# Documentation des outils ONTAP pour VMware vSphere

ONTAP tools for VMware vSphere 105

NetApp
August 06, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/ontap-tools-vmware-vsphere-105/index.html on August 06, 2026. Always check docs.netapp.com for the latest.

# Sommaire


Documentation des outils ONTAP pour VMware vSphere . . . 1
Notes de version . . . 2
Notes de version pour ONTAP tools . . . 2
Nouveautés des ONTAP tools for VMware vSphere 10.5 . . . 2
Plateformes ONTAP et versions de serveur vCenter prises en charge . . . 3
Comparaison des fonctionnalités des outils ONTAP pour 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
Contrôle d'accès basé sur les rôles (RBAC) avec ONTAP . . . 17
Déployez les outils ONTAP pour VMware vSphere . . . 21
Démarrage rapide des ONTAP tools for 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 . . . 24
Configuration système requise . . . 24
Exigences minimales de stockage et des applications . . . 24
Exigences relatives aux 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
ONTAP tools for VMware vSphere - Storage Replication Adapter (SRA) . . . 28
Exigences préalables au déploiement des ONTAP tools . . . 29
Feuille de travail 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 . . . 37
Collectez les fichiers journaux . . . 37
Codes d'erreur de déploiement . . . 37
Configurer les outils ONTAP pour VMware vSphere . . . 41
Ajoutez des instances de serveur vCenter aux outils ONTAP . . . 41
Enregistrez le fournisseur VASA auprès d'une instance de serveur vCenter dans ONTAP tools . . . 42
Installez le plug-in NFS VAAI à l'aide des ONTAP tools. . . . 43
Configurer les paramètres de l'hôte ESXi dans ONTAP tools . . . 44
Configurer les paramètres de multipath et de délai d'expiration du serveur ESXi . . . 44
Définissez les valeurs de l'hôte ESXi . . . 44
Configurer les rôles et privilèges des utilisateurs ONTAP pour les outils ONTAP . . . 45
Exigences de mappage d'agrégat SVM . . . 46
Créer manuellement l'utilisateur et le rôle ONTAP . . . 47
Mettez à niveau l'utilisateur ONTAP tools for VMware vSphere 10.1 vers l'utilisateur 10.3 . . . 55

Mettez à niveau l'utilisateur des ONTAP tools for VMware vSphere 10.3 vers l'utilisateur 10.4 . . . 57
Ajouter un système de stockage dorsal aux ONTAP tools . . . 57
Associer un système de stockage principal à une instance de serveur vCenter dans ONTAP tools . . . 60
Configurer l'accès réseau dans ONTAP tools . . . 60
Créer un datastore dans ONTAP tools . . . 61
Protégez les banques de données et les machines virtuelles . . . 66
Protéger un cluster hôte dans ONTAP tools . . . 66
Protéger à l'aide de la protection SRA . . . 67
Configurez SRA dans ONTAP tools pour protéger les banques de données . . . 67
Configurer SRA dans ONTAP tools for VMware vSphere pour les environnements SAN et NAS . . . 68
Configurer SRA dans ONTAP tools pour les environnements à grande échelle . . . 69
Configurez SRA sur l'appliance VMware Live Site Recovery à l'aide des ONTAP tools. . . . 70
Mettre à jour les informations d'identification SRA dans ONTAP tools . . . 71
Configurer les sites protégés et de récupération dans ONTAP tools . . . 72
Configurer les ressources du site protégé et du site de récupération . . . 74
Vérifier les systèmes de stockage répliqués dans ONTAP tools . . . 78
Protection contre le fan-out dans ONTAP tools . . . 78
Gérez les outils ONTAP pour VMware vSphere . . . 82
Découvrez le tableau de bord des ONTAP tools . . . 82
Comment les ONTAP tools gèrent les igroups et les politiques d'exportation . . . 83
Politiques d'export . . . 87
Comment les ONTAP tools gèrent les igroups . . . 88
Résumé rapide du comportement . . . 88
Contextes de groupe . . . 88
Comportement de dénomination . . . 90
Comportement selon le scénario . . . 90
Réutilisation personnalisée des igroups et comportement de l'API . . . 91
Vue de conversion native vers gérée . . . 91
Réutilisation des igroups natifs découverts . . . 92
Découvrez l'interface utilisateur du gestionnaire d'outils ONTAP . . . 92
Gérer les paramètres du gestionnaire ONTAP tools . . . 94
Modifier les paramètres AutoSupport des outils ONTAP . . . 94
Ajouter des serveurs NTP aux outils ONTAP . . . 95
Réinitialiser les informations d'identification du VASA Provider et du SRA dans ONTAP tools . . . 96
Modifier les paramètres de sauvegarde des outils ONTAP . . . 96
Activer les services ONTAP tools . . . 96
Modifier les paramètres de l'appliance ONTAP tools . . . 97
Ajouter des hôtes VMware vSphere aux outils ONTAP . . . 98
Gérer les datastores . . . 99
Monter les datastores NFS et VMFS dans ONTAP tools . . . 99
Démontez les datastores NFS et VMFS dans ONTAP tools . . . 99
Monter un datastore vVols dans ONTAP tools . . . 100
Redimensionner les datastores NFS et VMFS dans ONTAP tools . . . 101
Développez les datastores vVols dans les outils ONTAP . . . 101
Réduire la taille d'un vVols datastore dans ONTAP tools . . . 101

Supprimer les banques de données dans ONTAP tools . . . 102
Vues de stockage ONTAP pour les banques de données dans ONTAP tools . . . 103
Vue du stockage des machines virtuelles dans ONTAP tools . . . 103
Gérer les seuils de stockage dans ONTAP tools . . . 104
Gérer les backends de stockage dans ONTAP tools . . . 104
Découvrez le stockage . . . 104
Modifier les backends de stockage . . . 105
Supprimer les backends de stockage . . . 105
Vue détaillée du backend de stockage . . . 106
Gérez les instances de serveur vCenter dans les outils ONTAP . . . 106
Dissocier les systèmes de stockage de l'instance du serveur vCenter . . . 106
Modifier une instance de serveur vCenter . . . 107
Supprimer une instance de serveur vCenter . . . 107
Renouvelez le certificat du serveur vCenter . . . 108
Gérer les certificats des outils ONTAP . . . 110
Accédez à la console de maintenance des ONTAP tools for VMware vSphere . . . 112
Découvrez la console de maintenance des ONTAP tools . . . 112
Configurer l'accès de diagnostic à distance pour ONTAP tools . . . 113
Démarrer SSH sur les autres nœuds ONTAP tools . . . 114
Mettre à jour les informations d'identification du serveur vCenter dans ONTAP tools . . . 114
Modifier l'indicateur de validation du certificat dans ONTAP tools . . . 114
Rapports des outils ONTAP . . . 116
Gérer les machines virtuelles . . . 117
Considérations relatives à la migration et au clonage de machines virtuelles pour ONTAP tools . . . 117
Migrer des machines virtuelles vers des datastores vVols dans ONTAP tools . . . 118
Nettoyer les configurations VASA dans ONTAP tools . . . 119
Attacher ou détacher un disque de données d'une machine virtuelle dans ONTAP tools . . . 119
Découvrez les systèmes de stockage et les hôtes dans ONTAP tools . . . 120
Modifier les paramètres de l'hôte ESXi à l'aide des outils ONTAP . . . 121
Gérer les mots de passe . . . 121
Modifier le mot de passe du gestionnaire ONTAP tools . . . 121
Réinitialiser le mot de passe du gestionnaire d'outils ONTAP . . . 122
Réinitialiser le mot de passe utilisateur de l'application dans ONTAP tools . . . 122
Réinitialiser le mot de passe de la console de maintenance des ONTAP tools . . . 122
Gérer la protection du cluster hôte . . . 124
Modifier un cluster d'hôtes protégé dans ONTAP tools . . . 124
Supprimer la protection du cluster hôte dans ONTAP tools . . . 127
Récupérez la configuration des outils ONTAP . . . 127
Désinstaller les outils ONTAP . . . 128
Supprimez les volumes FlexVol après la désinstallation des ONTAP tools . . . 129
Mettre à niveau ONTAP tools for VMware vSphere . . . 130
Mettez à niveau ONTAP tools for VMware vSphere 10.x vers 10.5 . . . 130
Codes d'erreur de mise à niveau des ONTAP tools . . . 132
Migrez les ONTAP tools for VMware vSphere 9.xx vers 10.5 . . . 138
Migrez des ONTAP tools for VMware vSphere 9.xx vers 10.5 . . . 138

Migrez le fournisseur VASA et mettez à jour le SRA dans ONTAP tools . . . 138
Étapes de la migration du fournisseur VASA . . . 138
Étapes pour mettre à jour l'adaptateur de réplication de stockage (SRA) . . . 143
Automatisez à l'aide de l'API REST . . . 145
Découvrez l'API REST des ONTAP tools . . . 145
Fondation des services web REST . . . 145
Environnement du gestionnaire ONTAP tools . . . 145
Détails d'implémentation de l'API REST des ONTAP tools . . . 146
Comment accéder à l'API REST . . . 146
Détails HTTP . . . 147
Authentification . . . 148
Requêtes synchrones et asynchrones . . . 148
Effectuez votre premier appel API REST avec les ONTAP tools . . . 148
Avant de commencer . . . 149
Étape 1 : Obtenez un jeton d'accès . . . 149
Étape 2 : Émettre l'appel à l'API REST . . . 150
Référence de l'API REST des ONTAP tools . . . 150
Mentions légales . . . 151
Copyright . . . 151
Marques déposées . . . 151
Brevets . . . 151
Politique de confidentialité . . . 151
Open source . . . 151

# Documentation des outils ONTAP pour VMware vSphere

# Notes de version

## Notes de version pour ONTAP tools

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

Pour obtenir la liste complète des nouvelles fonctionnalités et améliorations, veuillez consulter Nouveautés des ONTAP tools for VMware vSphere 10.5.

Pour obtenir les informations de compatibilité les plus récentes, veuillez consulter "Outil NetApp Interoperability Matrix Tool".

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

Pour plus d'informations, veuillez consulter le "Notes de version des ONTAP tools for VMware vSphere 10.5". Vous devez vous connecter avec votre compte NetApp ou en créer un pour accéder aux notes de version.

## Nouveautés des ONTAP tools for VMware vSphere 10.5

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

- **Qualification de la plateforme**

ONTAP tools for VMware vSphere 10.5 ajoute la prise en charge des systèmes ASA r2, assurant la compatibilité avec les configurations matérielles et logicielles les plus récentes. Cette version inclut également l'intégration avec ONTAP 9.16.1 et 9.17.1, étendant les environnements pris en charge.

- **Qualifications et certifications VMware**

ONTAP tools for VMware vSphere 10.5 est conforme aux normes actuelles de certification d'interopérabilité VMware, prenant en charge à la fois l'hôte ESXi et le serveur vCenter.

- **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 ainsi l'expérience utilisateur et la conformité aux normes de sécurité. Elle propose des flux de validation de certificats optimisés pour sécuriser les communications entre ONTAP et ONTAP tools for VMware vSphere.

- **Améliorations de la réplication**

Cette version prend en charge la réplication VMFS avec groupe de cohérence hiérarchique, y compris SRA et SnapMirror active sync dans les systèmes ASA r2. Elle prend en charge les sauvegardes avec un RPO nul afin d'améliorer la protection des données et la récupération.

- **Mise à niveau et migration**

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

### Plateformes ONTAP et versions de serveur vCenter 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 obtenir les dernières informations sur la compatibilité des versions, consultez "Outil NetApp Interoperability Matrix Tool".

# Comparaison des fonctionnalités des outils ONTAP pour VMware vSphere 9 et 10

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

Pour obtenir les informations de compatibilité les plus récentes, veuillez consulter "Outil NetApp Interoperability Matrix Tool".

| Fonctionnalité | ONTAP tools 9.13 | ONTAP tools 10.2 et versions ultérieures |
|---|---|---|
| Proposition de valeur clé | Rationalisez et simplifiez les opérations du jour 0 au jour 2 grâce à des fonctionnalités améliorées de sécurité, de conformité et d'automatisation | Prise en charge étendue incluant 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 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 | ONTAP tools 9.13 | ONTAP tools 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 de ONTAP tools 10.5 et versions ultérieures 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 de performance, de capacité et de conformité des hôtes, rapports dynamiques sur les machines virtuelles et les banques de données | Tableaux de bord mis à jour concernant les performances, la capacité et la conformité des hôtes, 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 datastores iSCSI VMFS et NFS v3 avec protection sur trois sites, combinant SMAS et VMware Live Site Recovery. Prise en charge SRA de FCP avec VMFS. |
| Prise en charge du fournisseur VASA | VASA 4.0 | VASA 3.0 |

# Concepts

## Découvrez les outils ONTAP

ONTAP tools for VMware vSphere est un ensemble d'outils de gestion du cycle de vie des machines virtuelles. Il s'intègre à l'écosystème VMware pour simplifier le provisionnement des banques de données et assurer une protection de base des machines virtuelles. Il s'agit d'une collection de microservices à mise à l'échelle horizontale et pilotés par les événements, déployés sous forme d'Open Virtual Appliance (OVA).

Les outils ONTAP pour VMware vSphere prennent en charge :

- Fonctionnalités principales des machines virtuelles (VM) telles que la protection et la reprise après sinistre
- VASA Provider pour la gestion du stockage basée sur des règles
- Gestion du stockage basée sur des politiques
- Adaptateur de réplication de stockage (SRA)

**Haute disponibilité pour ONTAP tools for VMware**

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

La solution HA vous aide à vous rétablir rapidement après les types de pannes suivants :

- Défaillance de l'hôte - Seule la défaillance d'un seul nœud est prise en charge.
- panne de réseau
- Défaillance de la machine virtuelle (système d'exploitation invité)
- Échec de l'application (ONTAP tools)

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

Les outils ONTAP pour VMware vSphere ne prennent pas en charge la haute disponibilité vCenter.

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

# Concepts et termes clés dans ONTAP tools

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

**Autorité de certification (CA)**

Une autorité de certification (CA) est une entité de confiance qui délivre 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 la cohérence des données entre les unités de stockage et les volumes. Dans ONTAP, ils offrent une gestion simplifiée et des garanties de protection pour une charge de travail applicative répartie sur plusieurs volumes. En savoir plus "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 du cluster sont configurés en paires HA pour des opérations non perturbatrices.

### Numéro d'unité logique (LUN)

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

### Espace de noms et sous-système NVMe

Un espace de noms NVMe correspond à une quantité de mémoire non volatile pouvant être formatée en blocs logiques. Les espaces de noms sont l'équivalent des LUN pour les protocoles FC et iSCSI, et un sous-système NVMe est analogue à un igroup. Un sous-système NVMe peut être associé à des initiateurs afin que les initiateurs associés puissent accéder aux espaces de noms du sous-système.

### ONTAP tools Manager

ONTAP tools Manager offre ONTAP tools for VMware vSphere aux administrateurs un contrôle accru sur les instances de serveur vCenter gérées et les backends de stockage intégrés. Il aide à gérer les instances de serveur vCenter, les backends de stockage, les certificats, les mots de passe et les bundles de journaux.

### Open Virtual Appliance (OVA)

OVA est une norme ouverte pour l'empaquetage et la distribution d'appliances virtuelles ou de logiciels qui doivent être exécutés sur des machines virtuelles.

### Objectif de point de récupération (RPO)

L'objectif de point de restauration (RPO) mesure la fréquence à laquelle vous sauvegardez ou répliquez vos données. Il spécifie le moment précis où vous devez restaurer les données après une interruption de service pour reprendre les opérations commerciales. Par exemple, si une organisation a un RPO de 4 heures, elle peut tolérer la perte de 4 heures de données en cas de sinistre.

### SnapMirror active sync

SnapMirror active sync permet aux services métier de continuer à fonctionner même en cas de panne complète d'un site, en prenant en charge le basculement transparent des applications grâce à une copie secondaire. Aucune intervention manuelle ni script personnalisé n'est requis pour déclencher un basculement avec SnapMirror active sync. En savoir plus "SnapMirror active sync".

### Backends de stockage

Les backends de stockage constituent l'infrastructure de stockage sous-jacente que l'hôte ESXi utilise pour stocker les fichiers, les données et autres ressources des machines virtuelles. Ils permettent à l'hôte ESXi d'accéder aux données persistantes et de les gérer, en fournissant la capacité de stockage et les performances requises pour un environnement virtualisé.

#### Cluster global (infrastructure de stockage principale)

Les systèmes de stockage globaux, accessibles uniquement avec les identifiants du cluster ONTAP, sont intégrés via l'interface Manager des ONTAP tools. Ils peuvent être ajoutés avec des privilèges minimaux pour permettre la découverte des ressources essentielles du cluster nécessaires à la gestion des vVols. Les clusters globaux sont idéaux pour les scénarios de multitenance où un utilisateur SVM est ajouté localement pour la gestion des vVols.

#### backend de stockage local

Les backends de stockage locaux avec des identifiants de cluster ou de SVM sont ajoutés via l'interface utilisateur des ONTAP tools et sont limités à un vCenter. Lorsque vous utilisez des identifiants de cluster localement, les SVM associés sont automatiquement associés au vCenter pour gérer les vVols ou VMFS. Pour la gestion de VMFS, y compris SRA, ONTAP tools prend en charge les identifiants SVM sans nécessiter de cluster global.

### Adaptateur de réplication de stockage (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 de la Storage Virtual Machine (SVM) ainsi qu'au niveau de la configuration du cluster.

### Machine virtuelle de stockage (SVM)

SVM est l'unité de multitenancy dans ONTAP. À l'instar d'une machine virtuelle exécutée sur un hyperviseur, SVM est une entité logique qui abstrait les ressources physiques. SVM contient des volumes de données et une ou plusieurs LIF par lesquelles elle distribue les données aux clients.

### Configuration uniforme et non uniforme

- L'accès uniforme aux hôtes signifie que les hôtes de deux sites sont connectés à tous les chemins d'accès aux clusters de stockage des deux sites. Les chemins intersites sont étendus sur de longues distances.
- **Accès non uniforme aux hôtes** 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.

> L'accès uniforme à l'hôte est pris en charge pour tout déploiement de synchronisation active SnapMirror ; l'accès non uniforme à l'hôte est uniquement pris en charge pour les déploiements actifs/actifs symétriques. En savoir plus "SnapMirror vue d'ensemble de la synchronisation active dans ONTAP".

### Système de fichiers de machine virtuelle (VMFS)

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

#### Volumes virtuels (vVols)

vVols fournissent une abstraction au niveau du volume pour le stockage utilisé par une machine virtuelle. Il présente plusieurs avantages et constitue une alternative à l'utilisation d'un LUN traditionnel. Un datastore vVol est généralement associé à un seul LUN qui sert de conteneur pour les vVols.

#### Stratégie de stockage des machines virtuelles

Les stratégies de stockage des machines virtuelles sont créées dans le serveur vCenter sous Stratégies et profils. Pour les vVols, créez un ensemble de règles à l'aide des règles du fournisseur de type de stockage NetApp vVols.

#### Récupération de site en direct VMware

VMware Live Site Recovery, anciennement connu sous le nom de Site Recovery Manager (SRM), offre des fonctionnalités de continuité d'activité, de reprise après sinistre, de migration de site et de test non perturbateur pour les environnements virtuels VMware.

#### API VMware vSphere pour la gestion du stockage (VASA)

VASA est un ensemble d'API qui intègre les baies de stockage avec le serveur vCenter pour la gestion et l'administration. L'architecture repose sur plusieurs composants, notamment le fournisseur VASA, qui assure la communication entre VMware vSphere et les systèmes de stockage.

#### API de stockage VMware vSphere - Intégration des baies (VAAI)

VAAI est un ensemble d'API permettant 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 sur la baie. VAAI peut apporter des améliorations significatives des performances pour les tâches intensives en stockage.

#### vSphere Metro Storage Cluster

vSphere Metro Storage Cluster (vMSC) est une architecture qui permet et prend en charge vSphere dans un déploiement de cluster étendu. Les solutions vMSC sont prises en charge sur NetApp MetroCluster et SnapMirror active sync (anciennement SMBC). Ces solutions offrent une continuité d'activité renforcée en cas de panne de domaine. Le modèle de résilience dépend de vos choix de configuration spécifiques. En savoir plus "Cluster de stockage Metro VMware vSphere".

#### banque de données vVols

Le vVols datastore est une représentation logique d'un vVols container créé et maintenu par un VASA Provider.

#### RPO zéro

RPO signifie « objectif de point de récupération », soit le niveau de perte de données jugé acceptable sur une période donnée. Un 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 les rôles (RBAC) est un cadre de sécurité permettant de

contrôler l’accès aux ressources au sein d’une organisation. Le RBAC simplifie l’administration en définissant des rôles avec des niveaux d’autorité spécifiques pour effectuer des actions, au lieu d’attribuer des autorisations à chaque utilisateur. Les rôles définis sont attribués aux utilisateurs, ce qui contribue à réduire le risque d’erreur et simplifie la gestion du contrôle d’accès dans toute votre organisation.

Le modèle standard RBAC comprend plusieurs technologies ou phases d’implémentation de complexité croissante. Le résultat est que les déploiements RBAC réels, basés sur les besoins des éditeurs de logiciels et de leurs clients, peuvent différer et aller de relativement simples à très complexes.

### Composants RBAC

De manière générale, plusieurs composants sont inhérents à toute implémentation RBAC. Ces composants sont liés entre eux de différentes manières afin de définir les processus d’autorisation.

#### Privileges

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. Privileges peuvent également être définis pour restreindre l’accès aux points de terminaison REST API et aux commandes CLI. Chaque implémentation RBAC inclut des privilèges prédéfinis et peut également permettre aux administrateurs de créer des privilèges personnalisés.

#### Rôles

Un rôle est un conteneur regroupant un ou plusieurs privilèges. Les rôles sont généralement définis en fonction de tâches ou de fonctions spécifiques. Lorsqu’un rôle est attribué à un utilisateur, celui-ci reçoit tous les privilèges contenus dans ce rôle. À l’instar des privilèges, 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 par les privilèges sont exécutées sur ou avec les objets associés. Selon l’implémentation, les privilèges peuvent être accordés à un type d’objet ou à une instance d’objet spécifique.

#### Utilisateurs et groupes

Les utilisateurs sont affectés ou associés à un rôle appliqué après l’authentification. Certaines implémentations de RBAC n’autorisent qu’un seul rôle par utilisateur, tandis que d’autres permettent plusieurs rôles par utilisateur, avec éventuellement un seul rôle actif à la fois. L’attribution de rôles à des groupes peut encore simplifier l’administration de la sécurité.

#### Autorisations

Une permission est une définition qui associe un utilisateur ou un groupe, ainsi qu’un rôle, à un objet. Les permissions peuvent être utiles dans un modèle d’objet hiérarchique où elles peuvent éventuellement être héritées par les éléments 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. ONTAP tools for VMware vSphere 10 requiert des privilèges spécifiques à la fois dans vCenter et dans ONTAP pour effectuer ses opérations. Bien que les ONTAP tools automatisent les tâches de gestion du stockage, ils ne créent pas de comptes utilisateur ni dans vCenter ni dans ONTAP. Les comptes de service doivent être créés par un administrateur vSphere selon les besoins. Cette documentation fournit des instructions aux administrateurs pour attribuer les rôles et autorisations nécessaires à une gestion efficace des

ONTAP tools.

#### Serveur VMware vCenter

L'implémentation RBAC dans VMware vCenter Server est utilisée pour restreindre l'accès aux objets exposés via l'interface utilisateur du client vSphere. Dans le cadre de l'installation des ONTAP tools for VMware vSphere 10, l'environnement RBAC est étendu pour inclure des objets supplémentaires représentant les capacités des ONTAP tools. L'accès à ces objets est fourni via le plug-in distant. Voir "vCenter Server environnement RBAC" pour plus d'informations.

#### Cluster ONTAP

ONTAP tools for VMware vSphere 10 se connecte à un cluster ONTAP via l'API REST ONTAP pour effectuer des opérations liées au stockage. L'accès aux ressources de stockage est contrôlé par un rôle ONTAP associé à l'utilisateur ONTAP fourni lors de l'authentification. Voir "Environnement RBAC ONTAP" pour plus d'informations.

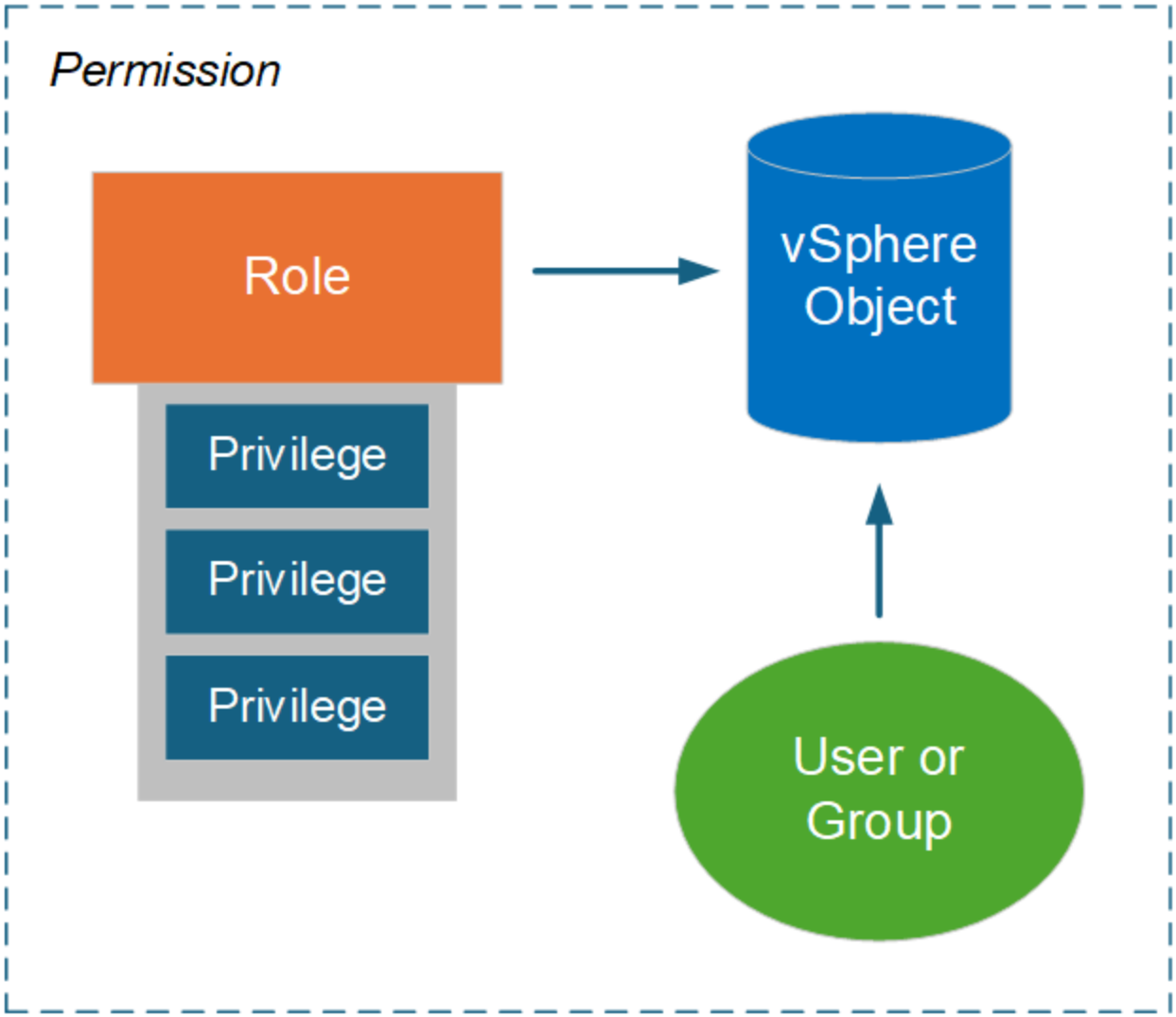
## RBAC avec VMware vSphere

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

VMware vCenter Server offre 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 de vCenter.

#### Illustration d'une autorisation de serveur vCenter

Une autorisation est la base pour appliquer le 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 de l'autorisation. Une illustration de haut niveau d'une autorisation vCenter est présentée dans la figure ci-dessous.




#### Composants d'une autorisation de serveur vCenter

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

### vSphere objets

Les autorisations sont associées à des objets vSphere, tels que le serveur vCenter, les hôtes ESXi, les machines virtuelles, les banques de données, les centres de données et les dossiers. En fonction des autorisations attribuées à l'objet, le serveur vCenter détermine les actions ou tâches que chaque utilisateur ou groupe peut effectuer sur cet objet. Pour les tâches spécifiques à ONTAP tools for VMware vSphere, toutes les autorisations sont attribuées et validées au niveau racine ou au niveau du dossier racine du serveur vCenter. Voir "Utilisez le contrôle d'accès basé sur les rôles (RBAC) avec le serveur vCenter" pour plus d'informations.

### Privileges et rôles

Il existe deux types de privilèges vSphere utilisés avec les ONTAP tools for VMware vSphere 10. Pour simplifier le travail avec le contrôle d'accès basé sur les rôles (RBAC) dans cet environnement, ONTAP tools fournit des rôles contenant les privilèges natifs et personnalisés requis. Les privilèges incluent :

- Privilèges natifs du serveur vCenter

  Voici les privilèges fournis par le serveur vCenter.

- Privilèges spécifiques aux outils ONTAP

  Ce sont des privilèges personnalisés propres aux ONTAP tools for VMware vSphere.

### Utilisateurs et groupes

Vous pouvez définir des utilisateurs et des groupes à l'aide d'Active Directory ou de l'instance locale du serveur vCenter. Associé à un rôle, vous pouvez créer une autorisation sur un objet dans 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 isolément. Au contraire, les utilisateurs et les groupes obtiennent l'accès à un objet via les privilèges de rôle dans le cadre de l'autorisation du serveur vCenter plus large.

### vCenter Server : considérations RBAC pour les ONTAP tools

Plusieurs aspects de l'implémentation RBAC des ONTAP tools for VMware vSphere 10 avec vCenter Server doivent être pris en compte avant de les utiliser dans un environnement de production.

#### vCenter rôles et le compte administrateur

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

#### hiérarchie des objets vSphere

L'inventaire des objets vSphere est organisé de manière hiérarchique. Par exemple, vous pouvez parcourir la hiérarchie comme suit :

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

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 ONTAP tools for VMware vSphere 10

Pour simplifier le travail avec le contrôle d'accès basé sur les rôles (RBAC) du serveur vCenter, ONTAP tools for VMware vSphere fournit des rôles prédéfinis adaptés à diverses tâches administratives.

> Vous pouvez créer des rôles personnalisés si nécessaire. Pour ce faire, clonez l'un des rôles existants des ONTAP tools et modifiez-le selon vos besoins. Après avoir effectué les modifications de configuration, les utilisateurs clients vSphere concernés doivent se déconnecter puis se reconnecter pour activer les changements.

Pour afficher les rôles ONTAP tools for VMware vSphere, sélectionnez **Menu** en haut du client vSphere, puis cliquez sur **Administration** et ensuite 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 du serveur vCenter.

Assurez-vous que ces privilèges sont configurés comme prérequis au processus de déploiement ou 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
  - Importer le stockage
  - Stockage de lecture
  - Synchroniser l'élément de bibliothèque
  - Synchroniser la bibliothèque abonnée
  - Afficher les paramètres de configuration
- Magasin de données
  - Allouer de l'espace
  - Parcourir le datastore
  - opérations de fichiers de bas niveau
  - Supprimer le fichier
  - Mettre à jour les fichiers de la machine virtuelle
  - Mise à jour des métadonnées de la machine virtuelle
- Gestionnaire d'agents ESX
  - View
- Dossier
  - Créer un dossier
- Hôte
  - Configuration
    - Paramètres avancés
    - Modifier les paramètres
    - Configuration 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
    - Configurer
- OvfManager
    - OvfConsumer Accès
- 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 vApp
    - Créer
    - Importer
    - Déplacer
    - Mise hors tension
    - Mise sous tension
    - Récupérer depuis l’URL
    - Afficher l’environnement OVF
- machine virtuelle
    - Modifier la configuration
        - Ajouter un disque existant
        - Ajouter un nouveau disque
        - Ajouter ou supprimer un appareil
        - Configuration avancée
        - Modifier le nombre de CPU
        - 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 invité
        - Mise à niveau de la compatibilité des machines virtuelles
    - Modifier l’inventaire
        - Créer à partir de l’existant
        - Créer nouveau
        - Déplacer
        - S’inscrire
        - Retirer
        - Annuler l’enregistrement
    - Interaction
        - Opération de sauvegarde sur machine virtuelle
        - Configurer le support CD
        - Configurer le support de disquette
        - Connectez des appareils
        - 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
        - Cloner le modèle
        - Personnaliser l’invité
        - Déployer le modèle
        - Modifier la spécification de personnalisation
        - Lire les spécifications de personnalisation
    - Gestion des instantanés
        - Créer un instantané
        - Supprimer l’instantané
        - Renommer le snapshot
        - Rétablir l’instantané

Il existe trois rôles prédéfinis, décrits ci-dessous.

**Administrateur de NetApp ONTAP tools for VMware vSphere**

Fournit tous les privilèges natifs du serveur vCenter et les privilèges spécifiques aux outils ONTAP requis pour

effectuer les tâches principales d'administrateur des ONTAP tools for VMware vSphere.

**NetApp ONTAP tools for VMware vSphere en lecture seule**

Fournit un accès en lecture seule aux outils ONTAP. Ces utilisateurs ne peuvent effectuer aucune action des outils ONTAP pour VMware vSphere soumise à un contrôle d'accès.

**NetApp ONTAP tools pour VMware vSphere Provision**

Fournit certains des privilèges natifs du serveur vCenter et des privilèges spécifiques aux outils ONTAP qui sont nécessaires au provisionnement du stockage. Vous pouvez effectuer les tâches suivantes :

- Créer de nouveaux datastores
- Gérer les datastores

#### vSphere objets et backends de stockage ONTAP

Les deux environnements RBAC fonctionnent de concert. Lors de l'exécution d'une tâche dans l'interface client vSphere, les rôles des outils ONTAP définis pour le serveur vCenter sont vérifiés en premier. Si l'opération est autorisée par vSphere, alors les privilèges du rôle ONTAP sont examinés. Cette seconde étape est effectuée en fonction du rôle ONTAP attribué à l'utilisateur lors de la création et de la configuration du stockage principal.

#### Utilisation du contrôle d'accès basé sur les rôles (RBAC) du serveur vCenter

Il y a quelques éléments à prendre en compte lors de la gestion des privilèges et des autorisations du serveur vCenter.

### Privilèges requis

Pour accéder à l'interface utilisateur ONTAP tools for VMware vSphere 10, vous devez disposer du privilège *View* spécifique à ONTAP tools. Si vous vous connectez à vSphere sans ce privilège et 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'attribution dans la hiérarchie des objets vSphere détermine les parties de l'interface utilisateur auxquelles vous pouvez accéder. L'attribution du privilège « View » à l'objet racine vous permet d'accéder aux ONTAP tools for VMware vSphere en cliquant sur l'icône NetApp.

Vous pouvez également attribuer le privilège d'affichage à un niveau d'objet vSphere inférieur. Cependant, cela limitera les menus des ONTAP tools for VMware vSphere auxquels vous pouvez accéder et utiliser.

### Attribution des autorisations

Vous devez utiliser les autorisations du serveur vCenter si vous souhaitez limiter l'accès aux objets et tâches vSphere. L'endroit où vous attribuez l'autorisation dans la hiérarchie des objets vSphere détermine les tâches ONTAP tools for VMware vSphere 10 que les utilisateurs peuvent effectuer.

Sauf si vous devez définir un accès plus restrictif, il est généralement conseillé d'attribuer les autorisations au niveau de l'objet racine ou du dossier racine.

Les autorisations disponibles avec ONTAP tools for VMware vSphere 10 s'appliquent aux objets non-vSphere personnalisés, tels que les systèmes de stockage. Dans la mesure du possible, vous devez attribuer ces autorisations à l'objet racine ONTAP tools for VMware vSphere, car il n'existe aucun objet vSphere auquel vous pouvez les attribuer. Par exemple, toute autorisation incluant le privilège « Ajouter/Modifier/Supprimer des systèmes de stockage » d'ONTAP tools for VMware vSphere doit être attribuée au niveau de l'objet racine.

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

Vous pouvez modifier une autorisation à tout moment. Si vous modifiez l'un des privilèges au sein d'une autorisation, les utilisateurs associés à l'autorisation doivent se déconnecter de vSphere puis se reconnecter pour que la modification soit prise en compte.

## Contrôle d'accès basé sur les rôles (RBAC) avec ONTAP

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

ONTAP offre un environnement RBAC robuste et extensible. Vous pouvez utiliser la fonctionnalité RBAC pour contrôler l'accès au stockage et aux opérations système exposées via l'API REST et le CLI. Il est utile de bien connaître l'environnement avant de l'utiliser avec un déploiement ONTAP tools for VMware vSphere 10.

#### Aperçu des options administratives

Plusieurs options s'offrent à vous lors de l'utilisation de ONTAP RBAC, selon votre environnement et vos objectifs. Un aperçu des principales décisions d'administration est présenté ci-dessous. Voir aussi "Automatisation ONTAP : aperçu de la sécurité RBAC" pour plus d'informations.

> ONTAP RBAC est conçu spécifiquement pour les environnements de stockage et est plus simple que l'implémentation RBAC fournie avec vCenter Server. Avec ONTAP, vous attribuez directement un rôle à l'utilisateur. La configuration explicite des autorisations, comme celle utilisée avec vCenter Server, n'est pas nécessaire avec ONTAP RBAC.

#### Types de rôles et de privilèges

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

- REST

  Les rôles REST ont été introduits avec ONTAP 9.6 et s'appliquent généralement aux utilisateurs accédant à ONTAP via l'API REST. Les privilèges inclus dans ces rôles sont définis en termes d'accès aux points de terminaison de l'API REST d'ONTAP et aux actions associées.

- Traditionnel

  Il s'agit des rôles hérités antérieurs à ONTAP 9.6. Ils demeurent un élément fondamental du RBAC. Les privilèges sont définis en termes d'accès aux commandes CLI ONTAP.

Bien que les rôles REST soient plus récents, les rôles traditionnels présentent certains avantages. Par exemple, des paramètres de requête supplémentaires peuvent être inclus afin de permettre aux Privileges de définir plus précisément les objets auxquels ils s'appliquent.

#### Portée

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

#### Définitions des rôles

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

#### Travailler avec les rôles REST ONTAP

Plusieurs points sont à prendre en compte lors de l'utilisation des rôles ONTAP REST inclus avec ONTAP tools for VMware vSphere 10.

#### Cartographie des rôles

Que vous utilisiez un rôle traditionnel ou REST, toutes les décisions d'accès ONTAP sont prises en fonction de la commande CLI sous-jacente. Mais comme les privilèges dans un rôle REST sont définis en termes de points de terminaison de l'API REST, ONTAP doit créer un rôle traditionnel *mappé* pour chacun des rôles REST. Par conséquent, chaque rôle REST correspond à un rôle traditionnel sous-jacent. Cela permet à ONTAP de 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 parallèles.

#### Définition d'un rôle REST à l'aide des privilèges de l'interface de ligne de commande

Comme ONTAP utilise systématiquement les commandes CLI pour déterminer les accès de base, il est possible d'exprimer un rôle REST à l'aide des privilèges des commandes CLI plutôt que des points de terminaison REST. Un avantage de cette approche est la granularité supplémentaire offerte par les rôles traditionnels.

#### Interface d'administration lors de la définition des rôles ONTAP

Vous pouvez créer des utilisateurs et des rôles avec l'interface de ligne de commande ONTAP (CLI) et l'API REST ONTAP. Cependant, il est plus pratique d'utiliser l'interface System Manager ainsi que le fichier JSON disponible via ONTAP tools Manager. Voir "Utilisez ONTAP RBAC avec les ONTAP tools for VMware vSphere 10" pour plus d'informations.

### Considérations RBAC ONTAP pour les outils ONTAP

Plusieurs aspects de la mise en œuvre du contrôle d'accès basé sur les rôles (RBAC) des ONTAP tools for VMware vSphere 10 avec ONTAP doivent être pris en compte avant de l'utiliser dans un environnement de production.

#### Aperçu du processus de configuration

ONTAP tools for VMware vSphere inclut 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 importer dans le cluster ONTAP. Vous pouvez créer l'utilisateur et adapter le rôle à votre environnement et à vos besoins en matière de sécurité.

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

#### 1. Préparer

Vous devez disposer d'identifiants d'administrateur à la fois pour ONTAP tools Manager et pour le cluster ONTAP.

#### 2. Téléchargez le fichier de définition JSON

Après vous être connecté à l'interface utilisateur de ONTAP tools Manager, vous pouvez télécharger le fichier JSON contenant les définitions RBAC.

#### 3. Créez un utilisateur ONTAP avec un rôle

Après vous être connecté à System Manager, vous pouvez créer l'utilisateur et le rôle :

1. Sélectionnez **Cluster** à gauche, puis **Settings**.
2. Faites défiler vers le bas jusqu'à **Utilisateurs et rôles** et cliquez −→.
3. Sélectionnez **Ajouter** sous **Utilisateurs** et sélectionnez **Virtualization products**.
4. Sélectionnez le fichier JSON sur votre poste de travail local et téléversez-le.

#### 4. Configurer le rôle

Pour définir ce 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 nouvel 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 principale des utilisateurs et des rôles

Les définitions RBAC sont intégrées à plusieurs fonctionnalités produit, notamment des combinaisons de VSC, VASA Provider et SRA. Vous devez sélectionner l'environnement ou les environnements où vous avez besoin de la prise en charge RBAC. Par exemple, si vous souhaitez que les rôles prennent en charge la fonctionnalité de plug-in distant, sélectionnez VSC. Vous devez également choisir le nom d'utilisateur et le mot de passe associé.

### Privileges

Les privilèges des rôles sont organisés en quatre ensembles en fonction du niveau d'accès requis pour le stockage ONTAP. Les privilèges sur lesquels les rôles sont basés comprennent :

- Découverte

  Ce rôle vous permet d'ajouter des systèmes de stockage.

- Créer un stockage

  Ce rôle vous permet de créer du stockage. Il inclut également tous les privilèges associés au rôle de découverte.

- Modifier le stockage

  Ce rôle vous permet de modifier le stockage. Il inclut également tous les privilèges associés aux rôles de découverte et de création de stockage.

- Détruire le stockage

  Ce rôle vous permet de supprimer du stockage. Il inclut également tous les privilèges associés aux rôles de découverte, de création et de modification de stockage.

### Générez l'utilisateur avec un rôle

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

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

**Exemple**

```
OTV_10_VSC_Discovery_Create
```

Le nouvel utilisateur sera ajouté à la liste sur 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 ONTAP tools for VMware vSphere

Configurez les outils ONTAP pour VMware vSphere grâce à cette section de démarrage rapide.

Commencez par effectuer ces tâches essentielles pour rendre les outils ONTAP opérationnels pour la gestion et le provisionnement du jour 0. Ensuite, effectuez les tâches optionnelles en fonction de votre environnement et de vos exigences en matière de protection.

Dans un premier temps, vous déploierez les outils ONTAP pour VMware vSphere sous la forme d'une configuration à nœud unique de petite taille fournissant les services de base pour la prise en charge des datastores NFS et VMFS. Pour étendre votre configuration afin d'ajouter des conteneurs par service, d'améliorer la résilience ou d'utiliser des datastores vVols et la haute disponibilité (HA), suivez d'abord ce workflow, puis poursuivez avec les étapes d'extension. Pour plus d'informations, consultez la "Flux de travail de déploiement HA".

**Planifiez votre déploiement**

Confirmez que votre environnement est prêt pour un déploiement pris en charge. Vérifiez que vos versions de vSphere, d'ONTAP et d'hôte ESXi sont compatibles avec la version des ONTAP tools. Allouez suffisamment de CPU, de mémoire et d'espace 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 le serveur vCenter est installé et accessible.

- "Outil Interoperability Matrix Tool"
- "Exigences et limites de configuration des outils ONTAP pour VMware vSphere"
- "Avant de commencer"

**Déployez les ONTAP tools pour VMwarevSphere**

Déployez l'appliance ONTAP tools pour établir les services de base pour les datastores NFS et VMFS.

Dans un premier temps, vous déploierez ONTAP tools for VMware vSphere sous la forme d'une configuration à nœud unique de petite taille. Si vous prévoyez d'étendre votre configuration pour utiliser des datastores vVols et la haute disponibilité (HA), vous le ferez une fois ce workflow terminé. Pour passer à une configuration HA, assurez-vous que l'ajout à chaud de processeurs et le branchement à chaud de mémoire sont activés.

Lors du déploiement, examinez attentivement les champs **Personnaliser le modèle**, en particulier le nom de l'hôte, l'utilisation de l'adresse IP des ONTAP tools et les exigences DNS.

- "Déployez les outils ONTAP pour VMware vSphere"

**Enregistrez et installez le plug-in client vCenter**

Ajoutez une instance de serveur vCenter pour enregistrer le plug-in client vCenter et appliquer les privilèges et rôles requis. Lorsque vous ajoutez une instance de serveur vCenter, ONTAP tools enregistre le plug-in distant, applique les privilèges personnalisés du plug-in et de l'API, crée des rôles personnalisés et ajoute un raccourci vers le plug-in dans l'interface utilisateur vSphere.

- "Ajoutez des instances de serveur vCenter aux outils ONTAP"

**Configurer les backends de stockage**

Connectez les ressources de stockage ONTAP pour permettre aux outils ONTAP de provisionner et de gérer les datastores. Ajoutez un backend de stockage à un cluster ONTAP. Dans les environnements multitenants où un serveur vCenter est associé à une SVM locataire, utilisez ONTAP tools Manager pour ajouter le cluster. Associez ensuite le backend de stockage au serveur vCenter afin de créer un mappage global pour cette instance vCenter.

Ajoutez les backends de stockage locaux avec des identifiants de cluster ou de SVM à l'aide de l'interface utilisateur des outils ONTAP. Ces backends de stockage sont limités à un seul vCenter. Lorsque vous utilisez des identifiants de cluster localement, les SVM associés sont automatiquement mappés au vCenter pour gérer les vVols ou VMFS. Pour la gestion de VMFS, y compris SRA, les outils ONTAP prennent en charge les identifiants de SVM sans nécessiter de cluster global.

- "Ajouter un backend de stockage"
- "Associez le système de stockage à une instance de serveur vCenter"

## Tâches suivantes facultatives

**Configurer les rôles et privilèges des utilisateurs ONTAP**

Configurez des rôles ONTAP personnalisés pour un accès à privilèges minimaux au lieu du compte administrateur par défaut.

- "Configurer les rôles et privilèges des utilisateurs ONTAP"

**Mettre à niveau les certificats pour plusieurs instances de serveur vCenter**

Mettez à niveau les certificats pour utiliser une communication basée sur des certificats de confiance entre plusieurs instances de serveur vCenter.

- "Gérer les certificats"

**Configurer la protection SRA**

Activez la fonctionnalité SRA pour configurer la protection contre les sinistres pour les datastores NFS et VMFS.

- "Activer les ONTAP tools for VMware vSphere services"
- "Configurez SRA sur l'appliance VMware Live Site Recovery"

**Activer la protection de synchronisation active SnapMirror**

Configurez la protection du cluster hôte avec la synchronisation active SnapMirror pour protéger les datastores VMFS. Dans les systèmes ONTAP, associez le cluster et la SVM requis, puis configurez la protection du cluster hôte dans ONTAP tools for VMware vSphere. Cette option s'applique uniquement aux datastores VMFS.

- "Protéger à l'aide de la protection du cluster hôte"

5 **Configurez la sauvegarde et la restauration pour votre déploiement d'outils ONTAP**

Mettez en place une stratégie de sauvegarde et de restauration pour protéger la configuration des ONTAP tools et récupérer rapidement en cas de panne.

La sauvegarde est activée par défaut dans ONTAP tools for VMware vSphere 10.5 et s'effectue toutes les 10 minutes. Planifiez des sauvegardes de votre configuration ONTAP tools for VMware vSphere que vous pouvez utiliser pour restaurer la configuration en cas de défaillance.

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

# Flux de travail de déploiement à haute disponibilité pour ONTAP tools

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

1 **Augmenter le déploiement**

Vous pouvez faire évoluer la configuration des ONTAP tools for VMware vSphere afin d'augmenter le nombre de nœuds dans le déploiement et de modifier la configuration pour un environnement HA.

- "Modifier la configuration des outils ONTAP pour VMware vSphere"

2 **Activer les services**

Pour configurer les banques 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 respectent les exigences de haute disponibilité, notamment en ce qui concerne la configuration correcte du réseau et du stockage.

Activez les services SRA pour utiliser ONTAP tools Storage Replication Adapter (SRA) pour VMware Site Recovery Manager (SRM) ou VMware Live Site Recovery (VLSR).

- "Activer les services VASA Provider et SRA"

3 **Mettre à niveau les certificats**

Si vous utilisez des banques de données vVol avec plusieurs instances de serveur vCenter, mettez à niveau le certificat auto-signé vers un certificat signé par une autorité de certification (CA).

- "Gérer les certificats"

# Exigences et limites de configuration des outils ONTAP pour VMware vSphere

Avant de déployer les ONTAP tools for VMware vSphere, vous devez vous familiariser avec les exigences d'espace du package de déploiement et certaines exigences de base du système hôte.

Vous pouvez utiliser ONTAP tools for VMware vSphere avec VMware vCenter Server Virtual Appliance (vCSA). Vous devez déployer ONTAP tools for VMware vSphere sur un environnement vSphere pris en charge qui inclut des hôtes ESXi.

## Configuration système requise

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

| Type de déploiement | Processeurs par nœud | Mémoire (Go) par nœud | Espace disque (Go) provisionné de manière épaisse par nœud |
|---|---|---|---|
| Petit | 9 | 18 | 350 |
| Moyen | 13 | 26 | 350 |
| Remarque importante : le déploiement à grande échelle est uniquement destiné à la configuration HA. | 17 | 34 | 350 |

Lorsque la sauvegarde est activée, chaque cluster ONTAP tools nécessite 50 Go d'espace supplémentaire sur le datastore où les machines virtuelles sont déployées. Par conséquent, une configuration non-HA requiert 400 Go et une configuration HA requiert 1 100 Go d'espace au total.

## Exigences minimales de stockage et des applications

| Stockage, hôte et applications | Exigences de version |
|---|---|
| ONTAP | 9.15.1, 9.16.1, et 9.17.0 |
| Hôtes ESXi pris en charge par ONTAP tools | 7.0.3 et suivantes |
| Outils ONTAP pris en charge vCenter Server | 7.0U3 et suivants |
| Fournisseur VASA | 3,0 |

| Stockage, hôte et applications | Exigences de version |
| --- | --- |
| Application OVA | 10,5 |
| Hôte ESXi pour déployer la machine virtuelle ONTAP tools | 7.0U3 et 8.0U3 |
| vCenter Server pour déployer la machine virtuelle ONTAP tools | 7.0 et 8.0 |

À partir de ONTAP tools for VMware vSphere 10.4, le matériel de la machine virtuelle passe de la version 10 à la version 17.

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

"Outil Interoperability Matrix Tool"

## Exigences relatives aux ports

Le tableau suivant présente les ports réseau que NetApp utilise et leurs fonctions. Il existe trois types de ports :

- 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 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 du cluster telles que le partage de données et la collaboration. Pour les déploiements à nœud unique, les ports inter-nœuds sont utilisés uniquement au sein du nœud et ne nécessitent pas d'accès externe. Les ports inter-nœuds peuvent accepter du 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 via des adresses ClusterIP. Ils ne sont pas exposés en externe et n'ont pas besoin d'être ajoutés aux règles du pare-feu.

Assurez-vous que tous les nœuds des ONTAP tools résident sur le même sous-réseau afin de 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 VASA Provider. Le certificat auto-signé et le certificat d'autorité de certification personnalisé de VASA Provider 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 (Restreindre 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 Domain Name System (DNS) pour la résolution de noms au sein du cluster. |
| NTP | 123 | UDP | Inter-nœud | Network Time Protocol (NTP) 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 |
| kube-controller | 10257 | TCP | Inter-nœud | Composant Kubernetes |
| cloud-controller | 10258 | TCP | Inter-nœud | Composant Kubernetes |
| kube-scheduler | 10259 | TCP | Inter-nœud | Composant Kubernetes |
| kube-proxy | 10249, 10256 | TCP | Inter-nœud | Composant Kubernetes |
| calico-node | 9091, 9099 | TCP | Inter-nœud | Composant réseau Calico. |
| containerd | 10010 | TCP | Inter-nœud | Service du démon de conteneur. |
| VXLAN (Flannel) | 8472 | UDP | Inter-nœud | Réseau superposé pour la communication entre les pods. |

Pour les déploiements à haute disponibilité, assurez-vous que le port UDP 8472 est ouvert entre tous les nœuds. Ce port permet la communication entre pods sur différents nœuds ; le bloquer interrompra la mise en réseau inter-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 de petite taille | 200 | 80 | 32 |
| Moyen non-HA | 250 | 100 | 32 |
| HA Small | 350 | 200 | 64 |
| HA Moyen | 600 | 200 | 128 |
| HA Large | 1024 | 250 | 256 |

## ONTAP tools for VMware vSphere - Storage Replication Adapter (SRA)

Le tableau suivant présente les nombres pris en charge par instance VMware Live Site Recovery à l'aide des ONTAP tools for VMware vSphere.

| vCenter Taille du déploiement | Petit | Moyen |
|---|---|---|
| Nombre total de machines virtuelles configurées pour la protection à l'aide de la réplication basée sur des baies | 2000 | 5000 |
| Nombre total de groupes de protection de réplication basés sur des baies | 250 | 250 |
| Nombre total de groupes de protection par plan de rétablissement | 50 | 50 |

| vCenter Taille du déploiement | Petit | Moyen |
|---|---|---|
| Nombre de banques de données répliquées | 255 | 255 |
| Nombre de machines virtuelles | 4000 | 7000 |

Le tableau suivant présente le nombre d'instances VMware Live Site Recovery et la taille de déploiement correspondante des ONTAP tools for VMware vSphere.

| Nombre d'instances VMware Live Site Recovery | Taille du déploiement des outils ONTAP |
|---|---|
| Jusqu'à 4 | Petit |
| 4 à 8 | Moyen |
| Plus de 8 | Grand |

Pour plus d'informations, consultez "Limites opérationnelles de VMware Live Site Recovery".

# Exigences préalables au déploiement des ONTAP tools

Assurez-vous que les exigences suivantes sont respectées avant de procéder au déploiement :

| Exigences | Votre statut |
|---|---|
| vSphere version, version ONTAP et version de l'hôte ESXi sont compatibles avec la version des ONTAP tools. | □ Oui □ Non |
| vCenter Server est installé et configuré | □ Oui □ Non |
| Le cache du navigateur est supprimé | □ Oui □ Non |
| Vous disposez des identifiants du serveur parent vCenter | □ Oui □ Non |
| Vous disposez des identifiants de connexion pour l'instance du serveur vCenter, à laquelle les ONTAP tools for VMware vSphere se connecteront après le déploiement pour l'enregistrement | □ Oui □ Non |
| Le nom de domaine sur lequel le certificat est émis est associé à l'adresse IP virtuelle dans un déploiement multi-vCenter où les certificats CA personnalisés sont obligatoires. | □ Oui □ Non |
| Vous avez exécuté la commande nslookup sur le nom de domaine pour vérifier si le domaine est résolu vers 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 ONTAP tools et les services internes sont accessibles depuis le serveur vCenter. | □ Oui □ Non |

| Exigences | Votre statut |
| --- | --- |
| Lorsque vous utilisez des SVM multi-locataires, vous disposez d'une LIF de gestion SVM sur chaque SVM. | □ Oui □ Non |

## Feuille de travail de déploiement

### Pour le déploiement à nœud unique

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

| Exigence | 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 ONTAP tools pour la communication interne. Cette adresse IP est utilisée pour la communication interne dans une configuration avec plusieurs instances ONTAP tools. Cette adresse IP ne doit pas être la même que l'adresse IP de l'application ONTAP tools. (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 ONTAP tools. 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 pour 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'hôtes, associez-les aux adresses IP disponibles dans DNS. Toutes les adresses IP doivent être sur le même VLAN sélectionné pour le déploiement.

**Pour le déploiement à haute disponibilité (HA)**

En plus des exigences de déploiement sur un seul nœud, vous aurez besoin des informations suivantes pour un déploiement HA :

| Exigence | Votre valeur |
|---|---|
| serveur DNS principal | |
| serveur DNS secondaire | |
| domaine de recherche DNS | |
| Nom d'hôte DNS pour le deuxième nœud | |
| Adresse IP du deuxième nœud | |
| Nom d'hôte DNS pour le 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 à la LIF via le port 443. Pour obtenir la liste complète des ports requis, consultez la section relative aux exigences de port à "Exigences et limites de configuration des outils ONTAP pour VMware vSphere".

## Paramètres de stockage ONTAP

Pour garantir une intégration transparente du stockage ONTAP avec ONTAP tools for VMware vSphere, tenez compte des paramètres suivants :

- Si vous utilisez le 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. "Découvrez le zonage 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 pairs ONTAP" et "Relations entre pairs SVM intercluster ONTAP" dans ONTAP avant d'utiliser SnapMirror.

# Déployer les outils ONTAP

L'appliance ONTAP tools for VMware vSphere est déployée sous la forme d'un nœud unique de petite taille, avec des services principaux pour prendre en charge les datastores NFS et VMFS. Le processus de déploiement des ONTAP tools 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 à haute disponibilité, une bibliothèque de contenu est requise. Dans VMware, une bibliothèque de contenu stocke les modèles de machines virtuelles, les modèles vApp et d'autres fichiers. Le déploiement avec une bibliothèque de contenu offre une expérience transparente, car il n'est pas dépendant de la connectivité réseau.

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

- Créez la bibliothèque de contenu sur un datastore partagé afin que tous les hôtes du cluster puissent y accéder.
- Configurez la bibliothèque de contenu avant de déployer l'OVA ONTAP tools for VMware vSphere.
- Assurez-vous que la bibliothèque de contenu est créée avant de configurer l'appliance pour la haute disponibilité.

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

Pour permettre un déploiement haute disponibilité ultérieur, évitez de déployer la machine virtuelle ONTAP tools directement sur un hôte ESXi. Déployez-la plutôt au sein d'un cluster d'hôtes ESXi ou d'un pool de ressources.

Suivez ces étapes pour créer une bibliothèque de contenu :

1. Téléchargez le fichier qui contient les fichiers binaires (*.ova*) et les certificats signés pour ONTAP tools for VMware vSphere depuis le "Site de support NetApp".
2. Connectez-vous au client vSphere
3. Sélectionnez le menu client vSphere et sélectionnez **bibliothèques de contenu**.
4. Sélectionnez **Créer** à droite de la page.
5. Donnez un nom à 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, sélectionnez **Importer un élément**, et importez le fichier OVA.

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

Avant de procéder au déploiement, configurez le Distributed Resource Scheduler (DRS) du cluster 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 configuration non-HA. Pour passer à un déploiement HA, vous devrez activer l'ajout à chaud de CPU et le hot-plug de mémoire. Vous pouvez effectuer cette étape lors du processus de déploiement ou modifier les paramètres de la VM après le déploiement.

**Étapes**

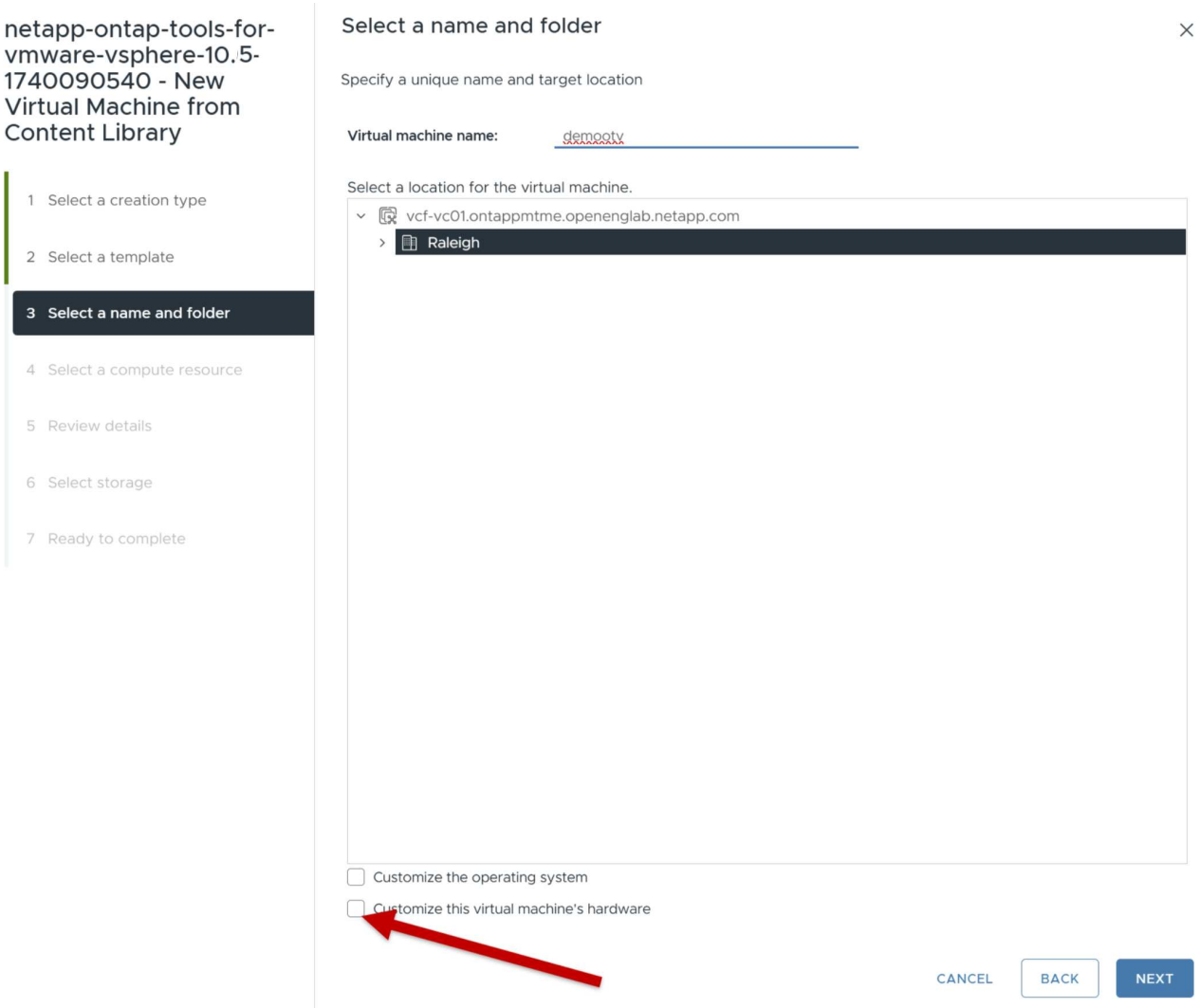
1. Téléchargez le fichier qui contient les binaires (*.ova*) et les certificats signés pour les ONTAP tools for VMware vSphere depuis le "Site de support NetApp". Si vous avez importé l'OVA dans la bibliothèque de contenu, vous pouvez ignorer cette étape et passer à la suivante.
2. Connectez-vous au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

Ne stockez jamais la machine virtuelle ONTAP tools for VMware vSphere sur les datastores vVols qu'elle gère.

4. Vous pouvez déployer le fichier OVA depuis la bibliothèque de contenu ou depuis le système local.

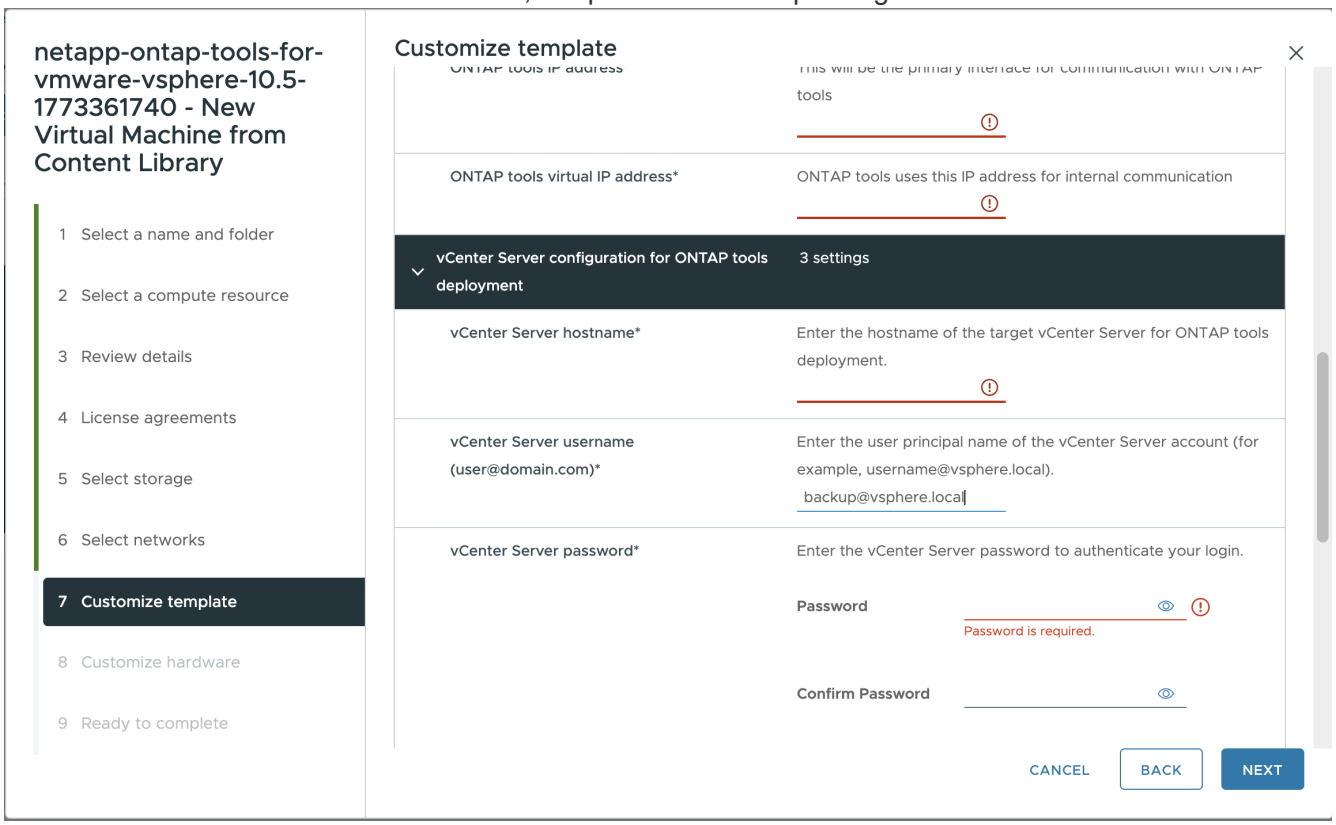
| À partir du système local | De la bibliothèque de contenu |
| --- | --- |
| a. Faites un clic droit et sélectionnez **Déployer le modèle OVF…**. b. Choisissez le fichier OVA à partir de l'URL ou accédez à son emplacement, puis sélectionnez **Suivant**. | a. Accédez à votre bibliothèque de contenu et sélectionnez l'élément que vous souhaitez déployer. b. Sélectionnez **Actions** > **Nouvelle machine virtuelle à partir de ce modèle** |

5. Dans le champ **Sélectionnez un nom et un dossier**, saisissez le nom de la machine virtuelle et choisissez son emplacement.
   - Si vous utilisez la version vCenter Server 8.0.3, sélectionnez l'option **Personnaliser le matériel de cette machine virtuelle**, ce 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 **Et ensuite ?** à la fin du déploiement.




6. Sélectionnez une ressource ordinateur et cliquez sur **Suivant**. Cochez éventuellement la case pour **Démarrer automatiquement la machine virtuelle déployée**.
7. Examinez les détails du modèle et sélectionnez **Suivant**.
8. Lisez et acceptez le contrat de licence, puis 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.




Les valeurs indiquées sur la page **Personnaliser le modèle** sont obligatoires pour un déploiement réussi.

Portez une attention particulière à ces champs :

- **Nom de l'hôte** : Saisissez le nom de l'hôte de la machine virtuelle ONTAP tools. Utilisez un format de nom d'hôte valide.
- **Adresse IP des outils ONTAP** : Il s'agit de l'interface de gestion principale utilisée pour accéder aux outils ONTAP.
- **Adresse IPv4** : Il s'agit de l'adresse IP du nœud utilisée pour le shell de diagnostic et l'accès SSH à des fins de dépannage et de maintenance.

Si vous utilisez des noms DNS pour l'hôte ou vCenter, assurez-vous que ces noms sont correctement résolus dans le DNS.

Le nom d'hôte vCenter correspond au nom de l'instance du serveur vCenter sur laquelle l'appliance ONTAP tools est déployée.

Si vous déployez 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 nécessaires au déploiement du modèle OVF. Pour plus de détails, consultez les rôles listés dans "Rôles inclus avec ONTAP tools for VMware vSphere 10".

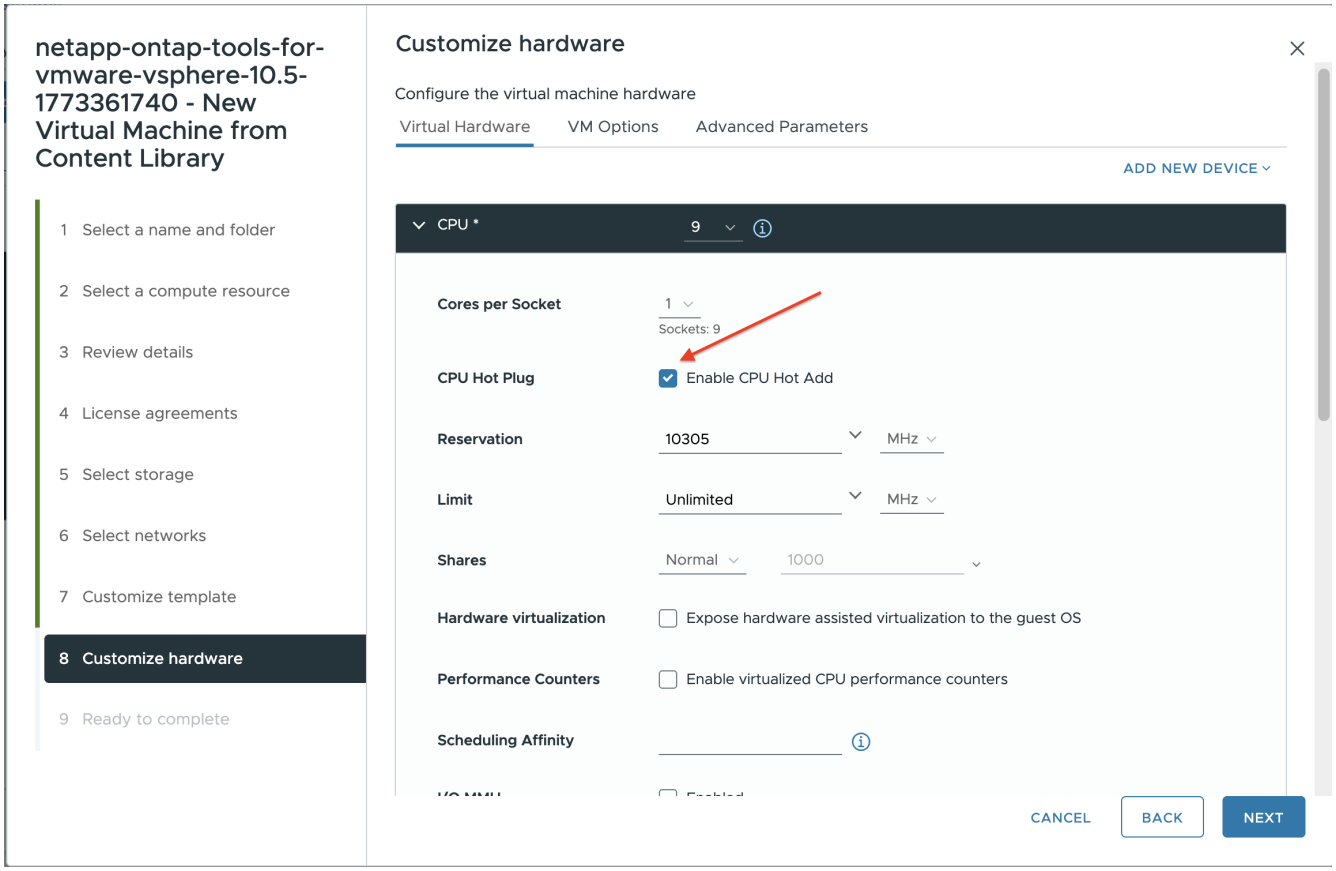
Pour l'instance vCenter qui sera gérée par ONTAP tools, assurez-vous que le compte utilisateur vCenter dispose des privilèges d'administrateur.

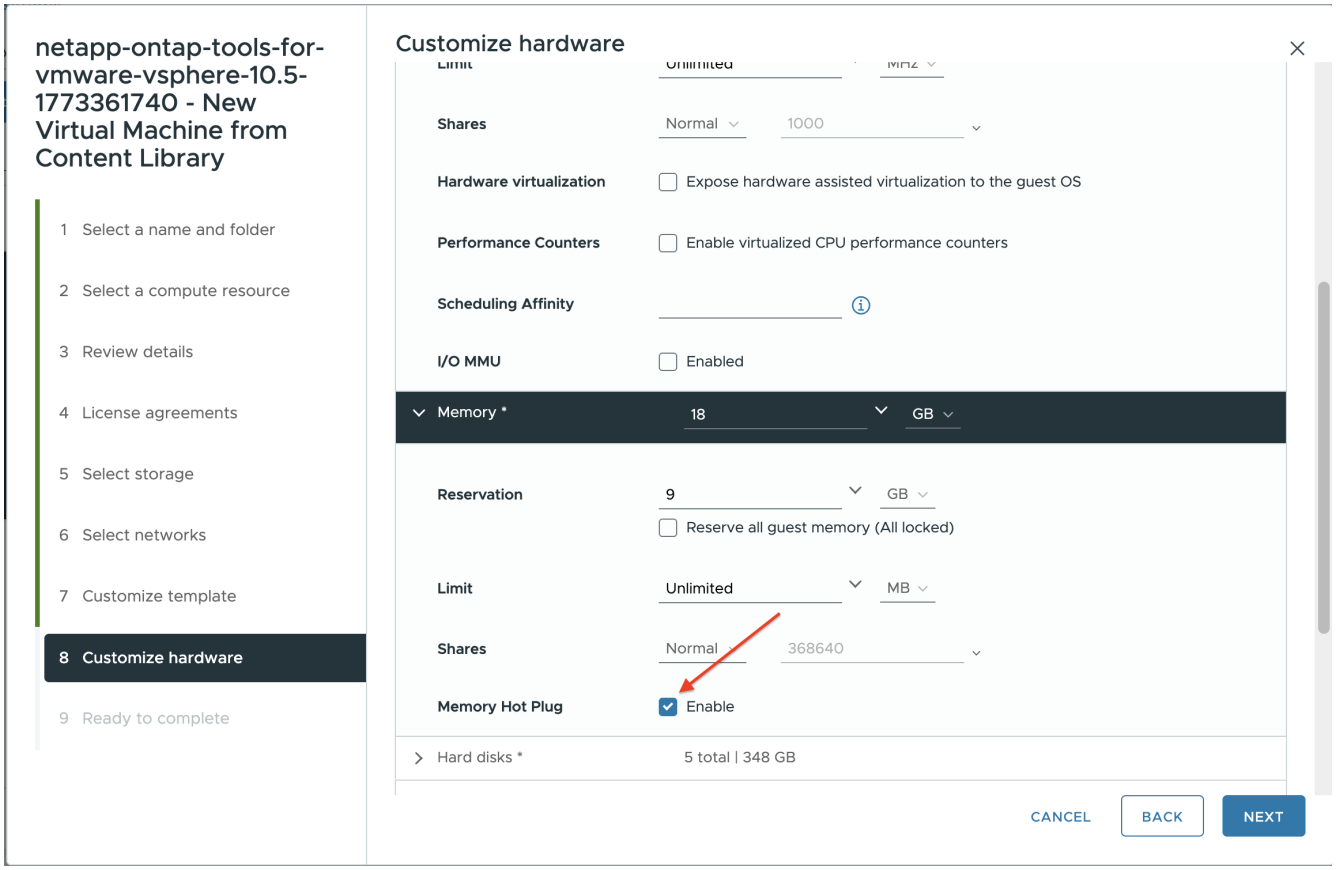
- Les noms d'hôtes doivent inclure des lettres (A-Z, a-z), des chiffres (0-9) et des tirets (-). Pour configurer une architecture double pile, spécifiez le nom de l'hôte associé à l'adresse IPv6.

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

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






13. Vérifiez les détails dans la fenêtre **Prêt à terminer**, puis sélectionnez **Terminer**.

    À mesure que la tâche de déploiement est créée, sa 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 dans la console web de la machine virtuelle.

En cas d'anomalies dans le formulaire OVF, une boîte de dialogue vous invitera à effectuer les corrections nécessaires. Utilisez la touche Tabulation pour naviguer, apportez les modifications nécessaires et sélectionnez **OK**. Vous disposez de trois tentatives pour résoudre tout problème. Si des problèmes persistent après trois tentatives, le processus d'installation s'arrêtera et il est conseillé de réessayer l'installation sur une nouvelle machine virtuelle.

**Quelle est la prochaine étape ?**

Si vous avez déployé ONTAP tools for VMware vSphere avec vCenter Server 7.0.3, suivez ces étapes après le déploiement.

1. Connectez-vous au client vCenter
2. Mettez hors tension le nœud des outils ONTAP.
3. Accédez à la machine virtuelle ONTAP tools for VMware vSphere sous **Inventaires** et sélectionnez l'option **Modifier les paramètres**.
4. Dans les options **CPU**, cochez la case **Enable CPU hot add**
5. Dans les options **Mémoire**, cochez la case **Activer** en face de **Memory hot plug**.

# Dépanner les erreurs de déploiement des outils ONTAP

En cas de problème de déploiement, consultez les journaux et les codes d'erreur pour diagnostiquer et résoudre les problèmes. À partir de ONTAP tools for VMware vSphere 10.5, les ensembles de journaux collectés à partir des pods incluent les journaux de MongoDB, RabbitMQ et Vault, ainsi que l'état et la description de tous les pods. Ces éléments s'ajoutent aux journaux de service existants des ONTAP tools, améliorant ainsi la capacité de support et de dépannage.

## Collectez les fichiers journaux

Vous pouvez collecter les fichiers journaux pour ONTAP tools for VMware vSphere à partir des options disponibles dans l'interface utilisateur du gestionnaire ONTAP tools. Le support technique peut vous demander de collecter les fichiers journaux pour aider à résoudre un problème.

> La génération de journaux à partir du gestionnaire d'outils ONTAP inclut tous les journaux pour toutes les instances de serveur vCenter. La génération de journaux à partir de l'interface utilisateur du client vCenter est limitée au serveur vCenter sélectionné.

**Étapes**

1. Lancez ONTAP tools Manager depuis un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis 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 bundle de journaux et sélectionnez **Générer**.

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

Suivez les étapes ci-dessous pour générer un bundle de journaux à l'aide de l'interface utilisateur du client vCenter :

**Étapes**

1. Connectez-vous au client vSphere.
2. Depuis la page d'accueil du vSphere Client, accédez à **Support** > **Log bundle** > **Generate**.
3. Indiquez l'étiquette du paquet journal et générez le paquet journal. Vous pouvez voir l'option de téléchargement lorsque les fichiers sont générés. Le téléchargement peut prendre un certain temps.

> Le fichier journal généré remplace le fichier journal généré au cours des 3 derniers jours ou des dernières 72 heures.

## Codes d'erreur de déploiement

Vous pourriez rencontrer des codes d'erreur lors du déploiement, du redémarrage et des opérations de

récupération des outils ONTAP pour VMware vSphere. Les codes d'erreur sont composés de cinq chiffres, où les deux premiers représentent le script ayant rencontré le problème et les trois derniers représentent le workflow spécifique dans ce script.

Tous les journaux d'erreurs sont enregistrés dans le fichier ansible-perl-errors.log sous le répertoire /var/log afin de 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 affichés sur cette page sont fournis à titre indicatif uniquement. Veuillez contacter l'équipe d'assistance si l'erreur persiste ou si aucune solution n'est mentionnée.

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

| Code d'erreur | Nom du script |
|---|---|
| 00 | firstboot-network-config.pl, mode déploiement |
| 01 | firstboot-network-config.pl, mode mise à niveau |
| 02 | firstboot-inputs-validation.pl |
| 03 | firstboot-deploy-otv-ng.pl, déploiement, HA |
| 04 | firstboot-deploy-otv-ng.pl, déploiement, non-HA |
| 05 | firstboot-deploy-otv-ng.pl, reboot |
| 06 | firstboot-deploy-otv-ng.pl, mise à niveau, HA |
| 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 spécifique survenue dans le script :

| Code d'erreur de déploiement | Flux de travail | Résolution |
|---|---|---|
| 049 | Pour le réseau et la validation, le script Perl les assignera également prochainement. | - |
| 050 | La génération de la clé SSH a échoué | Redémarrez la machine virtuelle principale (VM). |
| 053 | Échec de l'installation de RKE2 | Exécutez la commande suivante et redémarrez la VM principale ou redéployez : sudo rke2-killall.sh (toutes les VM) sudo rke2-uninstall.sh (toutes les VM). |
| 054 | Échec de la configuration de kubeconfig | Redéployer |
| 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. |

| | | |
|---|---|---|
| 059 | KubeVip le déploiement a échoué | Assurez-vous 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, redéployez. |
| 060 | Le déploiement de l'opérateur a échoué | Redémarrer |
| 061 | Le déploiement des services a échoué | Effectuez un débogage Kubernetes de base comme get pods, get rs, get svc, etc. dans l'espace de noms ntv-system pour plus de détails et les journaux d'erreurs dans /var/log/ansible-perl-errors.log et /var/log/ansible-run.log, puis redéployez. |
| 062 | Le déploiement des services ONTAP tools a échoué | Consultez les journaux d'erreurs à /var/log/ansible-perl-errors.log pour plus de détails et redéployez. |
| 065 | L'URL de la page Swagger est inaccessible | Redéployer |
| 066 | Les étapes de post-déploiement du certificat de passerelle ont échoué | Pour récupérer/terminer la mise à niveau, procédez comme suit :<br>• Activer le shell de diagnostic.<br>• Exécutez la commande 'sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy'.<br>• Consultez les journaux à /var/log/post-deploy-upgrade.log. |
| 088 | La configuration de la rotation des journaux pour journald a échoué | Vérifiez que les paramètres réseau de la machine virtuelle sont compatibles avec l'hôte qui l'héberge. Vous pouvez essayer de migrer la machine virtuelle vers un autre hôte et de la redémarrer. |
| 089 | La modification du propriétaire du fichier de configuration de rotation du journal récapitulatif a échoué | Redémarrez la machine virtuelle principale. |
| 096 | Installer le provisionneur de stockage dynamique | - |
| 108 | Le script de seeding a échoué | - |

| | | |
|---|---|---|
| 114 | La mise à jour du certificat interne dans la collection MongoDB a échoué | Si le déploiement échoue avec le code d'erreur 114, procédez comme suit :<br>• Activez le shell de diagnostic.<br>• Exécutez la commande suivante : `sudo perl /home/maint/scripts/post-deploy-upgrade.pl --internal_cert_update_collection`<br>• Consultez les journaux à `/var/log/otvng/post-deploy-upgrade.log` |

| Code d'erreur de redémarrage | Flux de travail | Résolution |
|---|---|---|
| 067 | Délai d'attente du serveur rke2 expiré. | - |
| 101 | Échec de la réinitialisation du mot de passe de l'utilisateur Maint/Console. | - |
| 102 | Échec de la suppression du fichier de mot de passe lors de la réinitialisation du mot de passe de l'utilisateur Maint/Console. | - |
| 103 | Échec de la mise à jour du mot de passe du nouvel utilisateur Maint/Console dans le coffre-fort. | - |
| 088 | La configuration de la rotation des journaux pour journald a échoué. | Vérifiez que les paramètres réseau de la machine virtuelle sont compatibles avec l'hôte qui l'héberge. Vous pouvez essayer de migrer la machine virtuelle vers un autre hôte et de la redémarrer. |
| 089 | La modification du propriétaire du fichier de configuration de rotation du journal récapitulatif a échoué. | Redémarrez la machine virtuelle. |

# Configurer les outils ONTAP pour VMware vSphere

## Ajoutez des instances de serveur vCenter aux outils ONTAP

Ajoutez des instances de serveur vCenter à ONTAP tools for VMware vSphere pour configurer, gérer et protéger vos banques de données virtuelles dans votre environnement vCenter Server. Lorsque vous ajoutez plusieurs instances de serveur vCenter, des certificats CA personnalisés sont requis pour une communication sécurisée entre ONTAP tools et chaque serveur vCenter.

**À propos de cette tâche**

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

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

- Les outils ONTAP enregistrent le plug-in client vCenter en tant que plug-in distant.
- Des privilèges personnalisés pour les plug-ins et les API sont appliqués à l'instance du serveur vCenter.
- Des rôles personnalisés sont créés pour gérer les utilisateurs.
- Le module complémentaire apparaît sous forme de raccourci dans l'interface utilisateur 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 domaine complet (FQDN), en veillant à ce que le SAN dans le certificat inclue 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 avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.
3. Sélectionnez **vCenters** > **Ajouter** pour intégrer les instances de serveur vCenter. Indiquez l'adresse IP ou le nom d'hôte vCenter, le nom d'utilisateur, le mot de passe et les détails du port.
4. Dans les options avancées, récupérez automatiquement le certificat du serveur vCenter (autorisez-le) ou téléversez-le manuellement.

> Vous n'avez pas besoin d'un compte administrateur pour ajouter des instances vCenter aux ONTAP tools. Vous pouvez créer un rôle personnalisé sans compte administrateur, avec des autorisations limitées. Consultez "Utilisez le contrôle d'accès basé sur les rôles (RBAC) du serveur vCenter avec les outils ONTAP pour VMware vSphere 10" pour plus de détails.

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

Utilisez les ONTAP tools for VMware vSphere pour enregistrer le VASA Provider auprès d'une instance de serveur vCenter. Cela permet la gestion basée sur des règles de stockage, la prise en charge des 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 pour le vCenter Server sélectionné.

**Étapes**

1. Connectez-vous au client vSphere.
2. Sélectionnez **Raccourcis** > **NetApp ONTAP tools** dans la section des modules d'extension.
3. Sélectionnez **Paramètres** > **Paramètres du fournisseur VASA**. Les ONTAP tools affichent l'état d'enregistrement du fournisseur VASA comme non enregistré.
4. Sélectionnez le bouton **S'inscrire** pour enregistrer le fournisseur VASA.
5. Veuillez saisir un nom et des identifiants pour le VASA Provider. Le nom d'utilisateur ne peut contenir que des lettres, des chiffres et des traits de soulignement. Le mot de passe doit comporter entre 8 et 256 caractères.
6. Sélectionnez **Register**.
7. Après une inscription réussie et un rafraîchissement de la page, ONTAP tools affiche le statut, le nom et la version du VASA Provider enregistré.

**Et ensuite**

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

**Étapes**

1. Accédez à l'instance du serveur vCenter.
2. Connectez-vous avec les identifiants d'administrateur.
3. Sélectionnez **Fournisseurs de stockage** > **Configurer**. Vérifiez que le fournisseur VASA intégré est correctement répertorié.

# Installez le plug-in NFS VAAI à l'aide des ONTAP tools.

Le plug-in NFS vStorage API for Array Integration (NFS VAAI) connecte VMware vSphere aux baies de stockage NFS. Utilisez 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 "NetApp NFS Plug-in pour VMware VAAI" package d'installation.
- Assurez-vous de disposer d'hôtes ESXi avec vSphere 7.0 U3 (dernier correctif ou version ultérieure) et ONTAP 9.14.1 ou version ultérieure.
- Montez un datastore NFS.

**Étapes**

1. Connectez-vous au client vSphere.
2. Sélectionnez **Raccourcis** > **NetApp ONTAP tools** dans la section des modules d'extension.
3. Sélectionnez **Paramètres** > **Outils NFS VAAI**.
4. Si vous avez déjà chargé le plug-in VAAI sur le serveur vCenter, sélectionnez **Modifier** dans **Version existante**. Si ce n'est pas le cas, sélectionnez **Charger**.
5. Parcourez et sélectionnez le fichier `.vib` puis sélectionnez **Téléverser** pour transférer le fichier vers ONTAP tools.
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 vSphere Web Client 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 manuellement l'hôte ESXi après l'installation.

   Après le redémarrage de l'hôte ESXi, ONTAP tools for VMware vSphere détecte et active automatiquement le plug-in NFS VAAI.

**Et ensuite ?**

Après avoir installé le plug-in NFS VAAI et redémarré votre hôte ESXi, configurez les règles d'export NFS pour le déchargement de copie VAAI. Assurez-vous que les règles d'export respectent les exigences suivantes :

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

Pour plus d'informations, consultez "Configurez les règles d'export NFS appropriées pour le déchargement de

copie VAAI" l'article de la base de connaissances.

**Informations connexes**

"Prise en charge de VMware vStorage over NFS"

"Activer ou désactiver NFSv4.0"

"Prise en charge ONTAP pour NFSv4.2"

# Configurer les paramètres de l'hôte ESXi dans ONTAP tools

La configuration des paramètres de chemin multiple et de délai d'expiration du serveur ESXi contribue à garantir la disponibilité des données et l'intégrité des données. Elle permet un basculement automatique vers un chemin de stockage de sauvegarde si le chemin principal devient indisponible.

## Configurer les paramètres de multipath et de délai d'expiration du serveur ESXi

Les ONTAP tools for VMware vSphere vérifient et configurent les paramètres multipath de l'hôte ESXi et les paramètres de délai d'expiration HBA qui fonctionnent le mieux avec les systèmes de stockage NetApp.

**À propos de cette tâche**

Ce processus peut prendre un certain temps, selon votre configuration et la charge de votre système. Vous pouvez suivre la progression dans le panneau Tâches récentes.

**Étapes**

1. Depuis la page d'accueil du client Web vSphere VMware, sélectionnez **Hôtes et 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 **Conformité de l'hôte ESXi** dans la vue d'ensemble (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 hôtes recommandés**, sélectionnez les hôtes que vous souhaitez mettre à jour pour utiliser les paramètres recommandés NetApp et sélectionnez **Suivant**.

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

6. Sur la page des paramètres, sélectionnez les valeurs recommandées selon vos besoins.
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 outils ONTAP pour VMware vSphere afin de configurer les délais d'attente et d'autres valeurs sur les hôtes ESXi pour des performances et un basculement optimaux. Ces valeurs sont définies sur la base des tests NetApp.

Vous pouvez définir les valeurs suivantes sur un hôte ESXi :

**Paramètres de l'adaptateur HBA/CNA**

Définit les paramètres suivants sur leurs valeurs par défaut :

- Disk.QFullSampleSize
- Disque.QFullThreshold
- Délais d'attente Emulex FC HBA
- Délais d'attente du HBA QLogic FC

**Paramètres MPIO**

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

Dans les environnements à hautes performances ou lors de tests avec un seul datastore LUN, ajustez le paramètre d'équilibrage de charge de la stratégie de sélection de chemin round-robin (VMW_PSP_RR) (PSP) afin d'améliorer les performances. Définissez la valeur IOPS par défaut de 1000 à 1.

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

**Paramètres NFS**

| Paramètre | Définissez cette valeur sur… |
|---|---|
| Net.TcpipHeapSize | 32 |
| Net.TcpipHeapMax | 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 backends de stockage avec 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 depuis ONTAP tools for VMware vSphere en utilisant *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 des privilèges d’administrateur pour le stockage principal.

**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 ONTAP tools pour le cluster, sélectionnez **Cluster** > **Paramètres** > volet **Utilisateurs et rôles**.
   b. Pour configurer un utilisateur ONTAP tools SVM, sélectionnez **Storage SVM** > **Paramètres** > **Utilisateurs et rôles**.
   c. Sélectionnez **Ajouter** sous Utilisateurs.
   d. Dans la boîte de dialogue **Ajouter un utilisateur**, sélectionnez **Produits de virtualisation**.
   e. **Parcourez** pour sélectionner et télécharger le fichier JSON ONTAP Privileges. 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 Product.

   f. Sélectionnez la capacité du produit **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 (Discovery, Create Storage, Modify Storage, Destroy Storage, NAS/SAN Role) dont l’utilisateur a besoin, puis sélectionnez **Add**.

ONTAP tools ajoute le nouveau rôle et l’utilisateur. Vous pouvez consulter les Privileges associés au rôle que vous avez configuré.

## Exigences de mappage d’agrégat SVM

Lors du provisionnement de datastores à l’aide d’identifiants utilisateur SVM, ONTAP tools for VMware vSphere crée des volumes sur l’agrégat spécifié dans l’API POST des datastores. ONTAP empêche les utilisateurs SVM de créer des volumes sur des agrégats non associés à la SVM. Associez la SVM aux agrégats requis à l’aide de l’API REST ou de l’interface de ligne de commande ONTAP avant de créer des volumes.

API REST :

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

ONTAP CLI :

```
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
```

## Créer manuellement l'utilisateur et le rôle ONTAP

Créez manuellement les utilisateurs et les rôles 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 des privilèges d'administration.
   a. Pour configurer les rôles des ONTAP tools du cluster, sélectionnez **Cluster** > **Paramètres** > **Utilisateurs et rôles**.
   b. Pour configurer les rôles des outils ONTAP du cluster SVM, sélectionnez **SVM de stockage** > **Paramètres** > **Utilisateurs et rôles**.
3. Créer des rôles :
   a. Sélectionnez **Ajouter** sous le tableau **Rôles**.
   b. Saisissez les détails du **nom du rôle** et des **attributs du 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** sous le tableau **Utilisateurs**.
   b. Dans la boîte de dialogue **Ajouter un utilisateur**, sélectionnez **System Manager**.
   c. Saisissez le **nom d'utilisateur**.
   d. Sélectionnez **Role** parmi les options créées à l'étape **Create Roles** ci-dessus.
   e. Saisissez les applications auxquelles vous souhaitez donner 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 de l'utilisateur** et **enregistrez** l'utilisateur.

#### Liste des privilèges minimaux requis pour un utilisateur de cluster à portée globale non administrateur

Cette page répertorie les privilèges minimaux requis pour un utilisateur de cluster à portée globale non administrateur sans fichier JSON. Si un cluster est à portée locale, utilisez le fichier JSON pour créer les utilisateurs, car ONTAP tools for VMware vSphere nécessite plus que les seuls privilèges de lecture pour le provisionnement sur ONTAP.

Vous pouvez accéder à la fonctionnalité en utilisant des API :

| API | Niveau d'accès | Utilisé pour |
|---|---|---|
| /api/cluster | Lecture seule | Découverte de la configuration du cluster |
| /api/cluster/licensing/licenses | Lecture seule | Vérification des licences spécifiques au protocole |
| /api/cluster/nodes | Lecture seule | découverte du type de plateforme |
| /api/security/accounts | Lecture seule | Découverte des privilèges |
| /api/security/roles | Lecture seule | Découverte des privilèges |
| /api/storage/aggregates | Lecture seule | Vérification de l'espace agrégé lors du provisionnement de la banque de données/du volume |
| /api/storage/cluster | Lecture seule | Pour obtenir les données d'espace et d'efficacité au niveau du cluster |
| /api/storage/disks | Lecture seule | Pour obtenir les disques associés dans un agrégat |
| /api/storage/qos/policies | Lire/Créer/Modifier | Gestion des politiques QoS et VM |
| /api/svm/svms | Lecture seule | Pour obtenir la configuration SVM lorsque le cluster est ajouté localement. |
| /api/network/ip/interfaces | Lecture seule | Ajouter un stockage backend - Pour identifier la portée de la LIF de gestion, il s'agit d'un cluster/SVM |
| /api/storage/availability-zones | Lecture seule | Découverte SAZ. Applicable à la version ONTAP 9.16.1 et aux systèmes ASA r2. |
| /api/cluster/metrocluster | Lecture seule | Obtient l'état et les détails de configuration de MetroCluster. |

**Créer un utilisateur à l'échelle du cluster basé sur l'API ONTAP pour ONTAP tools for VMware vSphere**

Les privilèges de découverte, de création, de modification et de suppression sont requis pour les opérations PATCH et la restauration automatique sur les datastores. L'absence de ces privilèges peut entraîner des problèmes de flux de travail et de nettoyage.

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

Pour créer un utilisateur à portée de cluster disposant de tous les privilèges mentionnés ci-dessus, exécutez 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
```

De plus, pour les versions ONTAP 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 sur 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
```

**Créer un utilisateur SVM à portée ONTAP basé sur l'API pour les ONTAP tools for VMware vSphere**

Exécutez les commandes suivantes pour créer un utilisateur SVM disposant de 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>
```

De plus, pour les versions ONTAP 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 nouvel utilisateur basé sur l'API en utilisant les rôles basés sur l'API créés précédemment, 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
```

## Mettez à niveau l'utilisateur ONTAP tools for VMware vSphere 10.1 vers l'utilisateur 10.3

Pour les utilisateurs de ONTAP tools for VMware vSphere 10.1 disposant d'un utilisateur à portée de cluster créé à l'aide du fichier JSON, utilisez les commandes ONTAP CLI avec les privilèges d'administrateur pour effectuer la mise à niveau vers la version 10.3.

Pour les fonctionnalités du produit :

- VSC
- VSC et VASA Provider
- VSC et SRA
- VSC, VASA Provider et SRA.

Privilèges du cluster :

*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 utilisateurs d'ONTAP tools for VMware vSphere 10.1 disposant d'un utilisateur SVM créé à l'aide du fichier json, utilisez les commandes ONTAP CLI avec des privilèges administrateur pour effectuer la mise à niveau vers la version 10.3.

Privilèges SVM :

*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
```

### Mettez à niveau l'utilisateur des ONTAP tools for VMware vSphere 10.3 vers l'utilisateur 10.4

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

Pour les utilisateurs d'ONTAP tools for VMware vSphere 10.3 disposant d'un utilisateur à portée de cluster créé à l'aide du fichier JSON et d'ONTAP version 9.16.1 ou supérieure, utilisez la commande CLI ONTAP avec des privilèges administrateur pour effectuer la mise à niveau vers la version 10.4.

Pour les fonctionnalités du produit :

- VSC
- VSC et VASA Provider
- VSC et SRA
- VSC, VASA Provider et SRA.

Privilèges du cluster :

```
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 outils ONTAP pour VMware vSphere pour ajouter et gérer les backends 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 backends de stockage à l'aide du gestionnaire des outils ONTAP 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 identifiants de cluster ou de SVM dans l'interface des ONTAP tools. Les systèmes de stockage locaux sont uniquement disponibles pour le vCenter Server sélectionné. ONTAP tools associe les SVM au vCenter Server pour la gestion des vVols ou des datastores VMFS. Pour les datastores VMFS et les workflows SRA, vous pouvez utiliser les identifiants SVM sans associer de cluster globalement.

Pour ajouter un stockage de sauvegarde global, utilisez les identifiants du cluster ONTAP dans ONTAP tools

Manager. Les stockages de sauvegarde globaux permettent aux workflows de découverte d'identifier les ressources du cluster nécessaires à la gestion des vVol. Dans les environnements multitenants, vous pouvez ajouter un utilisateur SVM localement pour gérer les datastores vVols.

Consultez l'article de la base de connaissances : "OTV 10 : Quelle est la portée globale et locale du storage backend" pour plus d'informations sur les systèmes de stockage globaux et locaux.

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 comporte un champ Subject Alternative Name (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 multi-locataires, vous pouvez ajouter un cluster de stockage backend globalement et une SVM localement pour utiliser les identifiants utilisateur SVM.

**Étapes**

1. Lancez ONTAP tools Manager depuis un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.
3. Sélectionnez **Storage Backends** dans la barre latérale.
4. Ajoutez le système de stockage principal et indiquez l'adresse IP ou le FQDN du serveur, le nom d'utilisateur et le mot de passe.

   Les interfaces logiques 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) depuis la console de maintenance. Pour obtenir des instructions, consultez "Modifier l'indicateur de validation du certificat".

6. Si le système de stockage que vous ajoutez fait partie d'une configuration MetroCluster, ONTAP tools Manager affiche un message contextuel vous invitant à ajouter le cluster apparié. Sélectionnez **Ajouter** et indiquez les détails du système de stockage apparié MetroCluster.

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

**Utilisation de l'interface utilisateur client vSphere**

Les datastores 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 des raccourcis, sélectionnez **NetApp ONTAP tools** dans la section des modules d'extension.
3. Sélectionnez **Storage Backends** dans la barre latérale.
4. Ajoutez le système de stockage et indiquez l'adresse IP du serveur, le nom d'utilisateur, le mot de passe et les détails du port.

   Vous pouvez ajouter un système de stockage à l'aide d'identifiants de cluster avec des LIF de gestion IPv4 ou IPv6. Pour ajouter directement un utilisateur SVM, fournissez des identifiants SVM ainsi qu'une LIF de gestion SVM. Si un cluster est déjà intégré, vous ne pouvez pas intégrer à nouveau un utilisateur SVM 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 stockage principal ajouté fait partie de la configuration MetroCluster, ONTAP tools affiche l'écran **Ajouter un homologue MetroCluster**. Sélectionnez **Ajouter un homologue** pour ajouter le stockage principal homologue.

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

Les ONTAP tools affichent le nouveau stockage de sauvegarde ajouté sur la page **Storage backends**. Si un certificat expire dans 30 jours ou moins, ONTAP tools affiche un avertissement dans la colonne de la date d'expiration du certificat. Après expiration, ONTAP tools marque le stockage de sauvegarde comme inconnu, car il ne peut pas se connecter au système de stockage.

**Informations connexes**

"OTV 10 : Quelle est la portée globale et locale du storage backend"

"Configuration des clusters dans une configuration MetroCluster"

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

Associez un système de stockage principal à une instance de serveur vCenter pour permettre l'accès à toutes les instances de serveur vCenter. Pour la configuration MetroCluster, lorsque vous associez un cluster de stockage principal, veillez également à associer son cluster homologue au serveur vCenter.

**Étapes**

1. Lancez ONTAP tools Manager depuis un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.
3. Sélectionnez vCenter dans la barre latérale.
4. Sélectionnez les points de suspension verticaux à côté de l'instance vCenter Server à laquelle vous souhaitez vous connecter aux backends de stockage.
5. Dans le menu déroulant, choisissez le stockage de sauvegarde 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 règle d'export sauf si vous configurez l'accès réseau. Vous pouvez modifier la règle d'export 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 plug-ins.
3. Dans le volet gauche d'ONTAP tools, accédez à **Paramètres** > **Gérer l'accès au réseau** > **Modifier**.

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

4. Sélectionnez **Enregistrer**.

# Créer un datastore dans ONTAP tools

Lorsque vous créez un datastore au niveau du cluster hôte, les ONTAP tools le montent sur tous les hôtes de destination et n'activent l'action que si vous disposez des privilèges requis.

**Interopérabilité entre les magasins de données natifs avec vCenter Server et les magasins de données gérés par les outils ONTAP**

À partir de ONTAP tools for VMware vSphere 10.4, ONTAP tools crée des igroups imbriqués pour les datastores, avec des igroups parents spécifiques aux datastores et des igroups enfants associés aux hôtes. Vous pouvez créer des igroups plats depuis ONTAP System Manager et les utiliser pour créer des datastores VMFS sans utiliser ONTAP tools. Consultez "Gérer les initiateurs SAN et les igroups" pour plus d'informations.

Après avoir intégré le stockage et exécuté la découverte des datastores, ONTAP tools transforme les igroups plats des datastores VMFS en igroups imbriqués. Vous ne pouvez pas utiliser les anciens igroups plats pour créer de nouveaux datastores. Utilisez l'interface ONTAP tools ou l'API REST pour réutiliser des igroups imbriqués.

#### Créer un magasin de données vVols

À partir de ONTAP tools for VMware vSphere 10.3, vous pouvez créer un datastore vVols sur les systèmes ASA r2 avec une efficacité d'espace en mode thin.vVol. Le VASA Provider crée un conteneur et les points de terminaison de protocole souhaités lors de la création du datastore vVol. Le VASA Provider n'attribue aucun volume de support à ce conteneur.

**Avant de commencer**

- Assurez-vous que les agrégats racines ne sont pas mappés sur la SVM.
- Assurez-vous que le fournisseur VASA est enregistré auprès du vCenter sélectionné.
- Dans le système de stockage ASA r2, le SVM doit être associé 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 d'hôtes ou un centre de données et sélectionnez **NetApp ONTAP tools** > **Create Datastore**.
3. Sélectionnez vVols comme **type de magasin de données**.
4. Saisissez le **nom du datastore** et les informations du **protocole**.

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

5. Sélectionnez la machine virtuelle de stockage sur laquelle vous souhaitez créer le datastore.
6. Dans les options avancées :
   - Si vous sélectionnez la **règles d'export personnalisée**, assurez-vous d'exécuter la découverte dans vCenter pour tous les objets. Il est déconseillé d'utiliser cette option.
   - Vous pouvez sélectionner un nom de **groupe d'initiateurs personnalisé** pour les protocoles iSCSI et FC.

   Dans le système de stockage ASA r2 de type 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. Cependant, vous ne pouvez pas combiner ces deux types de volumes pour créer une datastore vVols.

   Lors de la création d'un 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

Un datastore NFS connecte les hôtes ESXi à un stockage partagé via le 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 d'hôtes ou un centre de données et sélectionnez **NetApp ONTAP tools** > **Create datastore**.
3. Sélectionnez NFS dans le champ **Type de banque de données**.
4. Saisissez le nom, la taille et les informations de protocole de la banque de données 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 **Plateforme** et **VM de stockage** dans le volet **Stockage**.
6. Si vous sélectionnez **Custom export policy** dans 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 de datastore NFS en utilisant la règle de volume par défaut ou racine du SVM.

   - Dans les options avancées, le bouton bascule **Asymétrique** n'est visible que si performance ou capacité est sélectionné dans le menu déroulant plateforme.
   - Lorsque vous sélectionnez l'option **Tout** dans le menu déroulant de la plateforme, vous pouvez voir toutes les SVM dans le vCenter. La plateforme et l'indicateur asymétrique n'affectent pas la visibilité.
7. Dans le volet **Attributs de stockage**, sélectionnez l'agrégat pour la création du volume. Dans les options avancées, choisissez **Réserve d'espace** et **Activer la QoS** selon vos besoins.
8. Vérifiez les sélections dans le volet **Résumé** et sélectionnez **Terminer**.

ONTAP tools crée le datastore NFS et le monte 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 de VM pour les fonctionnalités vMotion et Haute Disponibilité.

Sur un cluster protégé :

- Vous pouvez uniquement créer des datastores VMFS. L'ajout d'un datastore VMFS à un cluster protégé le protège automatiquement.
- Vous ne pouvez pas créer de datastore sur un centre de données comportant un ou plusieurs clusters hôtes protégés.
- Vous ne pouvez pas créer de datastore sur un hôte ESXi si le cluster hôte parent est protégé par une « Automated Failover Duplex policy » (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 d'hôtes protégé par la stratégie « Automated Failover Duplex ».

#### Avant de commencer

- Activez les services et les LIF pour chaque protocole du côté stockage ONTAP.
- Associez 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. Examiner "Guide de compatibilité VMware"

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

  b. Vérifiez si le fournisseur de la carte d'interface réseau (NIC) prend en charge la carte NIC 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. Lors de l'utilisation de VMware vSphere 7, suivez les instructions sur le site VMware "Configurer la liaison VMkernel pour l'adaptateur NVMe over TCP" pour configurer la liaison de port NVMe/TCP. Lors de l'utilisation de VMware vSphere 8, suivez "Configuration de NVMe over TCP sur ESXi" pour configurer la liaison de port NVMe/TCP.
  e. Pour la version 7 de VMware vSphere, suivez les instructions de la page "Activez les adaptateurs logiciels NVMe over RDMA ou NVMe over TCP" pour configurer les adaptateurs logiciels NVMe/TCP. Pour la version 8 de VMware vSphere, suivez "Ajouter des adaptateurs logiciels NVMe over RDMA ou NVMe over TCP" pour configurer les adaptateurs logiciels NVMe/TCP.
  f. Exécutez "Découvrez les systèmes de stockage et les hôtes" l'action sur l'hôte ESXi. Pour plus d'informations, consultez "Comment configurer NVMe/TCP avec vSphere 8.0 Update 1 et ONTAP 9.13.1 pour les datastores VMFS".
- 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 votre ou vos hôtes ESXi.
  b. Effectuez le zonage SCSI complet.
  c. Assurez-vous que les hôtes ESXi et le système ONTAP sont connectés au niveau physique et logique.

Pour configurer un SVM ONTAP pour le protocole FC, reportez-vous à "Configurer une SVM pour FC".

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

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

**Étapes**

1. Connectez-vous au client vSphere.
2. Cliquez avec le bouton droit sur un système hôte, un cluster d'hôtes ou un centre de données et sélectionnez **NetApp ONTAP tools** > **Create Datastore**.
3. Sélectionnez le type de banque de données VMFS.
4. Saisissez le nom, la taille et les informations de protocole de la banque de données dans le volet **Nom et protocole**. Pour ajouter la nouvelle banque de données à un cluster VMFS existant, sélectionnez le cluster de banques de données dans les options avancées.
5. Sélectionnez une machine virtuelle de stockage dans le volet **Stockage**. Indiquez le **Nom du groupe d'initiateurs personnalisé** dans la section **Options avancées** si nécessaire. Vous pouvez choisir un igroup existant pour la datastore ou en créer un nouveau 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 des espaces de noms. ONTAP tools crée le sous-système d'espace de noms en utilisant un 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 **custom namespace subsystem name** des options avancées du volet **Storage**.

6. Dans le volet **attributs de stockage** :

   a. Sélectionnez **Aggregate** dans les options déroulantes.

   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 permettant d'activer la QoS.

   b. Les outils ONTAP créent une unité de stockage (LUN/Namespace) avec une réserve d'espace mince basée sur le protocole sélectionné.

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

   c. Sélectionnez le niveau de service **Performance** pour les systèmes de stockage ASA r2 avec un SVM à 12 nœuds constituant 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 d'ONTAP. Cependant, vous pouvez sélectionner l'option Performance ou Extreme selon vos besoins.

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

   Dans le type de stockage ASA r2, la création ou la sélection de volumes ne s'applique pas à la création d'unités de stockage (LUN/Namespace). 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 **Résumé** et sélectionnez **Terminer**.

   Si vous créez le datastore sur un cluster protégé, vous pouvez voir un message en lecture seule : « Le datastore est en cours de montage sur un cluster protégé. »

**Résultat**

Les outils ONTAP créent le datastore VMFS et le montent sur tous les hôtes.

# Protégez les banques de données et les machines virtuelles

## Protéger un cluster hôte dans ONTAP tools

ONTAP tools for VMware vSphere gèrent la protection des clusters d'hôtes. Toutes les banques de données appartenant à la SVM sélectionnée et montées sur un ou plusieurs hôtes du cluster sont protégées sous un cluster d'hôtes.

**Avant de commencer**

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

- Le cluster hôte contient des banques de données provenant d'une seule SVM.
- Les banques de données du cluster hôte ne sont pas montées sur des hôtes situés en dehors du cluster.
- Les banques de données montées sur le cluster hôte sont des banques de données VMFS utilisant le protocole iSCSI ou FC. Vous ne pouvez pas utiliser vVols, NFS ou des banques de données 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 un datastore.

**Étapes**

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

   Le type de stratégie peut être asynchrone ou AutomatedFailOverDuplex.

   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 backend de stockage au même vCenter où ONTAP tools for VMware vSphere est déployé.

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

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

7. Sélectionnez **Add**.
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 trois points.
9. Sélectionnez le bouton **Protéger**.

   Le système crée une tâche vCenter avec les détails de l'ID du travail 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 requête et n'attend pas la fin de la tâche.

10. Pour afficher les clusters d'hôtes protégés, accédez à **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**. 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 qui suit sa création, effectuez d'abord une découverte du stockage.

**Informations connexes**

"Cluster de stockage Metro VMware vSphere (vMSC)"

# Protéger à l'aide de la protection SRA

## Configurez SRA dans ONTAP tools pour protéger les banques de données

Les outils ONTAP pour VMware vSphere offrent la possibilité d'activer la fonctionnalité SRA pour configurer la reprise après sinistre.

**Avant de commencer**

- Vous devez avoir configuré votre instance de serveur vCenter et vos hôtes ESXi.
- Vous devez avoir déployé les outils ONTAP pour VMware vSphere.
- Vous devez avoir téléchargé le fichier SRA Adapter `.tar.gz` depuis le "Site de support NetApp".
- Vous devez avoir les mêmes planifications personnalisées SnapMirror sur les clusters ONTAP source et de destination avant d'exécuter les workflows SRA.
- "Activer les ONTAP tools for VMware vSphere services" pour activer la fonctionnalité SRA.

**Étapes**

1. Connectez-vous à l'interface de gestion de l'appliance VMware Live Site Recovery à l'aide de l'URL : `https://<srm_ip>:5480`, puis accédez à Adaptateurs de réplication de stockage dans l'interface de gestion de l'appliance 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. Analysez à nouveau les adaptateurs pour vérifier que les informations sont mises à jour sur la page VMware Live Site Recovery Storage Replication Adapters.

> Après un basculement, des actions telles qu'étendre, monter et supprimer peuvent ne pas être disponibles pour les banques de données. Effectuez une découverte des banques de données pour actualiser et afficher les actions appropriées dans le menu contextuel.

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

Lors d'une nouvelle configuration avec protection SRA, effectuez systématiquement un test de basculement. Ignorer le test de basculement pourrait entraîner l'échec de l'opération de reprotection.

Dans une configuration de distribution, après un basculement SnapMirror Active Sync où la source SnapMirror passe au site B pour Automated Failover Duplex et SnapMirror asynchrone, exécutez un test de basculement entre les sites B et C. Ignorer cette étape peut entraîner un échec de l'opération de reprotection.

**Informations connexes**

"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.

### Configurer SRA pour les environnements SAN

Les groupes de cohérence dans les flux de travail SRA ne sont pris en charge qu'avec les protocoles SAN (iSCSI et Fibre Channel) sur les systèmes de stockage Unified et ASA r2.

**Avant de commencer**

Vous devez avoir les programmes suivants installés sur le site protégé et le site de récupération :

- VMware Live Site Recovery : Le site VMware fournit la documentation d'installation de VMware Live Site Recovery.

  "À propos de VMware Live Site Recovery"

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

Pour les configurations du protocole iSCSI, notez les points suivants avant d'exécuter les workflows SRA :

- **Site protégé** : les adaptateurs de stockage iSCSI et les détails des LIF de données sont configurés automatiquement lors du provisionnement des banques de données. Aucune configuration manuelle n'est requise.
- Site de reprise d'activité : les adaptateurs de stockage iSCSI doivent être configurés manuellement sur chaque hôte ESXi inclus dans le mappage des ressources pour la reprise d'activité. Pour éviter de configurer les adaptateurs individuellement sur chaque hôte, créez un datastore de type iSCSI sur le site de reprise d'activité à l'aide de la SVM sur laquelle les workflows SRA sont configurés. Cette opération ajoute automatiquement l'adaptateur iSCSI et les adresses IP LIF de données requises à tous les hôtes ESXi mappés. Consultez "Configurer les magasins de données de substitution dans ONTAP tools" pour plus de détails.

**Étapes**

1. Vérifiez que les hôtes ESXi principaux sont connectés aux LUN du système de stockage principal sur le site protégé.

2. Vérifiez que les LUN sont dans des igroups qui ont l' `ostype`option définie sur *VMware* sur le système de stockage principal.
3. Vérifiez que les hôtes ESXi du site de reprise 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 procéder soit en vérifiant que les hôtes ESXi disposent de LUN locales connectées sur la SVM, soit en exécutant la commande `iscsi show initiators` sur les SVM. Vérifiez l'accès aux LUN mappées sur l'hôte ESXi pour vérifier la connectivité iSCSI.

#### Configurer SRA pour les environnements NAS

> Les groupes de cohérence ne sont pas pris en charge pour NFS dans les workflows SRA. Si des volumes de datastore NFS sont placés sous un groupe de cohérence et protégés, l'opération Discover Devices échouera. N'utilisez pas de groupes de cohérence lors de la protection des datastores NFS avec SRA.

**Avant de commencer**

Vous devez avoir les programmes suivants installés sur le site protégé et le site de récupération :

- VMware Live Site Recovery : Vous trouverez la documentation d'installation de VMware Live Site Recovery sur le site de 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 banques de données du site protégé contiennent des machines virtuelles qui sont enregistrées auprès du serveur vCenter.
2. Vérifiez que les hôtes ESXi du site protégé ont monté les volumes d'export NFS à partir de la machine virtuelle de stockage (SVM).
3. Vérifiez que les adresses IP valides sur lesquelles les exports NFS sont présents sont spécifiées dans le champ **NFS Addresses** lors de l'utilisation de l'assistant Array Manager pour ajouter des baies à VMware Live Site Recovery. N'utilisez pas le nom d'hôte NFS ni le FQDN dans le champ **NFS Addresses**.
4. Utilisez la commande `ping` sur chaque hôte ESXi du site de récupération pour vérifier que l'hôte possède un port VMkernel pouvant accéder aux adresses IP utilisées pour fournir les exports NFS depuis la 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 d'obtenir des performances optimales dans les environnements à grande échelle.

#### Paramètres du fournisseur de stockage

Vous devez définir les valeurs de délai d'expiration suivantes sur VMware Live Site Recovery pour un environnement mis à l'échelle :

| Paramètres avancés | Valeurs de délai d'attente |
|---|---|

| | |
|---|---|
| `StorageProvider.resignatureTimeout` | Augmentez la valeur du paramètre de 900 secondes à 12000 secondes. |
| `storageProvider.hostRescanDelaySec` | 60 |
| `storageProvider.hostRescanRepeatCnt` | 20 |
| `storageProvider.hostRescanTimeoutSec` | Définissez une valeur élevée (par exemple : 99999) |

Vous devez également activer l' `StorageProvider.autoResignatureMode`option.

Consultez "Modifier les paramètres du fournisseur de stockage" pour plus d'informations sur la modification des paramètres du fournisseur de stockage.

**Paramètres de stockage**

Lorsque vous atteignez un délai d'attente, augmentez les valeurs de `storage.commandTimeout` et `storage.maxConcurrentCommandCnt` à une valeur plus élevée.

> Le délai d'attente spécifié correspond à la valeur maximale. Il n'est pas nécessaire d'attendre que le délai d'attente maximal soit atteint. La plupart des commandes s'exécutent dans l'intervalle de délai d'attente maximal défini.

Consultez "Modifier les paramètres de stockage" pour modifier les paramètres du fournisseur SAN.

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

Après avoir déployé l'appliance VMware Live Site Recovery, configurez le Storage Replication Adapter (SRA) pour activer la gestion de la reprise après sinistre.

La configuration de SRA sur l'appliance VMware Live Site Recovery enregistre les informations d'identification des ONTAP tools for VMware vSphere au sein de l'appliance, ce qui permet 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 ONTAP tools Manager. Pour plus d'informations, consultez la "Activer les services" section.
- Ajoutez des serveurs vCenter à l'appliance ONTAP tools for VMware vSphere. Pour plus d'informations, consultez la "Ajouter des serveurs vCenter" section.
- Ajoutez des systèmes de stockage à ONTAP tools for VMware vSphere. Pour plus d'informations, consultez la "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 l'appliance VMware Live Site Recovery en utilisant le port (:5480). Pour obtenir des instructions, consultez "Reconfigurez l'appliance Site Recovery Manager".

**Étapes**

1. Sur l'écran de l'appliance VMware Live Site Recovery, sélectionnez **Storage Replication Adapter** > **New Adapter**.
2. Téléversez le fichier *.tar.gz* sur VMware Live Site Recovery.
3. Connectez-vous à l'appliance VMware Live Site Recovery à l'aide d'un compte administrateur via un client SSH tel que PuTTY.
4. Passez à 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, saisissez la commande permettant d'obtenir l'ID Docker utilisé par SRA : `docker ps -l`
7. Pour vous connecter à l'identifiant du conteneur, saisissez la commande : `docker exec -it -u srm <container id> sh`
8. Configurez VMware Live Site Recovery avec les outils ONTAP pour VMware vSphere, l'adresse IP et le mot de passe 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>`
   - Indiquez le mot de passe entre guillemets simples afin que le script Perl considère 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 (VASA Provider/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, allez à la page vCenter Server dans ONTAP tools Manager après avoir ajouté votre instance vCenter. Reportez-vous à la section "Ajouter des serveurs vCenter".
9. Analysez à nouveau les adaptateurs pour confirmer que les informations mises à jour apparaissent sur la page Storage Replication Adapters de VMware Live Site Recovery.

**Résultats** Un message de confirmation s'affiche, 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 auriez dû exécuter les étapes mentionnées dans le sujet "Configuration de SRA sur l'appliance VMware Live Site Recovery".

**Étapes**

1. Exécutez les commandes suivantes pour supprimer les informations d'identification des outils ONTAP mises en cache sur la machine VMware Live Site Recovery :
   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 -l --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv -password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>`Vous devez entourer la valeur du mot de passe d'une simple apostrophe.

Un message de confirmation s'affiche indiquant que les informations d'identification de stockage ont bien été enregistrées. SRA peut communiquer avec le serveur SRA en utilisant l'adresse IP, le port et les informations d'identification fournis.

#### Reconfigurez vCenter dans l'appliance VMware Live Site Recovery après un changement de certificat

Si le certificat vCenter change, par exemple après une mise à niveau vCenter, vous pouvez rencontrer une erreur d'empreinte numérique non concordante dans l'extension Site Recovery. Suivez les étapes ci-dessous pour résoudre ce problème.

**Étapes**

1. Reconfigurer vCenter dans l'appliance VMware Live Site Recovery

a. Ouvrez l'interface de gestion de l'appliance VMware Live Site Recovery dans un navigateur : `https://<SRM_IP>:5480`

b. Sélectionnez l'onglet **Résumé**.

c. Sélectionnez **Reconfigurer** pour la connexion au serveur vCenter.

Cette fonction récupère et accepte l'empreinte numérique du certificat la plus récente provenant de vCenter.

2. Reconnecter le site d'appairage (si l'erreur persiste)

Si l'erreur de non-concordance d'empreinte digitale persiste après reconfiguration :

a. Connectez-vous à l'interface utilisateur vCenter.

b. Accédez à l'extension **Site Recovery**.

c. Repérez la section **Appariement de sites**.

d. Sélectionnez **Reconnect** pour rétablir l'association du site avec le certificat mis à jour.

## 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'intégrer au groupe de banques de données existant ou ajouter une nouvelle banque de données et créer un nouveau volume ou groupe de cohérence pour la protection. Après avoir ajouté une nouvelle banque de données à un groupe de cohérence ou un volume protégé, mettez à jour SnapMirror et effectuez une découverte du stockage sur les sites protégé et de restauration. Vous pouvez exécuter la découverte manuellement ou selon un calendrier afin de garantir

que la nouvelle banque de données soit détectée et protégée.

### Associez les sites protégés et de récupération

Vous devez associer les sites protégés et de récupération créés à l'aide de votre vSphere Client pour permettre à l'adaptateur de réplication de stockage (SRA) de découvrir les systèmes de stockage.

> L'adaptateur de réplication de stockage (SRA) prend en charge la distribution avec une relation synchrone de type Automated Failover Duplex et une relation asynchrone SnapMirror sur groupe de cohérence. Cependant, la distribution avec deux relations asynchrones SnapMirror sur des groupes de cohérence ou des relations de distribution SnapMirror sur des volumes n'est pas prise en charge. Les relations de type Vault SnapMirror ne sont pas concernées par ces restrictions de distribution. La prise en charge des groupes de cohérence dans SRA est limitée aux protocoles SAN (iSCSI et fibre channel) sur les systèmes de stockage Unified et ASA r2. Les groupes de cohérence ne sont pas pris en charge pour NFS. Si des volumes de datastore NFS sont placés sous un groupe de cohérence, l'opération de découverte des périphériques échouera.

**Avant de commencer**

- Vous devez avoir installé VMware Live Site Recovery sur les sites protégés et de récupération.
- Vous devez avoir installé SRA sur les sites protégés et de restauration.

**Étapes**

1. Sur la page d'accueil du client vSphere, double-cliquez sur l'icône **Site Recovery** puis sélectionnez **Sites**.
2. Sélectionnez **Objets** > **Actions** > **Associer les sites**.
3. Dans la boîte de dialogue **Associer les serveurs Site Recovery Manager**, saisissez l'adresse du Platform Services Controller du site protégé, puis sélectionnez **Suivant**.
4. Dans la section Sélectionner le serveur vCenter, procédez comme suit :
   a. Vérifiez que le serveur vCenter du site protégé apparaît comme un candidat correspondant pour l'appariement.
   b. Saisissez les identifiants d'administrateur SSO, puis sélectionnez **Terminer**.
5. Si le système vous le demande, sélectionnez **Oui** pour accepter les certificats de sécurité.

**Résultat**

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

### Configurer les groupes de protection

**Avant de commencer**

Vous devez vous assurer que les sites source et cible sont configurés comme suit :

- Même version de VMware Live Site Recovery installée
- machines virtuelles
- Sites de protection et de récupération jumelés
- Les banques de données source et de destination doivent être montées sur leurs sites respectifs

**Étapes**

1. Connectez-vous à vCenter Server et sélectionnez **Récupération du site** > **Groupes de protection**.

2. Dans le volet **Groupes de protection**, sélectionnez **Nouveau**.
3. Spécifiez un nom et une description pour le groupe de protection, la direction, puis sélectionnez **Suivant**.
4. Dans le champ **Type**, sélectionnez l'option **Type field option…** comme groupes de banques de données (réplication basée sur des baies) pour les banques de données NFS et VMFS. Le domaine de panne est constitué des SVM dont la réplication est activée. Les SVM qui ont uniquement le peering implémenté et qui ne présentent aucun problème sont affichés.
5. Dans l'onglet Groupes de réplication, sélectionnez soit la paire de baies activée, soit les groupes de réplication contenant la machine virtuelle que vous avez configurée, puis sélectionnez **Suivant**.

   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 à un 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**.

## Configurer les ressources du site protégé et du site de récupération

### 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 permettre le mappage de chaque ressource du site protégé vers la ressource appropriée sur le site de récupération.

Vous devez effectuer les configurations de ressources suivantes :

- Cartographie des réseaux
- Mappages de dossiers
- Cartographie des ressources
- Magasins de données de substitution

#### Avant de commencer

Vous devez avoir connecté les sites protégés et de récupération.

#### Étapes

1. Connectez-vous à vCenter Server et sélectionnez **Récupération de site** > **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 ayant des noms correspondants** et sélectionnez **Suivant**.
   b. Sélectionnez les objets de centre de données requis pour les sites protégés et de récupération, puis sélectionnez **Add Mappings**.
   c. Sélectionnez **Suivant** après la création réussie des mappages.
   d. Sélectionnez l'objet utilisé précédemment pour créer le mappage inverse, puis sélectionnez **Terminer**.

**Résultat**

La page « Mappages réseau » affiche les ressources du site protégé et celles du site de récupération. Vous pouvez suivre la même procédure 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 récupération afin de permettre la communication entre eux.

**Avant de commencer**

Vous devez avoir connecté les sites protégés et de récupération.

**Étapes**

1. Connectez-vous à vCenter Server et sélectionnez **Récupération de site** > **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 dossier.
4. Dans l'assistant Créer un mappage de dossiers, procédez comme suit :
   a. Sélectionnez **Préparer automatiquement les mappages pour les dossiers aux noms correspondants** et sélectionnez **Suivant**.
   b. Sélectionnez les objets de centre de données requis pour les sites protégés et de récupération, puis sélectionnez **Add Mappings**.
   c. Sélectionnez **Suivant** après la création réussie des mappages.
   d. Sélectionnez l'objet utilisé précédemment pour créer le mappage inverse, puis sélectionnez **Terminer**.

**Résultat**

La page « Mappage des dossiers » affiche les ressources du site protégé et celles du site de récupération. Vous pouvez suivre la même procédure pour les autres dossiers de votre environnement.

### Configurer les mappages de ressources dans ONTAP tools

Vous devez cartographier vos ressources sur le site protégé et le site de récupération afin que les machines virtuelles soient configurées pour basculer vers l'un ou l'autre groupe d'hôtes.

**Avant de commencer**

Vous devez avoir connecté les sites protégés et de récupération.

> 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 **Récupération de site** > **Sites**.
2. Sélectionnez votre site protégé et sélectionnez **Gérer**.
3. Sélectionnez **Mappages de ressources** > **Nouveau** dans l'onglet Gérer pour créer un nouveau mappage de ressources.
4. Dans l'assistant Créer un mappage de ressources, procédez comme suit :

a. Sélectionnez **Préparer automatiquement les mappages pour les ressources ayant des noms correspondants** et sélectionnez **Suivant**.

b. Sélectionnez les objets de centre de données requis pour les sites protégés et de récupération, puis sélectionnez **Add Mappings**.

c. Sélectionnez **Suivant** après la création réussie des mappages.

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

**Résultat**

La page « Mappages de ressources » affiche les ressources du site protégé et celles du site de récupération. Vous pouvez suivre la même procédure pour les autres ressources de votre environnement.

### Configurer les magasins de données de substitution dans ONTAP tools

Configurez un datastore de substitution pour réserver de l'espace dans l'inventaire vCenter du site de récupération pour les machines virtuelles (VM) protégées. Les datastores de substitution nécessitent une capacité minimale, car les machines virtuelles de substitution sont petites et n'utilisent généralement que quelques centaines de kilo-octets.

**Avant de commencer**

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

**Étapes**

1. Connectez-vous à vCenter Server et sélectionnez **Récupération de site** > **Sites**.
2. Sélectionnez votre site protégé et sélectionnez **Gérer**.
3. Sélectionnez **Magasins de données de substitution** > **Nouveau** dans l'onglet gérer pour créer un nouveau magasin de données de substitution.
4. Sélectionnez le datastore approprié et cliquez sur **OK**.

   Les banques de données temporaires peuvent résider sur un stockage local ou distant, mais elles ne nécessitent pas de réplication.

5. Répétez les étapes 3 à 5 pour configurer un datastore de substitution pour le site de restauration.

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

Vous pouvez configurer l'adaptateur de réplication de stockage (SRA) en utilisant l'assistant Array Manager de VMware Live Site Recovery pour permettre les interactions entre VMware Live Site Recovery et les machines virtuelles de stockage (SVM).

**Avant de commencer**

- Vous devez avoir associé les sites protégés et les sites de récupération 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 récupération.

- Vous devez avoir activé les LIF de gestion SVM pour permettre la multitenance.

SRA prend en charge la gestion au niveau du cluster et au niveau des SVM. Si vous ajoutez du stockage au niveau du cluster, vous pouvez découvrir et effectuer des opérations sur toutes les SVM du cluster. Si vous ajoutez du stockage au niveau d'une SVM, vous ne pouvez gérer que cette SVM spécifique.

**Étapes**

1. Dans VMware Live Site Recovery, sélectionnez **Gestionnaires de baies** > **Ajouter un gestionnaire de baies**.
2. Saisissez les informations suivantes pour décrire la baie dans VMware Live Site Recovery :

   a. Saisissez un nom pour identifier le gestionnaire de la baie dans le champ **Nom d'affichage**.

   b. Dans le champ **Type de SRA**, sélectionnez **NetApp Storage Replication Adapter for ONTAP**.

   c. Saisissez les informations pour vous connecter au cluster ou à la SVM :

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

      Lors de la configuration du gestionnaire de baies, vous devez utiliser la même connexion (adresse IP) pour le système de stockage que celle utilisée pour intégrer le système de stockage dans ONTAP tools for VMware vSphere. Par exemple, si la configuration du gestionnaire de baies est au niveau SVM, alors le stockage sous ONTAP tools for VMware vSphere doit être ajouté au niveau SVM.

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

   e. Saisissez les volumes à découvrir dans le champ **Volume include list**.

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

      Par exemple, si vous souhaitez découvrir le volume src_vol1 qui est en 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 récupération.

   f. **(Facultatif)** Saisissez les volumes à exclure de la découverte dans le champ **Volume exclude list**.

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

   Par exemple, si vous souhaitez exclure le volume *src_vol1* qui est en SnapMirror relation avec le volume *dst_vol1*, vous devez spécifier *src_vol1* dans le champ du site protégé et *dst_vol1* dans le champ du site de récupération.

3. Sélectionnez **Suivant**.
4. Vérifiez que le tableau est détecté et affiché en bas de la fenêtre Ajouter un gestionnaire de tableaux, puis sélectionnez **Terminer**.

Vous pouvez suivre les mêmes étapes pour le site de récupération en utilisant les adresses IP de gestion SVM et les identifiants appropriés. Sur l'écran « Activer les paires de baies » de l'assistant « Ajouter un gestionnaire de baies », vous devez vérifier que la paire de baies correcte est sélectionnée et qu'elle est indiquée comme

prête à être activée.

## Vérifier les systèmes de stockage répliqués dans ONTAP tools

Après avoir configuré Storage Replication Adapter (SRA), vous devez vérifier que le site protégé et le site de récupération sont correctement appariés. Le système de stockage répliqué doit être détectable à la fois par le site protégé et le site de récupération.

**Avant de commencer**

- Vous devez avoir configuré votre système de stockage.
- Vous devez avoir associé le site protégé et le site de récupération à l'aide du gestionnaire de baies VMware Live Site Recovery.
- Vous devez avoir activé la licence FlexClone et la licence SnapMirror avant d'effectuer l'opération de basculement de test et l'opération de basculement pour SRA.
- Vous devez avoir les mêmes politiques SnapMirror et les mêmes calendriers sur les sites source et de destination.
- Si vous utilisez des stratégies SnapMirror personnalisées avec une planification personnalisée, vous devez configurer la même planification et la même stratégie sur les sites protégés et de récupération.
- Si vous utilisez des stratégies SnapMirror personnalisées (avec une planification par défaut ou personnalisée), vous devez effectuer une découverte du stockage à partir des outils ONTAP afin que la nouvelle stratégie soit reconnue. Sans cela, les workflows SRA, y compris le test de basculement et le basculement, échoueront. Effectuez la découverte du stockage aux points suivants :
  - Après avoir créé la politique personnalisée sur le site de récupération.
  - Après une opération de reprotection, qui recrée la policy sur le site protégé.

**Étapes**

1. Connectez-vous à votre serveur vCenter.
2. Accédez à **Récupération de site** > **Réplication basée sur des baies**.
3. Sélectionnez la paire de tableaux requise et vérifiez les détails correspondants.

   Les systèmes de stockage doivent être détectés sur le site protégé et le site de récupération avec le statut **Enabled**.

## Protection contre le fan-out dans ONTAP tools

Dans un scénario de protection par répartition, 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 second cluster ONTAP de destination. Les workflows de création, de modification et de suppression de la protection active SnapMirror maintiennent la protection synchrone. Les workflows de basculement et de reprotection de l'appliance VMware Live Site Recovery maintiennent la protection asynchrone.

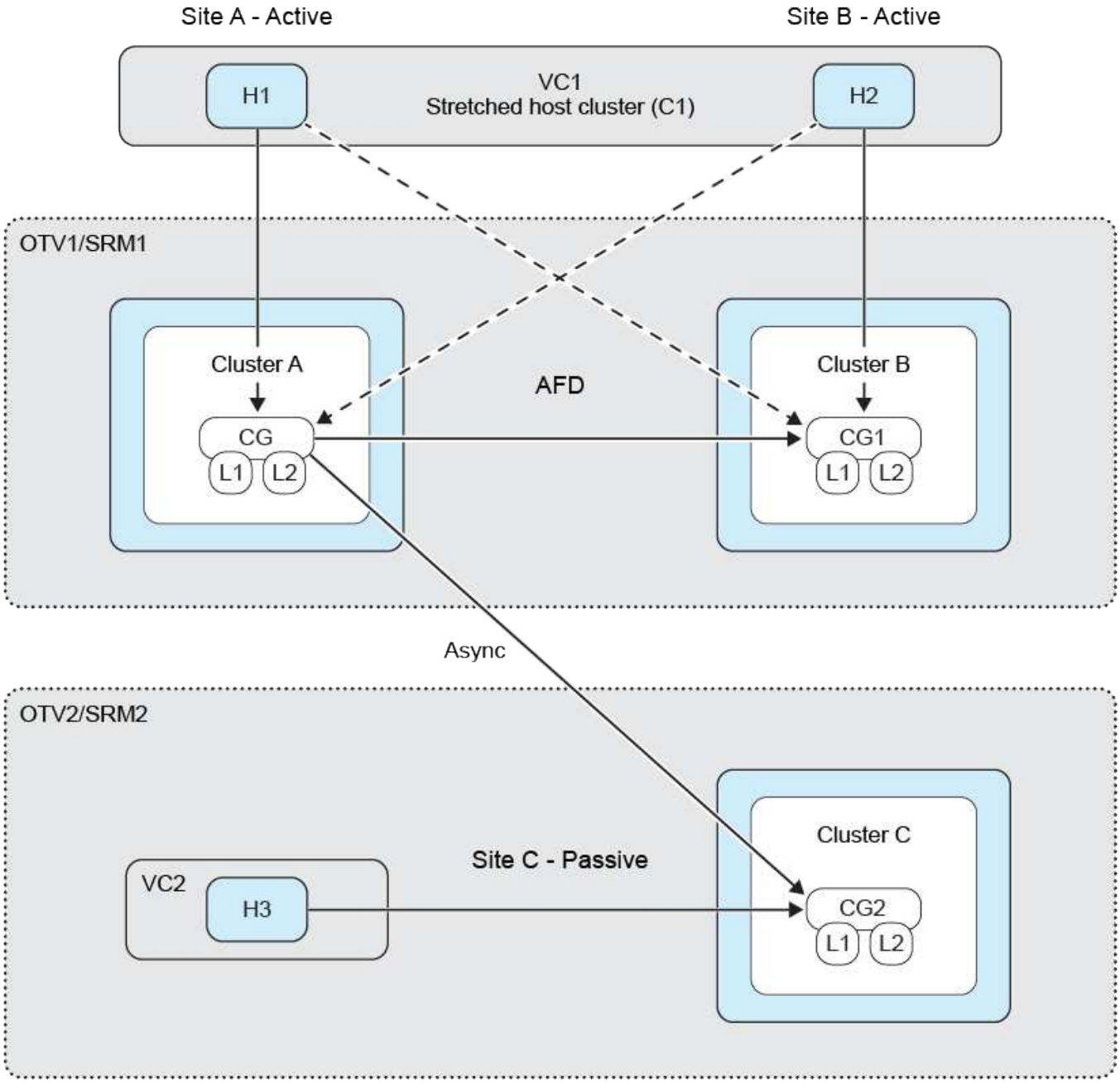
La fonction de diffusion n'est pas prise en charge pour les utilisateurs de SVM.

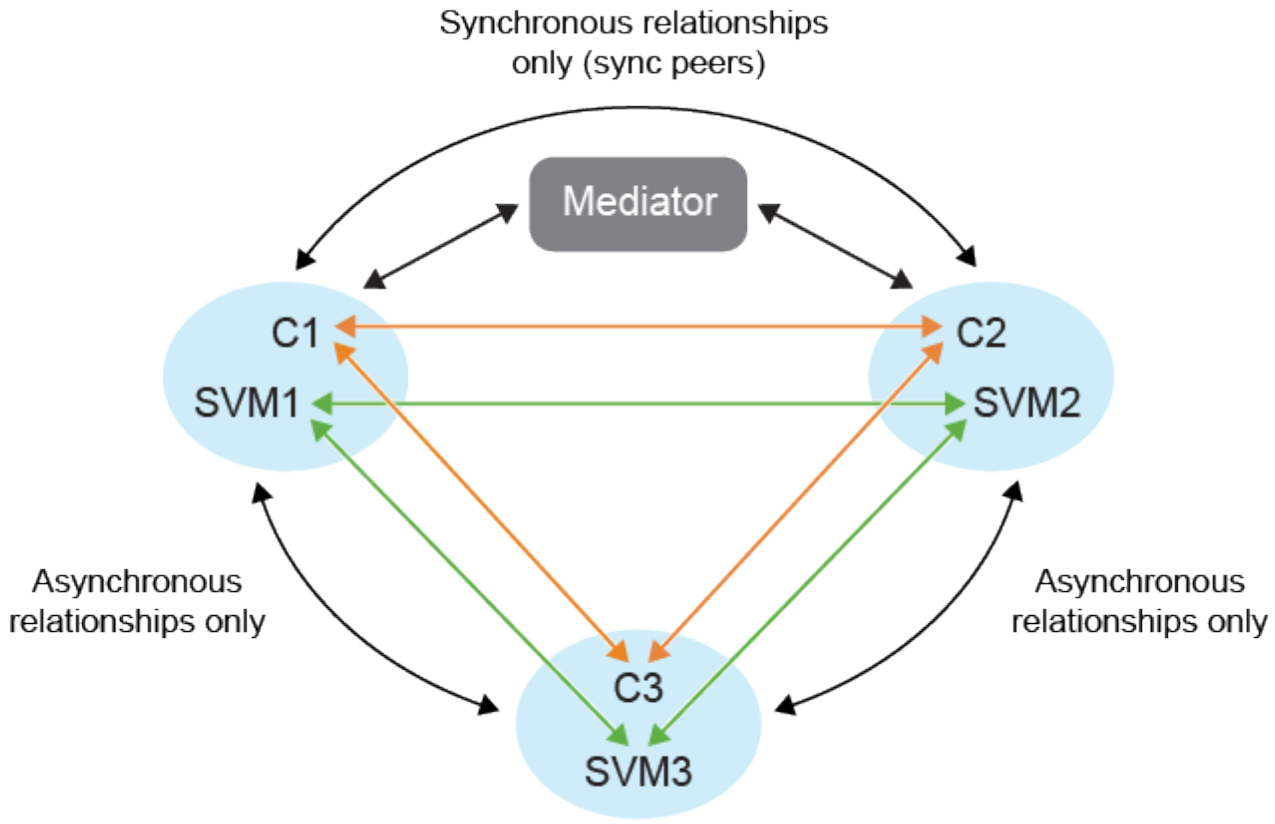
Pour configurer la protection par diffusion, mettez en peering les trois clusters de sites et les SVM.

Exemple :

| Si | alors |
| --- | --- |
| • Le groupe de cohérence source se trouve sur le cluster c1 et le SVM svm1<br>• Le premier groupe de cohérence se trouve sur le cluster c2 et le SVM svm2 et<br>• Le deuxième groupe de cohérence de destination se trouve sur le cluster c3 et la SVM svm3 | • Le cluster peering sur le cluster ONTAP source sera (C1, C2) et (C1, C3).<br>• Le cluster peering sur le premier cluster ONTAP de destination sera (C2, C1) et (C2, C3) et<br>• Le cluster peering sur le deuxième cluster ONTAP de destination sera (C3, C1) et (C3, C2).<br>• L'appairage SVM sur la SVM source sera (svm1, svm2) et (svm1, svm3).<br>• L'appairage SVM sur le premier SVM de destination sera (svm2, svm1) et (svm2, svm3) et<br>• Le peering SVM sur la deuxième destination svm sera (svm3, svm1) et (svm3, svm2). |

Le schéma suivant illustre la configuration de protection par dérivation :


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 de substitution. Les critères de sélection du magasin de données de substitution pour la protection progressive sont les suivants :
   - Ne placez pas le datastore de substitution dans le cluster hôte que vous protégez.
   - Si vous devez inclure le datastore de substitution dans le cluster hôte, ajoutez-le à l'appliance VMware Live Site Recovery avant de configurer la protection SnapMirror active sync. Avec cette configuration, vous pouvez laisser le datastore de substitution en dehors de la protection.

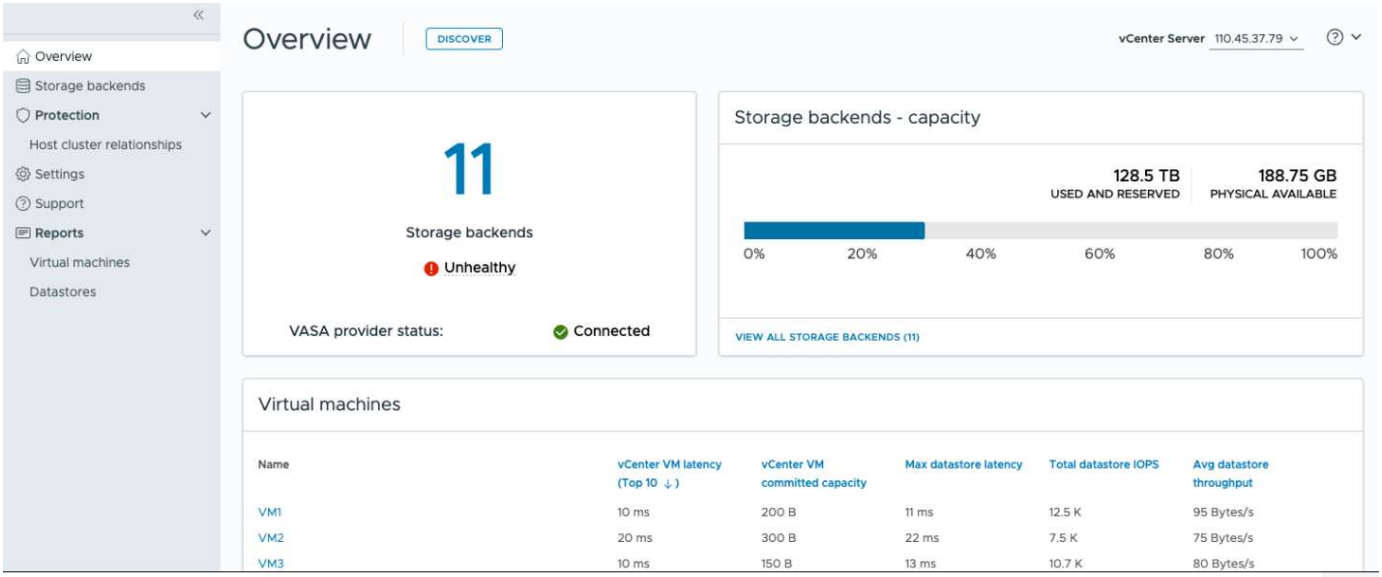
     Pour plus d'informations, consultez "Sélectionnez un datastore de remplacement"
2. Ajoutez des banques de données à la protection du cluster hôte en suivant "Modifier le cluster d'hôtes protégé". Ajoutez des types de stratégies asynchrones et synchrones.

# 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 des raccourcis du client vCenter ouvre la page de présentation. Ce tableau de bord fournit un résumé du plug-in ONTAP tools for VMware vSphere.

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




Depuis la page de présentation, vous pouvez exécuter l'action **Discovery**. L'action de découverte détecte les systèmes de stockage nouvellement ajoutés ou mis à jour, les hôtes, les banques de données, ainsi que l'état ou les relations de protection au niveau de vCenter. Exécutez une découverte à la demande sans attendre la découverte planifiée.

Le bouton **Découverte** n'est activé que si vous disposez du privilège requis pour effectuer la découverte.

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

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

| Carte | Description |
| --- | --- |

| | |
|---|---|
| Statut | La fiche d'état affiche le nombre de storage backends et l'état de santé global des storage backends et du VASA Provider. L'état des storage backends indique **Sain** lorsque tous les statuts des storage backends sont normaux et **Non sain** si un storage backend présente un problème (statut Inconnu/Injoignable/Dégradé). Sélectionnez l'infobulle pour ouvrir les détails de l'état des storage backends. Vous pouvez sélectionner n'importe quel storage backend pour plus de détails. Le lien **Autres états du VASA Provider** affiche l'état actuel du VASA Provider enregistré dans le vCenter Server. |
| Backends de stockage - Capacité | Cette fiche présente la capacité cumulée utilisée et disponible de tous les backends de stockage pour l'instance de serveur vCenter sélectionnée. Pour les systèmes de stockage ASA r2, les données de capacité ne sont pas affichées car le stockage est désagrégé. |
| machines virtuelles | Cette fiche présente les 10 machines virtuelles principales, classées par indicateur de performance. Vous pouvez sélectionner l'en-tête pour obtenir les 10 machines virtuelles principales pour l'indicateur sélectionné, triées par ordre croissant ou décroissant. Les modifications de tri et de filtrage effectuées sur la fiche persistent jusqu'à ce que vous modifiiez ou effaciez le cache du navigateur. |
| Datastores | Cette fiche présente les 10 meilleurs datastores, classés selon un indicateur de performance. Vous pouvez sélectionner l'en-tête pour afficher les 10 meilleurs datastores pour l'indicateur sélectionné, triés par ordre croissant ou décroissant. Les modifications de tri et de filtrage effectuées sur la fiche sont conservées jusqu'à ce que vous modifiiez ou vidiez le cache du navigateur. Un menu déroulant « Type de datastore » permet de sélectionner le type de datastore : NFS, VMFS ou vVols. |
| Carte de conformité hôte ESXi | Cette fiche indique si tous les hôtes ESXi (pour le vCenter sélectionné) respectent les paramètres 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 afficher 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'hôtes du protocole FC ou de noms de nœuds qualifiés iSCSI d'hôtes. Vous pouvez définir des igroups et les associer à des LUN pour contrôler quels initiateurs ont accès

aux LUN.

Dans ONTAP tools for VMware vSphere 9.x, les igroups étaient créés et gérés selon une structure plate, où chaque datastore dans vCenter était associé à un seul igroup. Ce modèle limitait la flexibilité et la réutilisation des igroups entre plusieurs datastores. ONTAP tools for VMware vSphere introduit les igroups imbriqués, où chaque datastore dans vCenter est associé à un igroup parent, tandis que chaque hôte est lié à un igroup enfant sous ce parent. Vous pouvez définir des igroups parents personnalisés avec des noms définis par l'utilisateur pour une réutilisation entre les datastores afin de faciliter la gestion des igroups. Comprenez le flux de travail des igroups pour gérer les LUN et les datastores dans ONTAP tools for VMware vSphere. Différents flux de travail génèrent des configurations d'igroups différentes, comme illustré dans les exemples suivants :

Les noms mentionnés sont donnés à titre d'exemple uniquement et ne correspondent pas à de vrais noms d'igroups. Les igroups gérés par ONTAP tools utilisent le préfixe « otv_ ». Les igroups personnalisés peuvent porter n'importe quel nom.

| Terme | Description |
|---|---|
| DS<number> | Magasin de données |
| iqn<number> | IQN de l'initiateur |
| hôte<number> | Hôte MoRef |
| lun<number> | ID LUN |
| <DSName>Igroup<number> | Groupe parent par défaut (géré par ONTAP tools) igroup |
| <Host-Moref>Igroup<number> | igroup enfant |
| CustomIgroup<number> | Groupe parent igroup personnalisé défini par l'utilisateur |
| ClassicIgroup<number> | Igroup utilisé dans les versions 9.x des outils ONTAP. |

**Exemple 1 :**

Créer un datastore sur un seul hôte avec un seul initiateur

**Flux de travail** : [Create] DS1 (lun1) : host1 (iqn1)

**Résultat**:

- DS1Igroup :
  - host1Igroup → (iqn1: lun1)

ONTAP crée le parent igroup DS1Igroup pour DS1 et associe le child igroup host1Igroup à lun1. Le système associe toujours les LUN à des child igroups.

**Exemple 2 :**

Monter la banque de données existante sur un hôte supplémentaire

**Flux de travail** : [Mount] DS1 (lun1) : host2 (iqn2)

**Résultat**:

- DS1Igroup :

- host1Igroup → (iqn1: lun1)
- host2Igroup → (iqn2: lun1)

Les outils ONTAP pour VMware vSphere créent un igroup enfant host2Igroup et l'ajoutent à l'igroup parent existant DS1Igroup.

**Exemple 3 :**

Démontez un datastore d'un hôte

**Workflow** : [Démonter] DS1 (lun1) : host1 (iqn1)

**Résultat**:

- DS1Igroup :
  - host2Igroup → (iqn2: lun1)

ONTAP tools for VMware vSphere suppriment host1Igroup de la hiérarchie. Le système ne supprime pas explicitement les igroups enfants. Il les supprime dans les deux cas suivants :

- Si aucun LUN n'est mappé, le système ONTAP supprime l'igroup enfant.
- Une tâche de nettoyage planifiée supprime les igroups enfants orphelins sans mappage LUN. Ces scénarios concernent uniquement les igroups gérés par les ONTAP tools, et non ceux créés sur mesure.

**Exemple 4 :**

Supprimer le datastore

**Flux de travail** : [Delete] DS1 (lun1) : host2 (iqn2)

**Résultat**:

- DS1Igroup :
  - host2Igroup → (iqn2: lun1)

Les igroups parents et enfants sont supprimés, sauf si un autre datastore réutilise l'igroup parent. Les igroups enfants ne sont pas explicitement supprimés

**Exemple 5 :**

Créez plusieurs datastores sous un igroup parent personnalisé

**Flux de travail** :

- [Créer] DS2 (lun2) : hôte1 (iqn1), hôte2 (iqn2)
- [Créer] DS3 (lun3): hôte1 (iqn1), hôte3 (iqn3)

**Résultat**:

- CustomIgroup1 :
  - host1Igroup → (iqn1 : lun2, lun3)
  - host2Igroup → (iqn2: lun2)
  - host3Igroup → (iqn3: lun3)

CustomIgroup1 est créé pour DS2 et réutilisé pour DS3. Les igroups enfants sont créés ou mis à jour sous le parent partagé, chaque igroup enfant étant associé à ses LUNs correspondants.

**Exemple 6 :**

Supprimez un datastore sous un igroup parent personnalisé.

**Flux de travail** : [Supprimer] DS2 (lun2) : hôte1 (iqn1), hôte2 (iqn2)

**Résultat**:

- CustomIgroup1 :
  - host1Igroup → (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.
- host1Igroup n'est pas supprimé car il est associé à lun3 de DS3. Les igroups personnalisés ne sont jamais supprimés, quel que soit leur statut de réutilisation.

**Exemple 7 :**

Agrandir le datastore vVols (Ajouter un volume)

**Flux de travail** :

Avant l'expansion :

[Développer] DS4 (lun4): hôte4 (iqn4)

- DS4Igroup : host4Igroup → (iqn4 : lun4)

Après l'expansion :

[Développer] DS4 (lun4, lun5) : hôte4 (iqn4)

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

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

**Exemple 8 :**

Réduire le datastore vVols (Supprimer le volume)

**Flux de travail** :

Avant le rétrécissement :

[Réduction] DS4 (lun4, lun5) : hôte4 (iqn4)

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

Après rétrécissement :

[Réduction] DS4 (lun4): hôte4 (iqn4)

- DS4Igroup : host4Igroup → (iqn4 : lun4)

Le LUN spécifié (lun5) est dé-mappé de l'igroup enfant. L'igroup reste actif tant qu'il possède au moins un LUN mappé.

**Exemple 9 :**

Migration des outils ONTAP 9 vers 10 (normalisation des igroups)

**Flux de travail**

ONTAP tools for VMware vSphere versions 9.x ne prennent pas en charge les igroups hiérarchiques. Lors de la migration vers les versions 10.3 ou supérieures, les igroups doivent être normalisés selon une structure hiérarchique.

Avant la migration :

[Migration] DS6 (lun6, lun7) : hôte6 (iqn6), hôte7 (iqn7) → ClassicIgroup1 (iqn6 & iqn7 : lun6, lun7)

La logique des ONTAP tools 9.x permet plusieurs initiateurs par igroup sans imposer de correspondance un-à-un entre hôte et igroup.

Après la migration :

[Migration] DS6 (lun6, lun7) : hôte6 (iqn6), hôte7 (iqn7) → ClassicIgroup1 : otv_ClassicIgroup1 (iqn6 & iqn7 : lun6, lun7)

Pendant la migration :

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

Cela garantit la conformité avec le modèle hiérarchique.

À partir d'ONTAP tools 10.5P2, les igroups migrés sont supprimés lorsqu'ils ne sont plus utilisés. Dans les versions précédentes, les igroups migrés n'étaient jamais supprimés. Remarque :

- Les igroups migrés ne peuvent pas être réutilisés entre les banques de données.
- Les igroups personnalisés (définis par l'utilisateur) ne sont jamais supprimés et peuvent toujours être réutilisés.

**Sujets connexes**

"À propos des igroups"

## Politiques d'export

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

Lorsque vous créez une banque de données NFS dans ONTAP tools for VMware vSphere, vous pouvez sélectionner une règle d'export existante ou en créer une nouvelle. La règle d'export est ensuite appliquée à la banque de données, garantissant que seuls les clients autorisés peuvent y accéder.

Lors du montage d'une banque de données NFS sur un nouvel hôte ESXi, ONTAP tools for VMware vSphere

ajoute l'adresse IP de l'hôte à la règle d'export associée à la banque de données. Cela permet au nouvel hôte d'accéder à la banque de données sans avoir à créer une nouvelle règle d'export.

Lorsque vous supprimez ou démontez une banque de données NFS d'un hôte ESXi, ONTAP tools for VMware vSphere supprime l'adresse IP de l'hôte de la règle d'export. Si aucun autre hôte n'utilise cette règle d'export, elle sera supprimée. Lorsque vous supprimez une banque de données NFS, ONTAP tools for VMware vSphere supprime la règle d'export associée à cette banque de données si elle n'est pas réutilisée par d'autres banques de données. Si la règle d'export est réutilisée, elle conserve l'adresse IP de l'hôte et ne change pas. Lorsque vous supprimez les banques de données, la règle d'export désassocie l'adresse IP de l'hôte et attribue une règle d'export par défaut, afin que les systèmes ONTAP puissent y accéder si nécessaire.

L'attribution des règles d'export diffère lorsqu'elles sont réutilisées sur différents datastores. Lorsque vous réutilisez la règle d'export, vous pouvez y ajouter la nouvelle adresse IP de l'hôte. Lorsque vous supprimez ou démontez un datastore qui utilise une règle d'export partagée, la règle ne sera pas supprimée. Elle reste inchangée et l'adresse IP de l'hôte n'est pas retirée, car elle est partagée avec les autres datastores. La réutilisation des règles d'export n'est pas recommandée, car cela peut entraîner des problèmes d'accès et de latence.

**Sujets connexes**

"Créer une règles d'export"

# Comment les ONTAP tools gèrent les igroups

Si vous gérez à la fois les machines virtuelles ONTAP tools et les systèmes de stockage ONTAP, il est important de comprendre comment les igroups se comportent, en particulier lors du déplacement de datastores d'environnements non gérés par ONTAP tools vers ceux qui le sont. Cette page explique comment ONTAP tools for VMware vSphere représente et gère les igroups. Il s'agit d'informations conceptuelles pour comprendre les différences de comportement entre les versions précédentes et le modèle actuel d'igroup imbriqué.

À partir de ONTAP tools for VMware vSphere 10.4, ONTAP tools crée et gère automatiquement les objets ONTAP et vCenter, simplifiant la gestion des datastores dans les environnements de datacenter VMware. À partir de ONTAP tools for VMware vSphere 10.5 P2, les igroups migrés sont également supprimés automatiquement lorsqu'ils ne sont plus utilisés.

## Résumé rapide du comportement

- Les datastores VMFS gérés par les outils ONTAP utilisent des igroups imbriqués : un igroup parent par contexte de datastore et des igroups enfants par hôte.
- Les mappages LUN sont appliqués aux igroups enfants.
- Les igroups parents personnalisés peuvent être réutilisés dans plusieurs datastores.
- Les igroups migrés depuis ONTAP tools 9.x ne peuvent pas être réutilisés.

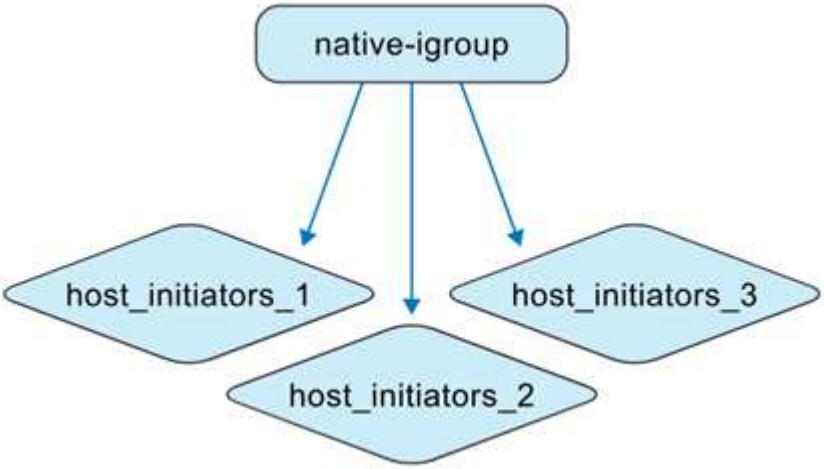
## Contextes de groupe

Les outils ONTAP pour VMware vSphere gèrent les igroups dans deux contextes.

**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

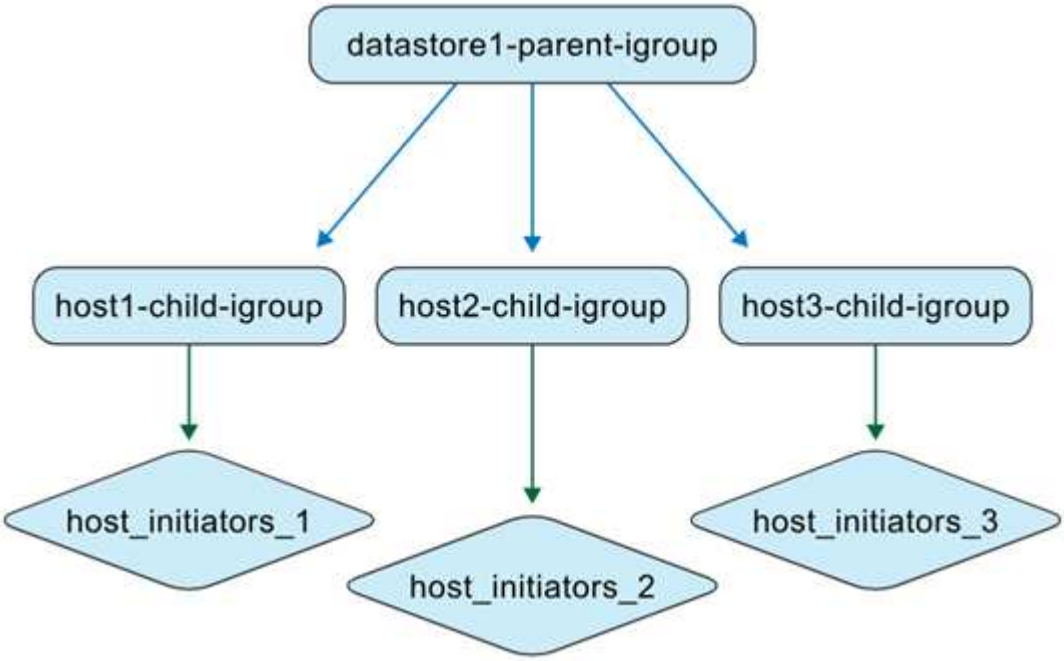
structures plates ou imbriquées. L'illustration suivante montre un igroup plat créé directement dans ONTAP.

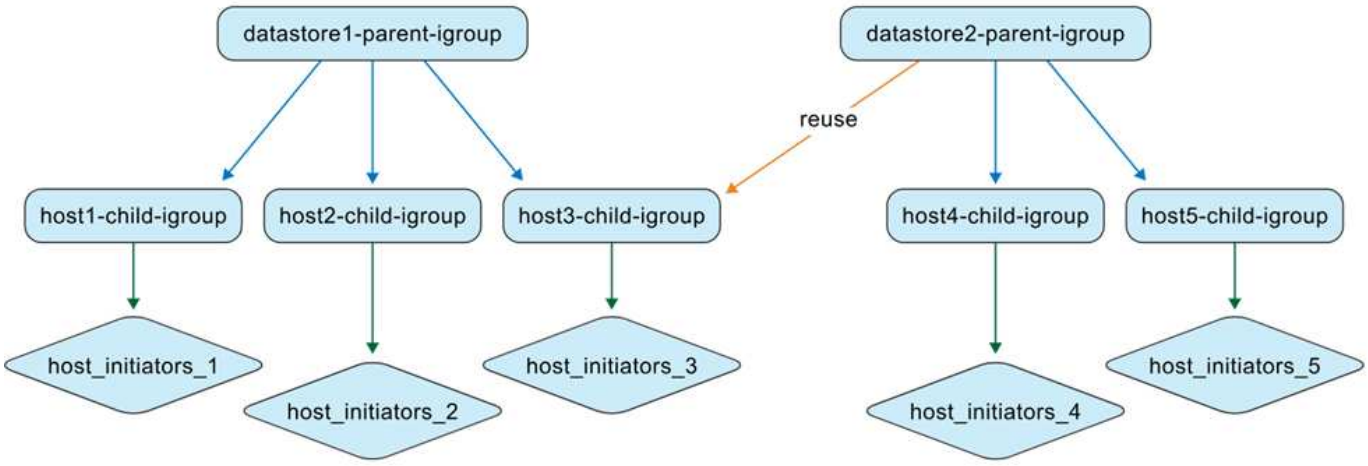



**Groupes igroups gérés par ONTAP tools**

Lorsque vous créez des banques de données, ONTAP tools for VMware vSphere crée des igroups dans une structure imbriquée.

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, ONTAP tools réutilise l'igroup au niveau de l'hôte pour une gestion efficace.






## Comportement de dénomination

Lorsque vous créez un datastore et laissez le champ igroup vide, ONTAP tools crée une structure igroup imbriquée par défaut.

- Modèle de nommage des igroups parents : `otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name>`
- Modèle de nommage des igroups enfants : `otv_<hostMoref>_<vcguid>`

L'interface des systèmes ONTAP affiche la relation entre les igroups parents et enfants dans le champ **Parent Initiator Group**.

## Comportement selon le scénario

| Scénario | Comportement du groupe parent | Comportement du groupe enfant | Cartographie et visibilité des LUN |
|---|---|---|---|
| Magasin de données créé avec les paramètres igroup par défaut | Un groupe igroup parent géré par défaut par les ONTAP tools est créé. | Des igroups enfants au niveau de l'hôte sont créés selon les besoins. | Les LUN sont mappées à des igroups enfants. La banque de données apparaît dans l'inventaire du serveur vCenter. |
| Magasin de données créé avec un nom d'igroup personnalisé | Un igroup parent personnalisé est créé avec le nom spécifié. | Les igroups enfants existants au niveau de l'hôte sont réutilisés en cas de chevauchement des hôtes. | Le nouveau LUN de la banque de données est mappé à l'igroup enfant réutilisé ou nouvellement créé. La banque de données apparaît dans le serveur vCenter. |
| Groupe igroup personnalisé existant réutilisé lors de la création du datastore | Un igroup parent personnalisé existant est sélectionné et réutilisé. | Les igroups enfants sont réutilisés ou étendus en fonction de l'appartenance à l'hôte. | Le nouveau LUN de la banque de données est mappé via l'igroup enfant associé. La banque de données apparaît dans le serveur vCenter. |

| Scénario | Comportement du groupe parent | Comportement du groupe enfant | Cartographie et visibilité des LUN |
|---|---|---|---|
| Le datastore et l'igroup sont créés nativement dans ONTAP et vCenter, puis découverts par les ONTAP tools | ONTAP tools crée un igroup parent dans son contexte de gestion et conserve le nom d'igroup d'origine. | ONTAP tools renomment l'igroup d'origine avec le `otv_` préfixe et le représentent comme un igroup enfant dans la hiérarchie. | Les mappages d'initiateurs restent inchangés. Seuls les igroups mappés aux banques de données sont convertis lors de la découverte. |

## Réutilisation personnalisée des igroups et comportement de l'API

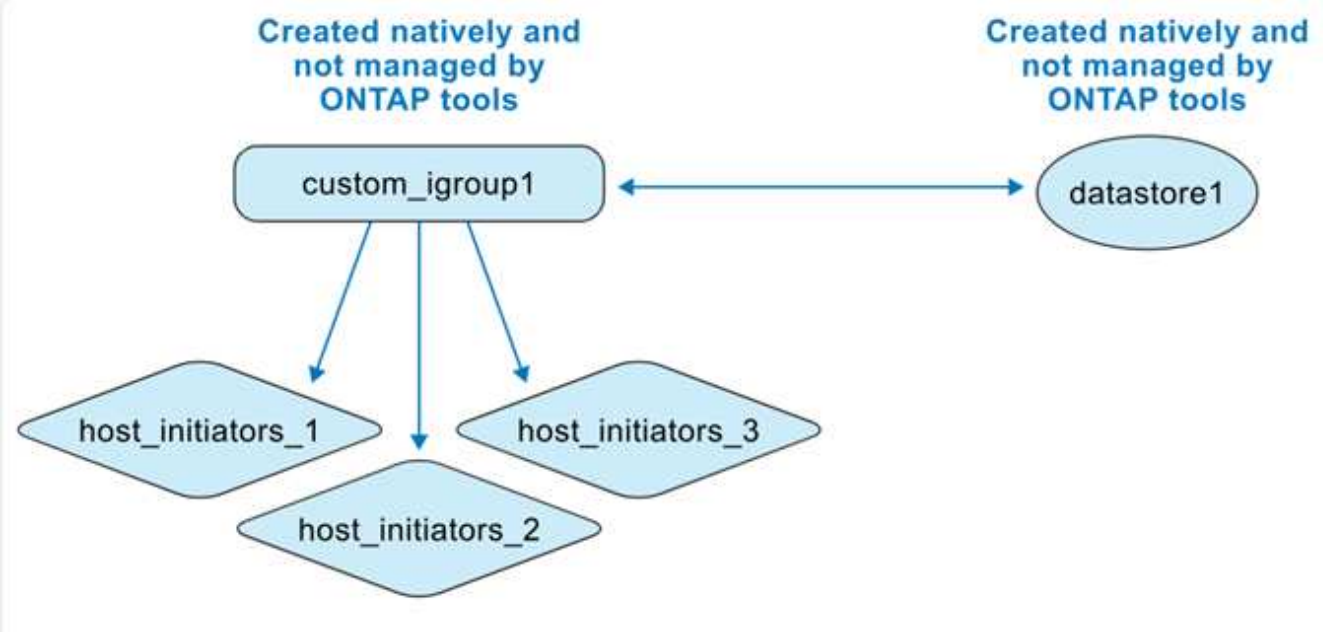
Dans l'interface utilisateur des ONTAP tools, vous pouvez réutiliser un igroup parent personnalisé existant à partir de la liste déroulante lors de la création d'un datastore.

Ce même comportement est pris en charge par l'API. Pour réutiliser un igroup existant lors de la création d'un datastore, fournissez l'UUID de l'igroup dans la charge utile de la requête API.

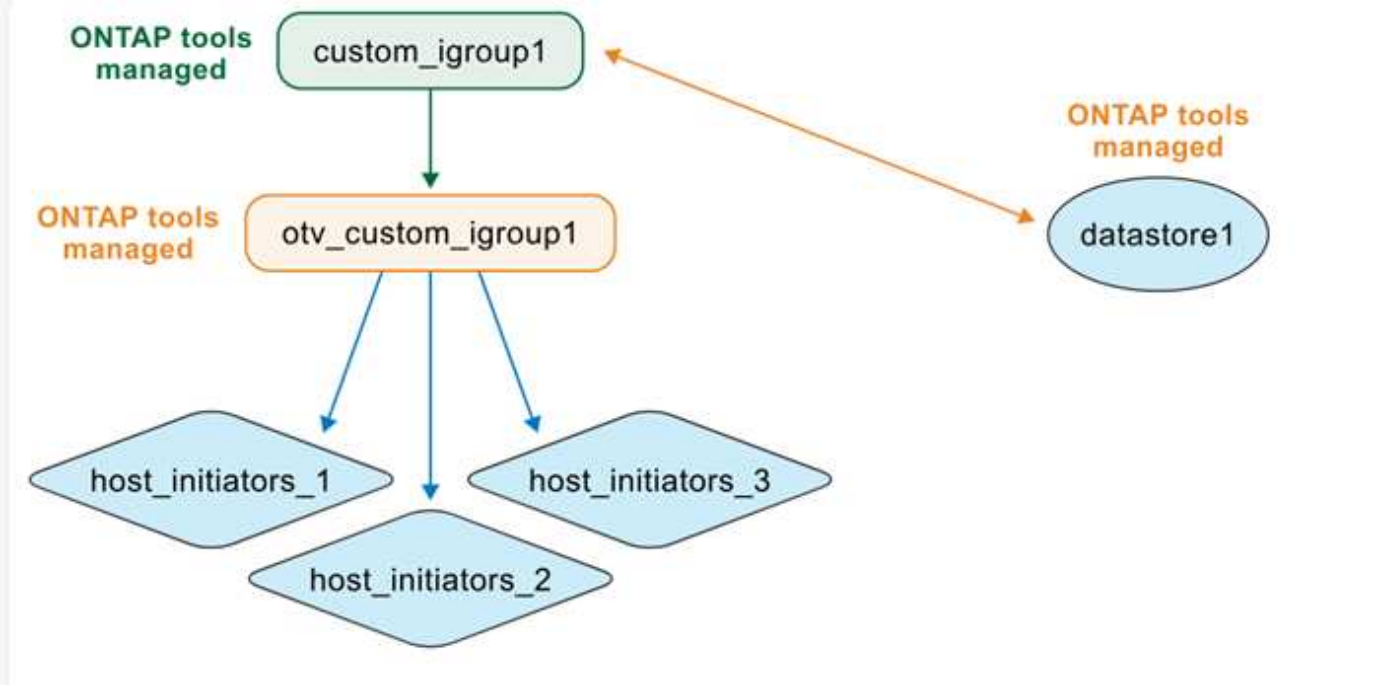
Seuls les igroups personnalisés peuvent être réutilisés. Les igroups migrés depuis ONTAP tools 9.x ne peuvent pas être réutilisés et, à partir de ONTAP tools 10.5 P2, sont automatiquement supprimés lorsqu'ils ne sont plus utilisés.

## Vue de conversion native vers gérée

Si vous créez directement l'igroup et le datastore dans les systèmes ONTAP et les environnements VMware, ONTAP tools ne gère pas initialement ces objets. Il en résulte une structure d'igroup plate.




Après la découverte des datastores, ONTAP tools identifie et enregistre les igroups mappés sur les datastores, puis les représente dans un modèle imbriqué. L'igroup parent est représenté au niveau du datastore, l'igroup existant est renommé avec le `otv_` préfixe en tant qu'igroup enfant, et les mappages d'initiateurs restent inchangés.




ONTAP tools for VMware vSphere ne détecte ni ne gère les igroups qui sont créés dans les systèmes ONTAP mais qui ne sont pas associés à une banque de données ou liés aux ONTAP tools. Lors de la découverte, ONTAP tools convertit uniquement les igroups qui sont associés aux banques de données détectées ; les autres igroups restent non gérés.

### Réutilisation des igroups natifs découverts

Après qu'ONTAP tools a géré un igroup natif découvert, cet igroup est disponible dans la liste déroulante du nom du groupe d'initiateurs personnalisé pour la création de datastore.

Le nouveau LUN de la banque de données est mappé au groupe d'interface enfant normalisé, par exemple, `otv_NativeIgroup1`.

ONTAP tools for VMware vSphere ne détecte ni n'utilise les igroups créés dans les systèmes ONTAP qui ne sont pas gérés par ONTAP tools ou qui ne sont pas liés à une banque de données.

# Découvrez l'interface utilisateur du gestionnaire d'outils ONTAP

ONTAP tools for VMware vSphere prend en charge la multi-location, permettant la gestion de plusieurs instances de serveur vCenter.

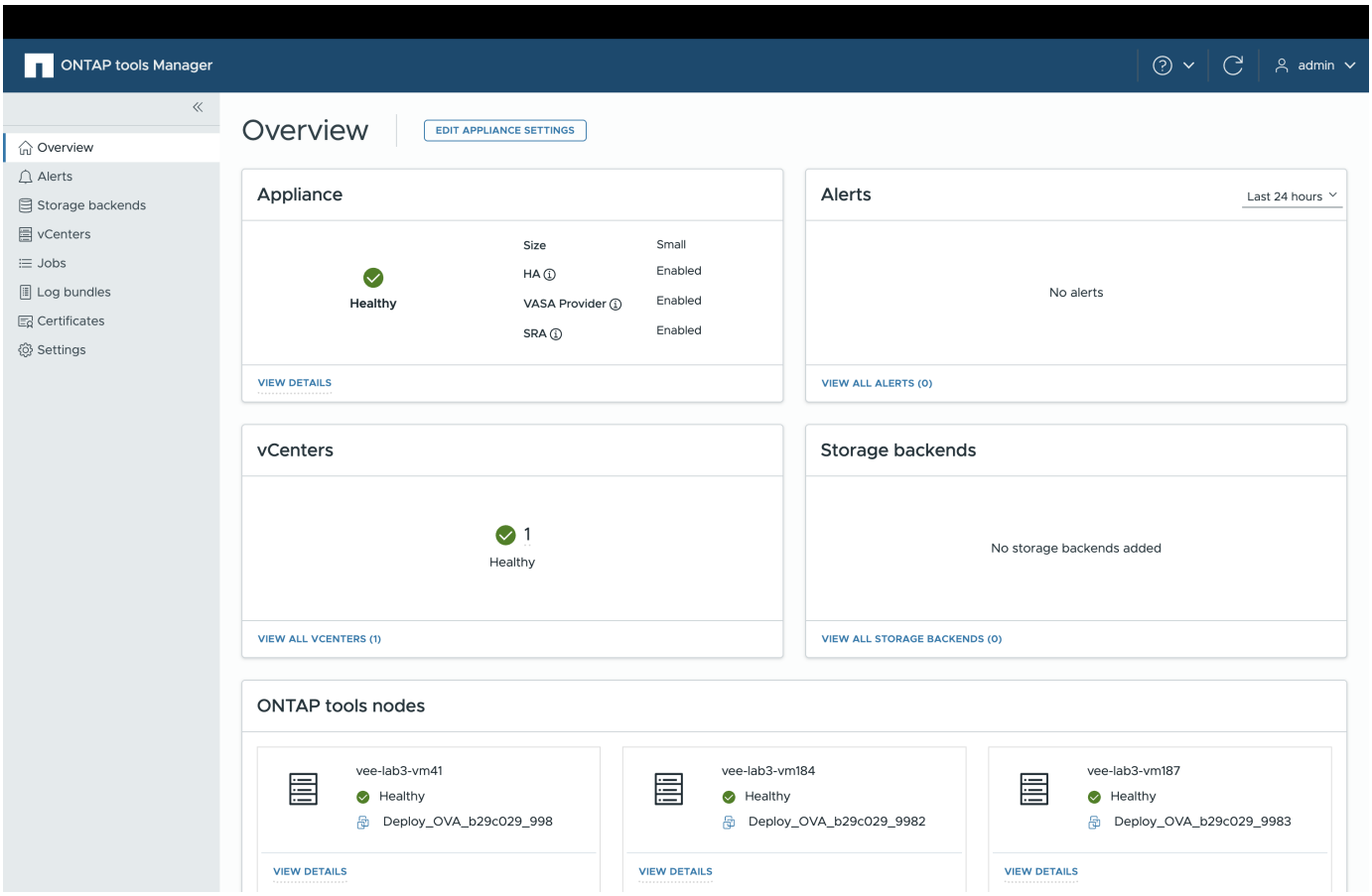
ONTAP tools Manager est une console Web permettant de gérer les ONTAP tools for VMware vSphere, vCenter Server instances, les backends de stockage et la configuration des appliances telles que la haute disponibilité (HA) et la mise à l'échelle des nœuds.

ONTAP tools Manager offre les fonctionnalités suivantes :

- Gérez les alertes - Affichez et filtrez les alertes générées par ONTAP tools for VMware vSphere.
- Gérez les systèmes de stockage backend : ajoutez et gérez des clusters de stockage ONTAP, et associez-les à des instances de serveur vCenter à l'échelle mondiale.

- Gérez les instances de serveur vCenter - Ajoutez et gérez les instances de serveur vCenter dans les outils ONTAP.
- Surveillez et déboguez les tâches asynchrones lancées depuis l'interface du plug-in ONTAP tools et l'interface ONTAP tools Manager. Vous pouvez filtrer les tâches par période, ajuster la taille de la page et consulter les détails de chaque tâche, y compris les erreurs et les sous-tâches. Cliquez sur le statut d'échec pour afficher 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 l'exploration de la tâche pour afficher les détails.
- Téléchargez les ensembles de journaux - Collectez les fichiers journaux pour dépanner les ONTAP tools for VMware vSphere.
- Gérez les certificats - Remplacez le certificat auto-signé par un certificat CA personnalisé, et renouvelez ou actualisez les certificats pour VASA Provider et ONTAP tools.
- Réinitialiser les mots de passe - Changez le mot de passe du VASA Provider et du SRA.
- Gérez les paramètres de l'appliance - Configurez l'appliance ONTAP tools, notamment en activant la haute disponibilité (HA) et en augmentant la taille des nœuds.

Pour accéder à ONTAP tools Manager, lancez `https://<ONTAPtoolsIP>:8443/virtualization/ui/` depuis le navigateur et connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.



| Carte | Description |
| --- | --- |
| Carte d’appliance | La fiche de l’appliance affiche l’état général de l’appliance ONTAP tools, 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 de l’appliance, la fiche affiche l’état du travail et les détails jusqu’à la fin de la modification. |
| Carte d’alertes | La fiche « Alertes » affiche les alertes des outils ONTAP classées par type, y compris les alertes au niveau des nœuds HA. Vous pouvez consulter les alertes détaillées en cliquant sur le lien du nombre, ce qui vous redirige vers la page des alertes filtrée par le type d’alerte sélectionné. |
| Carte vCenters | La carte vCenters affiche l’état de santé de toutes les instances vCenter Server gérées par ONTAP tools. Vous pouvez afficher les détails de chaque vCenter en sélectionnant le lien correspondant, ce qui vous dirigera vers une page contenant plus d’informations sur l’instance sélectionnée. |
| Carte des backends de stockage | La carte des backends de stockage affiche l’état de santé et de connectivité de tous les clusters de stockage ONTAP configurés dans ONTAP tools. Vous pouvez consulter les détails de chaque backend de stockage en sélectionnant le lien correspondant, ce qui vous dirige vers 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 concernant 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 ONTAP tools

## Modifier les paramètres AutoSupport des outils ONTAP

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

#### Désactiver AutoSupport

Lorsque vous désactivez AutoSupport, vous ne bénéficiez plus d’assistance proactive ni de surveillance.

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

**Étapes**

1. Lancez ONTAP tools Manager depuis un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis 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 fonctionnalité AutoSupport achemine les données via le serveur proxy pour une transmission sécurisée.

**Étapes**

1. Lancez ONTAP tools Manager depuis un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.
3. Sélectionnez **Paramètres** dans la barre latérale.
4. Sélectionnez l'option **Paramètres** > **Télémétrie** > **Modifier**.
5. Saisissez une **URL de proxy** valide et enregistrez les modifications.

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

## Ajouter des serveurs NTP aux outils ONTAP

Saisissez les informations du serveur NTP pour synchroniser les horloges de l'appliance ONTAP tools.

**Étapes**

1. Lancez ONTAP tools Manager depuis un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.
3. Sélectionnez l'option **Paramètres** > **Serveur NTP** > **Modifier**.
4. Saisissez le nom de domaine complet (FQDN), les adresses IPv4 ou IPv6 séparées par des virgules.

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

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

Si vous oubliez vos identifiants VASA Provider ou SRA, vous pouvez les réinitialiser avec un nouveau mot de passe à l'aide de l'interface ONTAP tools Manager. Le nouveau mot de passe doit comporter entre 8 et 256 caractères.

**Étapes**

1. Lancez ONTAP tools Manager depuis un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.
3. Sélectionnez l'option **Paramètres** > **VASA Provider / SRA credentials** > **Réinitialiser le mot de passe**.
4. Saisissez 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 de 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 cela empêche les ONTAP tools 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 ONTAP tools Manager depuis un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis 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 la sauvegarde.

## Activer les services ONTAP tools

Vous pouvez modifier le mot de passe de l'administrateur à l'aide de ONTAP tools Manager pour activer des services tels que VASA Provider, l'importation de la configuration vVols et la reprise après sinistre (SRA) à l'aide de ONTAP tools Manager.

**Étapes**

1. Lancez ONTAP tools Manager depuis un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.

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

   Lors de la première activation des services, vous devez créer les identifiants VASA Provider et SRA. Ces identifiants sont utilisés pour enregistrer ou 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 un service optionnel, assurez-vous que les serveurs vCenter gérés par ONTAP tools 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 depuis ONTAP tools 9.xx vers ONTAP tools 10.5.

# Modifier les paramètres de l'appliance ONTAP tools

Utilisez ONTAP tools Manager pour faire évoluer la configuration ONTAP tools for VMware vSphere, soit en augmentant le nombre de nœuds, soit en activant la haute disponibilité (HA). Par défaut, l'appliance ONTAP tools for VMware vSphere est déployée en configuration à nœud unique, sans haute disponibilité.

**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 l'OVA ONTAP tools for VMware vSphere est initialement déployé.
- Assurez-vous que l'ajout à chaud du processeur et le branchement à chaud de la mémoire sont activés.
- Dans le serveur vCenter, définissez le niveau d'automatisation du service de reprise après sinistre (DRS) sur partiellement automatisé. Après le déploiement de la haute disponibilité, rétablissez-le sur entièrement automatisé.
- Dans la configuration HA, les noms d'hôtes des nœuds doivent être en minuscules.

**Étapes**

1. Lancez ONTAP tools Manager depuis un navigateur Web :
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.
3. Sélectionnez **Modifier les paramètres de l'appareil** dans la section Vue d'ensemble.
4. Dans la section **Configuration**, augmentez la taille du nœud et activez la configuration HA. Utilisez les informations d'identification du serveur vCenter pour effectuer les modifications.

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

   Dans ONTAP tools for VMware vSphere, vous pouvez uniquement augmenter la taille des nœuds ; 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 moyenne et grande sont prises en charge.

5. Utilisez le bouton d'activation HA pour activer la configuration HA. Sur la page **Paramètres HA**, assurez-vous que :
   - La bibliothèque de contenu appartient au même serveur vCenter où s'exécutent les machines virtuelles des nœuds ONTAP tools. Les identifiants du serveur vCenter sont utilisés pour valider et télécharger le modèle OVA lors des modifications de l'appliance.
   - La machine virtuelle hébergeant les ONTAP tools n'est pas déployée directement sur un hôte 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 **Paramètres HA** de la fenêtre **Modifier les paramètres de l'appliance**, vous pouvez saisir les détails des nœuds 2 et 3. ONTAP tools for VMware vSphere prend en charge trois nœuds dans une configuration HA.

   > Les outils ONTAP pré-remplissent la plupart des options de saisie avec les détails réseau du nœud 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 que chaque hôte ESXi ne contient qu'une seule machine virtuelle ONTAP tools. Les entrées sont validées à chaque passage à la fenêtre suivante.

7. Vérifiez les détails dans la section **Résumé** et **Enregistrez** les modifications.

**Et ensuite ?**

La page **Aperçu** affiche l'état du déploiement. Vous pouvez également suivre l'état de la tâche de modification des paramètres de l'appliance 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 la haute disponibilité.

L'onglet **Alertes** du panneau de gauche répertorie les alertes pour ONTAP tools for VMware vSphere.

# Ajouter des hôtes VMware vSphere aux outils ONTAP

Ajoutez de nouveaux hôtes VMware vSphere aux ONTAP tools for VMware vSphere pour gérer et protéger les datastores sur les hôtes.

**Étapes**

1. Ajoutez un hôte à votre cluster VMware vSphere en suivant le flux de travail à la page : "Broadcom Documentation technique".
2. Après avoir ajouté l'hôte, accédez au menu principal des ONTAP tools et sélectionnez **Discover** dans le panneau d'aperçu. Attendez la fin du processus de découverte. Vous pouvez également attendre la fin de la découverte planifiée de l'hôte.

**Résultat**

Le nouvel hôte est désormais détecté et géré par ONTAP tools for VMware vSphere. Vous pouvez procéder à la gestion de la banque de données sur le nouvel hôte.

**Sujets connexes**

- "Monter un datastore vVols" sur de nouveaux hôtes.
- "Montez le datastore NFS et VMFS" sur de nouveaux hôtes.

# Gérer les datastores

## Monter les datastores NFS et VMFS dans ONTAP tools

Le montage d'une banque de données permet d'accéder au stockage sur des hôtes supplémentaires. Vous pouvez monter la banque de données sur les hôtes supplémentaires après avoir ajouté ces hôtes à votre environnement VMware.

> Lorsque vous ajoutez un nouvel hôte ESXi à l'aide de l' "Broadcom Documentation technique", attendez que la découverte planifiée de l'hôte soit terminée avant qu'il n'apparaisse dans ONTAP tools. Vous pouvez également lancer manuellement la découverte depuis l'écran de présentation des NetApp ONTAP tools.

**À propos de cette tâche**

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

**Étapes**

1. Depuis la page d'accueil du vSphere Client, sélectionnez **Hôtes et clusters**.
2. Dans le volet de navigation de gauche, sélectionnez les centres de données contenant les hôtes.
3. Pour monter des datastores NFS/VMFS sur un hôte ou un cluster d'hôtes, cliquez avec le bouton droit et sélectionnez **NetApp ONTAP tools** > **Mount Datastores**.
4. Sélectionnez les banques de données que vous souhaitez monter et sélectionnez **Monter**.

**Et ensuite ?**

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 la banque de données » supprime une banque de données NFS ou VMFS des hôtes ESXi. Elle est disponible pour les banques de données découvertes ou gérées par 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 vSphere client ouvre une boîte de dialogue et affiche la liste des 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 la base de données.

   Vous ne pouvez pas démonter la base de données de tous les hôtes. L'interface utilisateur vous suggère d'utiliser plutôt l'opération de suppression de la base de données.

4. Sélectionnez le bouton **Démonter**.

   Si la base de données fait partie d'un cluster d'hôtes protégé, un message d'avertissement s'affiche.

> Si la banque de données protégée est démontée, la protection actuelle peut entraîner une protection partielle. Consultez "Modifier le cluster d'hôtes protégé" pour activer une protection complète.

**Et ensuite ?**

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

## Monter un datastore vVols dans ONTAP tools

Vous pouvez monter un datastore VMware Virtual Volumes (vVols) sur un ou plusieurs hôtes supplémentaires afin de fournir un accès au stockage à ces hôtes. Vous pouvez démonter le datastore vVols uniquement via les API.

> Lorsque vous ajoutez un nouvel hôte ESXi à l'aide de l' "Broadcom Documentation technique", attendez que la découverte planifiée de l'hôte soit terminée avant qu'il n'apparaisse dans ONTAP tools. Vous pouvez également lancer manuellement la découverte depuis l'écran de présentation des NetApp ONTAP tools.

**Étapes**

1. Depuis la page d'accueil du vSphere Client, sélectionnez **Hôtes et clusters**.
2. Dans le volet de navigation, sélectionnez le centre de données qui contient le datastore.
3. Cliquez avec le bouton droit sur la banque de données et sélectionnez **NetApp ONTAP tools** > **Monter la banque de données**.
4. Dans la boîte de dialogue **Monter les banques de données sur les hôtes**, sélectionnez les hôtes sur lesquels vous souhaitez monter la banque de données, puis sélectionnez **Monter**.

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 l'espace de stockage des fichiers de vos machines virtuelles. Vous pouvez modifier la taille d'un datastore en fonction de l'évolution de vos besoins d'infrastructure.

**À propos de cette tâche**

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

**Étapes**

1. Depuis la page d'accueil du vSphere Client, sélectionnez **Hôtes et clusters**.
2. Dans le volet de navigation, sélectionnez le centre de données qui contient le datastore.
3. Cliquez avec le bouton droit sur la banque de données NFS ou VMFS et sélectionnez **NetApp ONTAP tools** > **Redimensionner la banque de données**.
4. Dans la boîte de dialogue Redimensionner, saisissez une nouvelle taille pour le datastore 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'objets vCenter, la section du plug-in affiche les actions prises en charge pour ONTAP tools for VMware vSphere. Des actions spécifiques sont activées en fonction du type de datastore et des privilèges actuels de l'utilisateur.

L'opération d'extension de la banque de données vVols n'est pas applicable aux banques de données vVols basées sur le système ASA r2.

**Étapes**

1. Depuis la page d'accueil du vSphere Client, sélectionnez **Hôtes et clusters**.
2. Dans le volet de navigation, sélectionnez le centre de données qui contient le datastore.
3. Cliquez avec le bouton droit sur le datastore et sélectionnez **NetApp ONTAP tools** > **Ajouter du stockage au datastore**.
4. Dans la fenêtre **Créer ou sélectionner des volumes**, vous pouvez créer de nouveaux volumes ou choisir parmi les volumes existants. Suivez les instructions à l'écran pour effectuer votre sélection.
5. Dans la fenêtre **Résumé**, vérifiez les sélections et sélectionnez **Développer**. Vous pouvez suivre la progression dans le panneau des 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 de suppression du stockage de la banque de données sur toute banque de données vVols gérée par les ONTAP tools dans vCenter Server.

Vous ne pouvez pas supprimer de 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 du datastore vVols n'est pas prise en charge pour les datastores vVols basés sur les systèmes ASA r2.

**Étapes**

1. Depuis la page d'accueil du vSphere Client, sélectionnez **Hôtes et clusters**.
2. Dans le volet de navigation, sélectionnez le centre de données qui contient le datastore.
3. Cliquez avec le bouton droit sur le datastore vVol et sélectionnez **NetApp ONTAP tools** > **Supprimer le stockage du datastore**.
4. Sélectionnez les volumes qui n'ont pas de vVols et sélectionnez **Supprimer**.

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

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

## Supprimer les banques de données dans ONTAP tools

Cette page décrit comment supprimer des datastores NFS, VMFS ou vVols à l'aide des outils ONTAP dans le serveur vCenter.

Lorsque vous supprimez un datastore, les actions suivantes sont effectuées en fonction du type de datastore :

- Le conteneur vVol est démonté.
- Si l'igroup n'est pas utilisé, ses initiateurs sont retirés de l'igroup.
- Le conteneur vVol est supprimé.
- Les volumes FlexVol® sont laissés sur la baie de stockage.

Vous pouvez supprimer le datastore uniquement si aucun vVols n'est présent sur le datastore sélectionné.

**Étapes**

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

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

   a. Dans le cas d'un datastore NFS ou VMFS, une boîte de dialogue apparaît avec la liste des machines virtuelles utilisant le datastore.

   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 datastores VMFS protégés sur les systèmes ASA r2, supprimez la protection avant de les supprimer. À partir de ONTAP 9.17.1 et ONTAP tools for VMware vSphere 10.5, vous pouvez supprimer un datastore protégé. S'il s'agit du seul datastore dans le groupe de protection, la protection du cluster hôte est supprimée automatiquement.

d. Pour les banques de données vVols, vous pouvez supprimer la banque de données uniquement s'il n'y a aucun vVols présent. La boîte de dialogue **Supprimer la banque de données** inclut une option permettant de retirer des volumes du cluster ONTAP.

e. Pour les banques de données vVols sur les systèmes ASA r2, vous ne pouvez pas supprimer les volumes sous-jacents d'ONTAP à l'aide de l'option **Supprimer la banque de données**.

3. Pour supprimer les volumes de stockage sous-jacents sur le stockage ONTAP, sélectionnez **Supprimer les volumes sur le cluster ONTAP**.

> Pour les banques de données VMFS sur un stockage ONTAP unifié faisant 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 igroups parents restent sur le système ONTAP. Les igroups enfants qui ne sont mappés à aucune LUN sont supprimés automatiquement. Les ONTAP tools effectuent un nettoyage quotidien pour supprimer les igroups parents par défaut non mappés. Supprimez manuellement les igroups parents personnalisés dans ONTAP. Les ONTAP tools ne peuvent pas réutiliser les igroups parents obsolètes.

## Vues de stockage ONTAP pour les banques de données dans ONTAP tools

Les ONTAP tools for 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 datastore.
2. Sélectionnez l'onglet **Configurer** dans le volet de droite.
3. Sélectionnez **NetApp ONTAP tools** > **ONTAP Storage**. L'affichage varie selon le type de magasin de données. Voir le tableau ci-dessous :

| Type de datastore | Informations disponibles |
|---|---|
| datastore NFS | La page **Détails du stockage** contient des informations sur les backends de stockage, les agrégats et les volumes. La page **Détails NFS** contient des données relatives au datastore NFS. |
| datastores VMFS | La page **Détails du stockage** contient des informations sur le système de stockage, les agrégats, les volumes et les zones de disponibilité du stockage (SAZ). La page **Détails de l'unité de stockage** contient des détails sur l'unité de stockage. |
| datastores vVols | Affiche la liste de tous les volumes. Vous pouvez ajouter ou supprimer du stockage depuis le panneau 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 que la machine virtuelle crée.

Cette vue s'applique aux VM disposant d'au moins un disque provenant d'un datastore vVols géré par ONTAP tools for VMware vSphere.

**Étapes**

1. Depuis le vSphere Client, accédez à la machine virtuelle.
2. Sélectionnez l'onglet **Monitor** dans le volet de droite.
3. Sélectionnez **NetApp ONTAP tools** > **Storage**. Les détails de **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 pour recevoir des notifications dans vCenter Server lorsque le volume et la capacité agrégée atteignent certains niveaux.

**Étapes :**

1. Connectez-vous au client vSphere.
2. Dans la page des raccourcis, sélectionnez **NetApp ONTAP tools** dans la section des modules d'extension.
3. Dans le volet gauche des ONTAP tools, 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**, puis sélectionnez **Enregistrer**. Vous pouvez rétablir les valeurs de seuil aux valeurs par défaut recommandées : 80 pour **Presque plein** et 90 pour **Plein**.

# Gérer les backends de stockage dans ONTAP tools

Les systèmes de stockage backend sont des systèmes que les hôtes ESXi utilisent pour le stockage des données.

## Découvrez le stockage

Vous pouvez lancer la découverte d'un système de stockage à la demande, sans attendre une découverte planifiée pour mettre à jour immédiatement les informations de stockage. Pour les configurations MetroCluster, exécutez manuellement la découverte des ONTAP tools après un basculement.

Suivez les étapes ci-dessous pour découvrir les systèmes de stockage.

**Étapes**

1. Connectez-vous au client vSphere.
2. Dans la page des raccourcis, sélectionnez **NetApp ONTAP tools** dans la section des modules d'extension.
3. Dans le volet gauche des ONTAP tools, accédez à **Storage Backends** et sélectionnez un storage backend.
4. Sélectionnez le menu à trois points verticaux et sélectionnez **Discover storage**

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

## Modifier les backends 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 de ONTAP tools Manager. Si le certificat expire dans 30 jours ou moins, ONTAP tools affiche un avertissement. Modifiez le backend de stockage et téléchargez le nouveau certificat depuis l'administrateur ONTAP.

Lorsque vous modifiez le stockage principal, ONTAP tools for VMware vSphere effectue une découverte du stockage principal afin de mettre à jour les détails du stockage.

Suivez les étapes de cette section pour modifier un backend de stockage.

1. Connectez-vous au client vSphere.
2. Dans la page des raccourcis, sélectionnez **NetApp ONTAP tools** dans la section des modules d'extension.
3. Dans le volet gauche des ONTAP tools, accédez à **Storage Backends** et sélectionnez un storage backend.
4. Sélectionnez le menu à trois points verticaux et sélectionnez **Modifier** pour modifier les identifiants ou le nom du port. Vous pouvez suivre la progression dans le panneau des tâches récentes.

Modifiez les clusters ONTAP globaux avec ONTAP tools Manager comme suit.

1. Lancez ONTAP tools Manager depuis un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.
3. Sélectionnez les systèmes de stockage dans la barre latérale.
4. Sélectionnez le Storage Backend que vous souhaitez modifier.
5. Sélectionnez le menu à trois points verticaux et sélectionnez **Modifier**.
6. Vous pouvez modifier les identifiants ou le port. Saisissez le **nom d'utilisateur** et le **mot de passe** pour modifier le backend de stockage.

## Supprimer les backends de stockage

Vous devez supprimer tous les datastores associés au stockage backend avant de le supprimer. Suivez les étapes ci-dessous pour supprimer un stockage backend.

1. Connectez-vous au client vSphere.
2. Dans la page des raccourcis, sélectionnez **NetApp ONTAP tools** dans la section des modules d'extension.
3. Dans le volet gauche des ONTAP tools, accédez à **Storage Backends** et sélectionnez un storage backend.
4. Sélectionnez le menu à trois points verticaux, puis **Supprimer**. Assurez-vous que le système de stockage ne contient aucun datastore. Vous pouvez suivre la progression dans le panneau des tâches récentes.

Vous pouvez supprimer les clusters ONTAP globaux à l'aide du Gestionnaire d'outils ONTAP.

1. Lancez ONTAP tools Manager depuis un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`

2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.
3. Sélectionnez **Storage Backends** dans la barre latérale.
4. Sélectionnez le backend de stockage que vous souhaitez supprimer
5. Sélectionnez le menu à trois points verticaux et sélectionnez **Supprimer**.

### Vue détaillée du backend de stockage

La page relative aux systèmes de stockage répertorie tous les systèmes de stockage. Vous pouvez effectuer des opérations de découverte, de modification et de suppression sur les systèmes de stockage que vous avez ajoutés, mais pas sur les SVM enfants individuelles du cluster.

Sélectionnez le cluster parent ou enfant pour afficher le résumé des composants. Pour le cluster parent, utilisez le menu déroulant Actions pour découvrir le stockage, le modifier ou supprimer le backend de stockage.

La page récapitulative fournit les informations suivantes :

- État du backend de stockage
- Informations sur la capacité
- Informations de base sur la VM
- 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 la SVM enfant, les informations sont les mêmes que pour le stockage principal parent.
- Privileges autorisés et restreints pour le stockage backend. Pour la SVM enfant, les informations sont identiques à celles du stockage backend parent. ONTAP tools affiche les privileges uniquement sur les stockages backend basés sur le cluster. Si vous ajoutez une SVM comme stockage backend, les informations relatives aux privileges ne sont pas affichées.
- La vue détaillée du cluster du système ASA r2 n'inclut pas l'onglet des niveaux locaux lorsque la propriété désagrégée est définie sur « true » pour le SVM ou le cluster.
- Pour les systèmes ASA r2 SVM, le portlet de capacité n'est pas affiché. Le portail de capacité est requis uniquement lorsque la propriété désagrégée est définie sur « true » pour la SVM ou le cluster.
- Pour les systèmes ASA r2 SVM, la section d'informations de base indique 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.

# Gérez les instances de serveur vCenter dans les outils ONTAP

Les instances de vCenter Server sont des plateformes de gestion centralisées qui vous permettent de contrôler les hôtes, les machines virtuelles et les systèmes de stockage.

### Dissocier les systèmes de stockage de l'instance du serveur vCenter

La page de liste des serveurs vCenter affiche le nombre de systèmes de stockage associés. Chaque instance de serveur vCenter a la possibilité d'être associée ou dissociée d'un système de stockage.

**Étapes**

1. Lancez ONTAP tools Manager depuis un navigateur Web :
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.
3. Sélectionnez l'instance de serveur vCenter requise dans la barre latérale.
4. Sélectionnez les points de suspension verticaux en face du serveur vCenter que vous souhaitez associer ou dissocier aux backends de stockage.
5. Sélectionnez **Dissocier le stockage backend**.

## Modifier une instance de serveur vCenter

Suivez les étapes ci-dessous pour modifier une instance de serveur vCenter.

1. Lancez ONTAP tools Manager depuis un navigateur Web :
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.
3. Sélectionnez l'instance de serveur vCenter appropriée dans la barre latérale
4. Sélectionnez les points de suspension verticaux en regard du 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 serveur vCenter

Supprimez tous les systèmes de stockage du vCenter Server avant de le supprimer.

1. Lancez ONTAP tools Manager depuis un navigateur Web :
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.
3. Sélectionnez les instances de serveur vCenter applicables dans la barre latérale
4. Sélectionnez les points de suspension verticaux en regard du serveur vCenter que vous souhaitez supprimer et sélectionnez **Supprimer**.

> Après avoir supprimé les instances de serveur vCenter, elles ne seront plus gérées par l'application.

Lorsque vous supprimez des instances de serveur vCenter dans ONTAP tools, les actions suivantes sont effectuées automatiquement :

- Le plug-in n'est pas enregistré.
- Les privilèges et les rôles des plug-ins sont supprimés.

## Renouvelez le certificat du serveur vCenter

ONTAP tools vous avertit lorsque le certificat vCenter approche de son expiration ou a expiré. Après avoir renouvelé le certificat vCenter, téléversez le nouveau certificat dans ONTAP tools en suivant les étapes ci-dessous :

1. Connectez-vous à l'interface de diagnostic à distance des ONTAP tools.
2. Obtenez le certificat vCenter renouvelé à partir de 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 en tant que fichier texte avec une `.pem` extension sur votre poste de travail.
5. Lancez ONTAP tools Manager depuis un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
6. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.
7. Sélectionnez l'instance de serveur vCenter appropriée dans la barre latérale
8. Sélectionnez les points de suspension verticaux en regard du 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 connexes**

"Configurer l’accès au diagnostic 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 Manager des outils ONTAP pour renouveler ce certificat ou le remplacer par un certificat CA personnalisé. Dans les déploiements multi-vCenter, l’utilisation de certificats CA personnalisés est requise.

**Avant de commencer**

Vous devez disposer des éléments suivants avant de commencer :

- Le nom de domaine associé à l’adresse IP virtuelle.
- Requête nslookup réussie du nom de domaine, confirmant qu’il se résout à la bonne adresse IP.
- Certificats créés avec le nom de domaine et l’adresse IP des outils ONTAP.

L’adresse IP des ONTAP tools doit correspondre à un nom de domaine complet (FQDN). Les certificats doivent contenir le même FQDN associé à l’adresse IP des ONTAP tools dans le champ sujet ou dans les noms alternatifs du sujet.

Il est impossible de passer d’un certificat signé par une autorité de certification à un certificat auto-signé.

#### Mettre à niveau le certificat des outils ONTAP

L'onglet ONTAP tools affiche des informations telles que le type de certificat (auto-signé/CA signé) et le nom de domaine. Lors du déploiement, un certificat auto-signé est généré par défaut. Vous pouvez renouveler le certificat ou le mettre à niveau vers un certificat CA.

**Étapes**

1. Lancez ONTAP tools Manager depuis un navigateur Web :
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.
3. Sélectionnez **Certificats** > **ONTAP tools** > **Renouveler** pour renouveler les certificats.

   Vous pouvez renouveler le certificat s'il a expiré ou si sa date d'expiration approche. L'option de renouvellement est disponible lorsque le type de certificat est signé par une autorité de certification (CA). Dans la fenêtre contextuelle, fournissez le certificat serveur, la clé privée, l'autorité de certification racine et les détails du certificat intermédiaire.

   Le système sera hors ligne jusqu'au renouvellement du certificat et vous serez déconnecté de l'interface ONTAP tools Manager.

4. Pour mettre à niveau le certificat auto-signé vers un certificat CA personnalisé, sélectionnez **Certificates** > **ONTAP tools** > **Upgrade to CA**.
   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 intermédiaire.
   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 à niveau le certificat.

      Le système sera hors ligne jusqu'à la fin de la mise à niveau et vous serez déconnecté de l'interface ONTAP tools Manager.

#### Mettre à niveau le certificat du fournisseur VASA

ONTAP tools for VMware vSphere est déployé avec un certificat auto-signé pour VASA Provider. Avec cela, seule une instance de serveur vCenter peut être gérée pour les datastores vVols. Lorsque vous gérez plusieurs instances de serveur vCenter et souhaitez activer la fonctionnalité vVols sur celles-ci, vous devez remplacer le certificat auto-signé par un certificat CA personnalisé.

**Étapes**

1. Lancez ONTAP tools Manager depuis un navigateur Web :
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les identifiants d'administrateur ONTAP tools for VMware vSphere que vous avez fournis lors du déploiement.
3. Sélectionnez **Certificates** > **VASA Provider** ou **ONTAP tools** > **Renew** pour renouveler les certificats.
4. Sélectionnez **Certificates** > **VASA Provider** ou **ONTAP tools** > **Upgrade to CA** pour mettre à niveau le certificat auto-signé vers un certificat d'autorité de certification 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 intermédiaire.

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 à niveau le certificat.

Le système sera hors ligne jusqu'à la fin de la mise à niveau et vous serez déconnecté de l'interface ONTAP tools Manager.

# Accédez à la console de maintenance des ONTAP tools for VMware vSphere

## Découvrez la console de maintenance des ONTAP tools

La console de maintenance pour 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 bundles 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 VMware tools depuis le serveur vCenter. Connectez-vous en utilisant le `maint` nom d'utilisateur et le 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 l' `diag` utilisateur lors de l'activation des diagnostics à distance.

Vous devez utiliser l'onglet **Résumé** de vos ONTAP tools for VMware vSphere déployés pour accéder à la console de maintenance. Lorsque vous sélectionnez , la console de maintenance démarre.

| Menu de la console | Options |
|---|---|
| Configuration de l'application | 1. Afficher le résumé de l'état du serveur<br>2. Modifier le niveau de journalisation pour les services ONTAP tools<br>3. Modifier l'indicateur de validation du certificat |
| Configuration du système | 1. Redémarrer la machine virtuelle<br>2. Arrêter la machine virtuelle<br>3. Modifier le mot de passe de l'utilisateur « maint »<br>4. Changer de fuseau horaire<br>5. Augmenter la taille du disque du jail (/jail)<br>6. Mise à niveau<br>7. Installer VMware Tools |

| | |
|---|---|
| Configuration réseau | 1. Afficher les paramètres d'adresse IP<br>2. Afficher les paramètres de recherche de nom de domaine<br>3. Modifier les paramètres de recherche du nom de domaine<br>4. Afficher les itinéraires statiques<br>5. Modifier les itinéraires statiques<br>6. Valider les modifications<br>7. Envoyer un ping à un hôte<br>8. Rétablir les paramètres par défaut |
| Assistance et diagnostics | 1. Accédez au shell de diagnostic<br>2. Activer l'accès au diagnostic à distance<br>3. Fournissez les identifiants vCenter pour la sauvegarde<br>4. Effectuer une sauvegarde |

## Configurer l'accès de diagnostic à distance pour ONTAP tools

Vous pouvez configurer ONTAP tools for VMware vSphere afin d'activer l'accès SSH pour l'utilisateur diag.

**Avant de commencer**

Activez l'extension VASA Provider pour votre instance de serveur vCenter.

**À propos de cette tâche**

L'utilisation de SSH pour accéder au compte utilisateur diag présente les limitations 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'un des événements suivants se produit :
  - Le délai expire.

    La session de connexion expire à minuit le lendemain.
  - Vous vous connectez à nouveau en tant qu'utilisateur diag via SSH.

**Étapes**

1. Depuis le serveur vCenter, ouvrez une console pour accéder au fournisseur VASA.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Saisissez `4` pour sélectionner **Assistance et diagnostics**.
4. Appuyez sur `2` Entrée pour sélectionner **Activer l'accès aux diagnostics à distance**.
5. Saisissez `y`dans la boîte de dialogue de 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 de procéder à la mise à niveau.

**Avant de commencer**

Activez l'extension VASA Provider pour votre instance de serveur vCenter.

**À propos de cette tâche**

Répétez cette procédure sur chaque nœud avant la mise à niveau.

**Étapes**

1. Depuis le serveur vCenter, ouvrez une console pour accéder au fournisseur VASA.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Appuyez sur `4` pour sélectionner Assistance et diagnostics.
4. Appuyez sur `1` Entrée pour sélectionner Accéder à l'interface de diagnostic.
5. Saisissez `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 du serveur vCenter à l'aide de la console de maintenance.

**Avant de commencer**

Vous devez disposer d'identifiants de connexion utilisateur de maintenance.

**À propos de cette tâche**

Si vous avez modifié les informations d'identification du serveur vCenter après le déploiement, mettez-les à jour en suivant cette procédure.

**Étapes**

1. Depuis le serveur vCenter, ouvrez une console pour accéder au fournisseur VASA.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Appuyez sur `2` pour sélectionner le menu de configuration système.
4. Saisissez `8` pour modifier les identifiants vCenter.

## Modifier l'indicateur de validation du certificat dans ONTAP tools

Par défaut, le paramètre de validation des certificats est activé (valeur « true »). Vous pouvez définir le paramètre de validation des certificats du backend de stockage ONTAP sur false si vous devez contourner les vérifications des certificats SAN. Ce paramètre ne s'applique pas aux certificats vCenter Server.

**Avant de commencer**

Vous devez disposer d'identifiants de connexion utilisateur de maintenance.

**Étapes**

1. Depuis le vCenter Server, ouvrez une console vers ONTAP tools.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Appuyez sur `1` pour sélectionner le menu **Configuration de l'application**.
4. Saisissez `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. Saisissez « y » pour activer/désactiver le drapeau ou « n » pour annuler.

Lorsque vous activez le paramètre de validation des certificats (défini sur true), ONTAP tools vérifie que tous les backends de stockage utilisent des certificats avec un Subject Alternative Name (SAN). Si un backend utilise un certificat sans SAN, vous ne pouvez pas activer la validation des certificats. Avant d'activer ce paramètre, vérifiez que tous les backends de stockage utilisent des certificats basés sur SAN. Si vous désactivez le paramètre de validation des certificats (défini sur false), ONTAP tools ignore la validation des certificats pour tous les backends de stockage configurés.

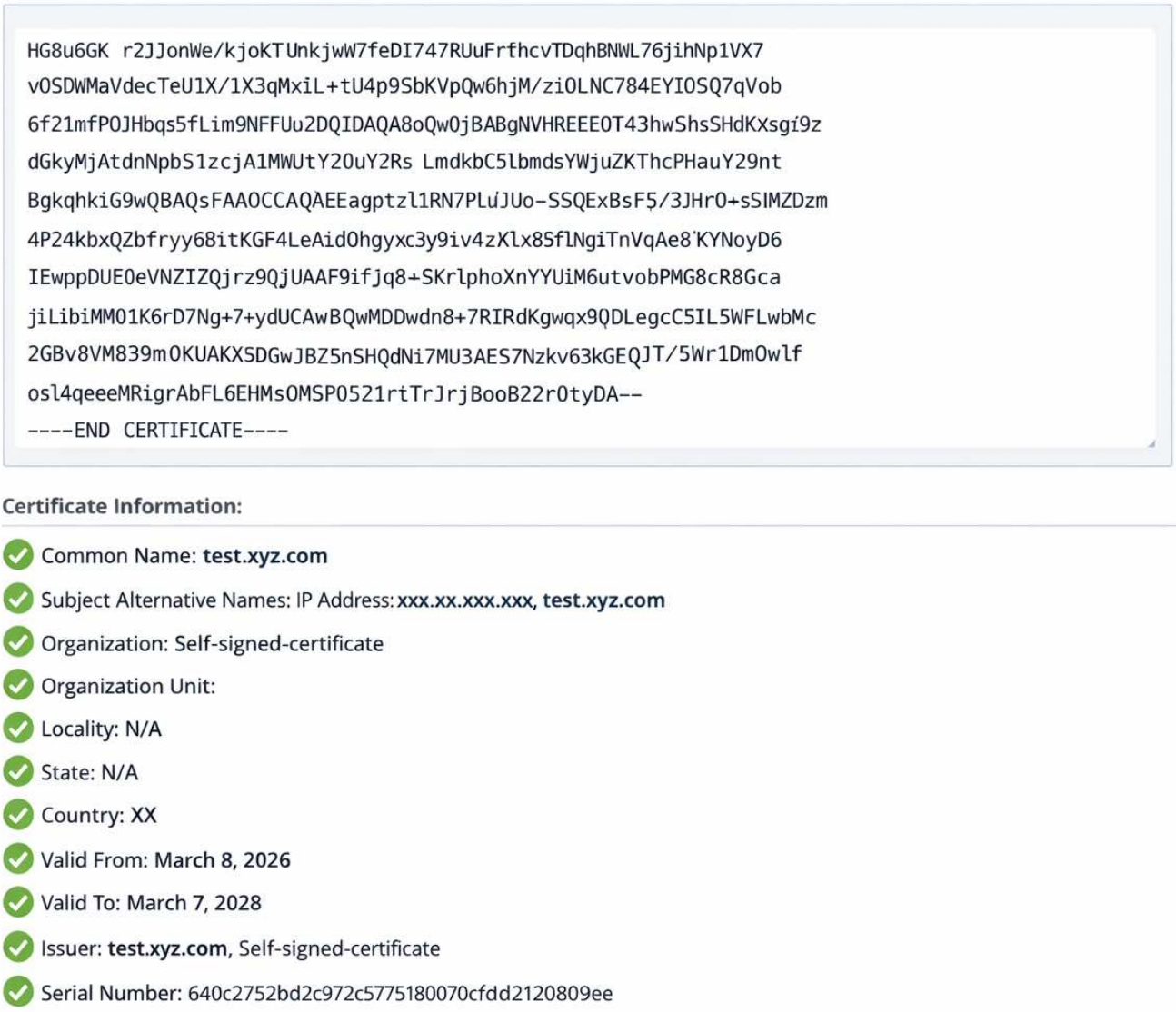
**Vérifiez les certificats basés sur SAN pour les backends de stockage**

Pour garantir une communication sécurisée et une validation correcte, vérifiez que tous les storage backends utilisent des certificats basés sur SAN :

1. Vérifiez que le certificat de gestion ONTAP comprend une entrée Subject Alternative Name (SAN).
2. Confirmez que les entrées SAN correspondent à l'adresse IP de gestion ONTAP ou au nom DNS, ou aux deux.
3. Assurez-vous que les détails utilisés pour l'onboarding ONTAP correspondent à l'adresse IP ou au nom DNS dans l'entrée SAN du certificat.

Le respect de ces étapes permet d'éviter les problèmes de validation des certificats et garantit que le système ONTAP est intégré de manière sécurisée.

L'exemple de certificat suivant présente les informations décodées :




# Rapports des 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 le rapport sur les machines virtuelles et les datastores.

Le rapport « Machines virtuelles » affiche la liste des machines virtuelles détectées (doivent posséder au moins un disque provenant de datastores de stockage basés sur ONTAP) avec des indicateurs de performance. Lorsque vous développez l'enregistrement de la machine virtuelle, l'interface affiche toutes les informations relatives au datastore liées aux disques.

Le rapport sur les banques de données répertorie les banques de données découvertes ou reconnues par ONTAP tools for VMware vSphere utilisant tout stockage ONTAP, avec des indicateurs de performance.

Vous pouvez utiliser l'option Gérer les colonnes pour masquer ou afficher différentes colonnes.

# Gérer les machines virtuelles

## Considérations relatives à la migration et au clonage de machines virtuelles pour ONTAP tools

ONTAP tools for VMware vSphere prennent en charge tous les principaux types de migration de machines virtuelles, y compris la migration de calcul uniquement (vMotion), la migration de stockage uniquement (Storage vMotion) et la migration combinée de calcul et de stockage sur l'ensemble des datastores. Ce document présente les points clés à prendre en compte et les bonnes pratiques pour garantir la réussite de la migration et du clonage des machines virtuelles, quel que soit le type de datastore sous-jacent.

### Migrer les machines virtuelles protégées

Vous pouvez migrer les machines virtuelles protégées vers :

- Le même datastore sur un hôte ESXi différent
- Un autre datastore compatible sur le même hôte ESXi
- Un autre datastore compatible sur un autre hôte ESXi

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 sur le même stockage, le fichier de métadonnées du volume FlexVol sous-jacent ne sera pas modifié.

Pour plus d'informations sur la migration des machines virtuelles, reportez-vous à la documentation Broadcom : "Broadcom Documentation technique".

### Cloner des machines virtuelles protégées

Vous pouvez cloner des machines virtuelles protégées vers les emplacements suivants :

- Le même conteneur du même FlexVol volume utilisant un groupe de réplication

  Le fichier de métadonnées du même volume FlexVol est mis à jour avec les détails de la machine virtuelle clonée.

- Le même conteneur d'un volume FlexVol différent utilisant un groupe de réplication

  Dans le volume FlexVol où est placée la machine virtuelle clonée, le fichier de métadonnées est mis à jour avec les détails de la machine virtuelle clonée.

- Un conteneur différent ou un datastore vVols

  Dans le volume FlexVol où est placée la machine virtuelle clonée, le fichier de métadonnées est mis à jour avec les détails de la machine virtuelle.

VMware ne prend actuellement pas en charge les machines virtuelles clonées sur un modèle de VM.

Il est possible de cloner un clone d'une machine virtuelle protégée.

Consultez la documentation Broadcom: "Création d'une machine virtuelle pour le clonage" pour plus de détails.

**instantanés de machines virtuelles**

ONTAP tools prend en charge les instantanés de machines virtuelles via les flux de travail VMware standard. Les instantanés sont des points de restauration temporaires destinés à des cas d'utilisation tels que les tests et la préparation de correctifs. Ils ne remplacent pas la sauvegarde ni la protection des données basée sur la réplication. L'exécution prolongée d'une machine virtuelle sur un instantané peut entraîner une instabilité et une perte de données.

Vous pouvez créer des instantanés cohérents en cas de panne (instantanés sans état de la mémoire, permettant de redémarrer la machine virtuelle dans un état cohérent) sur tous les types de datastores pris en charge. Les instantanés mis au repos, qui utilisent VMware Tools pour vider les données en mémoire sur le disque avant la capture, sont également pris en charge. Pour une présentation des types d'instantanés et de leur comportement, consultez "Aperçu des instantanés de machines virtuelles dans vSphere".

> Les instantanés mémoire capturent l'état de la mémoire en cours d'exécution et suspendent temporairement la machine virtuelle. Ils ne sont pas pris en charge dans les workflows des outils ONTAP. Si une machine virtuelle possède un instantané mémoire, vous devez le supprimer avant que la machine virtuelle puisse être incluse dans un groupe de cohérence ou une relation de cluster hôte gérée par les outils ONTAP.

Sur les systèmes de stockage ASA r2, le comportement des snapshots de machines virtuelles diffère de celui des autres types de stockage. Les snapshots sont en lecture seule. Lorsque vous mettez sous tension la machine virtuelle, VASA Provider crée un LUN à partir du snapshot en lecture seule et active les IOPS. Lorsque vous mettez hors tension la machine virtuelle, VASA Provider supprime le LUN et désactive les IOPS.

Pour plus d'informations sur la gestion des instantanés de machines virtuelles, reportez-vous à la documentation Broadcom "Broadcom Documentation technique".

## Migrer des machines virtuelles vers des datastores vVols dans ONTAP tools

Vous pouvez migrer des machines virtuelles depuis des datastores NFS et VMFS vers des datastores Virtual Volumes (vVols) afin de bénéficier d'une gestion des VM basée sur des stratégies et d'autres fonctionnalités vVols. Les datastores vVols vous permettent de répondre à des exigences de charge de travail accrues.

**Avant de commencer**

Assurez-vous que VASA Provider n'est pas exécuté sur les machines virtuelles que vous prévoyez de migrer. Si vous migrez une machine virtuelle exécutant VASA Provider vers un datastore vVols, vous ne pourrez effectuer aucune opération de gestion, y compris la mise sous tension des machines virtuelles qui se trouvent sur des datastores vVols.

**À propos de cette tâche**

Lorsque vous migrez d'un datastore NFS ou VMFS vers un datastore vVols, le serveur vCenter utilise les API vStorage pour l'intégration de baies (VAAI) lors du déplacement de données depuis des datastores VMFS, mais pas depuis un fichier VMDK NFS. Les déchargements VAAI réduisent généralement la charge sur l'hôte.

**Étapes**

1. Cliquez avec le bouton droit sur la machine virtuelle que vous souhaitez migrer et sélectionnez **Migrer**.
2. Sélectionnez **Modifier le stockage uniquement** et sélectionnez ensuite **Suivant**.
3. Sélectionnez un format de disque virtuel, une stratégie de stockage de machine virtuelle et un vVol datastore correspondant aux caractéristiques du datastore 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. Désenregistrez le plug-in en allant dans https://OTV_IP:8143/Register.html
2. Vérifiez que le plug-in n'est plus disponible sur le serveur vCenter.
3. Arrêtez les ONTAP tools for VMware vSphere VM.
4. Supprimez les ONTAP tools for 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.

### Connectez un disque de données à une machine virtuelle

Attachez un disque de données à une machine virtuelle pour ajouter plus de stockage.

**Étapes**

1. Connectez-vous au client vSphere.
2. Faites un clic 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 se trouve le disque.
5. Sélectionnez le disque que vous souhaitez attacher et sélectionnez le bouton **OK**.

**Résultat**

Le disque dur apparaît dans la liste des périphériques matériels virtuels.

### Détachez 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. Faites un clic droit sur une machine virtuelle dans l'inventaire et sélectionnez **Modifier les paramètres**.
3. Déplacez votre pointeur sur le disque et sélectionnez **Retirer**.

> Le disque est retiré de la machine virtuelle. Si d'autres machines virtuelles partagent le disque, les fichiers de ce dernier ne sont pas supprimés.

**Informations connexes**

"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

Lorsque ONTAP tools for VMware vSphere est lancé pour la première fois dans le client vSphere, il découvre 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 sous tension et connectés.
- Assurez-vous que toutes les machines virtuelles de stockage (SVM) à découvrir sont en cours d'exécution et que chaque nœud de cluster dispose d'au moins une interface logique de données (LIF) configurée pour le protocole de stockage utilisé (NFS ou iSCSI).

**À propos de cette tâche**

Vous pouvez découvrir de nouveaux systèmes de stockage ou mettre à jour les systèmes existants pour obtenir les informations les plus récentes sur leur capacité et leur configuration. Vous pouvez également modifier les identifiants ONTAP tools for VMware vSphere pour l'accès au système de stockage.

Lors de la découverte des systèmes de stockage, ONTAP tools for VMware vSphere collecte des informations à partir des hôtes ESXi gérés par l'instance du serveur vCenter.

**Étapes**

1. Depuis la page d'accueil du vSphere Client, sélectionnez **Hôtes et clusters**.
2. Cliquez avec le bouton droit sur le centre de données requis et sélectionnez **NetApp ONTAP tools** > **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 le statut `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 le statut `Authentication Failure`.

Une fois le processus de découverte terminé, effectuez les actions suivantes :

- Utilisez ONTAP tools for VMware vSphere pour configurer les paramètres de l'hôte ESXi pour les hôtes qui affichent l'icône d'alerte dans la colonne des paramètres de l'adaptateur, la colonne des paramètres MPIO ou la colonne des paramètres NFS.
- Veuillez fournir les identifiants du système de stockage.

# Modifier les paramètres de l'hôte ESXi à l'aide des outils ONTAP

Utilisez le tableau de bord des ONTAP tools dans VMware vSphere pour identifier les problèmes de configuration, sélectionner les hôtes ESXi, examiner les paramètres recommandés par NetApp et les appliquer.

**Avant de commencer**

Le portlet Systèmes hôtes ESXi affiche les problèmes liés aux paramètres de l'hôte ESXi. Sélectionnez un problème pour afficher le nom de l'hôte ou l'adresse IP.

**Étapes**

1. Connectez-vous au client vSphere.
2. Dans la page des raccourcis, sélectionnez **NetApp ONTAP tools** dans la section des modules d'extension.
3. Accédez au portlet **Conformité de l'hôte ESXi** dans la vue d'ensemble (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 NetApp et sélectionnez **Suivant**.

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

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

**Informations connexes**

"Configurer les paramètres de l'hôte ESXi"

# Gérer les mots de passe

## Modifier le mot de passe du gestionnaire ONTAP tools

Vous pouvez modifier le mot de passe administrateur à l'aide du Gestionnaire d'outils ONTAP.

**Étapes**

1. Lancez ONTAP tools Manager depuis 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 **administrateur** en haut à droite de l'écran et sélectionnez **Changer 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'interface utilisateur affiche les exigences relatives au mot de passe.
5. Sélectionnez **Modifier** pour appliquer les modifications.

## Réinitialiser le mot de passe du gestionnaire d'outils ONTAP

Si vous oubliez le mot de passe du gestionnaire ONTAP tools, vous pouvez rétablir l'accès administrateur à l'aide d'un jeton de réinitialisation généré à partir de la console de maintenance ONTAP tools for VMware vSphere.

**Étapes**

1. Ouvrez un navigateur Web et accédez à `https://<ONTAPtoolsIP>:8443/virtualization/ui/` pour accéder à ONTAP tools Manager.
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 de la console de maintenance des ONTAP tools for VMware vSphere :
   a. Connectez-vous au serveur vCenter et ouvrez la console de maintenance.
   b. Appuyez sur Entrée `2` pour sélectionner **Configuration système**.
   c. Appuyez sur `3` Entrée pour sélectionner **Modifier le mot de passe de l'utilisateur 'maint'**.
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 SRA et VASA Provider auprès du serveur vCenter en utilisant 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 ONTAP tools.
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.

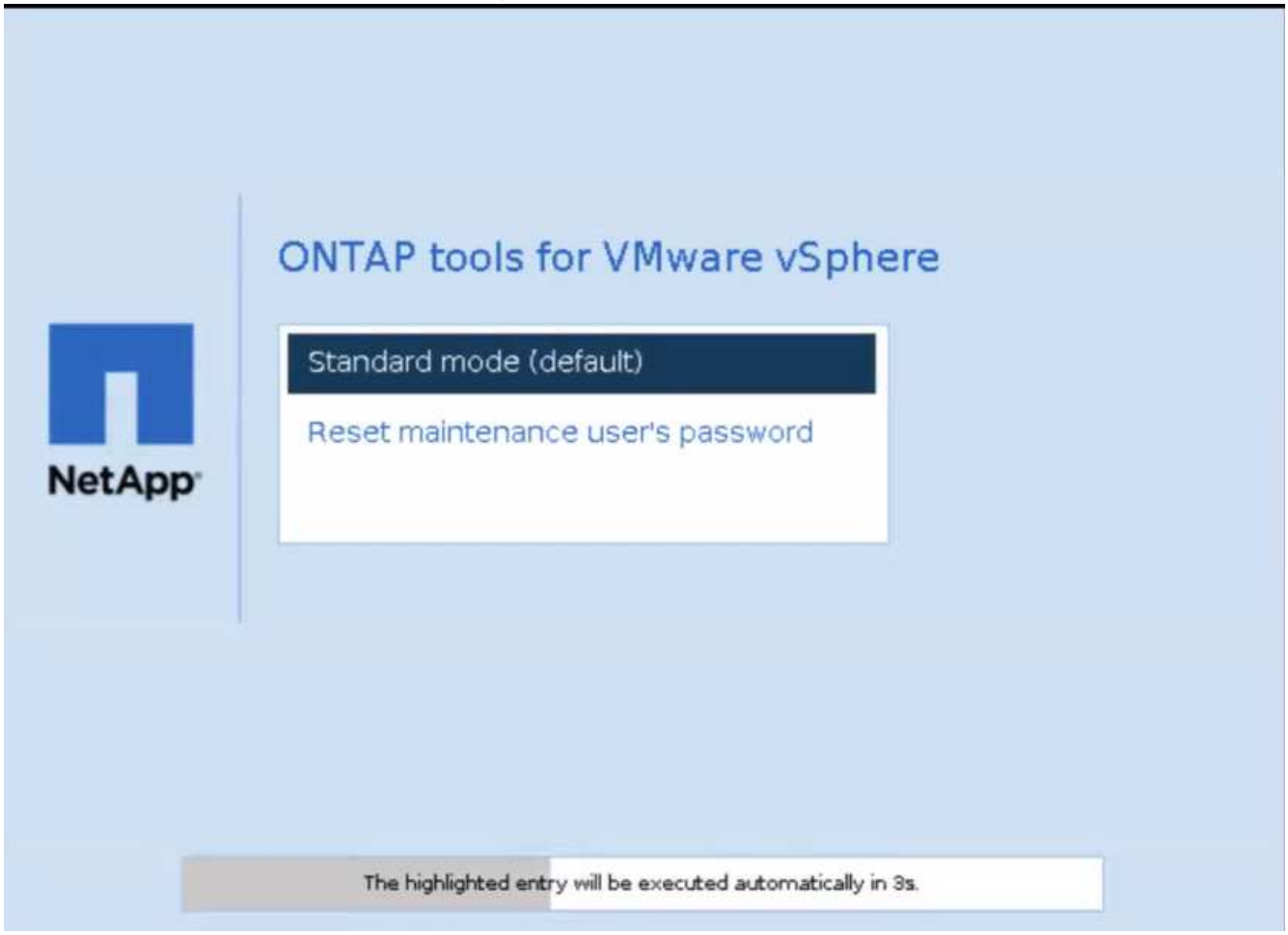
## Réinitialiser le mot de passe de la console de maintenance des ONTAP tools

Lors du redémarrage du système d'exploitation invité, le menu GRUB propose une option pour réinitialiser le mot de passe de l'utilisateur de la console de maintenance. Utilisez cette option pour mettre à jour le mot de passe de l'utilisateur de la console de maintenance sur la VM. Après la réinitialisation du mot de passe, la VM redémarre pour définir le nouveau mot de passe. Dans un scénario de déploiement HA, après le redémarrage de la VM, le mot de passe est automatiquement mis à jour sur les deux autres VMs.

Pour le déploiement HA des ONTAP tools for VMware vSphere, vous devez changer le mot de passe de l'utilisateur de la console de maintenance sur le nœud de gestion ONTAP tools, qui est node1.

**Étapes**

1. Connectez-vous à votre serveur vCenter
2. Faites un clic droit sur la machine virtuelle et sélectionnez **Alimentation** > **Redémarrer le système d'exploitation invité**. Lors du redémarrage du système, l'écran suivant s'affiche :




Vous avez 5 secondes pour choisir votre option. Appuyez sur n'importe quelle touche pour interrompre le processus et figer 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 disposez de trois tentatives. Le système redémarre après que vous avez saisi avec succès le nouveau mot de passe.
5. Appuyez sur **Entrée** pour continuer. Le système met à jour le mot de passe de la machine virtuelle.

Le même menu GRUB s'affiche au démarrage de la machine virtuelle. Cependant, vous devez utiliser l'option de réinitialisation du mot de passe uniquement avec l'option **Redémarrer le système d'exploitation invité**.

# Gérer la protection du cluster hôte

## Modifier un cluster d'hôtes protégé dans ONTAP tools

Vous pouvez modifier les paramètres de protection d'un cluster d'hôtes en une seule opération. 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.
- Modifiez une relation SnapMirror existante.

> Vous devez effectuer une découverte du stockage après avoir créé, modifié ou supprimé une protection pour un cluster d'hôtes afin que les modifications soient prises en compte. Si vous n'effectuez pas la découverte du stockage, les modifications seront prises en compte après le déclenchement de la découverte périodique du stockage.

### Surveiller la protection du cluster hôte

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 **NetApp ONTAP tools** > **Protection** > **Relations de clusters hôtes**.

   La colonne de protection affiche une icône indiquant l'état de la protection.

3. Placez le pointeur de votre souris sur l'icône pour afficher plus de détails.

### Ajouter 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 soit
   a. Accédez à **NetApp ONTAP tools** > **Protection** > **Relations de clusters hôtes**, sélectionnez le menu à trois points à côté du cluster et sélectionnez **Modifier** ou
   b. Cliquez avec le bouton droit sur un cluster hôte et sélectionnez **NetApp ONTAP tools** > **Protect Cluster**.
3. Si vous créez un datastore dans l'interface utilisateur vCenter, il apparaît comme non protégé. Vous pouvez consulter tous les datastores du cluster et leur état de protection dans une boîte de dialogue. Sélectionnez le bouton **Protéger** pour activer la protection.

Après avoir créé un datastore dans l'interface utilisateur du serveur vCenter, sélectionnez **Discover** sur la page d'aperçu pour afficher le datastore comme candidat à la protection dans le cluster hôte. L'état de protection passe à protégé après la prochaine découverte périodique de protection.

4. Si vous ajoutez un nouvel hôte ESXi, l'état de protection s'affiche comme partiellement protégé. Sélectionnez le menu à trois points sous les paramètres SnapMirror et sélectionnez **Modifier** pour définir la proximité du nouvel hôte ESXi 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 System Manager ou la CLI sur le SVM cible.

5. Après avoir effectué les modifications, sélectionnez **Enregistrer**.
6. Vous pouvez voir les modifications dans la fenêtre **Protect Cluster**.

ONTAP tools crée une tâche vCenter, et vous pouvez suivre sa progression dans le panneau **Tâches récentes**.

### Ajouter une nouvelle relation SnapMirror

**Étapes**

1. Connectez-vous au client vSphere.
2. Pour modifier les propriétés d'un cluster protégé, vous pouvez soit
   a. Accédez à **NetApp ONTAP tools** > **Protection** > **Relations de cluster d'hôtes**, sélectionnez le menu à trois points en face du cluster et sélectionnez **Modifier** ou
   b. Cliquez avec le bouton droit sur un cluster hôte et sélectionnez **NetApp ONTAP tools** > **Protect Cluster**.
3. Sélectionnez **Ajouter une relation**.
4. Ajoutez une nouvelle relation en tant que type de stratégie **asynchrone** ou **AutomatedFailOverDuplex**.
5. Sélectionnez **Protect**.

   Vous pouvez voir les modifications dans la fenêtre **Protect Cluster**.

ONTAP tools crée une tâche vCenter, et vous pouvez suivre sa progression dans le panneau **Tâches récentes**.

### Supprimez une relation SnapMirror existante

Pour supprimer une relation SnapMirror asynchrone, assurez-vous que le SVM ou le cluster du site secondaire est ajouté comme backend de stockage dans ONTAP tools for VMware vSphere. Vous ne pouvez pas supprimer toutes les relations SnapMirror en une seule fois. La suppression d'une relation entraîne également la suppression de la relation correspondante du cluster ONTAP. Lorsque vous supprimez une relation Automated Failover Duplex SnapMirror, le système dissocie les datastores 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 analyse à nouveau le site secondaire pour supprimer le LUN non mappé en tant que chemin actif depuis les hôtes.

**Étapes**

1. Connectez-vous au client vSphere.
2. Pour modifier les propriétés d'un cluster protégé, vous pouvez soit
   a. Accédez à **NetApp ONTAP tools** > **Protection** > **Relations de cluster d'hôtes**, sélectionnez le menu à trois points en face du cluster et sélectionnez **Modifier** ou
   b. Cliquez avec le bouton droit sur un cluster hôte et sélectionnez **NetApp ONTAP tools** > **Protect Cluster**.
3. Sélectionnez le menu à trois points sous les paramètres SnapMirror et sélectionnez **Supprimer**.
   - Si vous supprimez une relation asynchrone basée sur un type de stratégie d'un cluster d'hôtes protégé, vous devez supprimer manuellement les éléments de stockage du cluster de stockage tertiaire. Les éléments de stockage comprennent les groupes de cohérence, les volumes (pour les systèmes ONTAP), les unités de stockage (LUN/espaces de noms) et les 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 depuis l'interface.
   - Si vous supprimez une relation basée sur une stratégie de basculement automatique duplex (AFD) et que le groupe de cohérence est désormais hiérarchique pour les sauvegardes au niveau applicatif, un avertissement concernant l'impact sur les sauvegardes s'affiche. 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.

ONTAP tools crée une tâche vCenter, et vous pouvez suivre sa progression dans le panneau **Tâches récentes**.

### Modifier une relation SnapMirror existante

Pour modifier une relation SnapMirror asynchrone, assurez-vous que le SVM ou le cluster du site secondaire est ajouté comme backend de stockage dans ONTAP tools for VMware vSphere. Pour les relations SnapMirror Automated Failover Duplex, vous pouvez mettre à jour la proximité des hôtes pour les configurations uniformes ou l'accès des hôtes pour les configurations non uniformes. Le changement entre les types de stratégie Asynchronous et Automated Failover Duplex 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 soit
   a. Accédez à **NetApp ONTAP tools** > **Protection** > **Relations de cluster d'hôtes**, sélectionnez le menu à trois points en face du cluster et sélectionnez **Modifier** ou
   b. Cliquez avec le bouton droit sur un cluster hôte et sélectionnez **NetApp ONTAP tools** > **Protect 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 **Tâches récentes**.

### Supprimer la protection du cluster hôte dans ONTAP tools

Lorsque vous supprimez la protection du cluster hôte, les datastores ne sont plus protégés.

**Étapes**

1. Pour afficher la liste des clusters d'hôtes protégés, accédez à **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**.

   Sur cette page, vous pouvez surveiller les clusters d'hôtes protégés, l'état de protection, la relation SnapMirror et le statut. Sélectionnez les 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 trois points à côté du cluster, puis sélectionnez **Supprimer la protection**.
   - Si vous supprimez la protection d'un cluster hôte avec uniquement une relation SnapMirror asynchrone, vous devez supprimer manuellement les éléments de stockage. Les éléments de stockage comprennent les groupes de cohérence, les volumes (pour le système ONTAP), les unités de stockage (LUN) et les snapshots.
   - Si vous supprimez la protection d'un cluster hôte avec uniquement une relation de stratégie SnapMirror basée sur un basculement automatique en duplex et un groupe de cohérence non hiérarchique, vous pouvez supprimer les éléments de stockage associés sur le stockage secondaire directement depuis le même écran.
   - Si vous supprimez la protection d'un cluster hôte comportant à la fois des stratégies SnapMirror et un groupe de cohérence hiérarchique pour les sauvegardes, un avertissement concernant l'impact sur les sauvegardes s'affiche. Confirmez pour continuer. Après confirmation, supprimez les éléments de stockage associés sur le stockage secondaire. Si vous ne procédez pas au nettoyage, les éléments de stockage resteront sur le site secondaire.

# Récupérez la configuration des outils ONTAP

À partir de ONTAP tools for VMware vSphere 10.5, la fonction de sauvegarde est activée par défaut.

Le datastore où vous déployez les ONTAP tools for VMware vSphere machines virtuelles stocke les fichiers de sauvegarde. Un dossier nommé d'après l'adresse IP des ONTAP tools (les points remplacés par des tirets bas et suffixé par *OTV_backup*) conserve les deux fichiers de sauvegarde les plus récents (*OTV_backup_1.tar.enc* et *OTV_backup_2.tar.enc*) ainsi qu'un fichier d'information (*OTV_backup_info.txt*) contenant le nom de la dernière sauvegarde.

Assurez-vous que la nouvelle machine virtuelle utilise la même adresse IP des ONTAP tools et corresponde à la configuration système initiale, y compris les services activés, la taille du nœud et le mode HA.

**Étapes**

1. Téléchargez les fichiers de sauvegarde depuis le datastore de la machine virtuelle d'origine vers votre système local.
   a. Accédez à la section stockage et choisissez le datastore 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 initial.
3. Depuis le vCenter Server, ouvrez la console de maintenance.
4. Connectez-vous en tant qu'utilisateur de maintenance.
5. Saisissez `4` pour sélectionner **Assistance et diagnostics**.
6. Appuyez sur `2`Entrée 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. Consultez le fichier *OTV_backup_info.txt* pour identifier la sauvegarde la plus récente.
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 à l'interface 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, ONTAP tools restaure les services et les objets vCenter.

# Désinstaller les outils ONTAP

## La désinstallation des ONTAP tools for VMware vSphere supprime toutes les données dans les outils.

**Étapes**

1. Supprimez ou déplacez toutes les machines virtuelles des datastores gérés par ONTAP tools for VMware vSphere.
   - Pour supprimer les machines virtuelles, reportez-vous à "Supprimez et réenregistrez les machines virtuelles et les modèles de machines virtuelles"
   - Pour les déplacer vers un datastore non géré, reportez-vous à "Broadcom Documentation technique".
2. "Supprimer les datastores" créé sur ONTAP tools for VMware vSphere.
3. Si vous avez activé le fournisseur VASA, sélectionnez **Paramètres** > **Paramètres du fournisseur VASA** > **Désinscrire** dans ONTAP tools pour désinscrire les fournisseurs VASA de tous les serveurs vCenter.
4. Dissociez tous les systèmes de stockage de l'instance du serveur vCenter. Reportez-vous à "Dissocier les systèmes de stockage de l'instance du serveur vCenter".

5. Supprimez tous les backends de stockage. Reportez-vous à "Gérer les backends de stockage".
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 **Adaptateurs de réplication de stockage**.
   c. Sélectionnez la carte SRA appropriée, puis dans le menu déroulant, sélectionnez **Supprimer**.
   d. Confirmez que vous connaissez les résultats de la suppression de l'adaptateur et sélectionnez **Supprimer**.
7. Supprimez les instances de serveur vCenter intégrées à ONTAP tools for VMware vSphere. Consultez "Gérer les instances de serveur vCenter".
8. Mettez hors tension les machines virtuelles ONTAP tools for VMware vSphere depuis le serveur vCenter et supprimez les machines virtuelles.

**Quelle est la prochaine étape ?**

"Supprimer les volumes FlexVol"

# Supprimez les volumes FlexVol après la désinstallation des ONTAP tools

Lorsque vous utilisez un cluster ONTAP dédié pour le déploiement d'ONTAP tools for VMware, cela crée de nombreux volumes FlexVol inutilisés. Après avoir supprimé ONTAP tools for VMware vSphere, vous devez supprimer les volumes FlexVol afin d'éviter d'éventuels impacts sur les performances.

**Étapes**

1. Déterminez le type de déploiement des ONTAP tools for VMware vSphere à partir de la machine virtuelle du nœud de gestion des ONTAP tools. 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 describe persistentvolumes | grep internalName | awk -F'=' '{print $2}'*
3. Supprimez les machines virtuelles du vCenter Server. Consultez "Supprimez et réenregistrez les machines virtuelles et les modèles de machines virtuelles".
4. Supprimez les volumes FlexVol. Consultez "Supprimer un volume FlexVol". Saisissez le nom exact du volume FlexVol dans la commande CLI pour supprimer un volume.
5. Supprimez les igroups SAN du système de stockage ONTAP en cas de déploiement iSCSI. Consultez "Afficher et gérer les initiateurs SAN et les igroups".

# Mettre à niveau ONTAP tools for VMware vSphere

## Mettez à niveau ONTAP tools for VMware vSphere 10.x vers 10.5

Vous pouvez effectuer une mise à niveau depuis ONTAP tools for VMware vSphere 10.3 ou 10.4 vers 10.5. Cependant, pour effectuer une mise à niveau depuis ONTAP tools 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 procéder à la mise à niveau vers 10.5.

- Pour les systèmes ASA r2, assurez-vous de mettre à niveau ONTAP tools for VMware vSphere vers la version 10.5 et ONTAP vers la version 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 faible RPO ou une restauration par snapshot pour rétablir la configuration. Pour ONTAP tools for VMware vSphere 10.2 et versions antérieures, utilisez un RPO nul pour rétablir 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 échouera.
- Assurez-vous de disposer d'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 | Processeur (cœur) par nœud | Mémoire (Go) par nœud | Espace disque (Go) par nœud | Total CPU (cœurs) | Mémoire (Go) | Espace disque total (Go) |
|---|---|---|---|---|---|---|
| Non-HA de petite taille | 9 | 18 | 350 | 9 | 18 | 350 |
| Moyen non-HA | 13 | 26 | 350 | 13 | 26 | 350 |
| HA Small | 9 | 18 | 350 | 27 | 54 | 1050 |
| HA Moyen | 13 | 26 | 350 | 39 | 78 | 1050 |
| HA Large | 17 | 34 | 350 | 51 | 102 | 1050 |

- Assurez-vous que la fonction de branchement à chaud du CPU et de la RAM est activée.
- Activez la sauvegarde à faible RPO et assurez-vous qu'une sauvegarde soit visible dans l'interface vCenter Client. Téléchargez le dossier de sauvegarde avant la mise à niveau.
- Il est recommandé d'effectuer une sauvegarde avec un RPO faible. Cependant, dans un déploiement non HA, vous pouvez prendre un instantané au repos de la machine virtuelle ONTAP tools avant la mise à niveau.

Consultez "Modifier les paramètres de sauvegarde" et "Récupérez la configuration des outils ONTAP" pour plus d'informations sur la sauvegarde et la restauration.

**Étapes**

1. Téléversez l'ISO de mise à niveau des ONTAP tools for VMware vSphere dans la bibliothèque de contenu.
2. Sur la page de la machine virtuelle principale, 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 de modification des paramètres 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. Depuis le vCenter Server, ouvrez une console vers ONTAP tools.
6. Connectez-vous en tant qu'utilisateur de maintenance.
7. Saisissez **2** pour sélectionner le menu **Configuration système**.
8. Saisissez **6** 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 les outils ONTAP sont hébergés.

   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 nécessaires au déploiement du modèle OVF. Pour plus de détails, consultez les rôles listés dans "Rôles inclus avec ONTAP tools for VMware vSphere 10".

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

   Lors de la mise à niveau, si l'un des certificats du système de stockage intégré ne comporte pas d'entrée Subject Alternative Name (SAN), vous recevrez une invite indiquant le SAN manquant. Si vous choisissez de poursuivre sans valider le SAN, la mise à niveau continuera, mais cela n'est pas recommandé en raison des risques potentiels pour la sécurité.

10. Lors de la mise à niveau, les actions suivantes sont effectuées automatiquement :
    a. Le certificat de passerelle est renouvelé pour une période de validité d'un an. Lorsque vous supprimez l'ancien adaptateur SRA et chargez 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 ONTAP tools
    d. La sauvegarde est activée

**Et ensuite**

Après la mise à niveau vers ONTAP tools for VMware vSphere 10.5 :

- Surveillez les alertes système et prévoyez de renouveler le certificat de la passerelle avant son expiration dans un an.

- Supprimez l'adaptateur SRA des ONTAP tools 10.4 ou 10.3 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 jour, vous pouvez :

- Désactivez les services depuis l'interface utilisateur du gestionnaire
- Passer d'une configuration non-HA à une configuration HA
- Faites évoluer une petite configuration non-HA vers une configuration moyenne non-HA, ou vers une configuration moyenne ou grande HA.

**Informations connexes**

"Migrez des ONTAP tools for VMware vSphere 9.xx vers 10.5"

# Codes d'erreur de mise à niveau des ONTAP tools

Vous pourriez rencontrer des codes d'erreur lors de l'opération de mise à niveau des ONTAP tools for VMware vSphere. Les codes d'erreur comportent cinq chiffres, les deux premiers représentant le script ayant rencontré le problème et les trois derniers représentant le workflow spécifique dans ce script.

Tous les journaux d'erreurs sont enregistrés dans le fichier ansible-perl-errors.log afin de 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 affichés sur cette page sont fournis à titre indicatif uniquement. Veuillez contacter l'équipe d'assistance si l'erreur persiste ou si aucune solution n'est mentionnée.

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

| Code d'erreur | Nom du script |
|---|---|
| 00 | firstboot-network-config.pl, mode déploiement |
| 01 | firstboot-network-config.pl, mode mise à niveau |
| 02 | firstboot-inputs-validation.pl |
| 03 | firstboot-deploy-otv-ng.pl, déploiement, HA |
| 04 | firstboot-deploy-otv-ng.pl, déploiement, non-HA |
| 05 | firstboot-deploy-otv-ng.pl, reboot |
| 06 | firstboot-deploy-otv-ng.pl, mise à niveau, HA |
| 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 spécifique survenue dans le script :

| Code d’erreur de mise à niveau | Flux de travail | Résolution |
| --- | --- | --- |
| 052 | L’ISO peut être identique à la version actuelle ou correspondre à deux versions supérieures à la version actuelle. | Utilisez une version ISO compatible pour effectuer la mise à niveau depuis votre version actuelle. |
| 068 | La restauration des paquets Debian a échoué | Utilisez une récupération à RPO nul ou basée sur un instantané et réessayez la mise à niveau. |
| 069 | Échec de la restauration des fichiers | Utilisez une récupération à RPO nul ou basée sur un instantané et réessayez la mise à niveau. |
| 070 | Échec de la suppression de la sauvegarde | - |
| 071 | Le cluster Kubernetes n’était pas sain | - |
| 074 | Le montage ISO a échoué | Consultez le fichier /var/log/upgrade-run.log et réessayez la mise à niveau. |
| 075 | La vérification préalable de la mise à niveau a échoué | Réessayez la mise à niveau. |
| 076 | La mise à niveau du registre a échoué | Utilisez une récupération à RPO nul ou basée sur un instantané et réessayez la mise à niveau. |
| 077 | La restauration du registre a échoué | Utilisez une récupération à RPO nul ou basée sur un instantané et réessayez la mise à niveau. |
| 078 | La mise à niveau de l’opérateur a échoué | Utilisez une récupération à RPO nul ou basée sur un instantané et réessayez la mise à niveau. |
| 079 | La restauration de l’opérateur a échoué | Utilisez une récupération à RPO nul ou basée sur un instantané et réessayez la mise à niveau. |
| 080 | La mise à niveau des services a échoué | Utilisez une récupération à RPO nul ou basée sur un instantané et réessayez la mise à niveau. |
| 081 | La restauration des services a échoué | Utilisez une récupération à RPO nul ou basée sur un instantané et réessayez la mise à niveau. |
| 082 | La suppression des anciennes images du conteneur a échoué | Utilisez une récupération à RPO nul ou basée sur un instantané et réessayez la mise à niveau. |
| 083 | La suppression de la sauvegarde a échoué | Utilisez une récupération à RPO nul ou basée sur un instantané et réessayez la mise à niveau. |

| Code d'erreur de mise à niveau | Flux de travail | Résolution |
|---|---|---|
| 084 | Le retour de JobManager en production a échoué | Pour récupérer/terminer la mise à niveau, effectuez les étapes suivantes. 1. Activez l'interface de diagnostic 2. Exécutez la commande : *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 3. Consultez les journaux dans /var/log/post-deploy-upgrade.log |
| 087 | Les étapes post-mise à niveau ont échoué. | Pour récupérer/terminer la mise à niveau, effectuez les étapes suivantes. 1. Activez l'interface de diagnostic 2. Exécutez la commande *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 3. Consultez les journaux dans /var/log/post-deploy-upgrade.log |
| 088 | La configuration de la rotation des journaux pour journald a échoué | Vérifiez que les paramètres réseau de la machine virtuelle sont compatibles avec l'hôte qui l'héberge. Vous pouvez essayer de migrer la machine virtuelle vers un autre hôte et de la redémarrer. |
| 089 | La modification du propriétaire du fichier de configuration de rotation du journal récapitulatif a échoué | Réessayez la mise à niveau. |
| 095 | La mise à niveau du système d'exploitation a échoué | Aucune récupération n'est possible suite à la mise à niveau du système d'exploitation. Les services ONTAP tools sont mis à niveau et de nouveaux pods seront opérationnels. |
| 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 une récupération à RPO nul ou basée sur un instantané, puis réessayez la mise à niveau. |
| 098 | La copie du secret dockercred de ntv-system vers l'espace de noms du provisionneur de stockage dynamique a échoué | Consultez les journaux de mise à niveau et réessayez la mise à niveau. |
| 099 | Échec de la validation de l'ajout du nouveau disque dur | Ajoutez le nouveau disque dur à tous les nœuds en cas de déploiement HA et à un seul nœud en cas de déploiement non HA. |

| Code d’erreur de mise à niveau | Flux de travail | Résolution |
| --- | --- | --- |
| 109 | La sauvegarde des données du volume persistant a échoué | Consultez les journaux de mise à niveau et réessayez la mise à niveau. |
| 110 | La restauration des données du volume persistant a échoué | Utilisez une récupération à RPO nul ou basée sur un instantané et réessayez la mise à niveau. |
| 111 | La mise à jour des paramètres de délai d’expiration d’etcd pour RKE2 a échoué | Consultez les journaux de mise à niveau et réessayez la mise à niveau. |
| 112 | La désinstallation du provisionneur 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 | La restauration du noyau a échoué | - |
| 051 | La mise à niveau du provisionneur de stockage dynamique a échoué | Consultez les journaux de mise à niveau et réessayez la mise à niveau. |
| 056 | La suppression de la sauvegarde de migration a échoué | NA |
| 090 | La validation des certificats pour les systèmes de stockage et vCenter a échoué | Consultez les journaux de mise à niveau et le fichier journal à /var/log/cert_validation_error.log et réessayez la mise à niveau. |

| Code d'erreur de mise à niveau | Flux de travail | Résolution |
| --- | --- | --- |
| 114 | La mise à jour du certificat interne dans la collection MongoDB a échoué | Si la mise à niveau échoue avec le code d'erreur 114, procédez comme suit :<br>1. Connectez-vous à l'ISO de mise à niveau sur le nœud principal et activez le shell de diagnostic.<br>2. Monter l'ISO depuis la session SSH sur le nœud principal :<br>`sudo mount /dev/cdrom`<br>`sudo mount -o loop,ro /dev/cdrom/APPLIANCE_UPGRADE.bin /upgrade`<br>3. Installer les paquets Debian :<br>`sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vplatform.deb`<br>`sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vpupgrader.deb`<br>`sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vmware-tools.deb`<br>4. Copiez le fichier d'informations de compilation :<br>`sudo cp /upgrade/APPLIANCE_BUILD /`<br>Ajoutez les certificats à la collection en activant l'interface de diagnostic et en exécutant : |

À partir de ONTAP tools for VMware vSphere 10.3, le RPO zéro n'est pas pris en charge.

Apprenez-en davantage sur "Comment restaurer ONTAP tools for VMware vSphere en cas d'échec de la mise à niveau de la version 10.0 à 10.1"

5.

```
sudo perl
/home/maint/scripts
/post-deploy-
upgrade.pl
--internal_cert_upd
ate_collection
```

Consultez les journaux à `/var/log/otvng/post-deploy-upgrade.log`.

6. Redémarrez les nœuds :

```
sudo bash
/home/maint/scripts
/vault_decrypt.sh
cd
/home/maint/rke2-pb
sudo ansible-
playbook site.yaml
--tags
restart_nodes
--skip-tags
debian_upgrade,kern
el_upgrade,rescan_s
csi_bus,source_iso,
eject_upgrade,mount
Iso,upgradeNodes,re
gistryUpg,deleteOld
Images,wait,checkRe
achability,delete_o
tv_cr,uninstall_tri
dent,del_trident_im
ages,refresh_resour
ces,ntp_configure,n
tpd_uninstall
```

7. Effectuez les étapes suivant la mise à niveau :

```
sudo perl
/home/maint/scripts
/post-deploy-
upgrade.pl
--postupgrade
```

# Migrez les ONTAP tools for VMware vSphere 9.xx vers 10.5

## Migrez des ONTAP tools for VMware vSphere 9.xx vers 10.5

Le passage de la configuration NetApp ONTAP tools for VMware vSphere de la version 9.xx à la version 10.5 nécessite un processus de migration en raison des mises à jour et améliorations importantes du produit entre les versions.

Vous pouvez migrer des ONTAP tools for VMware vSphere 9.12D1, 9.13D2 et 9.13P2 vers ONTAP tools for VMware vSphere 10.5.

Si vous avez des datastores NFS et VMFS et aucun datastore vVols dans votre configuration, désinstallez simplement ONTAP tools 9.xx et déployez ONTAP tools 10.5. En revanche, si votre configuration contient des datastores vVols, vous devez procéder à la migration du VASA Provider et du SRA.

Le tableau suivant décrit le processus de migration dans ces deux scénarios différents.

| Si la configuration comporte des banques de données vVols | Si la configuration ne contient que des datastores NFS et VMFS |
|---|---|
| Étapes : 1. "Migrez le fournisseur VASA" 2. "Créer des stratégies de stockage de machines virtuelles" | Étapes : 1. Supprimez les outils ONTAP 9.xx de votre environnement. Consultez "Comment supprimer OTV 9.xx de votre environnement" l'article de la base de connaissances NetApp. 2. "Déployez et configurez les ONTAP tools for VMware vSphere 10.5" 3. "Mettre à jour le SRA" 4. "Créer des stratégies de stockage de machines virtuelles" |

Après la migration des ONTAP tools for VMware vSphere 9.xx vers 10.5, les datastores vVols utilisant le protocole NVMe/FC deviennent non opérationnels car ONTAP tools 10.5 prend en charge le protocole NVMe-oF uniquement avec les datastores 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 depuis ONTAP tools for VMware vSphere 9.xx vers 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 de la migration du fournisseur VASA

1. Pour activer le port Derby 1527 sur les ONTAP tools for VMware vSphere existants, activez l'utilisateur root et connectez-vous à l'interface de ligne de commande (CLI) via SSH. Ensuite, exécutez la commande suivante :

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. Déployez l'OVA pour ONTAP tools for VMware vSphere 10.5.
3. Ajoutez l'instance de serveur vCenter que vous souhaitez migrer vers ONTAP tools for VMware vSphere version 10.5. Consultez "Ajouter une instance de serveur vCenter" pour plus d'informations.
4. "Activer le fournisseur VASA" service sur 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. Consultez "Ajoutez un système de stockage à l'aide de l'interface client vSphere" pour plus d'informations.
6. Obtenez un jeton d'accès pour authentifier les requêtes d'API REST. Utilisez l'exemple suivant en remplaçant les variables par les 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": "$MYPASSWORD", "vcenter
hostname": "$MYVCENTER"}'
```

   Copiez et enregistrez le jeton d'accès renvoyé dans la réponse.

7. Utilisez l'API suivante depuis Swagger ou 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/`.

8. Vérifiez que l'opération a bien été effectuée en consultant les journaux :

```
tail -f
/var/log/post-
deploy-upgrade.log
```

```
sudo umount -l -f
/dev/cdrom
sudo eject
/dev/cdrom
```

**Méthode HTTP et point de terminaison**

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 de 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 requête 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 tâche. Enregistrez l'identifiant de la tâche pour l'utiliser à l'étape suivante.

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```

8. Utilisez l'URI suivante 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. Enregistrez le fournisseur VASA auprès des ONTAP tools for VMware vSphere. Pour obtenir des instructions, consultez "Enregistrez le fournisseur VASA".
10. 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.
11. Arrêtez les ONTAP tools for VMware vSphere storage provider 9.10/9.11/9.12/9.13 VASA Provider service en suivant ces étapes :
    a. Dans ONTAP tools 9.x, ouvrez la console web.
    b. Accédez à la console de maintenance.
    c. Appuyez sur `1`Entrée pour sélectionner le menu **Configuration de l'application**.
    d. Saisissez `5` pour arrêter les 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, le vCenter Server bascule vers ONTAP tools for VMware vSphere. Toutes les banques de données et les machines virtuelles deviennent accessibles et sont servies à partir d'ONTAP tools for VMware vSphere.

12. Les banques de données NFS et VMFS migrées apparaissent dans ONTAP tools for VMware vSphere 10.5 après la tâche de découverte des banques de données, qui peut prendre jusqu'à 30 minutes. Vérifiez leur visibilité sur la page de présentation.
13. Effectuez la migration du correctif à l'aide de l'API suivante dans Swagger ou dans Postman :

**Méthode HTTP et point de terminaison**

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_id>/migration-jobs/<migration_id>`
```

**Méthode HTTP et point de terminaison**

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_id>/migration-jobs/<migration_id>`
```

**Exemple de 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-migrate.

Après l'exécution de l'API de migration des correctifs, toutes les machines virtuelles sont conformes à la politique de stockage.

**Et ensuite**

Après avoir terminé la migration et enregistré ONTAP tools 10.5 sur le serveur vCenter, suivez ces étapes :

- Attendez que la **découverte** soit terminée, et le système actualise automatiquement les certificats sur tous les hôtes.
- Veuillez patienter avant de lancer les opérations sur les banques de données et les machines virtuelles. Le temps d'attente dépend du nombre d'hôtes, de banques de données et de machines virtuelles. Si vous ne patientez pas, des erreurs ponctuelles peuvent survenir.

Après la mise à niveau, si l'état de conformité de la machine virtuelle est obsolète, réappliquez la stratégie de stockage en suivant les étapes suivantes :

1. Accédez à la banque de données et sélectionnez **Résumé** > **Stratégies de stockage VM**.
2. Le système indique que l'état de conformité sous **conformité à la politique de stockage VM** est **obsolète**.
3. Sélectionnez la stratégie de Storage VM et la machine virtuelle correspondante.
4. Sélectionnez **Appliquer**.
5. L'état de conformité sous **Conformité à la politique de stockage VM** s'affiche comme conforme.

**Informations connexes**

- "Découvrez les outils ONTAP pour VMware vSphere 10 RBAC"
- "Mettez à niveau 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 correspond à l'emplacement où les machines virtuelles sont actuellement exécutées, tandis que le site de récupération est celui où les machines virtuelles seront restaurées. L'interface de l'appliance VMware Live Site Recovery affiche l'état du plan de récupération avec des détails sur les sites protégé et de récupération. Dans le plan de récupération, les boutons CLEANUP et REPROTECT sont désactivés, tandis que les boutons TEST et RUN restent activés. Cela indique que le site est prêt pour la restauration des données. Avant de migrer le SRA, vérifiez qu'un site est en état protégé et

que l’autre est en état de récupération.

> Ne lancez pas la migration si le basculement est terminé mais que la reprotection est en attente. Assurez-vous que le processus de reprotection est terminé avant de poursuivre la migration. Si un basculement de test est en cours, nettoyez le basculement de test et lancez la migration.

1. Suivez ces étapes pour supprimer l’adaptateur SRA des ONTAP tools pour VMware vSphere 9.xx dans VMware Site Recovery :
2. Accédez à la page de gestion de la configuration de VMware Live Site Recovery.
   a. Accédez à la section **Storage Replication Adapter**.
   b. Dans le menu à trois points, sélectionnez **Réinitialiser la configuration**.
   c. Dans le menu à trois points, sélectionnez **Supprimer**.
3. Effectuez ces étapes sur les sites de protection et de restauration.
   a. "Activer les ONTAP tools for VMware vSphere services"
   b. Configurez les outils ONTAP pour VMware vSphere 10.5 SRA à l’aide des étapes indiquées dans "Configurez SRA sur l’appliance VMware Live Site Recovery".
   c. Dans l’interface de VMware Live Site Recovery, exécutez **Discover Arrays** et **Discover Devices**. Vérifiez que les périphériques s’affichent comme avant la migration.

# Automatisez à l’aide de l’API REST

## Découvrez l’API REST des ONTAP tools

ONTAP tools for VMware vSphere 10 est un ensemble d’outils de gestion du cycle de vie des machines virtuelles. Il comprend une API REST robuste que vous pouvez utiliser dans vos processus d’automatisation.

### Fondation des services web REST

REST (Representational State Transfer) est un style de création d’applications web distribuées, incluant la conception d’API de services web. Il établit un ensemble de technologies pour exposer des ressources basées sur le serveur et gérer leur état.

#### Ressources et représentation de l’état

Les ressources sont les composants fondamentaux d’une application de services Web REST. La conception d’une API REST comporte deux tâches initiales importantes :

- Identifiez les ressources système ou serveur
- Définissez les états des ressources et les opérations de transition d’état associées

Les applications clientes peuvent afficher et modifier l’état des ressources via des flux de messages bien définis.

#### Messages HTTP

Le protocole de transfert hypertexte (HTTP) est le protocole utilisé par le client et le serveur de services web pour échanger des messages concernant 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 que plusieurs formats de messages soient disponibles, l’option la plus populaire est JavaScript Object Notation (JSON). JSON est une norme industrielle permettant de représenter des structures de données simples en texte brut et est utilisé pour transférer des informations d’état décrivant les ressources et les actions souhaitées.

#### Sécurité

La sécurité est un aspect important d’une API REST. En plus du protocole Transport Layer Security (TLS) utilisé pour protéger le trafic HTTP sur le réseau, l’API REST ONTAP tools for VMware vSphere 10 utilise également des jetons d’accès pour l’authentification. Vous devez obtenir un jeton d’accès et l’utiliser lors des appels d’API suivants.

#### Prise en charge des requêtes asynchrones

Les ONTAP tools for VMware vSphere 10 REST API exécutent la plupart des requêtes de manière synchrone et renvoient un code d’état lorsque l’opération est terminée. Elles prennent également en charge le traitement asynchrone pour les tâches nécessitant plus de temps pour s’achever.

### Environnement du gestionnaire ONTAP tools

Il existe plusieurs aspects de l’environnement ONTAP tools Manager que vous devez prendre en compte.

**machine virtuelle**

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 dans une machine virtuelle distincte.

**Adresse IP des outils ONTAP**

ONTAP tools for VMware vSphere 10 expose une adresse IP unique servant de passerelle vers les fonctionnalités de la machine virtuelle. Vous devez fournir l'adresse lors de la configuration initiale et elle est attribuée à un composant d'équilibreur de charge interne. L'adresse est utilisée par l'interface utilisateur de ONTAP tools Manager, ainsi que pour accéder directement à la page de documentation Swagger et à l'API REST.

**Deux API REST**

Outre l'API REST ONTAP tools for VMware vSphere 10, le cluster ONTAP possède sa propre API REST. ONTAP tools Manager 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 séparées et distinctes. Pour plus d'informations, consultez "Automatisation ONTAP".

# Détails d'implémentation de l'API REST des ONTAP tools

Bien que REST définisse un ensemble commun de technologies et de bonnes pratiques, l'implémentation précise de chaque API peut varier selon les choix de conception. Vous devez bien comprendre comment l'API REST des ONTAP tools for VMware vSphere 10 est conçue avant de l'utiliser.

L'API REST comprend plusieurs catégories de ressources, telles que vCenters et les agrégats. Consultez la "Référence API" pour plus d'informations.

## Comment accéder à l'API REST

Vous pouvez accéder à l'API REST des ONTAP tools for VMware vSphere 10 via l'adresse IP des ONTAP tools ainsi que le port. L'URL complète comporte plusieurs parties, notamment :

- Adresse IP et port des outils ONTAP
- version API
- Catégorie de ressources
- 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 identique pour chaque instance d'ONTAP tools for VMware vSphere 10 ; seules la catégorie de ressource et la ressource spécifique changent entre les points de terminaison.

Les adresses IP et les ports indiqués dans les exemples ci-dessous sont fournis à titre indicatif 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 pour lister les 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 HTTP

Les ONTAP tools for VMware vSphere 10 REST API utilisent HTTP et les paramètres associés pour agir sur les instances et collections de ressources. Les détails de l'implémentation HTTP sont présentés ci-dessous.

### Méthodes HTTP

Les méthodes ou verbes HTTP pris en charge par l'API REST sont présentés dans le tableau ci-dessous.

| Méthode | CRUD | Description |
|---|---|---|
| GET | Lire | Récupère les propriétés d'un objet pour une instance de ressource ou une collection. Il s'agit d'une opération de liste lorsqu'elle est utilisée avec une collection. |
| POST | Créer | Crée une nouvelle instance de ressource en fonction des paramètres d'entrée. |
| PUT | Mise à jour | Met à jour l'intégralité d'une instance de ressource avec le corps de la requête JSON fourni. Les valeurs clés non modifiables par l'utilisateur sont conservées. |
| CORRECTIF | Mise à jour | Demande qu'un ensemble de modifications sélectionnées dans la requête soit appliqué à l'instance de ressource. |
| SUPPRIMER | Supprimer | Supprime une instance de ressource existante. |

### En-têtes de requête et de réponse

Le tableau suivant récapitule les en-têtes HTTP les plus importants utilisés avec l'API REST.

| En-tête | Type | Notes d'utilisation |
|---|---|---|
| Accepter | Demande | Il s'agit du type de contenu que l'application cliente peut accepter. Les valeurs valides incluent '*/*` ou `application/json`. |
| x-auth | Demande | Contient un jeton d'accès identifiant l'utilisateur émettant la requête via l'application cliente. |
| 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 la réussite des appels qui ne créent pas de nouvelle instance de ressource. |

| Code | Signification | Description |
|---|---|---|
| 201 | Créé | Un objet a été créé avec succès avec un identifiant unique pour l'instance de ressource. |
| 202 | Accepté | La demande a été acceptée et une tâche en arrière-plan a été créée pour exécuter la demande. |
| 204 | Aucun contenu | La requête a réussi, bien qu'aucun contenu n'ait été renvoyé. |
| 400 | Mauvaise demande | La saisie de la requête 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 mentionnée dans la requête n'existe pas. |
| 409 | Conflit | La tentative de création d'un objet a échoué car l'objet existe déjà. |
| 500 | Erreur interne | Une erreur interne générale s'est produite sur le serveur. |

### Authentification

L'authentification d'un client auprès de l'API REST s'effectue à l'aide d'un jeton d'accès. Les caractéristiques pertinentes du jeton et du processus d'authentification sont les suivantes :

- Le client doit demander un jeton en utilisant les identifiants d'administrateur ONTAP tools Manager (nom d'utilisateur et mot de passe).
- Les jetons sont formatés en tant que JSON Web Token (JWT).
- Chaque jeton expire après 60 minutes.
- Les requêtes API provenant d'un client doivent inclure le jeton dans l' `x-auth`en-tête de la requête.

Reportez-vous à "Votre premier appel à l'API REST" pour un exemple de demande et d'utilisation d'un jeton d'accès.

### Requêtes synchrones et asynchrones

La plupart des appels d'API REST s'exécutent rapidement et sont donc synchrones. Autrement dit, ils renvoient un code d'état (par exemple 200) après qu'une requête a été terminée. Les requêtes qui prennent plus de temps à s'exécuter fonctionnent de manière asynchrone à l'aide d'une tâche en arrière-plan.

Après l'envoi d'un appel API qui s'exécute de manière asynchrone, le serveur renvoie un code d'état HTTP 202. Cela indique que la requête a été acceptée mais n'est pas encore terminée. Vous pouvez interroger la tâche en arrière-plan pour déterminer son état, y compris le succès ou l'échec.

Le traitement asynchrone est utilisé pour plusieurs types d'opérations de longue durée, y compris les opérations sur les datastores et vVol. Pour plus d'informations, consultez la catégorie du gestionnaire de tâches de l'API REST sur la page Swagger.

# Effectuez votre premier appel API REST avec les ONTAP tools

Vous pouvez effectuer un appel API à l'aide de curl pour commencer à utiliser les ONTAP

tools for VMware vSphere 10 REST API.

## Avant de commencer

Vous devez examiner les informations et paramètres requis dans les exemples curl.

**Informations requises**

Vous avez besoin des éléments suivants :

- ONTAP tools for VMware vSphere 10 adresse IP ou FQDN ainsi que le port
- Identifiants pour l'administrateur ONTAP tools Manager (nom d'utilisateur et mot de passe)

**Paramètres et variables**

Les exemples curl ci-dessous utilisent des variables de style Bash. Vous pouvez définir ces variables dans l'environnement Bash ou les modifier manuellement avant d'exécuter les commandes. Si vous définissez les variables, l'interpréteur de commandes substituera leurs valeurs dans chaque commande avant son exécution. Ces variables sont décrites dans le tableau ci-dessous.

| Variable | Description |
|---|---|
| $FQDN_IP_PORT | Le nom de domaine complet ou l'adresse IP du ONTAP tools Manager, ainsi que le numéro de port. |
| $MYUSER | Nom d'utilisateur pour le compte Manager des ONTAP tools. |
| $MYPASSWORD | Mot de passe associé au nom d'utilisateur du gestionnaire d'outils ONTAP. |
| $ACCESS_TOKEN | Le jeton d'accès émis par le gestionnaire ONTAP tools. |

Les commandes et résultats suivants dans l'interface de ligne de commande Linux illustrent comment définir et afficher une variable :

```
FQDN_IP_PORT=172.14.31.224:8443
echo $FQDN_IP
172.14.31.224:8443
```

## Étape 1 : Obtenez un jeton d'accès

Vous devez obtenir un jeton d'accès pour utiliser l'API REST. Un exemple de requête de jeton d'accès est présenté ci-dessous. Vous devez remplacer les valeurs par celles appropriées à 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 : Émettre l’appel à l’API REST

Une fois que vous avez obtenu un jeton d’accès, vous pouvez utiliser curl pour effectuer un appel à l’API REST. Incluez le jeton d’accès obtenu lors de la première étape.

**Exemple de curl**

```
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 vCenter VMware configurées dans ONTAP tools Manager.

# Référence de l’API REST des ONTAP tools

La documentation de référence de l’API REST des ONTAP tools for VMware vSphere 10 contient des informations détaillées sur tous les appels d’API. Cette documentation est utile lors du développement d’applications d’automatisation.

Vous pouvez accéder à la documentation de l’API REST des ONTAP tools for VMware vSphere 10 en ligne via l’interface utilisateur Swagger. Vous avez besoin de l’adresse IP ou du domaine complet (FQDN) du service de passerelle des ONTAP tools for VMware vSphere 10, ainsi que du port.

**Étapes**

1. Saisissez l’URL suivante dans votre navigateur, en remplaçant la variable par l’adresse IP et la combinaison de port appropriée, puis appuyez sur **Entrée**.

   `https://$FQDN_IP_PORT/`

   **Exemple**

   `https://10.61.25.33:8443/`

2. À titre d’exemple d’appel API individuel, faites défiler vers le bas jusqu’à la catégorie **vCenters** et sélectionnez **GET** à côté du point de terminaison `/virtualization/api/v1/vcenters`

# Mentions légales

Les mentions légales donnent accès aux déclarations de droits d'auteur, aux marques de commerce, aux brevets et plus encore.

## Copyright

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

## Marques déposées

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

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

## Brevets

Une liste actuelle des brevets détenus par NetApp peut être trouvée à :

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

## Politique de confidentialité

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

## Open source

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

"Avis concernant 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.