_PORT/`

   Exemple

   `https://10.61.25.33:8443/`

2. Comme exemple d'appel d'API individuel, faites défiler jusqu'à la catégorie **vCenters** et sélectionnez **OBTENIR** en regard du noeud final `/virtualization/api/v1/vcenters`

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.

"Avis concernant les ONTAP tools for VMware vSphere 10.5"

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.