Documentation des ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/ontap-tools-vmware-vsphere-104/index.html on September 29, 2025. Always check docs.netapp.com for the latest.

Sommaire

Documentation des ONTAP tools for VMware vSphere . . . 1
Notes de version . . . 2
- Notes de version . . . 2
- Nouveautés des ONTAP tools for VMware vSphere 10.4 . . . 2
- Comparaison des fonctionnalités des ONTAP tools for VMware vSphere 9 et ONTAP tools for VMware vSphere 10 . . . 3

Concepts . . . 5
- Présentation des ONTAP tools for VMware vSphere . . . 5
- Concepts et termes clés . . . 5
- Contrôle d'accès basé sur les rôles . . . 8
  - En savoir plus sur les ONTAP tools for VMware vSphere 10 RBAC . . . 8
  - RBAC avec VMware vSphere . . . 9
  - RBAC avec ONTAP . . . 13
- Haute disponibilité des ONTAP tools for VMware vSphere . . . 16
- Interface utilisateur du gestionnaire d'outils ONTAP . . . 16

Déployer les ONTAP tools for VMware vSphere . . . 19
- Démarrage rapide des ONTAP tools for VMware vSphere . . . 19
- Workflow de déploiement haute disponibilité (HA) . . . 21
- Exigences et limites de configuration des ONTAP tools for VMware vSphere . . . 21
  - Configuration requise . . . 21
  - Exigences minimales de stockage et d'application . . . 22
  - Exigences portuaires . . . 22
  - Limites de configuration pour déployer les ONTAP tools for VMware vSphere . . . 24
  - ONTAP tools for VMware vSphere - Adaptateur de réplication de stockage (SRA) . . . 25
- Avant de commencer… . . . 25
  - Feuille de travail de déploiement . . . 26
  - Configuration du pare-feu réseau . . . 27
  - Paramètres de stockage ONTAP . . . 27
- Déployer les ONTAP tools for VMware vSphere . . . 28
- Codes d'erreur de déploiement . . . 33

Configurer les ONTAP tools for VMware vSphere . . . 36
- Ajouter des instances de vCenter Server . . . 36
- Enregistrer le fournisseur VASA auprès d'une instance vCenter Server . . . 36
- Installer le plug-in NFS VAAI . . . 37
- Configurer les paramètres de l'hôte ESXi . . . 38
  - Configurer les paramètres de multi-chemin et de délai d'expiration du serveur ESXi . . . 38
  - Définir les valeurs de l'hôte ESXi . . . 39
- Configurer les rôles et privilèges des utilisateurs ONTAP . . . 40
  - Exigences de mappage d'agrégats SVM . . . 41
  - Créer un utilisateur et un rôle ONTAP manuellement . . . 41
  - Mettre à niveau les ONTAP tools for VMware vSphere 10.1 vers l'utilisateur 10.3 . . . 49
  - Mettre à niveau les ONTAP tools for VMware vSphere 10.3 vers l'utilisateur 10.4 . . . 51
- Ajouter un backend de stockage . . . 52

Associer un backend de stockage à une instance vCenter Server . . . 53
Configurer l'accès au réseau . . . 54
Créer un magasin de données . . . 54
Protéger les banques de données et les machines virtuelles . . . 60
Protéger à l'aide de la protection du cluster hôte . . . 60
Protégez-vous en utilisant la protection SRA . . . 61
Configurer SRA pour protéger les banques de données . . . 61
Configurer SRA pour les environnements SAN et NAS . . . 61
Configurer SRA pour les environnements à grande échelle . . . 63
Configurer SRA sur le dispositif VMware Live Site Recovery . . . 63
Mettre à jour les informations d'identification SRA . . . 64
Configurer les sites protégés et de récupération . . . 65
Configurer les ressources du site protégé et de récupération . . . 66
Vérifier les systèmes de stockage répliqués . . . 70
Protection en éventail . . . 71
Gérer les ONTAP tools for VMware vSphere . . . 74
Présentation du tableau de bord des ONTAP tools for VMware vSphere . . . 74
Interface utilisateur du gestionnaire d'outils ONTAP . . . 76
Comprendre les groupes d'application et les stratégies d'exportation dans les ONTAP tools for VMware vSphere . . . 77
Politiques d'exportation . . . 81
Comprendre les groupes gérés par les outils ONTAP . . . 82
Activer les ONTAP tools for VMware vSphere . . . 85
Modifier les ONTAP tools for VMware vSphere . . . 86
Gérer les magasins de données . . . 87
Monter des banques de données NFS et VMFS . . . 87
Démonter les banques de données NFS et VMFS . . . 88
Monter une banque de données vVols . . . 89
Redimensionner le magasin de données NFS et VMFS . . . 89
Développer les banques de données vVols . . . 89
Réduire la banque de données vVols . . . 90
Supprimer les banques de données . . . 90
Vues de stockage ONTAP pour les banques de données . . . 91
Vue de stockage de la machine virtuelle . . . 92
Gérer les seuils de stockage . . . 92
Gérer les backends de stockage . . . 92
Découvrir le stockage . . . 93
Modifier les backends de stockage . . . 93
Supprimer les backends de stockage . . . 93
Vue détaillée du backend de stockage . . . 94
Gérer les instances de vCenter Server . . . 95
Dissocier les backends de stockage de l'instance vCenter Server . . . 95
Modifier une instance de vCenter Server . . . 95
Supprimer une instance de vCenter Server . . . 95
Gérer les certificats . . . 96

Accéder aux ONTAP tools for VMware vSphere . . . 98
Présentation des ONTAP tools for VMware vSphere . . . 98
Configurer l'accès au diagnostic à distance . . . 99
Démarrer SSH sur d'autres nœuds . . . 100
Mettre à jour les informations d'identification de vCenter Server et ONTAP . . . 100
Rapports des outils ONTAP . . . 100
Collecter les fichiers journaux . . . 101
Gérer les machines virtuelles . . . 102
Considérations pour migrer ou cloner des machines virtuelles . . . 102
Migrer des machines virtuelles avec des banques de données NFS et VMFS vers des banques de données vVols . . . 103
Nettoyage VASA . . . 103
Attacher ou détacher un disque de données d'une machine virtuelle . . . 104
Découvrez les systèmes de stockage et les hôtes . . . 104
Modifier les paramètres de l'hôte ESXi à l'aide des outils ONTAP . . . 105
Gérer les mots de passe . . . 106
Modifier le mot de passe du gestionnaire d'outils ONTAP . . . 106
Réinitialiser le mot de passe du gestionnaire d'outils ONTAP . . . 106
Réinitialiser le mot de passe de l'utilisateur de l'application . . . 107
Réinitialiser le mot de passe utilisateur de la console de maintenance . . . 107
Gérer la protection du cluster d'hôtes . . . 108
Modifier le cluster d'hôtes protégé . . . 108
Supprimer la protection du cluster hôte . . . 111
Désactiver AutoSupport . . . 111
Mettre à jour l'URL du proxy AutoSupport . . . 112
Ajouter des serveurs NTP . . . 112
Créer une sauvegarde et récupérer la configuration des outils ONTAP . . . 112
Créer une sauvegarde et télécharger le fichier de sauvegarde . . . 113
Récupérer . . . 113
Désinstaller les ONTAP tools for VMware vSphere . . . 114
Supprimer les volumes FlexVol . . . 115
Mettre à niveau les ONTAP tools for VMware vSphere . . . 116
Mise à niveau des ONTAP tools for VMware vSphere 10.x vers 10.4 . . . 116
Codes d'erreur de mise à niveau . . . 119
Migrer les ONTAP tools for VMware vSphere 9.xx vers 10.4 . . . 124
Migrer des ONTAP tools for VMware vSphere 9.xx vers 10.4 . . . 124
Migrer le fournisseur VASA et mettre à jour le SRA . . . 124
Étapes pour migrer le fournisseur VASA . . . 124
Étapes pour mettre à jour l'adaptateur de réplication de stockage (SRA) . . . 127
Automatiser à l'aide de l'API REST . . . 129
En savoir plus sur les ONTAP tools for VMware vSphere 10 . . . 129
Fondation des services Web REST . . . 129
Environnement du gestionnaire d'outils ONTAP . . . 129
Détails d'implémentation des ONTAP tools for VMware vSphere 10 . . . 130
Comment accéder à l'API REST . . . 130

Détails HTTP . . . 131
Authentification . . . 132
Requêtes synchrones et asynchrones . . . 132
Votre premier appel d'API REST ONTAP tools for VMware vSphere 10 . . . 133
Avant de commencer . . . 133
Étape 1 : Acquérir un jeton d'accès . . . 133
Étape 2 : Émettre l'appel d'API REST . . . 134
Référence API pour les ONTAP tools for VMware vSphere 10 REST API . . . 134
Mentions légales . . . 135
Copyright . . . 135
Marques de commerce . . . 135
Brevets . . . 135
Politique de confidentialité . . . 135
Open source . . . 135

Documentation des ONTAP tools for VMware vSphere

Notes de version

Notes de version

Découvrez les fonctionnalités nouvelles et améliorées disponibles dans les ONTAP tools for VMware vSphere 10.4.

Pour une liste complète des nouvelles fonctionnalités et améliorations, reportez-vous àNouveautés des ONTAP tools for VMware vSphere 10.4 .

Pour en savoir plus sur la pertinence de la migration des ONTAP tools for VMware vSphere 9 vers les outils ONTAP 10.4 pour votre déploiement, consultezComparaison des fonctionnalités des ONTAP tools for VMware vSphere 9 et ONTAP tools for VMware vSphere 10 . La migration est prise en charge à partir des ONTAP tools for VMware vSphere 9.12-D et 9.13-D vers les ONTAP tools for VMware vSphere 10.4.

Pour plus d'informations, reportez-vous à la "Notes de publication des ONTAP tools for VMware vSphere 10.4" . Vous devez vous connecter avec votre compte NetApp ou créer un compte pour accéder aux notes de publication.

Nouveautés des ONTAP tools for VMware vSphere 10.4

Découvrez les nouvelles fonctionnalités disponibles dans les ONTAP tools for VMware vSphere 10.4.

Mise à jour	Description
"Prise en charge du système ASA r2 avec 12 nœuds par cluster"	Les ONTAP tools for VMware vSphere 10.4 prennent en charge les flux de travail pour les systèmes de stockage ASA r2 avec jusqu'à 12 nœuds par cluster, améliorant ainsi l'efficacité et l'évolutivité de la gestion des données. Il prend en charge les magasins de données vVols avec les protocoles iSCSI et FC, ainsi que les magasins de données VMFS avec les protocoles iSCSI, FC et NVMe, offrant des options de stockage flexibles et améliorées.
"Améliorations de l'interface utilisateur du gestionnaire d'outils ONTAP"	Vous pouvez désormais activer le serveur NTP pour une synchronisation horaire précise dans l'environnement et configurer les paramètres de télémétrie pour surveiller et analyser les performances du système à partir de l'interface du gestionnaire d'outils ONTAP . Ces paramètres ne sont plus disponibles dans la console de maintenance.
Capacités de sécurité améliorées	Les fonctionnalités de sécurité offrent désormais une protection améliorée et une conformité aux normes du secteur, offrant une expérience robuste et conviviale pour aider les administrateurs à gérer plus efficacement les environnements VMware.
"Capacités de reprise après sinistre SRA améliorées"	Les ONTAP tools for VMware vSphere 10.4 prennent désormais en charge les opérations de reprise après sinistre à l'aide de Site Recovery Appliance (SRA) avec des snapshots nommés personnalisés en plus des copies de snapshots planifiées SnapMirror .

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

Découvrez si la migration des ONTAP tools for VMware vSphere 9 vers les ONTAP tools for VMware vSphere 10.1 ou versions ultérieures vous convient.

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

Fonctionnalité	Outils ONTAP 9.13	Outils ONTAP 10.1	Outils ONTAP 10.2 et versions ultérieures
Proposition de valeur clé	Rationalisez et simplifiez les opérations du jour 0 au jour 2 grâce à des capacités de sécurité, de conformité et d'automatisation améliorées	Évolution des outils ONTAP 10.x vers la parité 9.xx tout en étendant la haute disponibilité, les performances et les limites d'évolutivité	Prise en charge étendue pour inclure FC pour VMFS et vVols, et NVMe-oF/FC, NVMe-oF/TCP pour VMFS uniquement. Facilité d'utilisation pour NetApp SnapMirror, configuration simple pour les clusters de stockage métropolitains vSphere et prise en charge de VMware Live Site Recovery sur trois sites
Qualification de la version ONTAP	ONTAP 9.9.1 à ONTAP 9.16.1	ONTAP 9.12.1 à ONTAP 9.14.1	ONTAP 9.12.1 à ONTAP 9.15.1 pour les outils ONTAP 10.2. ONTAP 9.14.1, 9.15.1, 9.16.0 et 9.16.1 pour les outils ONTAP 10.3. ONTAP 9.14.1, 9.15.1, 9.16.0 et 9.16.1 pour les outils ONTAP 10.4. ONTAP 9.16.1P3 et versions ultérieures sont requis pour les outils ONTAP 10.4 lors de l'utilisation des systèmes ASA r2.
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 VMware Site Recovery Manager (SRM) 8.7 vers VMware Live Site Recovery 9.0	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.7 vers VMware Live Site Recovery 9.0
Prise en charge du protocole	Magasins de données NFS et VMFS : NFS (v3 et v4.1), VMFS (iSCSI et FCP) Magasins de données vVols : iSCSI, FCP, NVMe/FC, NFS v3	Magasins de données NFS et VMFS : NFS (v3 et v4.1), VMFS (iSCSI) Magasins de données vVols : iSCSI, NFS v3	Magasins de données NFS et VMFS : NFS (v3 et v4.1), VMFS (iSCSI/FCP/NVMe-oF) Magasins de données vVols : iSCSI, FCP, NFS v3

Fonctionnalité	Outils ONTAP 9.13	Outils ONTAP 10.1	Outils ONTAP 10.2 et versions ultérieures
Évolutivité	Hôtes et machines virtuelles : 300 hôtes, jusqu'à 10 000 VM ; magasins de données : 600 NFS, jusqu'à 50 VMFS, jusqu'à 250 vVols ; vVols: jusqu'à 14 000	Hôtes et machines virtuelles : 600 hôtes vVols: jusqu'à 140 000	Hôtes et machines virtuelles : 600 hôtes vVols: jusqu'à 140 000
Observabilité	Tableaux de bord des performances, de la capacité et de la conformité de l'hôte Rapports dynamiques sur les machines virtuelles et les banques de données	Tableaux de bord mis à jour sur les performances, la capacité et la conformité de l'hôte Rapports dynamiques sur les machines virtuelles et les banques de données	Tableaux de bord mis à jour sur les performances, la capacité et la conformité de l'hôte Rapports dynamiques sur les machines virtuelles et les banques de données
Protection des données	Réplication SRA pour VMFS et NFS Réplication basée sur FlexVols pour vVols Intégration SCV et interopérable pour la sauvegarde	Réplication SRA pour les banques de données iSCSI VMFS et NFS v3	Réplication SRA pour les banques de données iSCSI VMFS et NFS v3, protection sur trois sites combinant SMAS et VMware Live Site Recovery.
Assistance aux fournisseurs VASA	VASA 4,0	VASA 3,0	VASA 3,0

Concepts

Présentation des ONTAP tools for VMware vSphere

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

Les ONTAP tools for VMware vSphere comprennent les éléments suivants :

- Fonctionnalités de la machine virtuelle telles que la protection de base et la reprise après sinistre
- Fournisseur VASA pour la gestion granulaire des machines virtuelles
- Gestion basée sur les politiques de stockage
- Adaptateur de réplication de stockage (SRA)

Concepts et termes clés

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

Systèmes ASA r2

Les nouveaux systèmes NetApp ASA r2 offrent une solution matérielle et logicielle unifiée qui crée une expérience simplifiée spécifique aux besoins des clients SAN uniquement. "En savoir plus sur les systèmes de stockage ASA r2" .

Autorité de certification (CA)

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

Groupe de cohérence (CG)

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

Double pile

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

Haute disponibilité (HA)

Les nœuds de 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 réseau de stockage (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 est une quantité de mémoire non volatile qui peut 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 au sein du sous-système.

Gestionnaire d'outils ONTAP

ONTAP Tools Manager offre davantage de contrôle aux ONTAP tools for VMware vSphere sur les instances vCenter Server gérées et les backends de stockage intégrés. Il permet de gérer les instances vCenter Server, les backends de stockage, les certificats, les mots de passe et les téléchargements de bundles de journaux.

Appareil virtuel ouvert (OVA)

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

Objectif de point de récupération (RPO)

Le RPO mesure la fréquence à laquelle vous sauvegardez ou répliquez les données. Il spécifie le moment exact auquel vous devez restaurer les données après une panne pour reprendre les opérations commerciales. Par exemple, si une organisation a un RPO de 4 heures, elle peut tolérer de perdre jusqu'à 4 heures de données en cas de sinistre.

Synchronisation active de SnapMirror

La synchronisation active SnapMirror permet aux services professionnels de continuer à fonctionner même en cas de panne totale du site, en prenant en charge le basculement transparent des applications à l'aide d'une copie secondaire. Aucune intervention manuelle ou script personnalisé n'est requis pour déclencher un basculement avec la synchronisation active SnapMirror . En savoir plus sur "Synchronisation active de SnapMirror" .

Backends de stockage

Les backends de stockage sont l'infrastructure de stockage sous-jacente que l'hôte ESXi utilise pour stocker les fichiers, les données et d'autres ressources de la machine virtuelle. Ils permettent à l'hôte ESXi d'accéder aux données persistantes et de les gérer, offrant ainsi la capacité de stockage et les performances requises pour un environnement virtualisé.

Cluster global (backend de stockage)

Les backends de stockage globaux, disponibles uniquement avec les informations d'identification du cluster ONTAP , sont intégrés via l'interface du gestionnaire d'outils ONTAP . Ils peuvent être ajoutés avec des privilèges minimaux pour permettre la découverte des ressources de cluster essentielles nécessaires à la gestion des vVols . Les clusters globaux sont idéaux pour les scénarios multi-locataires où un utilisateur SVM est ajouté localement pour la gestion des vVols .

Backend de stockage local

Les backends de stockage locaux avec des informations d'identification de cluster ou SVM sont ajoutés via l'interface utilisateur des outils ONTAP et sont limités à un vCenter. Lors de l'utilisation des informations d'identification du cluster localement, les SVM associés sont automatiquement mappés avec vCenter pour gérer les vVols ou VMFS. Pour la gestion VMFS, y compris SRA, les outils ONTAP prennent en charge les informations d'identification SVM sans avoir besoin d'un cluster global.

Adaptateur de réplication de stockage (SRA)

SRA est le logiciel spécifique au fournisseur de stockage installé à l'intérieur du dispositif VMware Live Site Recovery. L'adaptateur permet la communication entre Site Recovery Manager et un contrôleur de stockage au niveau de la machine virtuelle de stockage (SVM) et la configuration au niveau du cluster.

Machine virtuelle de stockage (SVM)

SVM est l'unité de multilocation dans ONTAP. Comme une machine virtuelle exécutée sur un hyperviseur, SVM est une entité logique qui fait abstraction des ressources physiques. SVM contient des volumes de données et un ou plusieurs LIF via lesquels ils fournissent des données aux clients.

Configuration uniforme et non uniforme

- **L'accès uniforme à l'hôte** signifie que les hôtes de deux sites sont connectés à tous les chemins vers les clusters de stockage sur les deux sites. Les chemins intersites s'étendent sur des distances.
- **L'accès hôte non uniforme** signifie que les hôtes de chaque site sont connectés uniquement au cluster du même site. Les chemins intersites et les chemins étirés 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 symétriques actifs/actifs. En savoir plus sur "Présentation de la synchronisation active SnapMirror dans ONTAP" .

Système de fichiers de machine virtuelle (VMFS)

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

Volumes virtuels (vVols)

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

Politique de stockage des machines virtuelles

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

Récupération de site VMware Live

VMware Live Site Recovery, anciennement connu sous le nom de Site Recovery Manager (SRM), offre des fonctionnalités de continuité des activités, de reprise après sinistre, de migration de site et de test sans interruption pour les environnements virtuels VMware.

API VMware vSphere pour la reconnaissance du stockage (VASA)

VASA est un ensemble d'API qui intègrent des baies de stockage à vCenter Server pour la gestion et l'administration. L'architecture repose sur plusieurs composants, dont le fournisseur VASA, qui gère la communication entre VMware vSphere et les systèmes de stockage.

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

VAAI est un ensemble d'API qui permet la communication entre les hôtes VMware vSphere ESXi et les périphériques de stockage. Les API incluent un ensemble d'opérations primitives utilisées par les hôtes pour décharger les opérations de stockage sur la baie. VAAI peut fournir des améliorations de performances significatives pour les tâches gourmandes en stockage.

Cluster de stockage vSphere Metro

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

Banque de données vVols

Le magasin de données vVols est une représentation de magasin de données logique d'un conteneur vVols créé et maintenu par un fournisseur VASA.

Zéro RPO

RPO signifie « objectif de point de récupération », c'est-à-dire la quantité de perte de données jugée acceptable pendant une période donnée. Zéro RPO signifie qu'aucune perte de données n'est acceptable.

Contrôle d'accès basé sur les rôles

En savoir plus sur les ONTAP tools for VMware vSphere 10 RBAC

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. RBAC simplifie l'administration en définissant des rôles avec des niveaux d'autorité spécifiques pour effectuer des actions, au lieu d'attribuer une autorisation à des utilisateurs individuels. Les rôles définis sont attribués aux utilisateurs, ce qui permet de réduire le risque d'erreur et de simplifier la gestion du contrôle d'accès dans votre organisation.

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

Composants RBAC

À un niveau élevé, il existe plusieurs composants qui sont généralement inclus dans chaque implémentation RBAC. Ces composants sont liés entre eux de différentes manières dans le cadre de la définition des 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. Des Privileges peuvent également être définis pour restreindre l'accès aux points de terminaison de l'API REST et aux commandes CLI. Chaque implémentation RBAC inclut des privilèges prédéfinis et peut également permettre aux administrateurs de créer des privilèges personnalisés.

Rôles

Un *rôle* est un conteneur qui inclut un ou plusieurs privilèges. Les rôles sont généralement définis en fonction de tâches ou de fonctions particulières. Lorsqu'un rôle est attribué à un utilisateur, celui-ci reçoit tous les privilèges contenus dans le rôle. Et comme pour les privilèges, les implémentations incluent des rôles prédéfinis et permettent généralement la création de rôles personnalisés.

Objets

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

Utilisateurs et groupes

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

Autorisations

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

Deux environnements RBAC

Il existe deux environnements RBAC distincts que vous devez prendre en compte lorsque vous travaillez avec les ONTAP tools for VMware vSphere 10.

Serveur VMware vCenter

L'implémentation RBAC dans VMware vCenter Server est utilisée pour restreindre l'accès aux objets exposés via l'interface utilisateur de vSphere Client. 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 fonctionnalités des outils ONTAP . L'accès à ces objets est assuré par le module d'extension distant. Voir"Environnement RBAC vCenter Server" pour plus d'informations.

Cluster ONTAP

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

RBAC avec VMware vSphere

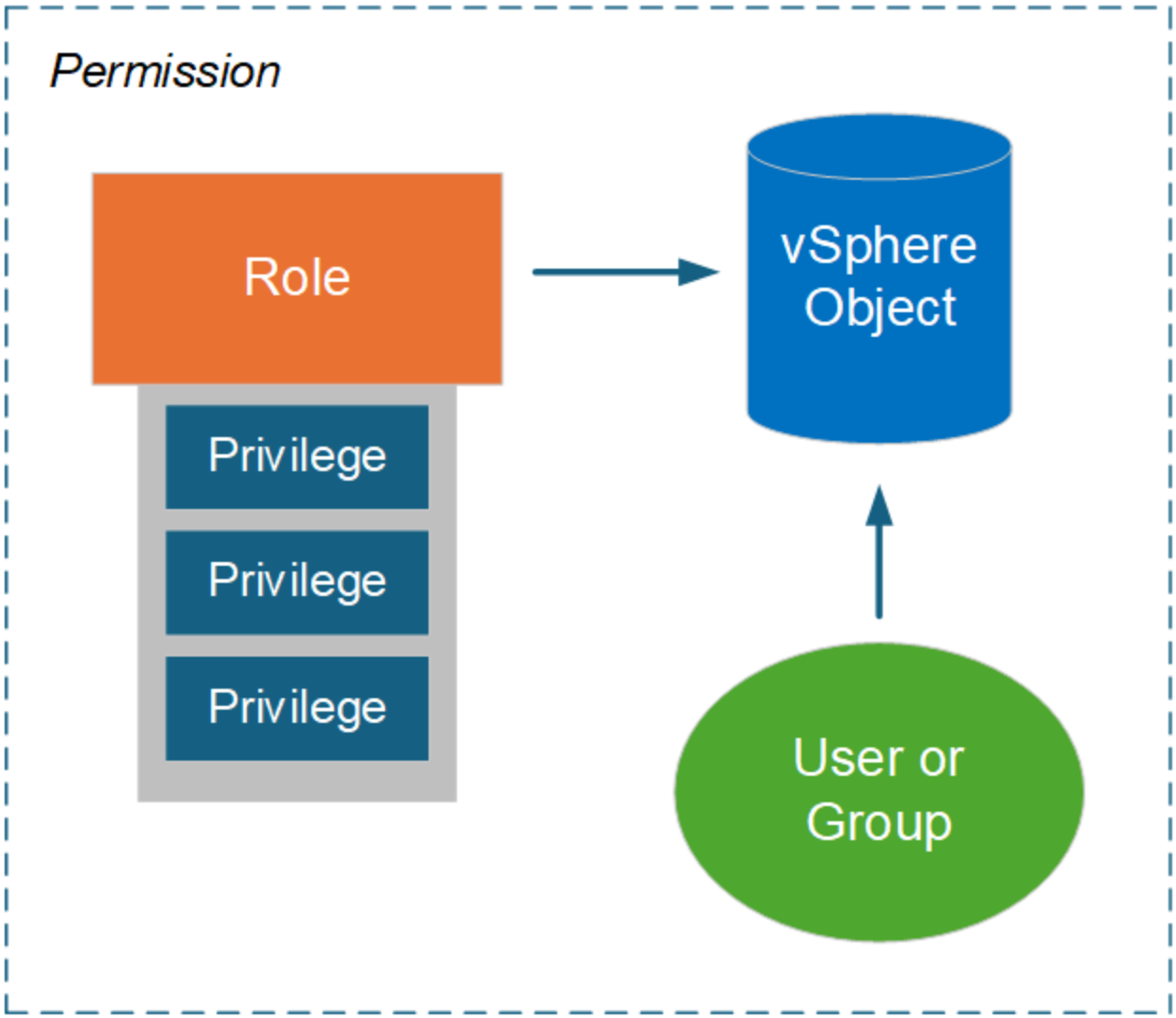
Environnement vCenter Server RBAC avec ONTAP tools for VMware vSphere 10

VMware vCenter Server fournit une fonctionnalité RBAC qui vous permet de contrôler

l'accès aux objets vSphere. Il s'agit d'un élément important des services de sécurité d'authentification et d'autorisation centralisés de vCenter.

Illustration d'une autorisation vCenter Server

Une autorisation constitue la base de l'application du contrôle d'accès dans l'environnement vCenter Server. Il est appliqué à un objet vSphere avec un utilisateur ou un groupe inclus dans la définition d'autorisation. Une illustration de haut niveau d'une autorisation vCenter est fournie dans la figure ci-dessous.



Composants d'une autorisation vCenter Server

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

objets vSphere

Les autorisations sont associées aux objets vSphere, tels que vCenter Server, les hôtes ESXi, les machines virtuelles, les banques de données, les centres de données et les dossiers. En fonction des autorisations attribuées à l'objet, vCenter Server détermine quelles actions ou tâches peuvent être effectuées sur l'objet par

chaque utilisateur ou groupe. Pour les tâches spécifiques aux ONTAP tools for VMware vSphere, toutes les autorisations sont attribuées et validées au niveau de la racine ou du dossier racine de vCenter Server. Voir "Utiliser 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 RBAC dans cet environnement, les outils ONTAP fournissent des rôles contenant les privilèges natifs et personnalisés requis. Les privilèges comprennent :

- Privilèges natifs du serveur vCenter

  Ce sont les privilèges fournis par vCenter Server.

- Privilèges spécifiques aux outils ONTAP

  Il s'agit de privilèges personnalisés propres aux ONTAP tools for VMware vSphere.

Utilisateurs et groupes

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

Utiliser vCenter Server RBAC avec les ONTAP tools for VMware vSphere 10

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

Rôles vCenter et compte administrateur

Vous devez uniquement définir et utiliser les rôles vCenter Server personnalisés si vous souhaitez limiter l'accès aux objets vSphere et aux tâches administratives associées. Si la limitation de l'accès n'est pas nécessaire, vous pouvez utiliser un compte 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 les ONTAP tools for VMware vSphere 10.

Hiérarchie des objets vSphere

L'inventaire des objets vSphere est organisé dans une hiérarchie. 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 les ONTAP tools for VMware vSphere 10

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

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

Pour afficher les ONTAP tools for VMware vSphere , sélectionnez **Menu** en haut du client vSphere et cliquez sur **Administration**, puis sur **Rôles** sur la gauche. Il existe trois rôles prédéfinis comme décrit ci-dessous.

ONTAP tools for VMware vSphere NetApp ONTAP pour VMware vSphere Administrator

Fournit tous les privilèges natifs de vCenter Server et les privilèges spécifiques aux outils ONTAP requis pour effectuer les tâches d'administrateur des ONTAP tools for VMware vSphere .

Outils NetApp ONTAP tools for VMware vSphere en lecture seule

Fournit un accès en lecture seule aux outils ONTAP . Ces utilisateurs ne peuvent pas exécuter d' ONTAP tools for VMware vSphere dont l'accès est contrôlé.

ONTAP tools for VMware vSphere NetApp ONTAP pour VMware vSphere Provision

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

- Créer de nouveaux magasins de données
- Gérer les magasins de données

Objets vSphere et backends de stockage ONTAP

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

Travailler avec vCenter Server RBAC

Il y a quelques éléments à prendre en compte lorsque vous travaillez avec les privilèges et autorisations de vCenter Server.

Privilèges requis

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

Le niveau d'affectation dans la hiérarchie des objets vSphere détermine les parties de l'interface utilisateur auxquelles vous pouvez accéder. L'attribution du privilège Affichage 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 Affichage à un autre niveau d'objet vSphere inférieur. Cependant, cela limitera les ONTAP tools for VMware vSphere auxquels vous pouvez accéder et que vous pouvez utiliser.

Attribution des autorisations

Vous devez utiliser les autorisations vCenter Server 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 ONTAP

tools for VMware vSphere 10 que les utilisateurs peuvent effectuer.

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

Les autorisations disponibles avec les ONTAP tools for VMware vSphere 10 s'appliquent aux objets non vSphere personnalisés, tels que les systèmes de stockage. Si possible, vous devez attribuer ces autorisations aux ONTAP tools for VMware vSphere, car il n'existe aucun objet vSphere auquel vous pouvez les attribuer. Par exemple, toute autorisation qui inclut un privilège « Ajouter/Modifier/Supprimer des systèmes de stockage » des 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 dans la hiérarchie des objets, vous pouvez configurer l'autorisation afin qu'elle soit transmise et héritée par les objets enfants. Si nécessaire, vous pouvez attribuer des autorisations supplémentaires aux objets enfants qui remplacent les autorisations héritées du parent.

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

RBAC avec ONTAP

Environnement ONTAP RBAC avec ONTAP tools for VMware vSphere 10

ONTAP fournit un environnement RBAC robuste et extensible. Vous pouvez utiliser la fonctionnalité RBAC pour contrôler l'accès aux opérations de stockage et système telles qu'exposées via l'API REST et la CLI. Il est utile de se familiariser avec l'environnement avant de l'utiliser avec un déploiement ONTAP tools for VMware vSphere 10.

Aperçu des options administratives

Plusieurs options sont disponibles lors de l'utilisation ONTAP RBAC en fonction de votre environnement et de vos objectifs. Un aperçu des principales décisions administratives est présenté ci-dessous. Voir aussi "ONTAP Automation : Présentation de la sécurité RBAC" pour plus d'informations.

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

Types de rôles et de privilèges

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

- REPOS

  Les rôles REST ont été introduits avec ONTAP 9.6 et sont généralement appliqués aux utilisateurs 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 ONTAP et aux actions associées.

- Traditionnel

  Il s'agit des rôles hérités inclus avant ONTAP 9.6. Ils continuent d'être un aspect fondamental du RBAC. Les privilèges sont définis en termes d'accès aux commandes CLI ONTAP .

Bien que les rôles REST aient été introduits plus récemment, les rôles traditionnels présentent certains avantages. Par exemple, des paramètres de requête supplémentaires peuvent éventuellement être inclus afin que les privilèges définissent plus précisément les objets auxquels ils sont appliqués.

Portée

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

Définitions des rôles

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

Travailler avec les rôles REST ONTAP

Plusieurs éléments doivent être pris en compte lors de l'utilisation des rôles ONTAP REST inclus avec les 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 d'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 en parallèle.

Définition d'un rôle REST à l'aide des privilèges CLI

Étant donné ONTAP utilise toujours les commandes CLI pour déterminer l'accès à un niveau de base, il est possible d'exprimer un rôle REST à l'aide des privilèges de commande CLI au lieu des points de terminaison REST. L'un des avantages de cette approche est la granularité supplémentaire disponible avec les rôles traditionnels.

Interface d'administration lors de la définition des rôles ONTAP

Vous pouvez créer des utilisateurs et des rôles avec l'interface de ligne de commande ONTAP et l'API REST. Cependant, il est plus pratique d'utiliser l'interface du gestionnaire système avec le fichier JSON disponible via le gestionnaire d'outils ONTAP . Voir "Utiliser ONTAP RBAC avec les ONTAP tools for VMware vSphere 10" pour plus d'informations.

Utiliser ONTAP RBAC avec les ONTAP tools for VMware vSphere 10

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

Aperçu du processus de configuration

Les ONTAP tools for VMware vSphere 10 incluent la prise en charge de la création d'un utilisateur ONTAP avec un rôle personnalisé. Les définitions sont regroupées dans un fichier JSON que vous pouvez télécharger sur le cluster ONTAP . Vous pouvez créer l'utilisateur et personnaliser le rôle en fonction de votre environnement et de vos besoins de sécurité.

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

1. Préparer

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

2. Télécharger le fichier de définition JSON

Après vous être connecté à l'interface utilisateur du gestionnaire d'outils ONTAP , vous pouvez télécharger le fichier JSON contenant les définitions RBAC.

3. Créer un utilisateur ONTAP avec un rôle

Après vous être connecté au Gestionnaire système, vous pouvez créer l'utilisateur et le rôle :

1. Sélectionnez **Cluster** sur la gauche puis **Paramètres**.
2. Faites défiler jusqu'à **Utilisateurs et rôles** et cliquez sur −→ .
3. Sélectionnez **Ajouter** sous **Utilisateurs** et sélectionnez **Produits de virtualisation**.
4. Sélectionnez le fichier JSON sur votre poste de travail local et téléchargez-le.

4. Configurer le rôle

Dans le cadre de la définition du rôle, vous devez prendre plusieurs décisions administratives. VoirConfigurer le rôle à l'aide du Gestionnaire système pour plus de détails.

Configurer le rôle à l'aide du Gestionnaire système

Une fois que vous avez commencé à créer un nouvel utilisateur et un nouveau 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 des utilisateurs et des rôles principaux

Les définitions RBAC sont regroupées sous forme de plusieurs fonctionnalités de produit, notamment des combinaisons de VSC, VASA Provider et SRA. Vous devez sélectionner l'environnement ou les environnements dans lesquels 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 à distance, sélectionnez VSC. Vous devez également choisir le nom d'utilisateur et le mot de passe associé.

Privileges

Les privilèges de rôle sont organisés en quatre ensembles en fonction du niveau d'accès nécessaire au stockage ONTAP . Les privilèges sur lesquels sont basés les rôles incluent :

- Découverte

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

- Créer un espace de 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 à la découverte et à la création de rôles de stockage.

- Détruire le stockage

Ce rôle vous permet de détruire le stockage. Il inclut également tous les privilèges associés à la découverte, à la création de stockage et à la modification des rôles de stockage.

Générer l'utilisateur avec un rôle

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

- Valeur de préfixe constante définie dans le fichier JSON (par exemple « OTV_10 »)
- Capacité 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.

Haute disponibilité des ONTAP tools for VMware vSphere

Les ONTAP tools for VMware vSphere prennent en charge une configuration haute disponibilité (HA) pour aider à fournir une fonctionnalité ininterrompue des ONTAP tools for VMware vSphere en cas de panne.

La solution de haute disponibilité (HA) permet une récupération rapide après des pannes causées par :

- Panne de l'hôte

  Seule la défaillance d'un seul nœud est prise en charge.

- Panne de réseau
- Panne de machine virtuelle (panne du système d'exploitation invité)
- Crash de l'application (outils ONTAP)

Aucune configuration supplémentaire n'est requise pour les ONTAP tools for VMware vSphere afin de fournir une haute disponibilité (HA).

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

Pour activer la fonctionnalité HA, l'ajout à chaud du processeur et le branchement à chaud de la mémoire doivent être activés lors du déploiement ou ultérieurement dans les paramètres des ONTAP tools for VMware vSphere VM.

Interface utilisateur du gestionnaire d'outils ONTAP

Les ONTAP tools for VMware vSphere sont un système multi-locataire capable de gérer plusieurs instances de vCenter Server. ONTAP Tools Manager offre davantage de contrôle à l'administrateur des ONTAP tools for VMware vSphere sur les instances

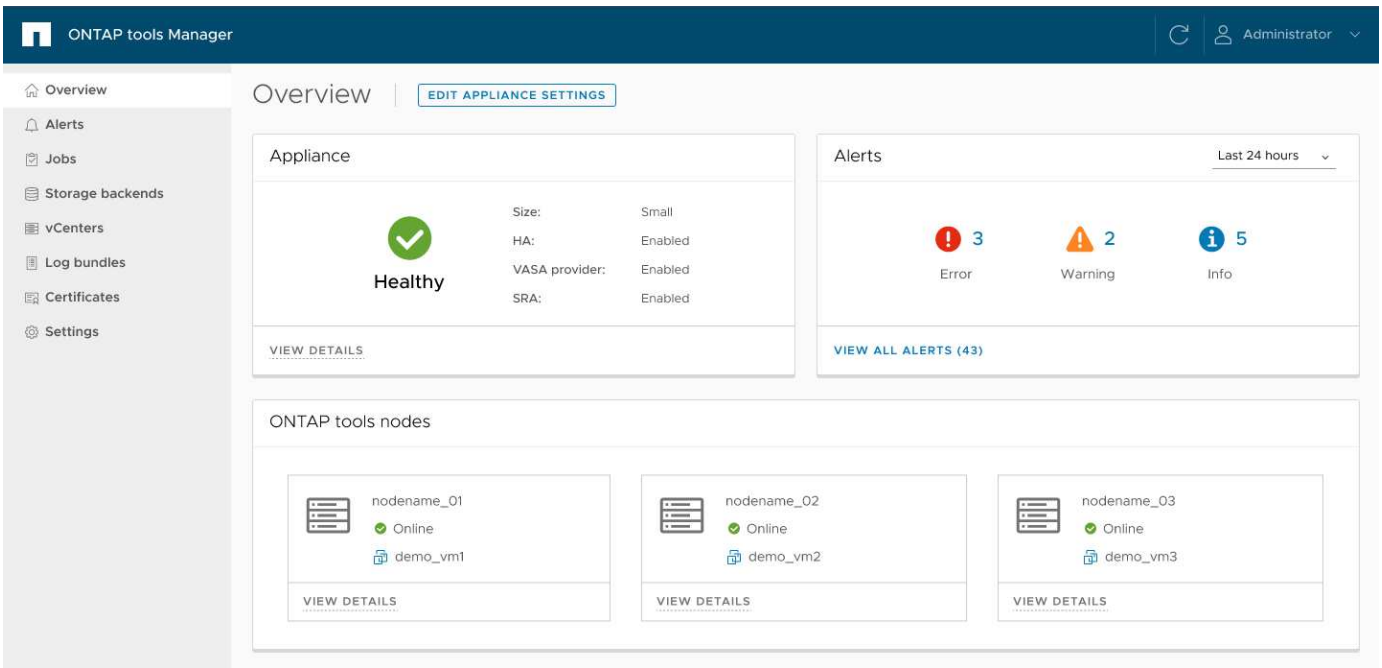
vCenter Server gérées et les backends de stockage intégrés.

ONTAP Tools Manager aide à :

- Gestion des instances vCenter Server - Ajoutez et gérez les instances vCenter Server aux outils ONTAP .
- Gestion du backend de stockage - Ajoutez et gérez les clusters de stockage ONTAP aux ONTAP tools for VMware vSphere et mappez-les aux instances vCenter Server intégrées à l'échelle mondiale.
- Téléchargements de bundles de journaux - Collectez les fichiers journaux pour les ONTAP tools for VMware vSphere.
- Gestion des certificats - Remplacez le certificat auto-signé par un certificat CA personnalisé et renouvelez ou actualisez tous les certificats des outils VASA Provider et ONTAP .
- Gestion des mots de passe - Réinitialiser le mot de passe de l'application OVA de l'utilisateur.

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

La section Présentation du gestionnaire d'outils ONTAP permet de gérer la configuration de l'appliance, comme la gestion des services, la mise à l'échelle de la taille des nœuds et l'activation de la haute disponibilité (HA). Vous pouvez également surveiller les informations globales des outils ONTAP liées aux nœuds, telles que l'état, les détails du réseau et les alertes.



Carte	Description
Carte d’appareil	La carte de l’appareil fournit l’état général de l’appareil des outils ONTAP . Il affiche les détails de configuration de l’appareil et l’état des services activés. Pour plus d’informations sur l’appliance des outils ONTAP , sélectionnez le lien **Afficher les détails**. Lorsqu’une tâche d’action de modification des paramètres d’un appareil est en cours, le portlet de l’appareil affiche l’état et les détails de la tâche.
Carte d’alertes	La carte Alertes répertorie les alertes des outils ONTAP par type, y compris les alertes au niveau du nœud HA. Vous pouvez consulter la liste des alertes en sélectionnant le texte du compteur (lien hypertexte). Le lien vous dirige vers la page d’affichage des alertes filtrées par le type sélectionné.
vCenters	La carte vCenter affiche l’état de santé des vCenters du système.
Backends de stockage	La carte des backends de stockage affiche l’état de santé des backends de stockage du système.
Carte des nœuds d’outils ONTAP	La carte des nœuds des outils ONTAP affiche la liste des nœuds avec le nom du nœud, le nom de la machine virtuelle du nœud, l’état et toutes les données liées au réseau. Vous pouvez sélectionner **Afficher les détails** pour afficher les détails supplémentaires liés au nœud sélectionné. [REMARQUE] Dans une configuration non HA, un seul nœud est affiché. Dans la configuration HA, trois nœuds sont affichés.

Déployer les ONTAP tools for VMware vSphere

Démarrage rapide des ONTAP tools for VMware vSphere

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

Dans un premier temps, vous déploierez les ONTAP tools for VMware vSphere sous la forme d'une configuration de nœud unique de petite taille qui fournit des services de base pour prendre en charge les banques de données NFS et VMFS. Si vous devez étendre votre configuration pour utiliser les banques de données vVols et la haute disponibilité (HA), vous le ferez après avoir terminé ce workflow. Pour plus d'informations, reportez-vous à la "Flux de travail de déploiement HA" .

1 **Planifiez votre déploiement**

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

Assurez-vous que le serveur vCenter est installé et accessible.

- "Outil de matrice d'interopérabilité"
- "Exigences et limites de configuration des ONTAP tools for VMware vSphere"
- "Avant de commencer"

2 **Déployer les ONTAP tools for VMware vSphere**

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

- "Déployer les ONTAP tools for VMware vSphere"

3 **Ajouter des instances de vCenter Server**

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

- "Ajouter des instances de vCenter Server"

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

Configurez de nouveaux rôles et privilèges d'utilisateur pour la gestion des backends de stockage à l'aide du fichier JSON fourni avec les ONTAP tools for VMware vSphere.

- "Configurer les rôles et privilèges des utilisateurs ONTAP"

5 Configurer les backends de stockage

Ajoutez un backend de stockage à un cluster ONTAP . Pour les configurations multi-locataires où vCenter agit en tant que locataire avec un SVM associé, utilisez ONTAP Tools Manager pour ajouter le cluster. Associez le backend de stockage au vCenter Server pour le mapper globalement à l'instance vCenter Server intégrée.

Ajoutez les backends de stockage locaux avec les informations d'identification de cluster ou SVM à l'aide de l'interface utilisateur des outils ONTAP . Ces backends de stockage sont limités à un seul vCenter. Lors de l'utilisation des informations d'identification du cluster localement, les SVM associées sont automatiquement mappées au vCenter pour gérer les vVols ou VMFS. Pour la gestion VMFS, y compris SRA, les outils ONTAP prennent en charge les informations d'identification SVM sans avoir besoin d'un cluster global.

- "Ajouter un backend de stockage"
- "Associer le backend de stockage à une instance vCenter Server"

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

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

- "Gérer les certificats"

7 (Facultatif) Configurer la protection SRA

Activez la fonctionnalité SRA pour configurer la reprise après sinistre et protéger les banques de données NFS ou VMFS.

- "Activer les ONTAP tools for VMware vSphere"
- "Configurer SRA sur le dispositif VMware Live Site Recovery"

8 (Facultatif) Activer la protection de synchronisation active SnapMirror

Configurez les ONTAP tools for VMware vSphere afin de gérer la protection du cluster hôte pour la synchronisation active SnapMirror . Effectuez le cluster ONTAP et le peering SVM dans les systèmes ONTAP pour utiliser la synchronisation active SnapMirror . Ceci s'applique uniquement aux banques de données VMFS.

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

9 Configurer la sauvegarde et la récupération de vos ONTAP tools for VMware vSphere

Planifiez des sauvegardes de vos ONTAP tools for VMware vSphere que vous pouvez utiliser pour récupérer la configuration en cas de panne.

- "Créer une sauvegarde et récupérer la configuration des outils ONTAP"

Workflow de déploiement haute disponibilité (HA)

Si vous utilisez des banques de données vVols , vous devez étendre le déploiement initial des outils ONTAP à une configuration haute disponibilité (HA) et activer les services du fournisseur VASA.

1 **Augmenter le déploiement**

Vous pouvez étendre la configuration des ONTAP tools for VMware vSphere afin d'augmenter le nombre de nœuds dans le déploiement et de modifier la configuration vers une configuration HA.

- "Modifier les ONTAP tools for 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 répondent aux exigences HA, y compris les configurations de réseau et de stockage appropriées.

Activez les services SRA pour utiliser les outils ONTAP 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 vCenter Server, 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 ONTAP tools for VMware vSphere

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

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

Configuration requise

- **Exigences d'espace du package d'installation par nœud**
  - 15 Go pour les installations à provisionnement léger
  - 348 Go pour les installations à provisionnement épais

- **Exigences de dimensionnement du système hôte** La mémoire recommandée en fonction de la taille du déploiement est indiquée dans le tableau ci-dessous. Pour déployer la haute disponibilité (HA), vous aurez besoin de trois fois la taille de l'appliance spécifiée dans le tableau.

Type de déploiement	CPU par nœud	Mémoire (Go) par nœud	Espace disque (Go) provisionné en épaisseur par nœud
Petit	9	18	350
Moyen	13	26	350
REMARQUE importante : le déploiement à grande échelle concerne uniquement la configuration HA.	17	34	350

Lorsque la sauvegarde est activée, chaque cluster d'outils ONTAP a besoin de 50 Go d'espace supplémentaires sur la banque de données où les machines virtuelles sont déployées. Par conséquent, le non-HA nécessite 400 Go et le HA nécessite 1 100 Go d'espace au total.

Exigences minimales de stockage et d'application

Stockage, hôte et applications	Exigences de version
ONTAP	9.14.1, 9.15.1, 9.16.0, 9.16.1 et 9.16.1P3 FAS, ASA série A, ASA série C, AFF série A, AFF série C et ASA r2.
Les outils ONTAP prennent en charge les hôtes ESXi	7.0.3 et versions ultérieures
Outils ONTAP pris en charge par vCenter Server	7.0U3 et versions ultérieures
Fournisseur VASA	3,0
Demande OVA	10,4
Hôte ESXi pour déployer la machine virtuelle des outils ONTAP	7.0U3 et 8.0U3
vCenter Server pour déployer la machine virtuelle des outils ONTAP	7.0 et 8.0

À partir des 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, de vCenter Server, des hôtes ESXi et des applications plug-in.

"Outil de matrice d'interopérabilité"

Exigences portuaires

Le tableau suivant présente les ports réseau utilisés par NetApp et leurs fonctions. Assurez-vous que ces ports sont ouverts et accessibles pour faciliter le bon fonctionnement et la communication au sein du système.

Assurez-vous que les configurations réseau nécessaires sont en place pour autoriser le trafic sur ces ports et le bon fonctionnement des services associés. Selon vos politiques de sécurité, vous devrez peut-être configurer des pare-feu ou d'autres dispositifs de sécurité pour autoriser ce trafic au sein de votre réseau.

Port	Protocole	Description
8143	TCP	Connexions HTTP/HTTPS pour les outils ONTAP .
8043	TCP	Connexions HTTP/HTTPS pour les outils ONTAP .
9060	TCP	Connexions HTTP/HTTPS pour les outils ONTAP .
22	TCP	Ansible utilise ce port SSH pour la communication lors du provisionnement du cluster. Ce port est requis pour des fonctionnalités telles que la modification du mot de passe de l'utilisateur de maintenance, les messages d'état et la mise à jour des valeurs sur les trois nœuds en cas de configuration HA.
443	TCP	Il s'agit du port de transmission pour les communications entrantes pour le service VASA Provider. Le certificat auto-signé du fournisseur VASA et le certificat CA personnalisé sont hébergés sur ce port.
8443	TCP	Ce port héberge la documentation de l'API via Swagger et l'application d'interface utilisateur Manager.
2379	TCP	Il s'agit du port par défaut pour les requêtes client telles que get, put, delete ou watch pour les clés dans le magasin de valeurs de clés etcd.
2380	TCP	Il s'agit du port par défaut pour la communication de serveur à serveur pour le cluster etcd utilisé pour l'algorithme de consensus raft sur lequel etcd s'appuie pour la réplication et la cohérence des données.
7472	TCP/UDP	Il s'agit du port du service de métriques Prometheus.
7946	TCP/UDP	Ce port est utilisé pour la découverte du réseau de conteneurs de Docker.

9083	TCP	Ce port est un port de service utilisé en interne pour le service VASA Provider.
1162	UDP	Il s'agit du port des paquets de trap SNMP.
6443	TCP	Source : nœuds d'agents RKE2. Destination : nœuds du serveur REK2. Description : API Kubernetes
9345	TCP	Source : nœuds d'agents RKE2. Destination : nœuds du serveur REK2. Description : API du superviseur REK2
8472	TCP+UDP	Tous les nœuds doivent pouvoir atteindre d'autres nœuds via le port UDP 8472 lorsque Flannel VXLAN est utilisé. Source : tous les nœuds RKE2. Destination : tous les nœuds REK2. Description : Canal CNI avec VXLAN
10250	TCP	Source : tous les nœuds RKE2. Destination : tous les nœuds REK2. Description : Métriques Kubelet
30000-32767	TCP	Source : tous les nœuds RKE2. Destination : tous les nœuds REK2. Description : plage de ports NodePort
123	TCP	Ntpd utilise ce port pour effectuer la validation du serveur NTP.
137-139	TCP/UDP	Partage de paquets SMB/Windows.
6789	TCP	Moniteur Ceph (MON)
3300	TCP	Moniteur Ceph (MON)
6800-7300	TCP	Gestionnaires Ceph, OSD et système de fichiers (MDS).
80	TCP	Passerelle RADOS Ceph (RGW)
9080	TCP	Connexions HTTP/HTTPS VP (uniquement à partir de 127.0.0.0/8 pour IPv4 ou ::1/128 pour IPv6).

Limites de configuration pour déployer les ONTAP tools for VMware vSphere

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

Déploiement	Taper	Nombre de vVols	Nombre d'hôtes
Non-HA	Petit (S)	~12 000	32

Non-HA	Moyen (M)	~24K	64
Haute disponibilité	Petit (S)	~24K	64
Haute disponibilité	Moyen (M)	~50 000	128
Haute disponibilité	Grand (L)	~100 000	256 [REMARQUE] Le nombre d'hôtes dans le tableau indique le nombre total d'hôtes provenant de plusieurs vCenter.

ONTAP tools for VMware vSphere - Adaptateur de réplication de stockage (SRA)

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

Taille du déploiement vCenter	Petit	Moyen
Nombre total de machines virtuelles configurées pour la protection à l'aide de la réplication basée sur une baie	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 récupération	50	50
Nombre de banques de données répliquées	255	255
Nombre de machines virtuelles	4000	7000

Le tableau suivant indique le nombre de VMware Live Site Recovery et les 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" .

Avant de commencer…

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

Exigences	Votre statut
La version vSphere, la version ONTAP et la version de l'hôte ESXi sont compatibles avec la version des outils ONTP.	☐ Oui ☐ Non
L'environnement vCenter Server est installé et configuré	☐ Oui ☐ Non
Le cache du navigateur est supprimé	☐ Oui ☐ Non
Vous disposez des informations d'identification du serveur vCenter parent	☐ Oui ☐ Non
Vous disposez des informations de connexion pour l'instance vCenter Server, 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 mappé à l'adresse IP virtuelle dans un déploiement multi-vCenter où les certificats CA personnalisés sont obligatoires.	☐ Oui ☐ Non
Vous avez exécuté la vérification nslookup sur le nom de domaine pour vérifier si le domaine est résolu à l'adresse IP prévue.	☐ Oui ☐ Non
Le certificat est créé avec le nom de domaine et l'adresse IP des outils ONTAP .	☐ Oui ☐ Non
L'application des outils ONTAP et les services internes sont accessibles depuis le serveur vCenter.	☐ Oui ☐ Non
Lorsque vous utilisez des SVM multilocataires, vous disposez d'un LIF de gestion SVM sur chaque SVM.	☐ Oui ☐ Non

Feuille de travail de déploiement

Pour un déploiement à nœud unique

Utilisez la feuille de calcul suivante pour collecter les informations requises pour les ONTAP tools for VMware vSphere :

Exigence	Votre valeur
Adresse IP pour l'application des outils ONTAP . Il s'agit de l'adresse IP permettant d'accéder à l'interface Web des outils ONTAP	
Adresse IP virtuelle des outils ONTAP pour la communication interne. Cette adresse IP est utilisée pour la communication interne dans une configuration avec plusieurs instances d'outils ONTAP . Cette adresse IP ne doit pas être la même que l'adresse IP de l'application des outils ONTAP .	
Nom d'hôte DNS pour le premier nœud	

Exigence	Votre valeur
Serveur DNS principal	
Serveur DNS secondaire	
Domaine de recherche DNS	
Adresse IPv4 pour le premier nœud. Il s'agit d'une adresse IPv4 unique pour l'interface de gestion des nœuds sur le réseau de gestion.	
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, mappez-les aux adresses IP libres sur le DNS. Toutes les adresses IP doivent être sur le même VLAN sélectionné pour le déploiement.

Pour un déploiement à haute disponibilité (HA)

Outre les exigences de déploiement d'un nœud unique, vous aurez besoin des informations suivantes pour le 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

Ouvrez les ports requis pour les adresses IP dans votre pare-feu réseau. Les outils ONTAP doivent pouvoir atteindre ce LIF via le port 443. Se référer à"Exigences portuaires" pour les dernières mises à jour.

Paramètres de stockage ONTAP

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

- Si vous utilisez Fibre Channel (FC) pour la connectivité de stockage, configurez le zonage sur vos commutateurs FC pour connecter les hôtes ESXi aux LIF FC du SVM. "En savoir plus sur le zonage FC et

FCoE avec les systèmes ONTAP"

- Pour utiliser la réplication SnapMirror gérée par les outils ONTAP , l'administrateur de stockage ONTAP doit créer "Relations entre homologues du cluster ONTAP" et "Relations entre homologues SVM intercluster ONTAP" dans ONTAP avant d'utiliser SnapMirror.

Déployer les ONTAP tools for VMware vSphere

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

Avant de commencer

Dans VMware, une bibliothèque de contenu est un objet conteneur qui stocke des modèles de VM, des modèles d'application virtuelle et d'autres types de fichiers. Le déploiement avec une bibliothèque de contenu offre une expérience fluide, car elle ne dépend pas de la connectivité réseau.

> Vous devez stocker la bibliothèque de contenu sur une banque de données partagée afin que tous les hôtes d'un cluster puissent y accéder. Créez une bibliothèque de contenu pour stocker l'OVA avant de configurer l'appliance sur la configuration HA. Ne supprimez pas le modèle de bibliothèque de contenu après le déploiement.

> Pour activer le déploiement HA ultérieurement, ne déployez pas la machine virtuelle hébergeant les outils ONTAP directement sur un hôte ESXi. Déployez-le plutôt sur un cluster ou un pool de ressources.

Si vous n'avez pas de bibliothèque de contenu, suivez ces étapes pour en créer une :

Créer une bibliothèque de contenu Si vous prévoyez d'utiliser uniquement un petit déploiement de nœud unique, la création d'une bibliothèque de contenu n'est pas nécessaire.

1. Téléchargez le fichier contenant les binaires (*.ova*) et les certificats signés pour les ONTAP tools for VMware vSphere à partir du "Site de support NetApp" .
2. Connectez-vous au client vSphere
3. Sélectionnez le menu 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 et sélectionnez **Importer l'élément** et importez le fichier OVA.

> Pour plus d'informations, reportez-vous à "Création et utilisation de la bibliothèque de contenu" blog.

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

Les ONTAP tools for VMware vSphere sont initialement déployés en tant que configuration non HA. Pour évoluer vers un déploiement HA, vous devrez activer le plug-in à chaud du processeur et le plug-in à chaud de

la mémoire. Vous pouvez effectuer cette étape dans le cadre du processus de déploiement ou modifier les paramètres de la machine virtuelle après le déploiement.

Étapes

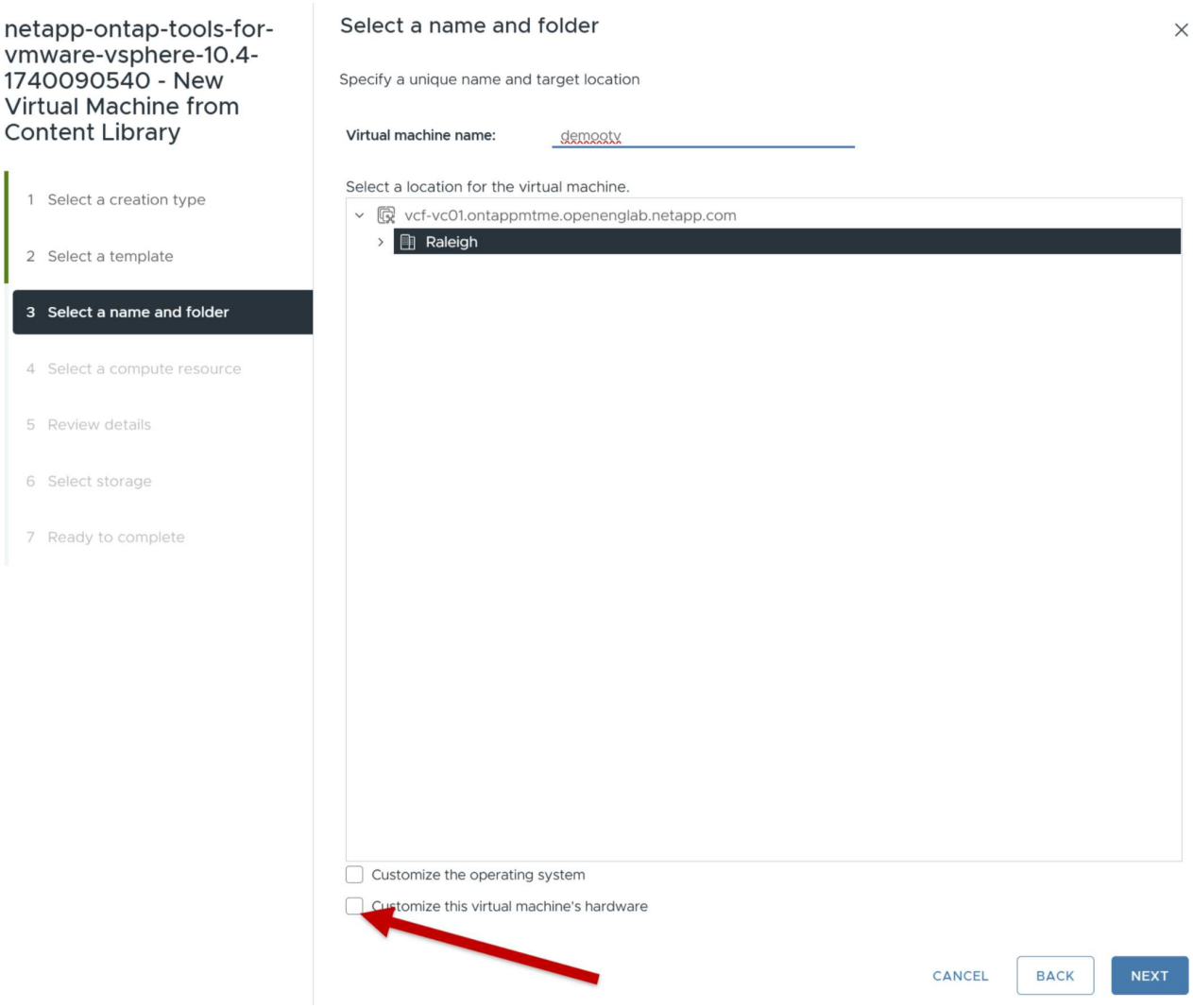
1. Téléchargez le fichier contenant les binaires (*.ova*) et les certificats signés pour les ONTAP tools for VMware vSphere à partir du "Site de support NetApp" . Si vous avez importé l'OVA dans la bibliothèque de contenu, vous pouvez ignorer cette étape et passer à l'étape suivante.
2. Connectez-vous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

   Ne stockez jamais les ONTAP tools for VMware vSphere sur les banques de données vVols qu'elle gère.

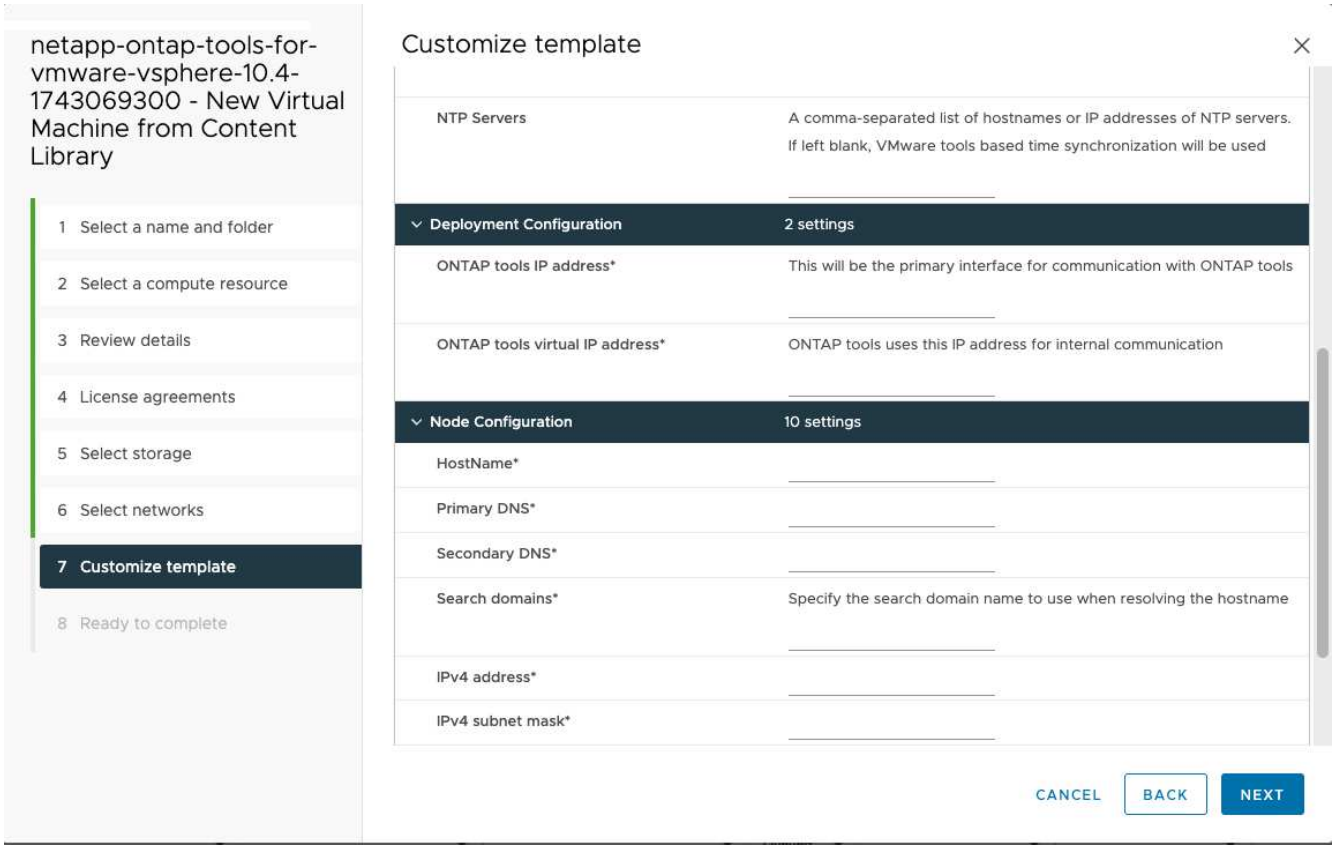
4. Vous pouvez déployer l'OVA à partir de la bibliothèque de contenu ou du système local.

Du système local	De la bibliothèque de contenu
a. Cliquez avec le bouton droit de la souris et sélectionnez **Déployer le modèle OVF…**. b. Choisissez le fichier OVA à partir de l'URL ou accédez à son emplacement, puis sélectionnez **Suivant**.	a. Accédez à votre bibliothèque de contenu et sélectionnez l'élément à déployer. b. Sélectionnez **Actions** > **Nouvelle machine virtuelle à partir de ce modèle**.

5. Dans le champ **Sélectionnez un nom et un dossier**, entrez 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 **Quelle est la prochaine étape ?** à la fin du déploiement.



6. Sélectionnez une ressource informatique et sélectionnez **Suivant**. Vous pouvez également cocher la case **Mettre sous tension automatiquement la machine virtuelle déployée**.
7. Vérifiez les détails du modèle et sélectionnez **Suivant**.
8. Lisez et acceptez le contrat de licence et sélectionnez **Suivant**.
9. Sélectionnez le stockage pour la configuration et le format du disque et 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 et sélectionnez **Suivant** .

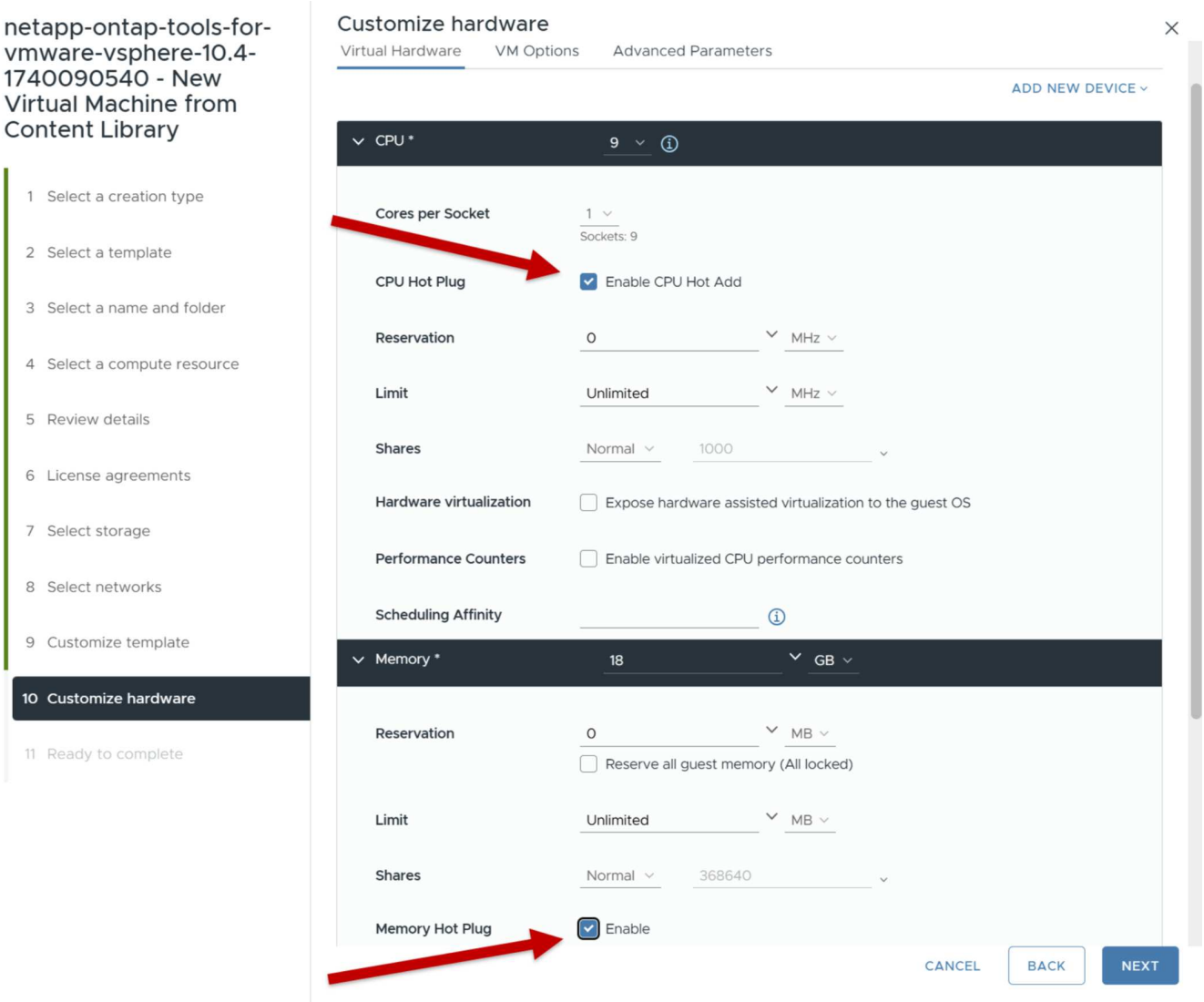


- Les informations sont validées lors de l'installation. En cas d'écart, un message d'erreur s'affiche sur la console Web et vous êtes invité à le corriger.
- Les noms d'hôtes doivent inclure des lettres (AZ, az), des chiffres (0-9) et des tirets (-). Pour configurer la double pile, spécifiez le nom d'hôte mappé à l'adresse IPv6.

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

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

12. Lorsque vous utilisez la version vCenter Server 8.0.3, dans la fenêtre **Personnaliser le matériel**, activez les options **Ajout à chaud du processeur** et **Prise à chaud de la mémoire** pour autoriser la fonctionnalité HA.



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

    Au fur et à mesure que la tâche de déploiement est créée, la progression est affichée 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.

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

Quelle est la prochaine étape ?

Si vous disposez des 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 aux ONTAP tools for VMware vSphere sous **Inventaires** et sélectionnez l'option **Modifier les paramètres**.
4. Sous les options **CPU**, cochez la case **Activer l'ajout à chaud du processeur**
5. Sous les options **Mémoire**, cochez la case **Activer** en regard de **Prise en charge à chaud de la mémoire**.

Codes d'erreur de déploiement

Vous pouvez rencontrer des codes d'erreur lors des opérations de déploiement, de redémarrage et de récupération des ONTAP tools for VMware vSphere . Les codes d'erreur comportent cinq chiffres, les deux premiers chiffres représentant le script qui a rencontré le problème et les trois derniers chiffres représentant le flux de travail spécifique dans ce script.

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

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

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

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

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

053	Échec de l'installation de RKE2	Exécutez ce qui suit et redémarrez la machine virtuelle principale ou redéployez : sudo rke2-killall.sh (toutes les machines virtuelles) sudo rke2-uninstall.sh (toutes les machines virtuelles).
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-la.
059	Le déploiement de KubeVip a échoué	Assurez-vous que l'adresse IP virtuelle pour le 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-vous.
060	Le déploiement de l'opérateur a échoué	Redémarrage
061	Le déploiement des services a échoué	Effectuez le débogage Kubernetes de base comme obtenir des pods, obtenir des rs, obtenir des 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 et redéployez.
062	Le déploiement des services des outils ONTAP a échoué	Reportez-vous aux journaux d'erreurs dans /var/log/ansible-perl-errors.log pour plus de détails et redéployer.
065	L'URL de la page Swagger n'est pas accessible	Redéployer
066	Les étapes de déploiement post-certificat de passerelle ont échoué	Procédez comme suit pour récupérer/terminer la mise à niveau : * Activez le shell de diagnostic. * Exécutez la commande « sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy ». * Vérifiez les journaux dans /var/log/post-deploy-upgrade.log.

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

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

Configurer les ONTAP tools for VMware vSphere

Ajouter des instances de vCenter Server

Ajoutez des instances vCenter Server aux 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 vCenter Server, des certificats d'autorité de certification personnalisés sont requis pour une communication sécurisée entre les outils ONTAP et chaque vCenter Server.

À propos de cette tâche

En s'intégrant à vCenter, les outils ONTAP vous permettent d'effectuer des tâches de stockage telles que le provisionnement, les snapshots et la protection des données directement à partir du client vSphere, éliminant ainsi le besoin de passer à des consoles de gestion de stockage distinctes.

Étapes

1. Ouvrez un navigateur Web et accédez à l'URL : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les informations d'identification d'administrateur des ONTAP tools for VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **vCenters** > **Ajouter** pour intégrer les instances de vCenter Server. Fournissez votre adresse IP ou nom d'hôte vCenter, votre nom d'utilisateur, votre mot de passe et les détails du port.

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

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

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

Enregistrer le fournisseur VASA auprès d'une instance vCenter Server

Vous pouvez enregistrer le fournisseur VASA auprès d'une instance vCenter Server à l'aide des ONTAP tools for VMware vSphere. La section Paramètres du fournisseur VASA affiche l'état d'enregistrement du fournisseur VASA pour le vCenter Server sélectionné. Dans un déploiement multi-vCenter, assurez-vous de disposer de certificats d'autorité de certification personnalisés pour chaque instance de vCenter Server.

Étapes

1. Connectez-vous au client vSphere.
2. Sélectionnez **Raccourcis** > *Outils NetApp ONTAP * dans la section plug-ins.
3. Sélectionnez **Paramètres** > **Paramètres du fournisseur VASA**. Le statut d'enregistrement du fournisseur VASA sera affiché comme non enregistré.
4. Sélectionnez le bouton **Enregistrer** pour enregistrer le fournisseur VASA.
5. Saisissez un nom et des informations d'identification pour le fournisseur VASA. Le nom d'utilisateur ne peut contenir que des lettres, des chiffres et des traits de soulignement. La longueur du mot de passe doit être comprise entre 8 et 256 caractères.
6. Sélectionnez **S'inscrire**.
7. Après une inscription et une actualisation de la page réussies, le statut, le nom et la version du fournisseur VASA enregistré s'affichent. Après l'inscription, l'action de désinscription est activée.

Quelle est la prochaine étape

Vérifiez que le fournisseur VASA intégré est répertorié sous Fournisseur VASA à partir du client vCenter :

Étapes

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

Installer le plug-in NFS VAAI

Le plug-in NFS vStorage API for Array Integration (NFS VAAI) est un composant logiciel qui intègre VMware vSphere et les baies de stockage NFS. Installez le plug-in NFS VAAI à l'aide des ONTAP tools for VMware vSphere afin d'exploiter les fonctionnalités avancées de votre baie de stockage NFS pour décharger certaines opérations liées au stockage des hôtes ESXi vers la baie de stockage elle-même.

Avant de commencer

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

Étapes

1. Connectez-vous au client vSphere.
2. Sélectionnez **Raccourcis** > *Outils NetApp ONTAP * dans la section plug-ins.
3. Sélectionnez **Paramètres** > **Outils NFS VAAI**.
4. Lorsque le plug-in VAAI est téléchargé sur vCenter Server, sélectionnez **Modifier** dans la section **Version existante**. Si un plug-in VAAI n'est pas téléchargé sur le serveur vCenter, sélectionnez le bouton **Télécharger**.
5. Parcourez et sélectionnez le `.vib` fichier et sélectionnez **Télécharger** pour télécharger le fichier vers les outils ONTAP .

6. Sélectionnez **Installer sur l'hôte ESXI**, sélectionnez l'hôte ESXi sur lequel vous souhaitez installer le plug-in NFS VAAI, puis sélectionnez **Installer**.

   Seuls les hôtes ESXi éligibles pour l'installation du plug-in sont affichés. Vous pouvez surveiller la progression de l'installation dans la section des tâches récentes du client Web vSphere.

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

   Lorsque l'administrateur VMware redémarre l'hôte ESXi, les ONTAP tools for VMware vSphere détectent et activent automatiquement le plug-in NFS VAAI.

Quelle est la prochaine étape ?

Après avoir installé le plug-in NFS VAAI et redémarré votre hôte ESXi, vous devez configurer les stratégies d'exportation NFS correctes pour le déchargement de copie VAAI. Lors de la configuration de VAAI dans un environnement NFS, configurez les règles de politique d'exportation en tenant compte des exigences suivantes :

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

Pour plus d'informations sur la procédure, reportez-vous à "Configurer les politiques d'exportation NFS correctes pour le déchargement de copie VAAI" Article de la base de connaissances.

Informations connexes

"Prise en charge de VMware vStorage sur NFS"

"Activer ou désactiver NFSv4.0"

"Prise en charge ONTAP pour NFSv4.2"

Configurer les paramètres de l'hôte ESXi

La configuration des paramètres de délai d'expiration et de multi-chemin du serveur ESXi garantit une haute disponibilité et l'intégrité des données en permettant de basculer de manière transparente vers un chemin de stockage de sauvegarde en cas de défaillance d'un chemin principal.

Configurer les paramètres de multi-chemin et de délai d'expiration du serveur ESXi

Les ONTAP tools for VMware vSphere vérifient et définissent les paramètres multichemin 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

Selon votre configuration et la charge du système, ce processus peut prendre beaucoup de temps. La progression de la tâche est affichée dans le panneau Tâches récentes.

Étapes

1. Depuis la page d'accueil du client Web VMware vSphere, sélectionnez **Hôtes et clusters**.

2. Cliquez avec le bouton droit sur un hôte et sélectionnez * Outils NetApp ONTAP * > * Mettre à jour les données de l'hôte *.
3. Sur la page des raccourcis du client Web VMware vSphere, sélectionnez * Outils NetApp ONTAP * sous la section Plug-ins.
4. Accédez à la carte **Conformité de l'hôte ESXi** dans la présentation (tableau de bord) du plug-in ONTAP tools for VMware vSphere .
5. Sélectionnez le lien **Appliquer les paramètres recommandés**.
6. Dans la fenêtre **Appliquer les paramètres d'hôte recommandés**, sélectionnez les hôtes que vous souhaitez mettre à jour pour qu'ils soient conformes aux paramètres recommandés par NetApp et sélectionnez **Suivant**.

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

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

Définir les valeurs de l'hôte ESXi

À l'aide des ONTAP tools for VMware vSphere, vous pouvez définir des délais d'expiration et d'autres valeurs sur les hôtes ESXi pour garantir les meilleures performances et un basculement réussi. Les valeurs définies par les ONTAP tools for VMware vSphere sont basées sur des tests NetApp internes.

Vous pouvez définir les valeurs suivantes sur un hôte ESXi :

Paramètres de l'adaptateur HBA/CNA

Définit les paramètres suivants sur les valeurs par défaut :

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

Paramètres MPIO

Les paramètres MPIO définissent les chemins préférés pour les systèmes de stockage NetApp . Ils déterminent lesquels des chemins disponibles sont optimisés (par opposition aux chemins non optimisés qui traversent le câble d'interconnexion) et définissent le chemin préféré sur l'un de ces chemins.

Dans les environnements hautes performances ou lorsque vous testez les performances avec une seule banque de données LUN, envisagez de modifier le paramètre d'équilibrage de charge de la stratégie de sélection de chemin (PSP) à tour de rôle (VMW_PSP_RR) du paramètre IOPS par défaut de 1 000 à une valeur de 1.

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

Paramètres NFS

Paramètre	Définissez cette valeur sur…
Taille du tas Net.Tcpip	32
Net.TcpipHeapMax	1024 Mo
NFS.MaxVolumes	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128 ou plus
NFS.HeartbeatMaxFailures	10
Fréquence de battement de cœur NFS	12
Délai d'expiration du battement de cœur NFS	5

Configurer les rôles et privilèges des utilisateurs ONTAP

Vous pouvez configurer de nouveaux rôles et privilèges d'utilisateur pour la gestion des backends de stockage à l'aide du fichier JSON fourni avec les ONTAP tools for VMware vSphere et ONTAP System Manager.

Avant de commencer

- Vous devez avoir téléchargé le fichier de privilèges ONTAP à partir des ONTAP tools for VMware vSphere en utilisant *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip*.
- Vous devez avoir téléchargé le fichier ONTAP Privileges à partir des outils ONTAP en utilisant `https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip`.

> Vous pouvez créer des utilisateurs au niveau du cluster ou directement au niveau des machines virtuelles de stockage (SVM). Vous pouvez également créer des utilisateurs sans utiliser le fichier user_roles.json et si cela est fait, vous devez disposer d'un ensemble minimum de privilèges au niveau SVM.

- Vous devez vous être connecté avec des privilèges d'administrateur pour le backend de stockage.

Étapes

1. Extrayez le fichier *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* 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, procédez comme suit :
   a. Pour configurer l'utilisateur des outils Cluster ONTAP , sélectionnez le volet **Cluster** > **Paramètres** > **Utilisateurs et rôles**.
   b. Pour configurer l'utilisateur des outils SVM ONTAP , sélectionnez le volet **Stockage SVM** > **Paramètres** > **Utilisateurs et rôles**.
   c. Sélectionnez **Ajouter** sous Utilisateurs.
   d. Dans la boîte de dialogue **Ajouter un utilisateur**, sélectionnez **Produits de virtualisation**.
   e. **Parcourir** pour sélectionner et télécharger le fichier JSON des Privileges ONTAP .

Le champ Produit est rempli automatiquement.

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

   Le champ **Rôle** est automatiquement renseigné en fonction de la capacité du produit sélectionnée.

g. Entrez le nom d'utilisateur et le mot de passe requis.

h. Sélectionnez les privilèges (Découverte, Créer un stockage, Modifier un stockage, Détruire un stockage, Rôle NAS/SAN) requis pour l'utilisateur, puis sélectionnez **Ajouter**.

Le nouveau rôle et le nouveau utilisateur sont ajoutés et vous pouvez voir les privilèges détaillés sous le rôle que vous avez configuré.

Exigences de mappage d'agrégats SVM

Pour utiliser les informations d'identification de l'utilisateur SVM pour le provisionnement des banques de données, les ONTAP tools for VMware vSphere créent en interne des volumes sur l'agrégat spécifié dans l'API POST des banques de données. ONTAP n'autorise pas la création de volumes sur des agrégats non mappés sur une SVM à l'aide des informations d'identification de l'utilisateur SVM. Pour résoudre ce problème, vous devez mapper les SVM avec les agrégats à l'aide de l'API REST ou de la CLI ONTAP comme décrit ici.

API REST :

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

CLI ONTAP :

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

Créer un utilisateur et un rôle ONTAP manuellement

Suivez les instructions de cette section pour créer l'utilisateur et les rôles manuellement sans utiliser 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'administrateur.
   a. Pour configurer les rôles des outils ONTAP du cluster, sélectionnez le volet **Cluster** > **Paramètres** > **Utilisateurs et rôles**.
   b. Pour configurer les rôles des outils SVM ONTAP du cluster, sélectionnez **Storage SVM** > **Paramètres** > volet **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 l'accès correspondant à partir de 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 **Gestionnaire système**.
   c. Entrez le **Nom d'utilisateur**.
   d. Sélectionnez **Rôle** parmi les options créées à l'étape **Créer des rôles** ci-dessus.
   e. Saisissez les applications auxquelles donner accès et la méthode d'authentification. ONTAPI et HTTP sont les applications requises et le type d'authentification est **Mot de passe**.
   f. Définissez le **Mot de passe de l'utilisateur** et **Enregistrez** l'utilisateur.

Liste des privilèges minimaux requis pour les utilisateurs de cluster à portée globale non administrateurs

Les privilèges minimaux requis pour un utilisateur de cluster global non administrateur créé sans utiliser le fichier JSON des utilisateurs sont répertoriés dans cette section. Si un cluster est ajouté localement, il est recommandé d'utiliser le fichier JSON pour créer les utilisateurs, car les ONTAP tools for VMware vSphere nécessitent plus que de simples privilèges de lecture pour le provisionnement sur ONTAP.

Utilisation des API :

API	Niveau d'accès	Utilisé pour
/api/cluster	Lecture seule	Découverte de la configuration du cluster
/api/cluster/licensing/licences	Lecture seule	Vérification des licences pour les licences spécifiques au protocole
/api/cluster/nœuds	Lecture seule	Découverte du type de plate-forme
/api/sécurité/comptes	Lecture seule	Découverte des privilèges
/api/sécurité/rôles	Lecture seule	Découverte des privilèges
/api/storage/aggregates	Lecture seule	Vérification de l'espace agrégé lors de l'approvisionnement du magasin de données/volume
/api/storage/cluster	Lecture seule	Pour obtenir les données d'espace et d'efficacité au niveau du cluster
/api/storage/disques	Lecture seule	Pour obtenir les disques associés dans un agrégat
/api/storage/qos/policies	Lire/Créer/Modifier	Gestion de la qualité de service et des politiques de machines virtuelles
/api/svm/svms	Lecture seule	Pour obtenir la configuration SVM dans le cas où le cluster est ajouté localement.

/api/réseau/ip/interfaces	Lecture seule	Ajouter un backend de stockage - Pour identifier la portée du LIF de gestion est Cluster/SVM
/api/storage/zones-de-disponibilité	Lecture seule	Découverte SAZ. Applicable aux versions ONTAP 9.16.1 et ultérieures et aux systèmes ASA r2.

Créer des ONTAP tools for VMware vSphere ONTAP

> Vous avez besoin de découvrir, de créer, de modifier et de détruire des Privileges pour effectuer des opérations PATCH et une restauration automatique en cas de défaillance sur les banques de données. L'absence de tous ces privilèges entraîne des perturbations du flux de travail et des problèmes de nettoyage.

La création ONTAP tools for VMware vSphere ONTAP avec des privilèges de découverte, de création de stockage, de modification de stockage et de destruction de stockage permet de lancer des découvertes et de gérer les flux de travail des outils ONTAP .

Pour créer un utilisateur à l'échelle du cluster avec 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
```

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 les versions ONTAP 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 des ONTAP tools for VMware vSphere ONTAP

Pour créer un utilisateur de portée SVM avec tous les privilèges, exécutez les commandes suivantes :

```
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 à l'aide des rôles basés sur l'API créés ci-dessus, exécutez la commande suivante :

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

Exemple:

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

Pour déverrouiller le compte, pour activer l'accès à l'interface de gestion, exécutez la commande suivante :

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

Exemple:

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

Mettre à niveau les ONTAP tools for VMware vSphere 10.1 vers l'utilisateur 10.3

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

Pour les fonctionnalités du produit :

- VSC
- Fournisseur VSC et VASA

- VSC et SRA
- VSC, fournisseur VASA et SRA.

Privilèges du cluster :

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "vserver nvme namespace show" -access all

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "vserver nvme subsystem show" -access all

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "vserver nvme subsystem host show" -access all

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "vserver nvme subsystem map show" -access all

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "vserver nvme show-interface" -access read

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "vserver nvme subsystem host add" -access all

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "vserver nvme subsystem map add" -access all

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "suppression-de-l'espace-de-noms-vserver-nvme" -access-all

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "suppression-du-sous-système-vserver nvme" -access-all

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "supprimer l'hôte du sous-système vserver nvme" -access all

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "vserver nvme subsystem map remove" -access all

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

Privilèges SVM :

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "vserver nvme namespace show" -access all -vserver <nom-de-serveur-v>

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "vserver nvme subsystem show" -access all -vserver <nom-de-serveur-v>

security login role create -role <nom-de-rôle-existant> -cmddirname "vserver nvme subsystem host show" -access all -vserver <nom-de-serveur-v>

security login role create -role <nom-de-rôle-existant> -cmddirname "vserver nvme subsystem map show" -access all -vserver <nom-de-serveur-v>

security login role create -role <nom-de-rôle-existant> -cmddirname "vserver nvme show-interface" -access read -vserver <nom-de-serveur-v>

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "vserver nvme subsystem host add" -access all -vserver <nom-de-serveur-v>

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "vserver nvme subsystem map add" -access all -vserver <nom-de-serveur-v>

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "suppression-de-l'espace-de-noms-vserver-nvme" -access-all -vserver <nom-de-vserver>

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "suppression-du-sous-système-vserver-nvme" -access-all -vserver <nom-du-serveur-v>

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "supprimer l'hôte du sous-système NVME vserver" -access all -vserver <nom-de-serveur-v>

création de rôle de connexion de sécurité -role <nom-de-rôle-existant> -cmddirname "supprimer la carte du sous-système vserver nvme" -access all -vserver <nom-de-vserver>

L'ajout de la commande *vserver nvme namespace show* et *vserver nvme subsystem show* au rôle existant ajoute les commandes suivantes.

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

Mettre à niveau les ONTAP tools for VMware vSphere 10.3 vers l'utilisateur 10.4

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

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

Pour les fonctionnalités du produit :

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

Privilèges du cluster :

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

Ajouter un backend de stockage

L'ajout d'un backend de stockage vous permet d'intégrer un cluster ONTAP .

À propos de cette tâche

Dans le cas de configurations multi-locataires où vCenter agit en tant que locataire avec un SVM associé, utilisez ONTAP Tools Manager pour ajouter le cluster. Associez le backend de stockage au vCenter Server pour le mapper globalement à l'instance vCenter Server intégrée. Le locataire vCenter doit intégrer les machines virtuelles de stockage (SVM) souhaitées. Cela permet à un utilisateur SVM de provisionner des banques de données vVols . Vous pouvez ajouter du stockage dans vCenter à l'aide du SVM.

Ajoutez les backends de stockage locaux avec les informations d'identification de cluster ou SVM à l'aide de l'interface utilisateur des outils ONTAP . Ces backends de stockage sont limités à un seul vCenter. Lors de l'utilisation des informations d'identification du cluster localement, les SVM associées sont automatiquement mappées au vCenter pour gérer les vVols ou VMFS. Pour la gestion VMFS, y compris SRA, les outils ONTAP prennent en charge les informations d'identification SVM sans avoir besoin d'un cluster global.

Utilisation du gestionnaire d'outils ONTAP

> Dans une configuration multi-locataire, vous pouvez ajouter un cluster back-end de stockage globalement et SVM localement pour utiliser les informations d'identification de l'utilisateur SVM.

Étapes

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

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

Utilisation de l'interface utilisateur du client vSphere

> Lors de la configuration d'un backend de stockage via l'interface utilisateur du client vSphere, il est important de noter que les banques de données vVols ne prennent pas en charge l'ajout direct d'un utilisateur SVM.

1. Connectez-vous au client vSphere.
2. Dans la page des raccourcis, sélectionnez * Outils NetApp ONTAP * sous la section plug-ins.
3. Sélectionnez **Backends de stockage** dans la barre latérale.
4. Ajoutez le backend de stockage et fournissez l'adresse IP du serveur, le nom d'utilisateur, le mot de passe et les détails du port.

   > Pour ajouter directement un utilisateur SVM, vous pouvez ajouter des informations d'identification basées sur le cluster et des LIF de gestion d'adresses IPv4 et IPv6 ou fournir des informations d'identification basées sur SVM avec un LIF de gestion SVM.

Quelle est la prochaine étape ?

La liste est actualisée et vous pouvez voir le backend de stockage nouvellement ajouté dans la liste.

Associer un backend de stockage à une instance vCenter Server

Associez un backend de stockage au vCenter Server pour créer un mappage entre le backend de stockage et l'instance vCenter Server intégrée à l'échelle mondiale.

Étapes

1. Lancez le gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`

2. Connectez-vous avec les informations d'identification d'administrateur des ONTAP tools for VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez vCenter dans la barre latérale.
4. Sélectionnez les points de suspension verticaux par rapport à l'instance vCenter Server que vous souhaitez associer aux backends de stockage.
5. Sélectionnez le backend de stockage dans la liste déroulante pour associer l'instance vCenter Server au backend de stockage requis.

Configurer l'accès au réseau

Si vous n'avez pas configuré l'accès réseau, toutes les adresses IP découvertes à partir de l'hôte ESXi sont ajoutées à la stratégie d'exportation par défaut. Vous pouvez le configurer pour ajouter quelques adresses IP spécifiques à la politique d'exportation et exclure le reste. Cependant, lorsque vous effectuez une opération de montage sur les hôtes ESXi exclus, l'opération échoue.

Étapes

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

   Pour ajouter plusieurs adresses IP, séparez la liste par des virgules, une plage, un routage inter-domaines sans classe (CIDR) ou une combinaison des trois.

4. Sélectionnez **Enregistrer**.

Créer un magasin de données

Lorsque vous créez une banque de données au niveau du cluster hôte, la banque de données est créée et montée sur tous les hôtes de la destination, et l'action est activée uniquement si l'utilisateur actuel dispose du privilège d'exécution.

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

Les ONTAP tools for VMware vSphere 10 créent des igroups imbriqués pour les banques de données, avec des igroups parents spécifiques aux banques de données et des igroups enfants mappés aux hôtes. Vous pouvez créer des groupes i plats à partir du gestionnaire système ONTAP et les utiliser pour créer des banques de données VMFS sans utiliser les outils ONTAP . Se référer à "Gérer les initiateurs et les groupes SAN" pour plus d'informations.

Lorsque le stockage est intégré aux outils ONTAP et que la découverte de banque de données est exécutée, les groupes i plats et les banques de données VMFS deviennent gérés par les outils ONTAP et sont convertis en groupes i imbriqués. Vous ne pouvez pas utiliser les groupes i plats précédents pour créer de nouveaux magasins de données ; vous devez utiliser l'interface utilisateur des outils ONTAP ou l'API REST pour réutiliser les groupes i imbriqués.

Créer une banque de données vVols

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

Avant de commencer

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

Étapes

1. Connectez-vous au client vSphere.
2. Cliquez avec le bouton droit sur un système hôte, un cluster hôte ou un centre de données et sélectionnez * Outils NetApp ONTAP * > * Créer une banque de données *.
3. Sélectionnez vVols **Type de magasin de données**.
4. Saisissez le **Nom du magasin de données** 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 dans laquelle vous souhaitez créer la banque de données.
6. Sous options avancées :
   - Si vous sélectionnez la **politique d'exportation personnalisée**, assurez-vous d'exécuter la découverte dans vCenter pour tous les objets. Il est recommandé de ne pas utiliser cette option.
   - Vous pouvez sélectionner le nom du **groupe d'initiateurs personnalisé** pour les protocoles iSCSI et FC.

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

7. Dans le volet **Attributs de stockage**, vous pouvez créer de nouveaux volumes ou utiliser les volumes existants. Cependant, vous ne pouvez pas combiner ces deux types de volumes pour créer une banque de données vVols .

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

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

Créer une banque de données NFS

Une banque de données VMware Network File System (NFS) utilise le protocole NFS pour connecter les hôtes ESXi à un périphérique de stockage partagé via un réseau. Les banques de données NFS sont couramment utilisées dans les environnements VMware vSphere et offrent plusieurs avantages, tels que la simplicité et la flexibilité.

Étapes

1. Connectez-vous au client vSphere.
2. Cliquez avec le bouton droit sur un système hôte, un cluster hôte ou un centre de données et sélectionnez * Outils NetApp ONTAP * > * Créer une banque de données *.
3. Sélectionnez NFS dans le champ **Type de magasin de données**.
4. Saisissez le nom, la taille et les informations de protocole du magasin de données dans le volet **Nom et protocole**. Sélectionnez **Cluster de banque de données** et **Authentification Kerberos** 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 **Politique d'exportation personnalisée** sous les options avancées, exécutez la découverte dans vCenter pour tous les objets. Il est recommandé de ne pas utiliser cette option.

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

   - Dans les options avancées, le bouton bascule **Asymétrique** n'est visible que si les performances ou la capacité sont sélectionnées dans la liste déroulante de la plateforme.
   - Lorsque vous choisissez l'option **Tout** dans la liste déroulante de la plate-forme, vous pouvez voir les SVM qui font partie du vCenter, quelle que soit la plate-forme ou l'indicateur asymétrique.
7. Sélectionnez l'agrégat pour la création de volume dans le volet **Attributs de stockage**. Dans les options avancées, choisissez **Réserve d'espace** et **Activer QoS** selon vos besoins.
8. Vérifiez les sélections dans le volet **Résumé** et sélectionnez **Terminer**.

Le magasin de données NFS est créé et monté sur tous les hôtes.

Créer une banque de données VMFS

Virtual Machine File System (VMFS) est un système de fichiers en cluster qui stocke les fichiers de machine virtuelle dans les environnements VMware vSphere. VMFS permet à plusieurs hôtes ESXi d'accéder simultanément aux mêmes fichiers de machine virtuelle, activant ainsi des fonctionnalités telles que vMotion et la haute disponibilité.

Sur un cluster protégé :

- Vous ne pouvez créer que des banques de données VMFS. Lorsque vous ajoutez une banque de données VMFS à un cluster protégé, la banque de données devient automatiquement protégée.
- Vous ne pouvez pas créer une banque de données sur un centre de données avec un ou plusieurs clusters d'hôtes protégés.
- Vous ne pouvez pas créer de banque de données sur l'hôte ESXi si le cluster d'hôte parent est protégé par une relation de type « Politique de duplex de basculement automatisé » (configuration uniforme/non uniforme).
- Vous pouvez créer une banque de données VMFS uniquement sur un hôte ESXi protégé par une relation asynchrone. Vous ne pouvez pas créer et monter une banque de données sur un hôte ESXi qui fait partie d'un cluster d'hôtes protégé par la stratégie « Duplex de basculement automatisé ».

Avant de commencer

- Activez les services et les LIF pour chaque protocole côté stockage ONTAP .
- Mapper SVM pour agréger l'utilisateur SVM dans le système de stockage ASA r2.
- Configurez l'hôte ESXi si vous utilisez le protocole NVMe/TCP :
  a. Passez en revue le "Guide de compatibilité VMware"

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

  b. Vérifiez si le fournisseur de la carte d'interface réseau (NIC) prend en charge la carte réseau ESXi avec le protocole NVMe/TCP.
  c. Configurez la carte réseau ESXi pour NVMe/TCP conformément aux spécifications du fournisseur de la carte réseau.
  d. Lorsque vous utilisez la version VMware vSphere 7, suivez les instructions sur le site VMware "Configurer la liaison VMkernel pour l'adaptateur NVMe sur TCP" pour configurer la liaison de port NVMe/TCP. Lorsque vous utilisez la version VMware vSphere 8, suivez "Configuration de NVMe sur TCP sur ESXi" , pour configurer la liaison du port NVMe/TCP.
  e. Pour la version VMware vSphere 7, suivez les instructions de la page "Activer les adaptateurs logiciels NVMe sur RDMA ou NVMe sur TCP" pour configurer les adaptateurs logiciels NVMe/TCP. Pour la version VMware vSphere 8, suivez "Ajoutez des adaptateurs NVMe sur RDMA ou NVMe sur TCP" pour configurer les adaptateurs logiciels NVMe/TCP.
  f. Courir"Découvrez les systèmes de stockage et les hôtes" 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 banques de données 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 vos hôtes ESXi.
  b. Zonage SCSI complet.
  c. Assurez-vous que les hôtes ESXi et le système ONTAP sont connectés au niveau d'une couche physique et logique.

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

Pour plus d'informations sur l'utilisation du protocole NVMe/FC avec VMware vSphere 8.0, reportez-vous à "Configuration de l'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 hôte ou un centre de données et sélectionnez * Outils NetApp ONTAP * > * Créer une banque de données *.
3. Sélectionnez le type de banque de données VMFS.
4. Saisissez le nom, la taille et les informations de protocole du magasin de données dans le volet **Nom et protocole**. Si vous choisissez d'ajouter la nouvelle banque de données à un cluster de banques de données VMFS existant, sélectionnez le sélecteur de cluster de banques de données sous Options avancées.

5. Sélectionnez la machine virtuelle de stockage dans le volet **Stockage**. Indiquez le **Nom du groupe d'initiateurs personnalisé** dans la section **Options avancées** selon les besoins. Vous pouvez choisir un igroup existant pour le magasin de données ou créer un nouveau igroup avec un nom personnalisé.

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

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

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

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

   b. Conformément au protocole sélectionné, une unité de stockage (LUN/Namespace) est créée avec une réserve d'espace de type thin.

   > 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 de performances** pour les systèmes de stockage ASA r2 avec 12 nœuds SVM qui est un cluster hétérogène. Cette option n'est pas disponible si le SVM sélectionné est un cluster homogène ou utilise un utilisateur SVM.

      « Tout » est la valeur par défaut du niveau de service de performance (PSL). Ce paramètre crée l'unité de stockage à l'aide de l'algorithme de placement équilibré ONTAP . Cependant, vous pouvez sélectionner l'option performance ou extrême 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 volume ne s'applique pas à la création d'unité de stockage (LUN/espace de noms). Par conséquent, ces options ne sont pas affichées.

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

7. Vérifiez les détails du magasin de données dans le volet **Résumé** et sélectionnez **Terminer**.

> Si vous créez la banque de données sur un cluster protégé, vous pouvez voir un message en lecture seule : « La banque de données est en cours de montage sur un cluster protégé. »

Résultat

Le magasin de données VMFS est créé et monté sur tous les hôtes.

Protéger les banques de données et les machines virtuelles

Protéger à l'aide de la protection du cluster hôte

Les ONTAP tools for VMware vSphere gèrent la protection des clusters hôtes. Tous les magasins de données appartenant au SVM sélectionné et montés sur un ou plusieurs hôtes du cluster sont protégés sous un cluster hôte.

Avant de commencer

Assurez-vous que les conditions préalables suivantes sont remplies :

- Le cluster hôte dispose de banques de données provenant uniquement d'une seule SVM.
- Le magasin de données monté sur le cluster hôte ne doit pas être monté sur un hôte extérieur au cluster.
- Tous les magasins de données montés sur le cluster hôte doivent être des magasins de données VMFS avec le protocole iSCSI/FC. Les magasins de données vVols, NFS ou VMFS avec les protocoles NVMe/FC et NVMe/TCP ne sont pas pris en charge.
- Les banques de données formant FlexVol/LUN montées sur le cluster hôte ne doivent pas faire partie d'un groupe de cohérence (CG) existant.
- Les banques de données formant FlexVol/LUN montées sur le cluster hôte ne doivent pas faire partie d'une relation SnapMirror existante.
- Le cluster hôte doit avoir au moins une banque de données.

Étapes

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

   Le type de politique peut être asynchrone ou automatiséFailOverDuplex.

   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 les ONTAP tools for VMware vSphere sont déployés.

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

7. Si vous choisissez une configuration d'hôte non uniforme, sélectionnez l'accès à l'hôte (source/cible) pour chaque hôte à l'intérieur de ce cluster.
8. Sélectionnez **Ajouter**.
9. Dans la fenêtre **Protéger le cluster**, vous ne pouvez pas modifier le cluster protégé pendant l'opération de création. Vous pouvez supprimer et ajouter à nouveau la protection. Pendant l'opération de modification de la protection du cluster d'hôtes, l'option de modification est disponible. Vous pouvez modifier ou supprimer les relations à l'aide des options du menu à points de suspension.
10. Sélectionnez le bouton **Protéger**.

    Une tâche vCenter est créée avec les détails de l'ID de tâche et sa progression est affichée dans le panneau des tâches récentes. Il s'agit d'une tâche asynchrone ; l'interface utilisateur affiche uniquement l'état de soumission de la demande et n'attend pas que la tâche soit terminée.

11. Pour afficher les clusters d'hôtes protégés, accédez à * Outils NetApp ONTAP * > **Protection** > **Relations entre les clusters d'hôtes**.

Protégez-vous en utilisant la protection SRA

Configurer SRA pour protéger les banques de données

Les ONTAP tools for 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 vCenter Server et configuré l'hôte ESXi.
- Vous devez avoir déployé les ONTAP tools for VMware vSphere.
- Vous auriez dû télécharger l'adaptateur SRA `.tar.gz` fichier du "Site de support NetApp" .
- Les clusters ONTAP source et de destination doivent avoir les mêmes planifications SnapMirror personnalisées créées avant d'exécuter les workflows SRA.
- "Activer les ONTAP tools for VMware vSphere" pour activer la capacité SRA.

Étapes

1. Connectez-vous à l'interface de gestion du dispositif 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 du dispositif VMware VMware Live Site Recovery.
2. Sélectionnez **Nouvel adaptateur**.
3. Téléchargez le programme d'installation *.tar.gz* du plug-in SRA sur VMware Live Site Recovery.
4. Analysez à nouveau les adaptateurs pour vérifier que les détails sont mis à jour sur la page Adaptateurs de réplication de stockage VMware Live Site Recovery.

Configurer SRA 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

Avant de commencer

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

- Récupération de site VMware Live

  La documentation sur l'installation de VMware Live Site Recovery est disponible sur le site VMware.

  "À propos de VMware Live Site Recovery"

- SRA

  L'adaptateur est installé sur VMware Live Site Recovery.

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 le `ostype` option définie sur *VMware* sur le système de stockage principal.
3. Vérifiez que les hôtes ESXi sur le site de récupération disposent d'une connectivité iSCSI appropriée à la machine virtuelle de stockage (SVM). Les hôtes ESXi du site secondaire doivent avoir accès au stockage du site secondaire et les hôtes ESXi du site principal doivent avoir accès au stockage du site principal.

   Vous pouvez le faire soit en vérifiant que les hôtes ESXi ont des LUN locaux connectés sur la SVM ou sur le `iscsi show initiators` commande sur les SVM. Vérifiez l'accès LUN pour les LUN mappés dans l'hôte ESXi pour vérifier la connectivité iSCSI.

Configurer SRA pour les environnements NAS

Avant de commencer

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

- Récupération de site VMware Live

  La documentation sur l'installation de VMware Live Site Recovery est disponible sur le site VMware.

  "À propos de VMware Live Site Recovery"

- SRA

  L'adaptateur est installé sur VMware Live Site Recovery et le serveur SRA.

Étapes

1. Vérifiez que les banques de données du site protégé contiennent des machines virtuelles enregistrées auprès de vCenter Server.
2. Vérifiez que les hôtes ESXi sur le site protégé ont monté les volumes d'exportation NFS à partir de la machine virtuelle de stockage (SVM).
3. Vérifiez que des adresses valides, telles que l'adresse IP ou le nom de domaine complet (FQDN) sur lesquels les exportations NFS sont présentes, sont spécifiées dans le champ « Adresses NFS » lorsque vous utilisez l'assistant Gestionnaire de baies pour ajouter des baies à VMware Live Site Recovery.

N'utilisez pas le nom d'hôte NFS dans le champ « Adresses NFS ».

4. Utilisez le `ping` commande sur chaque hôte ESXi sur le site de récupération pour vérifier que l'hôte dispose d'un port VMkernel qui peut accéder aux adresses IP utilisées pour traiter les exportations NFS à partir du SVM.

Configurer SRA pour les environnements à grande échelle

Vous devez configurer les intervalles de délai d'expiration de stockage conformément aux paramètres recommandés pour l'adaptateur de réplication de stockage (SRA) afin de fonctionner de manière optimale dans des 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 évolutif :

Paramètres avancés	Valeurs de délai d'attente
`StorageProvider.resignatureTimeout`	Augmentez la valeur du paramètre de 900 secondes à 12 000 secondes.
`storageProvider.hostRescanDelaySec`	60
`storageProvider.hostRescanRepeatCnt`	20
`storageProvider.hostRescanTimeoutSec`	Définissez une valeur élevée (par exemple : 99999)

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

Se référer à "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.

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

Se référer à "Modifier les paramètres de stockage" pour modifier les paramètres du fournisseur SAN.

Configurer SRA sur le dispositif VMware Live Site Recovery

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

La configuration de SRA sur l'appliance VMware Live Site Recovery enregistre les ONTAP tools for VMware

vSphere au sein de l'appliance, permettant ainsi la communication entre VMware Live Site Recovery et SRA.

Avant de commencer

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

Étapes

1. Sur l'écran du dispositif VMware Live Site Recovery, sélectionnez **Adaptateur de réplication de stockage** > **Nouvel adaptateur**.
2. Téléchargez le fichier *.tar.gz* sur VMware Live Site Recovery.
3. Connectez-vous au dispositif VMware Live Site Recovery à l'aide d'un compte administrateur via un client SSH tel que PuTTY.
4. Passez à l'utilisateur root en utilisant la commande : `su root`
5. Exécutez la commande `cd /var/log/vmware/srm` pour accéder au répertoire des journaux.
6. À l'emplacement du journal, entrez la commande pour obtenir l'ID Docker utilisé par SRA : `docker ps -l`
7. Pour vous connecter à l'ID du conteneur, entrez la commande : `docker exec -it -u srm <container id> sh`
8. Configurez VMware Live Site Recovery avec les ONTAP tools for VMware vSphere à l'aide de la commande : `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
   - Fournissez le mot de passe entre guillemets simples afin que le script Perl traite les caractères spéciaux comme faisant partie du mot de passe, et non comme des délimiteurs.
   - Vous pouvez définir le nom d'utilisateur et le mot de passe de l'application (fournisseur VASA/SRA) dans ONTAP Tools Manager lors de la première activation de ces services. Utilisez ces informations d'identification pour enregistrer SRA auprès de VMware Live Site Recovery.
   - Pour localiser le GUID vCenter, accédez à la page vCenter Server dans ONTAP Tools Manager après avoir ajouté votre instance vCenter. Se référer à"Ajouter des serveurs vCenter" section.
9. Analysez à nouveau les adaptateurs pour confirmer que les détails mis à jour apparaissent sur la page Adaptateurs de réplication de stockage VMware Live Site Recovery.

Résultats

Un message de confirmation s'affiche, indiquant que les informations d'identification de stockage ont été enregistrées. SRA peut désormais 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

Pour que VMware Live Site Recovery communique 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 devriez avoir exécuté les étapes mentionnées dans le sujet"Configuration de SRA sur le dispositif VMware Live Site Recovery" .

Étapes

1. Exécutez les commandes suivantes pour supprimer le nom d'utilisateur et le mot de passe des outils ONTAP mis en cache dans le dossier de 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 -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv -password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>`Vous devez avoir une seule apostrophe autour de la valeur du mot de passe.

      Un message de réussite confirmant que les informations d'identification de stockage sont enregistrées s'affiche. SRA peut communiquer avec le serveur SRA en utilisant l'adresse IP, le port et les informations d'identification fournis.

Configurer les sites protégés et de récupération

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

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

Sites de protection et de récupération des paires

Vous devez associer les sites protégés et de récupération créés à l'aide de votre client vSphere 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 de synchronisation de type Duplex de basculement automatisé et une relation asynchrone SnapMirror sur le groupe de cohérence. Cependant, la distribution en éventail avec deux SnapMirror asynchrones sur un groupe de cohérence ou la distribution en éventail avec deux SnapMirrors sur un volume n'est pas prise en charge.

Avant de commencer

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

- Vous devez avoir SRA installé sur les sites protégés et de récupération.

Étapes

1. Double-cliquez sur **Site Recovery** sur la page d'accueil de vSphere Client et sélectionnez **Sites**.
2. Sélectionnez **Objets** > **Actions** > **Sites appariés**.
3. Dans la boîte de dialogue **Pair Site Recovery Manager Servers**, entrez l'adresse du Platform Services Controller du site protégé, puis sélectionnez **Suivant**.
4. Dans la section Sélectionner vCenter Server, procédez comme suit :
   a. Vérifiez que le serveur vCenter du site protégé apparaît comme un candidat correspondant à associer.
   b. Saisissez les informations d'identification administratives SSO, puis sélectionnez **Terminer**.
5. Si vous y êtes invité, sélectionnez **Oui** pour accepter les certificats de sécurité.

Résultat

Les sites protégés et de récupération apparaîtront dans la boîte de dialogue Objets.

Configurer les groupes de protection

Avant de commencer

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

- Même version de VMware Live Site Recovery installée
- Machines virtuelles
- Sites protégés et de récupération appariés
- Les magasins de données source et de destination doivent être montés sur des sites respectifs

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **Site Recovery** > **Groupes de protection**.
2. Dans le volet **Groupes de protection**, sélectionnez **Nouveau**.
3. Spécifiez un nom et une description pour le groupe de protection, la direction et sélectionnez **Suivant**.
4. Dans le champ **Type**, sélectionnez l'option **Type** comme groupes de banques de données (réplication basée sur une baie) pour les banques de données NFS et VMFS. Le domaine d'erreur ne comprend que les SVM avec réplication activée. Les SVM pour lesquelles seul le peering est implémenté et qui ne présentent aucun problème sont affichées.
5. Dans l'onglet Groupes de réplication, sélectionnez la paire de baies activée ou 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 au nouveau plan de récupération**.
7. Dans l'onglet Prêt à terminer, vérifiez les détails du groupe de protection que vous avez créé, puis sélectionnez **Terminer**.

Configurer les ressources du site protégé et de récupération

Configurer les mappages réseau

Vous devez configurer vos mappages de ressources tels que les réseaux de machines virtuelles, les hôtes ESXi et les dossiers sur les deux sites pour 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 :

- Cartographies de réseau
- Mappages de dossiers
- Cartographie des ressources
- Magasins de données d'espace réservé

Avant de commencer

Vous devez avoir connecté les sites protégés et de récupération.

Étapes

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

Résultat

La page Mappages réseau affiche les ressources du site protégé et les ressources du site de récupération. Vous pouvez suivre les mêmes étapes pour d'autres réseaux de votre environnement.

Configurer les mappages de dossiers

Vous devez mapper vos dossiers sur le site protégé et le site de récupération pour 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 **Site Recovery** > **Sites**.
2. Sélectionnez votre site protégé et sélectionnez **Gérer**.
3. Sélectionnez **Mappages de dossiers** > icône **Dossier** dans l'onglet Gérer pour créer un nouveau mappage de dossiers.

4. Dans l'assistant de création de mappage de dossiers, procédez comme suit :
    a. Sélectionnez **Préparer automatiquement les mappages pour les dossiers avec des noms correspondants** et sélectionnez **Suivant**.
    b. Sélectionnez les objets du centre de données requis pour les sites protégés et de récupération et sélectionnez **Ajouter des mappages**.
    c. Sélectionnez **Suivant** une fois les mappages créés avec succès.
    d. Sélectionnez l'objet utilisé précédemment pour créer le mappage inversé, puis sélectionnez **Terminer**.

Résultat

La page Mappages de dossiers affiche les ressources du site protégé et les ressources du site de récupération. Vous pouvez suivre les mêmes étapes pour d'autres réseaux de votre environnement.

Configurer les mappages de ressources

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

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 **Site Recovery** > **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 de création de mappage de ressources, procédez comme suit :
    a. Sélectionnez **Préparer automatiquement les mappages pour les ressources avec des noms correspondants** et sélectionnez **Suivant**.
    b. Sélectionnez les objets du centre de données requis pour les sites protégés et de récupération et sélectionnez **Ajouter des mappages**.
    c. Sélectionnez **Suivant** une fois les mappages créés avec succès.
    d. Sélectionnez l'objet utilisé précédemment pour créer le mappage inversé, puis sélectionnez **Terminer**.

Résultat

La page Mappages de ressources affiche les ressources du site protégé et les ressources du site de récupération. Vous pouvez suivre les mêmes étapes pour d'autres réseaux de votre environnement.

Configurer des magasins de données d'espace réservé

Vous devez configurer un magasin de données d'espace réservé pour réserver un emplacement dans l'inventaire vCenter du site de récupération pour la machine virtuelle protégée (VM). Ce magasin de données n'a pas besoin d'être volumineux, car les VM

d'espace réservé sont petites et n'utilisent que quelques centaines de kilo-octets, voire moins.

Avant de commencer

- Vous devez avoir connecté les sites protégés et de récupération.
- Vous devriez avoir configuré vos mappages de ressources.

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **Site Recovery** > **Sites**.
2. Sélectionnez votre site protégé et sélectionnez **Gérer**.
3. Sélectionnez **Magasins de données d'espace réservé** > **Nouveau** dans l'onglet Gérer pour créer un nouveau magasin de données d'espace réservé.
4. Sélectionnez le magasin de données approprié et sélectionnez **OK**.

> Les magasins de données d'espace réservé peuvent être locaux ou distants et ne doivent pas être répliqués.

5. Répétez les étapes 3 à 5 pour configurer une banque de données d'espace réservé pour le site de récupération.

Configurer SRA à l'aide du gestionnaire de baies

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

Avant de commencer

- Vous devez avoir 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 baies.
- 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 activer la multilocation.

SRA prend en charge la gestion au niveau du cluster et la gestion au niveau SVM. Si vous ajoutez du stockage au niveau du cluster, vous pouvez alors découvrir et effectuer des opérations sur toutes les SVM du cluster. Si vous ajoutez du stockage au niveau SVM, vous ne pouvez gérer que ce 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 tableau dans le champ **Nom d'affichage**.
   b. Dans le champ **Type SRA**, sélectionnez **Adaptateur de réplication de stockage NetApp pour ONTAP**.
   c. Saisissez les informations pour vous connecter au cluster ou au SVM :
      - Si vous vous connectez à un cluster, vous devez saisir le LIF de gestion du cluster.

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

> Lors de la configuration du gestionnaire de baies, vous devez utiliser la même connexion (adresse IP) pour le système de stockage qui a été utilisé pour intégrer le système de stockage dans les ONTAP tools for VMware vSphere. Par exemple, si la configuration du gestionnaire de baies est limitée à SVM, le stockage sous les 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 **Nom de la SVM** ou laissez-le vide pour gérer toutes les SVM du cluster.

e. Saisissez les volumes à découvrir dans le champ **Liste des volumes inclus**.

   Vous pouvez entrer le volume source sur le site protégé et le volume de destination répliqué sur le site de récupération.

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

f. **(Facultatif)** Saisissez les volumes à exclure de la découverte dans le champ **Liste d'exclusion de volumes**.

   Vous pouvez entrer le volume source sur le site protégé et le volume de destination répliqué sur le site de récupération.

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

Vous pouvez suivre les mêmes étapes pour le site de récupération en utilisant les adresses IP et les informations d'identification de gestion SVM appropriées. 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 s'affiche comme prête à être activée.

Vérifier les systèmes de stockage répliqués

Vous devez vérifier que le site protégé et le site de récupération sont correctement couplés après la configuration de l'adaptateur de réplication de stockage (SRA). Le système de stockage répliqué doit être détectable à la fois par le site protégé et par le site de récupération.

Avant de commencer

- Vous devriez 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 et planifications SnapMirror sur les sites source et de destination.

Étapes

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

   Les systèmes de stockage doivent être découverts sur le site protégé et sur le site de récupération avec le statut « Activé ».

Protection en éventail

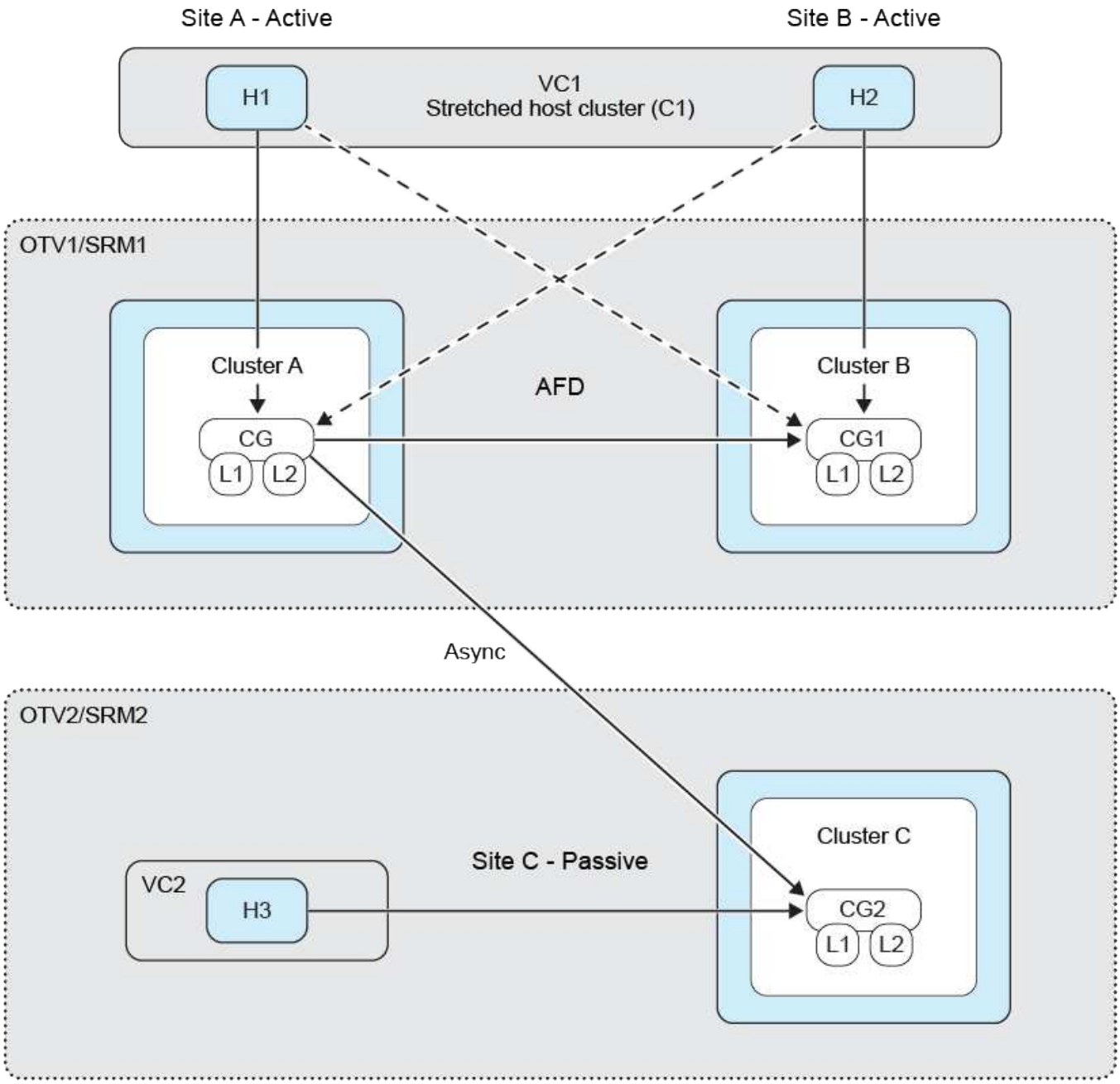
Dans une protection en éventail, le groupe de cohérence est doublement protégé avec une relation synchrone sur le premier cluster ONTAP de destination et avec une relation asynchrone sur le deuxième cluster ONTAP de destination. Les flux de travail de création, de modification et de suppression de la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

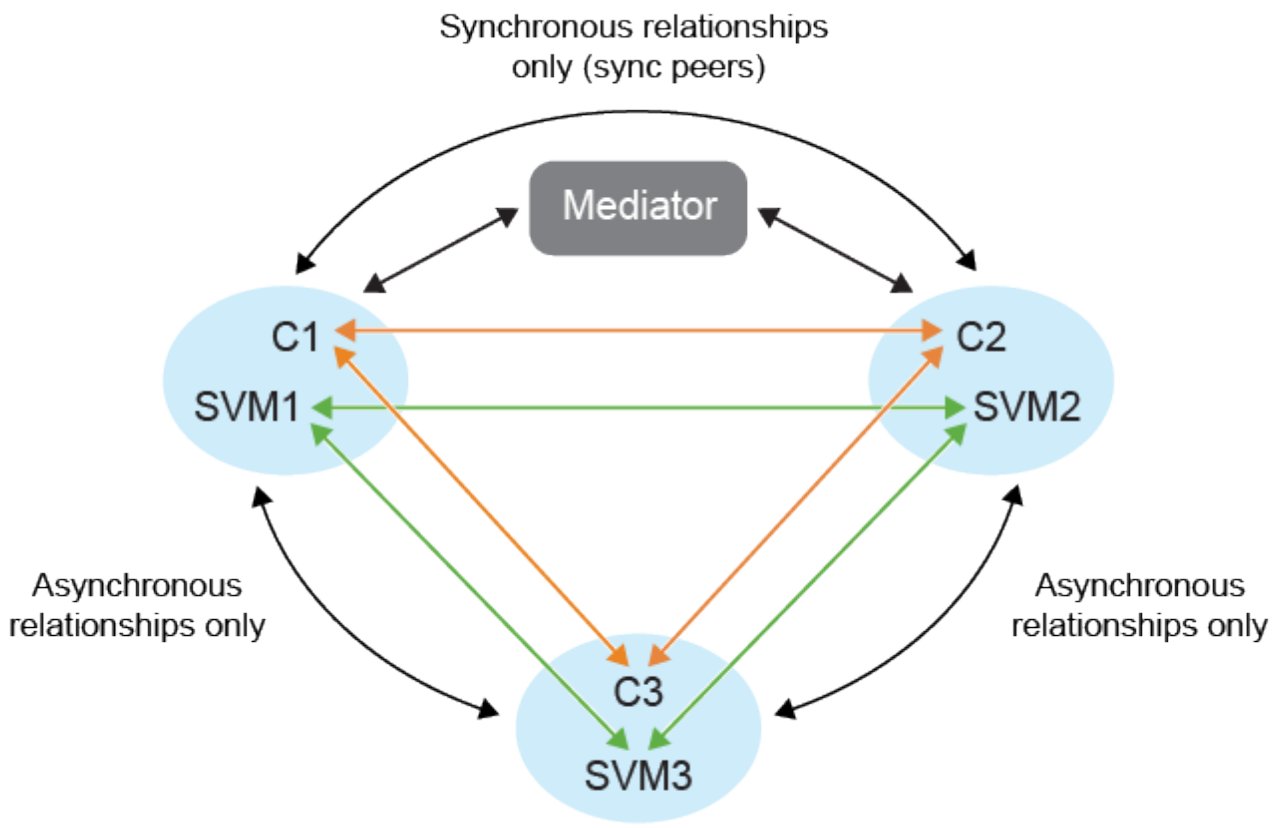
Afin d'établir une protection en éventail, vous devez associer trois clusters de sites et SVM.

Exemple:

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

Le schéma suivant montre la configuration de la protection contre le déploiement :


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



Mesures

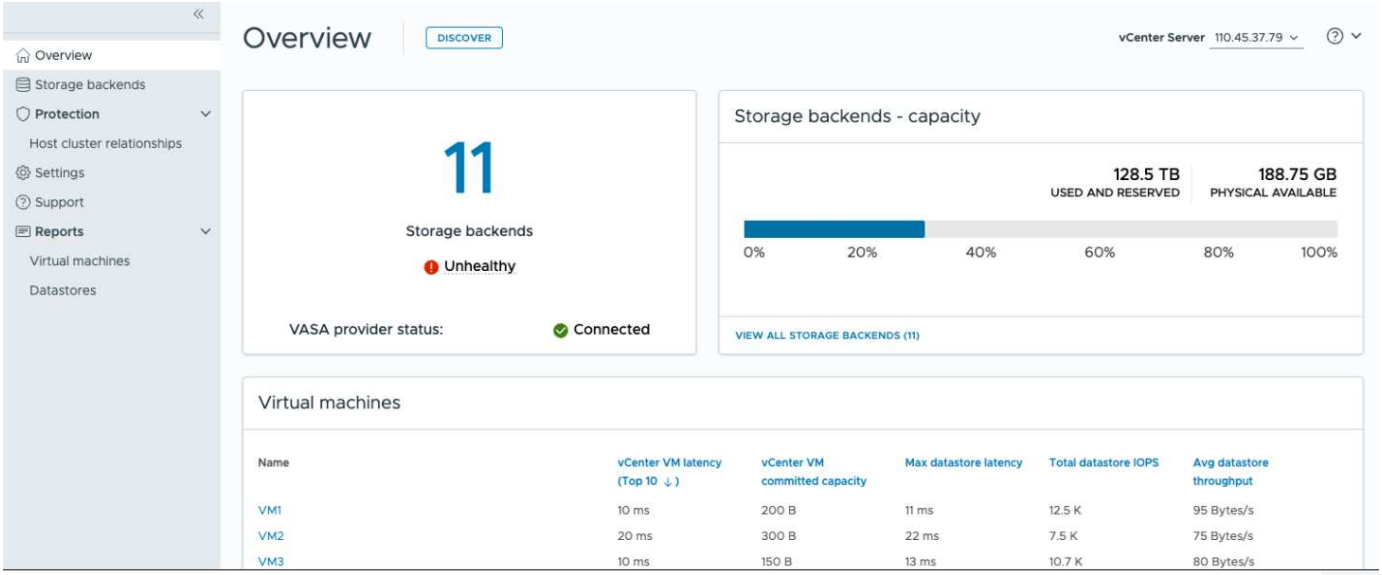
1. Créez un nouveau magasin de données d'espace réservé. Référer "Sélectionnez un magasin de données d'espace réservé"
2. Ajouter une banque de données à la protection du cluster hôte"Modifier le cluster d'hôtes protégé" . Vous devez ajouter des types de politiques asynchrones et synchrones.

Gérer les ONTAP tools for VMware vSphere

Présentation du tableau de bord des ONTAP tools for VMware vSphere

Lorsque vous sélectionnez l'icône du plug-in ONTAP tools for VMware vSphere dans la section Raccourcis du client vCenter, l'interface utilisateur accède à la page de présentation. Cette page agit comme un tableau de bord vous fournissant le résumé des ONTAP tools for VMware vSphere .

Dans le cas d'une configuration Enhanced Linked Mode (ELM), la liste déroulante de sélection de vCenter Server apparaît et vous pouvez sélectionner un vCenter Server souhaité pour voir les données qui le concernent. Cette liste déroulante est disponible pour toutes les autres vues de liste du plug-in. La sélection de vCenter Server effectuée sur une page persiste dans les onglets du plug-
in.



Depuis la page d'aperçu, vous pouvez exécuter l'action **Découverte**. L'action de découverte exécute la découverte au niveau de vCenter pour détecter tous les backends de stockage, hôtes, banques de données et états/relations de protection nouvellement ajoutés ou mis à jour. Vous pouvez exécuter une découverte d'entités à la demande sans avoir à attendre la découverte planifiée.

> Le bouton Action ne sera activé que si vous avez le privilège d'effectuer l'action de découverte.

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

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

Carte	Description

Statut	La carte d'état indique le nombre de backends de stockage et l'état de santé général des backends de stockage et du fournisseur VASA. L'état des backends de stockage indique **Sain** lorsque l'état de tous les backends de stockage est normal et il indique **Mauvais état** si l'un des backends de stockage présente un problème (état Inconnu/Inaccessible/Dégradé). Sélectionnez l'info-bulle pour ouvrir les détails d'état des backends de stockage. Vous pouvez sélectionner n'importe quel backend de stockage pour plus de détails. Le lien **Autres états du fournisseur VASA** affiche l'état actuel du fournisseur VASA enregistré dans vCenter Server.
Backends de stockage - Capacité	Cette carte affiche la capacité totale utilisée et disponible de tous les backends de stockage pour l'instance vCenter Server sélectionnée. Pour les systèmes de stockage ASA r2, les données de capacité ne sont pas affichées, car il s'agit d'un système désagrégé.
Machines virtuelles	Cette carte montre les 10 meilleures machines virtuelles classées par mesure de performance. Vous pouvez sélectionner l'en-tête pour obtenir les 10 meilleures machines virtuelles pour la métrique sélectionnée, triées par ordre croissant ou décroissant. Les modifications de tri et de filtrage apportées à la carte persistent jusqu'à ce que vous modifiiez ou effaciez le cache du navigateur.
Magasins de données	Cette carte montre les 10 meilleurs magasins de données triés par mesure de performance. Vous pouvez sélectionner l'en-tête pour obtenir les 10 premiers magasins de données pour la métrique sélectionnée, triés par ordre croissant ou décroissant. Les modifications de tri et de filtrage apportées à la carte persistent jusqu'à ce que vous modifiiez ou effaciez le cache du navigateur. Il existe une liste déroulante Type de magasin de données pour sélectionner le type de magasins de données : NFS, VMFS ou vVols.
Carte de conformité de l'hôte ESXi	Cette carte affiche l'état de conformité global de tous les paramètres des hôtes ESXi (pour le vCenter sélectionné) par rapport aux paramètres d'hôte NetApp recommandés par groupe/catégorie de paramètres. Vous pouvez sélectionner le lien **Appliquer les paramètres recommandés** pour appliquer les paramètres recommandés. Vous pouvez sélectionner l'état de conformité des hôtes pour voir la liste des hôtes.

Interface utilisateur du gestionnaire d'outils ONTAP

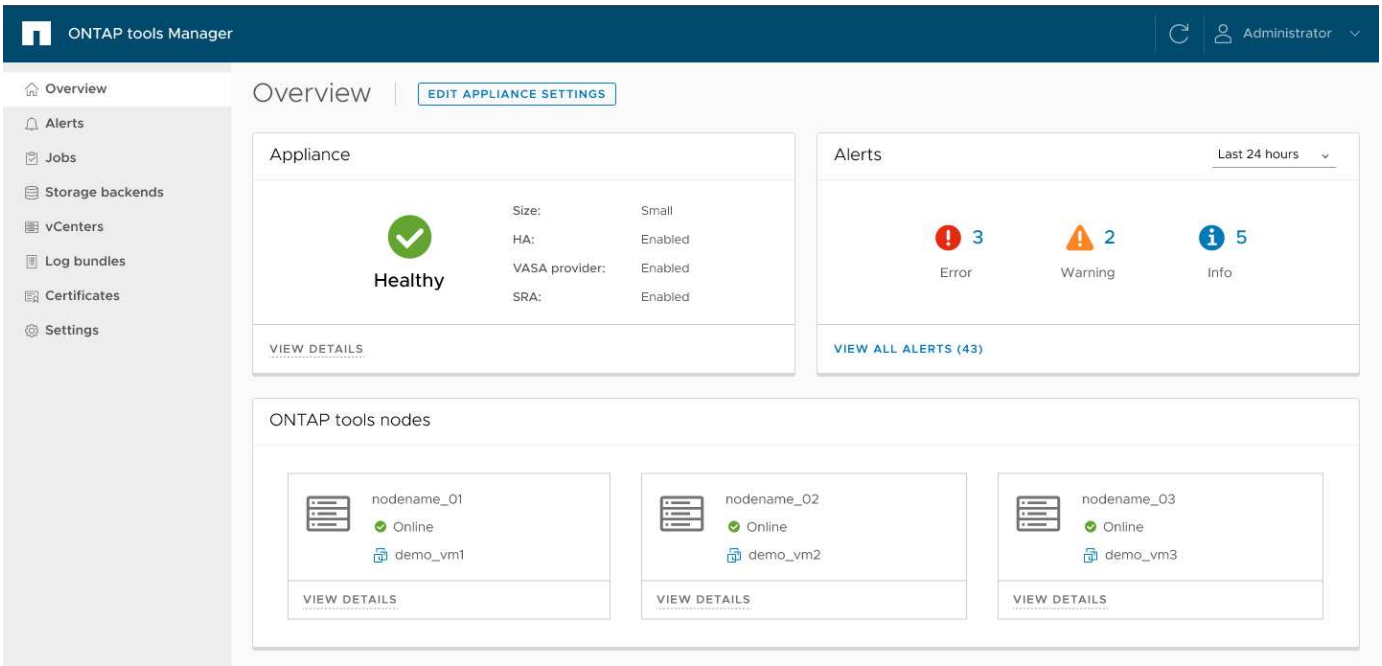
Les ONTAP tools for VMware vSphere sont un système multi-locataire capable de gérer plusieurs instances de vCenter Server. ONTAP Tools Manager offre davantage de contrôle à l'administrateur des ONTAP tools for VMware vSphere sur les instances vCenter Server gérées et les backends de stockage intégrés.

ONTAP Tools Manager aide à :

- Gestion des instances vCenter Server - Ajoutez et gérez les instances vCenter Server aux outils ONTAP .
- Gestion du backend de stockage - Ajoutez et gérez les clusters de stockage ONTAP aux ONTAP tools for VMware vSphere et mappez-les aux instances vCenter Server intégrées à l'échelle mondiale.
- Téléchargements de bundles de journaux - Collectez les fichiers journaux pour les ONTAP tools for VMware vSphere.
- Gestion des certificats - Remplacez le certificat auto-signé par un certificat CA personnalisé et renouvelez ou actualisez tous les certificats des outils VASA Provider et ONTAP .
- Gestion des mots de passe - Réinitialiser le mot de passe de l'application OVA de l'utilisateur.

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

La section Présentation du gestionnaire d'outils ONTAP permet de gérer la configuration de l'appliance, comme la gestion des services, la mise à l'échelle de la taille des nœuds et l'activation de la haute disponibilité (HA). Vous pouvez également surveiller les informations globales des outils ONTAP liées aux nœuds, telles que l'état, les détails du réseau et les alertes.



Carte	Description
Carte d'appareil	La carte de l'appareil fournit l'état général de l'appareil des outils ONTAP . Il affiche les détails de configuration de l'appareil et l'état des services activés. Pour plus d'informations sur l'appliance des outils ONTAP , sélectionnez le lien **Afficher les détails**. Lorsqu'une tâche d'action de modification des paramètres d'un appareil est en cours, le portlet de l'appareil affiche l'état et les détails de la tâche.
Carte d'alertes	La carte Alertes répertorie les alertes des outils ONTAP par type, y compris les alertes au niveau du nœud HA. Vous pouvez consulter la liste des alertes en sélectionnant le texte du compteur (lien hypertexte). Le lien vous dirige vers la page d'affichage des alertes filtrées par le type sélectionné.
vCenters	La carte vCenter affiche l'état de santé des vCenters du système.
Backends de stockage	La carte des backends de stockage affiche l'état de santé des backends de stockage du système.
Carte des nœuds d'outils ONTAP	La carte des nœuds des outils ONTAP affiche la liste des nœuds avec le nom du nœud, le nom de la machine virtuelle du nœud, l'état et toutes les données liées au réseau. Vous pouvez sélectionner **Afficher les détails** pour afficher les détails supplémentaires liés au nœud sélectionné. [REMARQUE] Dans une configuration non HA, un seul nœud est affiché. Dans la configuration HA, trois nœuds sont affichés.

Comprendre les groupes d'application et les stratégies d'exportation dans les ONTAP tools for VMware vSphere

Les groupes d'initiateurs (igroups) sont des tables de noms de port mondiaux (WWPN) d'hôtes de protocole FC ou de noms de nœuds qualifiés d'hôtes iSCSI. Vous pouvez définir des igroups et les mapper aux LUN pour contrôler quels initiateurs ont accès aux LUN.

Dans les ONTAP tools for VMware vSphere 9.x, les igroups étaient créés et gérés dans une structure plate, où chaque banque de données dans vCenter était associée à un seul igroup. Ce modèle limitait la flexibilité et la réutilisation des igroups sur plusieurs banques de données. Les ONTAP tools for VMware vSphere 10.x introduisent des igroups imbriqués, où chaque banque de données de vCenter est associée à un igroup parent, tandis que chaque hôte est lié à un igroup enfant sous ce parent. Vous pouvez définir des groupes parents personnalisés avec des noms définis par l'utilisateur pour les réutiliser dans plusieurs banques de données, permettant une gestion plus flexible et interconnectée des groupes. La compréhension du flux de travail igroup est essentielle pour gérer efficacement les LUN et les banques de données dans les ONTAP tools for VMware vSphere. Différents flux de travail génèrent des configurations igroup variables, comme illustré dans les exemples suivants :

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

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

Exemple 1 :
Créer une banque de données sur un seul hôte avec un initiateur

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

Résultat:

- Groupe DS1I :
  - hôte1Igroupe → (iqn1 : lun1)

Un groupe parent DS1Igroup est créé sur les systèmes ONTAP pour DS1, avec un groupe enfant host1Igroup mappé à lun1. Les LUN sont toujours mappés aux groupes enfants.

Exemple 2 :
Monter la banque de données existante sur un hôte supplémentaire

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

Résultat:

- Groupe DS1I :
  - hôte1Igroupe → (iqn1 : lun1)
  - hôte2Igroupe → (iqn2 : lun1)

Un groupe i enfant host2Igroup est créé et ajouté au groupe i parent existant DS1Igroup.

Exemple 3 :
Démonter une banque de données d'un hôte

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

Résultat:

- Groupe DS1I :
  - hôte2Igroupe → (iqn2 : lun1)

Le groupe host1Igroup est supprimé de la hiérarchie. Les groupes enfants ne sont pas explicitement supprimés. La suppression se produit dans ces deux conditions :

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

Exemple 4 :

Supprimer la banque de données

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

Résultat:

- Groupe DS1I :
  - hôte2Igroupe → (iqn2 : lun1)

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

Exemple 5 :

Créer plusieurs banques de données sous un groupe parent personnalisé

Flux de travail:

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

Résultat:

- CustomIgroup1 :
  - hôte1Igroup → (iqn1 : lun2, lun3)
  - hôte2Igroupe → (iqn2 : lun2)
  - hôte3Igroupe → (iqn3: lun3)

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

Exemple 6 :

Supprimez une banque de données sous un groupe parent personnalisé.

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

Résultat:

- CustomIgroup1 :
  - hôte1Igroupe → (iqn1 : lun3)

    - hôte3Igroupe → (iqn3: lun3)
- Même si CustomIgroup1 n’est pas réutilisé, il n’est pas supprimé.
- Si aucun LUN n’est mappé, le système ONTAP supprime host2Igroup.
- Le groupe hôte1 n’est pas supprimé, car il est mappé sur lun3 de DS3. Les groupes personnalisés ne sont jamais supprimés, quel que soit leur statut de réutilisation.

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

Flux de travail:

Avant l’extension :

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

- DS4Igroup : host4Igroup → (iqn4 : lun4)

Après l’expansion :

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

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

Un nouveau LUN est créé et mappé à l’hôte igroup enfant existant host4Igroup.

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

Flux de travail:

Avant rétrécissement :

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

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

Après rétrécissement :

[Rétrécir] DS4 (lun4) : host4 (iqn4)

- DS4Igroup : host4Igroup → (iqn4 : lun4)

Le LUN spécifié (lun5) n’est pas mappé à partir du groupe i enfant. Le groupe reste actif tant qu’il possède au moins un LUN mappé.

Exemple 9 :
Migration des outils ONTAP 9 vers 10 (normalisation igroup)

Flux de travail

Les outils ONTAP pour les versions VMware vSPhere 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 dans la structure hiérarchique.

Avant la migration :

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

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

Après la migration :

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

Pendant la migration :

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

Cela garantit le respect du modèle hiérarchique.

Sujets connexes

"À propos des igroups"

Politiques d'exportation

Les politiques d'exportation contrôlent l'accès aux banques de données NFS dans les ONTAP tools for VMware vSphere. Ils définissent quels clients peuvent accéder aux magasins de données et quelles autorisations ils ont. Les politiques d'exportation sont créées et gérées dans les systèmes ONTAP et peuvent être associées aux banques de données NFS pour appliquer le contrôle d'accès. Chaque politique d'exportation se compose de règles qui spécifient les clients (adresses IP ou sous-réseaux) autorisés à accéder et les autorisations accordées (lecture seule ou lecture-écriture).

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

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

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

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

Sujets connexes

"Créer une politique d'exportation"

Comprendre les groupes gérés par les outils ONTAP

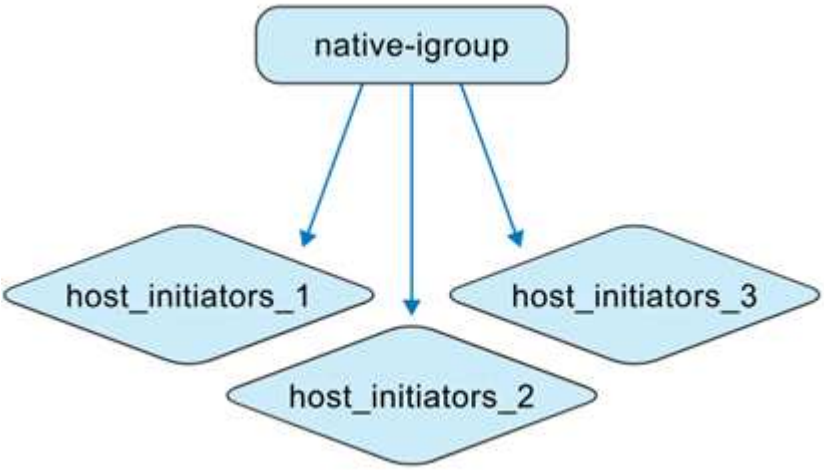
Lors de la gestion des machines virtuelles des outils ONTAP et des systèmes de stockage ONTAP , la compréhension du comportement des groupes d'applications est essentielle, en particulier lors de la migration de banques de données depuis des environnements d'outils non ONTAP vers la gestion des outils ONTAP . Cette section décrit comment les igroups sont mis à jour pendant cette transition.

Les ONTAP tools for VMware vSphere 10.4 simplifient la gestion des banques de données en automatisant la création et la maintenance des objets ONTAP et vCenter dans les environnements de centre de données VMware.

Les ONTAP tools for VMware vSphere 10.4 interprètent les igroups dans deux contextes différents :

igroups gérés par des outils non ONTAP

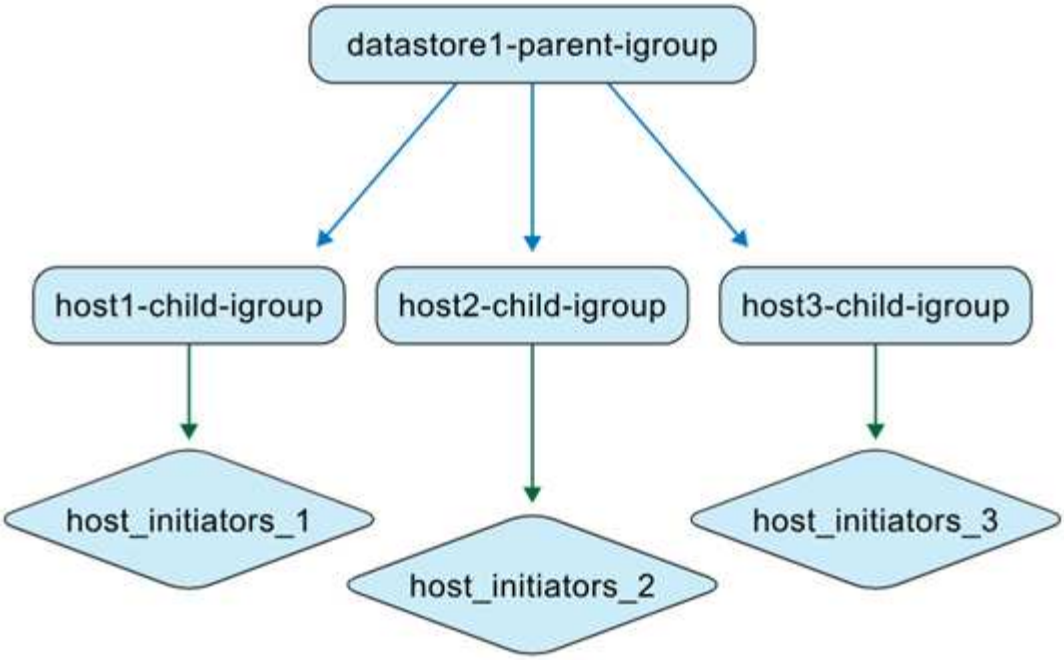
En tant qu'administrateur de stockage, vous pouvez créer des igroups sur le système ONTAP sous forme de structures plates ou imbriquées. L'illustration montre un igroup plat créé dans le système ONTAP .

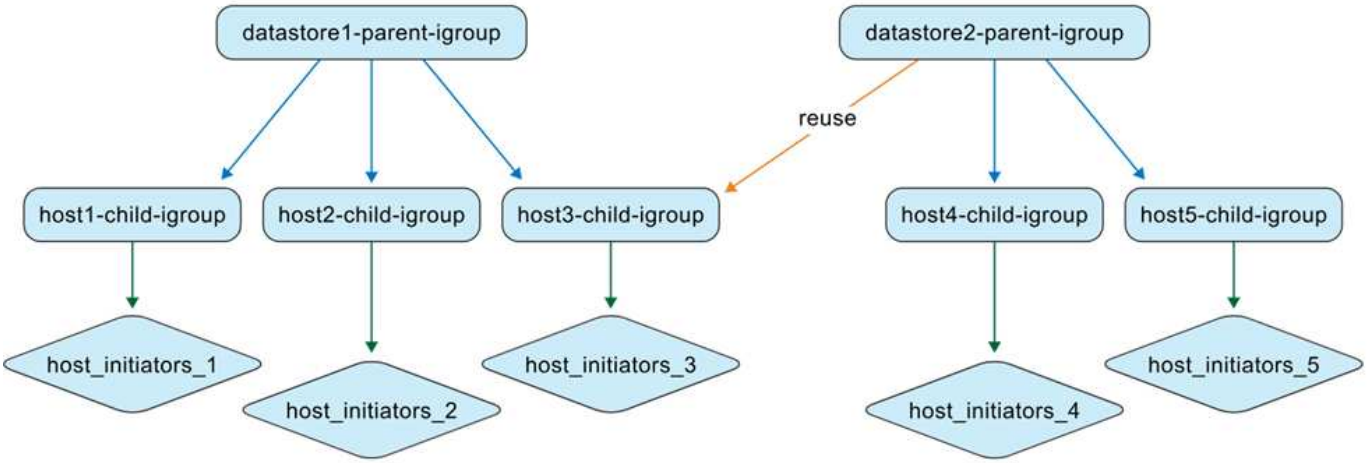


igroups gérés par les outils ONTAP

Lorsque vous créez des banques de données, les ONTAP tools for VMware vSphere 10.4 créent automatiquement des igroups à l'aide d'une structure imbriquée pour un mappage LUN plus facile.

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





Voici quelques cas d' ONTAP tools for VMware vSphere .

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

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

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

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

Lors de la création d'une banque de données dans les outils ONTAP , vous pouvez saisir un nom de groupe

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

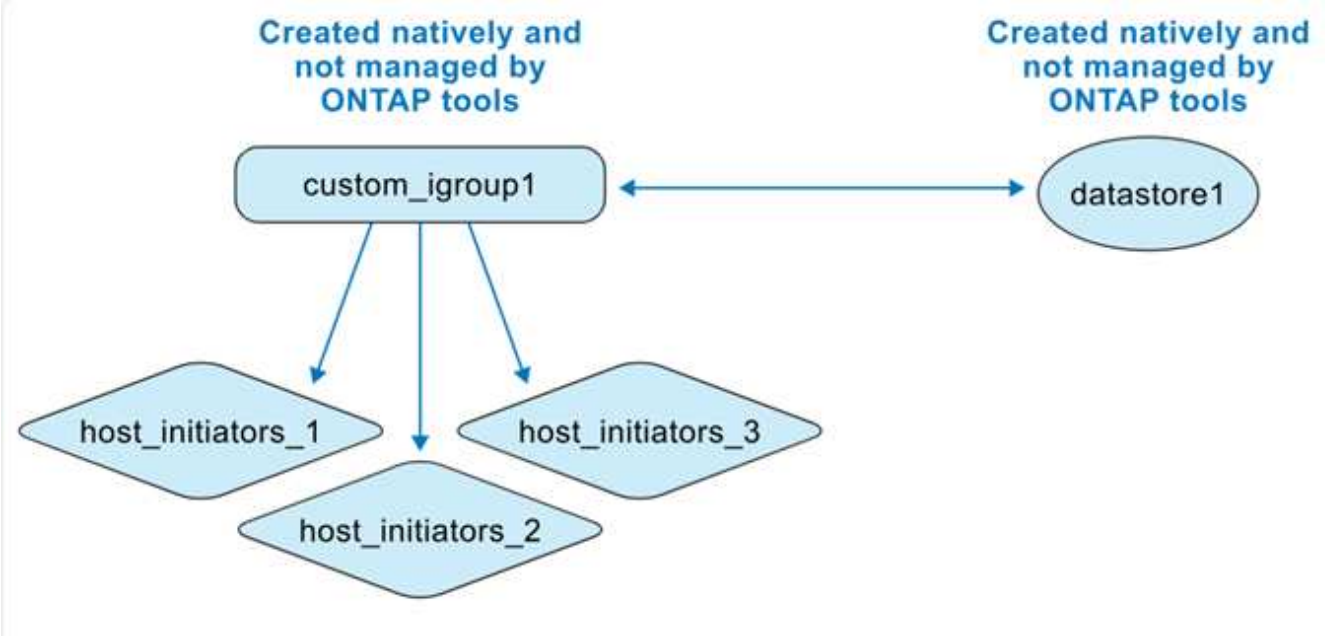
Lorsque vous réutilisez le nom du groupe i lors de la création du magasin de données

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

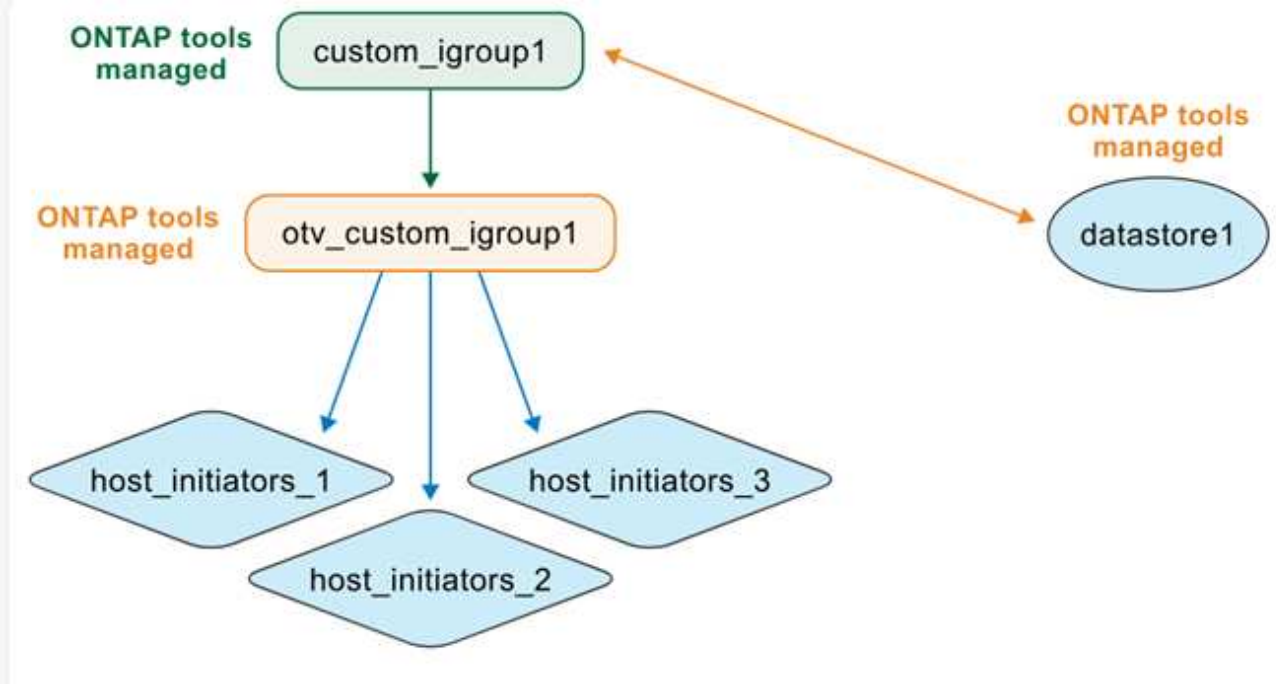
Cette opération peut également être effectuée à l'aide de l'API. Pour réutiliser un igroup existant lors de la création d'une banque de données, spécifiez l'UUID igroup dans la charge utile de la demande d'API.

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

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



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



Vous pouvez créer une banque de données directement dans vCenter Server et la placer ultérieurement sous la gestion des outils ONTAP . Tout d'abord, créez un igroup plat dans les systèmes ONTAP et mappez-y un LUN. Après avoir exécuté la découverte de banque de données dans les outils ONTAP , le groupe i plat est converti en une structure imbriquée. Les outils ONTAP gèrent ensuite l'igroup, en le renommant avec le préfixe « otv_ ». Le LUN reste mappé au même igroup tout au long de ce processus.

Comment les outils ONTAP réutilisent les igroups créés nativement

Vous pouvez provisionner une banque de données dans les outils ONTAP à l'aide d'un igroup créé à l'origine dans les systèmes ONTAP , après sa gestion par les outils ONTAP . Ces groupes i apparaissent dans la liste déroulante des noms de groupe d'initiateurs personnalisés. Le nouveau LUN pour le magasin de données est ensuite mappé au groupe enfant normalisé correspondant, tel que « otv_NativeIgroup1 ».

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

Activer les ONTAP tools for VMware vSphere

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

Étapes

1. Lancez le gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les informations d'identification d'administrateur des ONTAP tools for VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **Modifier les paramètres de l'appareil** dans la section Aperçu.
4. Dans la section **Services**, vous pouvez activer des services optionnels tels que VASA Provider,

l'importation de la configuration vVols et la reprise après sinistre (SRA) selon vos besoins.

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

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

L'option *Autoriser l'importation de la configuration vVols * s'affiche uniquement lorsque le service VASA Provider est activé. Cette option permet la migration des données vVols des outils ONTAP 9.xx vers les outils ONTAP 10.4.

Modifier les ONTAP tools for VMware vSphere

À l'aide du gestionnaire d'outils ONTAP , augmentez la configuration des ONTAP tools for VMware vSphere afin d'augmenter le nombre de nœuds dans le déploiement ou de modifier la configuration vers une configuration haute disponibilité (HA). Les ONTAP tools for VMware vSphere sont initialement déployés dans une configuration non HA à nœud unique.

> Pour migrer vers HA lorsque la sauvegarde non HA est activée, désactivez d'abord la sauvegarde et réactivez-la après la migration.

Avant de commencer

- Assurez-vous que votre modèle OVA a la même version OVA que le nœud 1. Le nœud 1 est le nœud par défaut sur lequel les ONTAP tools for VMware vSphere OVA sont initialement déployés.
- Assurez-vous que l'ajout à chaud du processeur et le branchement à chaud de la mémoire sont activés.
- Dans vCenter Server, définissez le niveau d'automatisation du service de récupération après sinistre (DRS) sur partiellement automatisé. Après avoir déployé HA, rétablissez-le en mode entièrement automatisé.
- Les noms d'hôtes des nœuds dans la configuration HA doivent être en minuscules.

Étapes

1. Lancez le gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les informations d'identification d'administrateur des ONTAP tools for VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **Modifier les paramètres de l'appareil** dans la section Aperçu.
4. Dans la section **Configuration**, vous pouvez augmenter la taille du nœud et activer la configuration HA selon vos besoins. Vous avez besoin des informations d'identification de vCenter Server pour effectuer des modifications.

   Lorsque les outils ONTAP sont en configuration HA, vous pouvez modifier les détails de la bibliothèque de contenu. Vous devez fournir à nouveau le mot de passe pour la nouvelle soumission de modification.

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

5. Utilisez le bouton bascule HA pour activer la configuration HA. Sur la page **Paramètres HA**, assurez-vous que :
   - La bibliothèque de contenu appartient au même vCenter Server sur lequel s'exécutent les machines virtuelles du nœud d'outils ONTAP . Les informations d'identification de vCenter Server sont utilisées pour valider et télécharger le modèle OVA pour les modifications de l'appliance.
   - La machine virtuelle hébergeant les outils ONTAP n'est pas directement déployée sur un hôte 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. Les ONTAP tools for VMware vSphere prennent en charge trois nœuds dans la configuration HA.

   > La plupart des options de saisie sont pré-remplies avec les détails du réseau du nœud 1 pour faciliter le flux de travail. Cependant, vous pouvez modifier les données d'entrée avant d'accéder à la page finale 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 premier nœud.

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

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

Quelle est la prochaine étape ?

La page **Aperçu** affiche l'état du déploiement. À l'aide de l'ID de tâche, vous pouvez également suivre l'état de la tâche de modification des paramètres de l'appareil à partir de la vue des tâches.

Si le déploiement HA échoue et que l'état du nouveau nœud indique « Nouveau », supprimez la nouvelle machine virtuelle dans vCenter avant de réessayer l'opération d'activation de HA.

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

Gérer les magasins de données

Monter des banques de données NFS et VMFS

Le montage d'un magasin de données fournit un accès au stockage à des hôtes supplémentaires. Vous pouvez monter la banque de données sur les hôtes supplémentaires après avoir ajouté les hôtes à votre environnement VMware.

À propos de cette tâche

- Certaines actions de clic droit sont désactivées ou indisponibles selon la version du client vSphere et le

type de banque de données sélectionné.

  - Si vous utilisez le client vSphere 8.0 ou des versions ultérieures, certaines des options de clic droit sont masquées.
  - Des versions vSphere 7.0U3 à vSphere 8.0, même si les options apparaissent, l'action sera désactivée.

- L'option de montage de la banque de données est désactivée lorsque le cluster hôte est protégé par des configurations uniformes.

Étapes

1. Depuis la page d'accueil de 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 magasins de données NFS/VMFS sur un hôte ou un cluster d'hôtes, cliquez avec le bouton droit de la souris et sélectionnez * Outils NetApp ONTAP * > * Monter les magasins de données *.
4. Sélectionnez les banques de données que vous souhaitez monter et sélectionnez **Monter**.

Quelle est la prochaine étape ?

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

Démonter les banques de données NFS et VMFS

L'action Démonter la banque de données démonte une banque de données NFS ou VMFS des hôtes ESXi. L'action de démontage de la banque de données est activée pour les banques de données NFS et VMFS qui sont découvertes ou gérées par les ONTAP tools for VMware vSphere.

Étapes

1. Connectez-vous au client vSphere.
2. Cliquez avec le bouton droit sur un objet de banque de données NFS ou VMFS et sélectionnez **Démonter la banque de données**.

   Une boîte de dialogue s'ouvre et répertorie les hôtes ESXi sur lesquels la banque de données est montée. 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 banque de données.

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

4. Sélectionnez le bouton **Démonter**.

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

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

Quelle est la prochaine étape ?

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

Monter une banque de données vVols

Vous pouvez monter une banque de données VMware Virtual Volumes (vVols) sur un ou plusieurs hôtes supplémentaires pour fournir un accès au stockage à des hôtes supplémentaires. Vous ne pouvez démonter la banque de données vVols que via les API.

Étapes

1. Depuis la page d'accueil de vSphere Client, sélectionnez **Hôtes et clusters**.
2. Dans le volet de navigation, sélectionnez le centre de données qui contient le magasin de données.
3. Cliquez avec le bouton droit sur le magasin de données et sélectionnez * Outils NetApp ONTAP * > * Monter le magasin 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**.

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

Redimensionner le magasin de données NFS et VMFS

Le redimensionnement d'un magasin de données vous permet d'augmenter le stockage de vos fichiers de machine virtuelle. Vous pouvez modifier la taille d'un magasin de données à mesure que vos besoins en infrastructure évoluent.

À propos de cette tâche

Vous ne pouvez augmenter que la taille d'un magasin de données NFS et VMFS. Un FlexVol volume qui fait partie d'une banque de données NFS et VMFS ne peut pas diminuer en dessous de la taille existante, mais peut augmenter de 120 % au maximum.

Étapes

1. Depuis la page d'accueil de vSphere Client, sélectionnez **Hôtes et clusters**.
2. Dans le volet de navigation, sélectionnez le centre de données qui contient le magasin de données.
3. Cliquez avec le bouton droit sur la banque de données NFS ou VMFS et sélectionnez * Outils NetApp ONTAP * > * Redimensionner la banque de données *.
4. Dans la boîte de dialogue Redimensionner, spécifiez une nouvelle taille pour la banque de données et sélectionnez **OK**.

Développer les banques de données vVols

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

> 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 de vSphere Client, sélectionnez **Hôtes et clusters**.

2. Dans le volet de navigation, sélectionnez le centre de données qui contient le magasin de données.
3. Cliquez avec le bouton droit sur le magasin de données et sélectionnez * Outils NetApp ONTAP * > * Ajouter du stockage au magasin de données *.
4. Dans la fenêtre **Créer ou sélectionner des volumes**, vous pouvez soit créer de nouveaux volumes, soit choisir parmi les volumes existants. L'interface utilisateur est explicite. Suivez les instructions selon votre choix.
5. Dans la fenêtre **Résumé**, vérifiez les sélections et sélectionnez **Développer**. Vous pouvez suivre la progression dans le panneau des tâches récentes.

Réduire la banque de données vVols

L'action Supprimer la banque de données supprime la banque de données lorsqu'il n'y a aucun vVols sur la banque de données sélectionnée.

> L'opération de réduction de la banque de données vVols n'est pas prise en charge pour la banque de données vVols basée sur le système ASA r2.

Étapes

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

   > L'option permettant de sélectionner le volume sur lequel réside le vVols 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

L'action Supprimer le stockage de la banque de données est prise en charge sur tous les ONTAP tools for VMware vSphere les banques de données vVols découvertes ou gérées par VMware vSphere dans vCenter Server. Cette action permet la suppression de volumes des banques de données vVols .

L'option de suppression est désactivée lorsqu'il y a des vVols résidant sur un volume particulier. En plus de supprimer des volumes de la banque de données, vous pouvez supprimer le volume sélectionné sur le stockage ONTAP .

La tâche de suppression de banque de données des ONTAP tools for VMware vSphere dans vCenter Server effectue les opérations suivantes :

- Démonte le conteneur vVol.
- Nettoie le groupe i. Si igroup n'est pas utilisé, supprime iqn de igroup.
- Supprime le conteneur Vvol.

- Laisse les volumes Flex sur la baie de stockage.

Suivez les étapes ci-dessous pour supprimer la banque de données NFS, VMFS ou vVOL des outils ONTAP du vCenter Server :

Étapes

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

   > Vous ne pouvez pas supprimer les banques de données si des machines virtuelles utilisent cette banque de données. Vous devez déplacer les machines virtuelles vers un autre magasin de données avant de supprimer le magasin de données. Vous ne pouvez pas cocher la case Supprimer le volume si la banque de données appartient à un cluster hôte protégé.

   a. Dans le cas d'un magasin de données NFS ou VMFS, une boîte de dialogue apparaît avec la liste des machines virtuelles qui utilisent le magasin de données.
   b. Si la banque de données VMFS est créée sur des systèmes ASA r2 et si elle fait partie de la protection, vous devez déprotéger la banque de données avant de la supprimer.
   c. Dans le cas des banques de données vVols , l'action de suppression de la banque de données supprime la banque de données uniquement lorsqu'aucun vVols n'est associé à celle-ci. La boîte de dialogue Supprimer la banque de données fournit une option permettant de supprimer des volumes du cluster ONTAP .
   d. Dans le cas des banques de données vVols basées sur des systèmes ASA r2, la case à cocher permettant de supprimer les volumes de sauvegarde n'est pas applicable.
3. Pour supprimer les volumes de sauvegarde sur le stockage ONTAP , sélectionnez *Supprimer les volumes sur le cluster ONTAP *.

   > Vous ne pouvez pas supprimer le volume sur le cluster ONTAP pour une banque de données VMFS qui fait partie du cluster hôte protégé.

Vues de stockage ONTAP pour les banques de données

Les ONTAP tools for VMware vSphere affichent la vue latérale du stockage ONTAP des banques de données et de leurs volumes dans l'onglet de configuration.

Étapes

1. Depuis le client vSphere, accédez au magasin de données.
2. Sélectionnez l'onglet **Configurer** dans le volet de droite.
3. Sélectionnez * Outils NetApp ONTAP * > * Stockage ONTAP *. Selon le type de banque de données, la vue change. Reportez-vous au tableau ci-dessous pour plus d'informations :

Type de magasin de données	Informations disponibles

Banque de données NFS	La page **Détails de stockage** contient des informations sur les backends de stockage, les agrégats et le volume. La page **Détails NFS** contient des données relatives à la banque de données NFS.
Banques de données VMFS	La page **Détails de stockage** contient les détails du backend de stockage, de l'agrégat, du volume et de la zone de disponibilité de stockage (SAZ). La page **Détails de l'unité de stockage** contient les détails de l'unité de stockage.
Magasins de données vVols	Répertorie tous les volumes. Vous pouvez étendre ou supprimer du stockage à partir du volet de stockage ONTAP . Cette vue n'est pas prise en charge pour la banque de données vVols basée sur le système ASA r2.

Vue de stockage de la machine virtuelle

La vue de stockage affiche la liste des vVols créés par la machine virtuelle.

> Cette vue s'applique à la machine virtuelle sur laquelle est monté au moins un disque associé à la banque de données vVols gérée par les ONTAP tools for VMware vSphere .

Étapes

1. Depuis le client vSphere, accédez à la machine virtuelle.
2. Sélectionnez l'onglet **Moniteur** dans le volet de droite.
3. Sélectionnez * Outils NetApp ONTAP * > **Stockage**. Les détails du **Stockage** apparaissent dans le volet de droite. Vous pouvez voir la liste des vVols présents sur la VM.

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

Gérer les seuils de stockage

Vous pouvez définir le seuil pour recevoir des notifications dans vCenter Server lorsque le volume et la capacité globale atteignent certains niveaux.

Mesures:

1. Connectez-vous au client vSphere.
2. Dans la page des raccourcis, sélectionnez * Outils NetApp ONTAP * sous la section plug-ins.
3. Dans le volet gauche des outils ONTAP , accédez à **Paramètres** > **Paramètres de seuil** > **Modifier**.
4. Dans la fenêtre **Modifier le seuil**, indiquez les valeurs souhaitées dans les champs **Presque plein** et **Plein** et sélectionnez **Enregistrer**. Vous pouvez réinitialiser les chiffres aux valeurs recommandées, soit 80 pour presque plein et 90 pour plein.

Gérer les backends de stockage

Les backends de stockage sont des systèmes que les hôtes ESXi utilisent pour le

stockage des données.

Découvrir le stockage

Vous pouvez exécuter la découverte d'un backend de stockage à la demande sans attendre qu'une découverte planifiée mette à jour les détails de stockage.

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

Étapes

1. Connectez-vous au client vSphere.
2. Dans la page des raccourcis, sélectionnez * Outils NetApp ONTAP * sous la section plug-ins.
3. Dans le volet gauche des outils ONTAP , accédez à **Backends de stockage** et sélectionnez un backend de stockage.
4. Sélectionnez le menu des ellipses verticales et sélectionnez **Découvrir le stockage**

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

Modifier les backends de 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 * Outils NetApp ONTAP * sous la section plug-ins.
3. Dans le volet gauche des outils ONTAP , accédez à **Backends de stockage** et sélectionnez un backend de stockage.
4. Sélectionnez le menu des ellipses verticales et sélectionnez **Modifier** pour modifier les informations d'identification ou le nom du port. Vous pouvez suivre la progression dans le panneau des tâches récentes.

Vous pouvez effectuer l'opération de modification pour les clusters ONTAP globaux à l'aide du gestionnaire d'outils ONTAP en procédant comme suit.

1. Lancez le gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les informations d'identification d'administrateur des ONTAP tools for VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez les backends de stockage dans la barre latérale.
4. Sélectionnez le backend de stockage que vous souhaitez modifier.
5. Sélectionnez le menu des ellipses verticales et sélectionnez **Modifier**.
6. Vous pouvez modifier les informations d'identification 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 magasins de données attachés au backend de stockage avant de supprimer le backend de stockage. Suivez les étapes ci-dessous pour supprimer un backend de stockage.

1. Connectez-vous au client vSphere.

2. Dans la page des raccourcis, sélectionnez * Outils NetApp ONTAP * sous la section plug-ins.
3. Dans le volet gauche des outils ONTAP , accédez à **Backends de stockage** et sélectionnez un backend de stockage.
4. Sélectionnez le menu des ellipses verticales et sélectionnez **Supprimer**. Assurez-vous que le backend de stockage ne contient aucun magasin de données. Vous pouvez suivre la progression dans le panneau des tâches récentes.

Vous pouvez effectuer l'opération de suppression pour les clusters ONTAP globaux à l'aide du gestionnaire d'outils ONTAP .

1. Lancez le gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les informations d'identification d'administrateur des ONTAP tools for VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **Backends de stockage** dans la barre latérale.
4. Sélectionnez le backend de stockage que vous souhaitez supprimer
5. Sélectionnez le menu des ellipses verticales et sélectionnez **Supprimer**.

Vue détaillée du backend de stockage

La page backend de stockage répertorie tous les backends de stockage. Vous pouvez effectuer des opérations de découverte, de modification et de suppression de stockage sur les backends de stockage que vous avez ajoutés et non sur le SVM enfant individuel sous le cluster.

Lorsque vous sélectionnez le cluster parent ou l'enfant sous le backend de stockage, vous pouvez voir le résumé global du composant. Lorsque vous sélectionnez le cluster parent, vous disposez d'une liste déroulante d'actions à partir de laquelle vous pouvez effectuer les opérations de découverte, de stockage, de modification et de suppression.

La page récapitulative fournit les détails suivants :

- État du backend de stockage
- Informations sur la capacité
- Informations de base sur la machine virtuelle
- Informations réseau telles que l'adresse IP et le port du réseau. Pour le SVM enfant, les informations seront les mêmes que celles du backend de stockage parent.
- Privileges autorisés et restreints pour le backend de stockage. Pour le SVM enfant, les informations seront les mêmes que celles du backend de stockage parent. Les Privileges ne sont affichés que sur les backends de stockage basés sur des clusters. Si vous ajoutez SVM comme backend de stockage, les informations sur les privilèges ne seront pas affichées.
- La vue détaillée du cluster système ASA r2 n'inclut pas l'onglet des niveaux locaux lorsque la propriété désagrégée est définie sur « vrai » pour le SVM ou le cluster.
- Pour les systèmes SVM ASA r2, le portlet de capacité n'est pas affiché. Le portail de capacité n'est requis que lorsque la propriété désagrégée est définie sur « vrai » pour le SVM ou le cluster.
- Pour les systèmes ASA r2 SVM, la section d'informations de base indique le type de plate-forme.

L'onglet Interface fournit des informations détaillées sur l'interface.

L'onglet Niveaux locaux fournit des informations détaillées sur la liste agrégée.

Gérer les instances de vCenter Server

Les instances vCenter Server sont des plates-formes de gestion centrales qui vous permettent de contrôler les hôtes, les machines virtuelles et les backends de stockage.

Dissocier les backends de stockage de l'instance vCenter Server

La page de liste de vCenter Server affiche le nombre associé de backends de stockage. Chaque instance de vCenter Server a la possibilité de s'associer ou de se dissocier d'un backend de stockage.

Étapes

1. Lancez le gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les informations d'identification d'administrateur des ONTAP tools for VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez l'instance vCenter Server requise dans la barre latérale.
4. Sélectionnez les points de suspension verticaux en regard du serveur vCenter que vous souhaitez associer ou dissocier des backends de stockage.
5. Sélectionnez **Dissocier le backend de stockage**.

Modifier une instance de vCenter Server

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

1. Lancez le gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les informations d'identification d'administrateur des ONTAP tools for VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez l'instance vCenter Server applicable dans la barre latérale
4. Sélectionnez les points de suspension verticaux par rapport au serveur vCenter que vous souhaitez modifier et sélectionnez **Modifier**.
5. Modifiez les détails de l'instance vCenter Server et sélectionnez **Modifier**.

Supprimer une instance de vCenter Server

Vous devez supprimer tous les backends de stockage attachés au vCenter Server avant de le supprimer.

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

Une fois les instances de vCenter Server supprimées, elles ne seront plus gérées par l'application.

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

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

Gérer les certificats

Un certificat auto-signé est généré pour les outils ONTAP et VASA Provider par défaut lors du déploiement. À l'aide de l'interface du gestionnaire d'outils ONTAP , vous pouvez renouveler le certificat ou le mettre à niveau vers une autorité de certification personnalisée. Les certificats CA personnalisés sont obligatoires dans un déploiement multi-vCenter.

Avant de commencer

- Le nom de domaine sur lequel le certificat est émis doit être mappé à l'adresse IP virtuelle.
- Exécutez la vérification nslookup sur le nom de domaine pour vérifier si le domaine est résolu à l'adresse IP prévue.
- Les certificats doivent être créés avec le nom de domaine et l'adresse IP des outils ONTAP .

Une adresse IP d'outils ONTAP doit correspondre à un nom de domaine complet (FQDN). Les certificats doivent contenir le même nom de domaine complet mappé à l'adresse IP des outils ONTAP dans le sujet ou dans les noms alternatifs du sujet.

Vous ne pouvez pas passer d'un certificat signé par une autorité de certification à un certificat auto-signé.

Certificat de mise à niveau des outils ONTAP

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

Étapes

1. Lancez le gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les informations d'identification d'administrateur des ONTAP tools for VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **Certificats** > **Outils ONTAP * > *Renouveler** pour renouveler les certificats.

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

   > Le système sera hors ligne jusqu'à ce que le certificat soit renouvelé et vous serez déconnecté de l'interface du gestionnaire d'outils ONTAP .

4. Pour mettre à niveau le certificat auto-signé vers un certificat CA personnalisé, sélectionnez l'option **Certificats** > **Outils ONTAP * > *Mettre à niveau vers 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 pour lequel vous avez généré ce certificat et mettez à niveau le certificat.

   > Le système sera hors ligne jusqu'à ce que la mise à niveau soit terminée et vous serez déconnecté de l'interface du gestionnaire d'outils ONTAP .

Mettre à niveau le certificat du fournisseur VASA

Les ONTAP tools for VMware vSphere sont déployés avec un certificat auto-signé pour VASA Provider. Avec cela, une seule instance de vCenter Server peut être gérée pour les banques de données vVols . Lorsque vous gérez plusieurs instances de vCenter Server et que vous souhaitez activer la fonctionnalité vVols sur celles-ci, vous devez remplacer le certificat auto-signé par un certificat d'autorité de certification personnalisé.

Étapes

1. Lancez le gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les informations d'identification d'administrateur des ONTAP tools for VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **Certificats** > **Fournisseur VASA** ou **Outils ONTAP * > *Renouveler** pour renouveler les certificats.
4. Sélectionnez **Certificats** > **Fournisseur VASA** ou **Outils ONTAP * > *Mettre à niveau vers l'autorité de certification** 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 pour lequel vous avez généré ce certificat et mettez à niveau le certificat.

> Le système sera hors ligne jusqu'à ce que la mise à niveau soit terminée et vous serez déconnecté de l'interface du gestionnaire d'outils ONTAP .

Accéder aux ONTAP tools for VMware vSphere

Présentation des ONTAP tools for VMware vSphere

Vous pouvez gérer vos configurations d'application, de système et de réseau à l'aide de la console de maintenance des outils ONTAP . Vous pouvez modifier votre mot de passe administrateur et votre mot de passe de maintenance. Vous pouvez également générer des bundles de support, définir différents niveaux de journalisation, afficher et gérer les configurations TLS et démarrer des diagnostics à distance.

Vous devez avoir installé les outils VMware après avoir déployé les ONTAP tools for VMware vSphere pour accéder à la console de maintenance. Vous devriez utiliser `maint` comme le nom d'utilisateur et le mot de passe que vous avez configurés lors du déploiement pour vous connecter à la console de maintenance des outils ONTAP . Vous devez utiliser **nano** pour éditer les fichiers dans la console de maintenance ou de connexion root.

> Vous devez définir un mot de passe pour le `diag` utilisateur lors de l'activation des diagnostics à distance.

Vous devez utiliser l'onglet **Résumé** de vos ONTAP tools for VMware vSphere 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 2. Modifier le niveau LOG pour les services VASA Provider et SRA
Configuration du système	1. Redémarrer la machine virtuelle 2. Arrêter la machine virtuelle 3. Modifier le mot de passe de l'utilisateur « maint » 4. Changer de fuseau horaire 5. Augmenter la taille du disque de prison (/jail) 6. Mise à niveau 7. Installer VMware Tools

Configuration du réseau	1. Afficher les paramètres d'adresse IP 2. Afficher les paramètres de recherche de nom de domaine 3. Modifier les paramètres de recherche de nom de domaine 4. Afficher les itinéraires statiques 5. Modifier les itinéraires statiques 6. Valider les modifications 7. Envoyer un ping à un hôte 8. Restaurer les paramètres par défaut
Assistance et diagnostic	1. Accéder au shell de diagnostic 2. Activer l'accès au diagnostic à distance 3. Fournir les informations d'identification vCenter pour la sauvegarde 4. Prendre une sauvegarde

Configurer l'accès au diagnostic à distance

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

Avant de commencer

L'extension du fournisseur VASA doit être activée pour votre instance vCenter Server.

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 temps expire.

    La session de connexion reste valable uniquement jusqu'à minuit le lendemain.
  - Vous vous connectez à nouveau en tant qu'utilisateur de diagnostic à l'aide de SSH.

Étapes

1. Depuis vCenter Server, ouvrez une console sur VASA Provider.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrer `4` pour sélectionner Support et Diagnostics.
4. Entrer `2` pour sélectionner Activer l'accès aux diagnostics à distance.
5. Entrer `y` dans la boîte de dialogue Confirmation pour activer l'accès au diagnostic à distance.

6. Saisissez un mot de passe pour l'accès au diagnostic à distance.

Démarrer SSH sur d'autres nœuds

Vous devez démarrer SSH sur d'autres nœuds avant de procéder à la mise à niveau.

Avant de commencer

L'extension du fournisseur VASA doit être activée pour votre instance vCenter Server.

À propos de cette tâche

Effectuez cette procédure sur chacun des nœuds avant la mise à niveau.

Étapes

1. Depuis vCenter Server, ouvrez une console sur VASA Provider.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrer `4` pour sélectionner Support et Diagnostics.
4. Entrer `1` pour sélectionner Accéder au shell de diagnostic.
5. Entrer `y` pour continuer.
6. Exécutez la commande *sudo systemctl restart ssh*.

Mettre à jour les informations d'identification de vCenter Server et ONTAP

Vous pouvez mettre à jour l'instance vCenter Server et les informations d'identification ONTAP à l'aide de la console de maintenance.

Avant de commencer

Vous devez disposer des informations de connexion de l'utilisateur de maintenance.

À propos de cette tâche

Si vous avez modifié les informations d'identification de vCenter Server, ONTAP ou Data LIF après le déploiement, vous devez mettre à jour les informations d'identification à l'aide de cette procédure.

Étapes

1. Depuis vCenter Server, ouvrez une console sur VASA Provider.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrer `2` pour sélectionner le menu de configuration du système.
4. Entrer `9` pour modifier les informations d'identification ONTAP .
5. Entrer `10` pour modifier les informations d'identification de vCenter.

Rapports des outils ONTAP

Le plug-in ONTAP tools for VMware vSphere fournit des rapports pour les machines virtuelles et les banques de données. Lorsque vous sélectionnez l'icône du plug-in NetApp ONTAP tools for VMware vSphere dans la section Raccourcis du client vCenter,

l'interface utilisateur accède à la page Présentation. Sélectionnez l'onglet Rapports pour afficher la machine virtuelle et le rapport des banques de données.

Le rapport Machines virtuelles affiche la liste des machines virtuelles découvertes (doivent avoir au moins un disque provenant de banques de données basées sur le stockage ONTAP) avec des mesures de performances. Lorsque vous développez l'enregistrement de la machine virtuelle, toutes les informations relatives au magasin de données liées au disque s'affichent.

Le rapport sur les magasins de données affiche la liste des ONTAP tools for VMware vSphere qui sont provisionnés à partir du backend de stockage ONTAP de tous types avec des mesures de performances.

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

Collecter les fichiers journaux

Vous pouvez collecter des fichiers journaux pour les ONTAP tools for VMware vSphere à partir des options disponibles dans l'interface utilisateur du gestionnaire des outils ONTAP . 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 de toutes les instances de vCenter Server. La génération de journaux à partir de l'interface utilisateur du client vCenter est limitée au serveur vCenter sélectionné.

Étapes

1. Lancez le gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les informations d'identification d'administrateur des ONTAP tools for VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **Lots de journaux** dans la barre latérale.

   Cette opération peut prendre plusieurs minutes.
4. Sélectionnez **Générer** pour générer les fichiers journaux.
5. Saisissez l'étiquette du groupe 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 de vSphere Client, accédez à **Support** > **Log bundle** > **Générer**.
3. Indiquez l'étiquette du fichier journal et générez-le. L'option de téléchargement s'affiche une fois les fichiers générés. Le téléchargement peut prendre un certain temps.

> Le groupe de journaux généré remplace le groupe de journaux qui a été généré au cours des 3 derniers jours ou 72 dernières heures.

Gérer les machines virtuelles

Considérations pour migrer ou cloner des machines virtuelles

Vous devez être conscient de certaines considérations lors de la migration de machines virtuelles existantes dans votre centre de données.

Migrer des machines virtuelles protégées

Vous pouvez migrer les machines virtuelles protégées vers :

- Même banque de données vVols dans un hôte ESXi différent
- Différents magasins de données vVols compatibles sur le même hôte ESXi
- Différents magasins de données vVols compatibles sur un hôte ESXi différent

Si la machine virtuelle est migrée vers un autre FlexVol volume, le fichier de métadonnées correspondant est également mis à jour avec les informations de la machine virtuelle. Si une machine virtuelle est migrée vers un autre hôte ESXi mais avec le même stockage, le fichier de métadonnées du FlexVol volume sous-jacent ne sera pas modifié.

Cloner des machines virtuelles protégées

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

- Même conteneur du même FlexVol volume utilisant le groupe de réplication

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

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

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

- Conteneur différent ou magasin de données vVols

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

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

Le clone de clone d'une machine virtuelle protégée est pris en charge.

Se référer à "Création d'une machine virtuelle pour le clonage" pour plus de détails.

Instantanés de machines virtuelles

Actuellement, seuls les instantanés de machines virtuelles sans mémoire sont pris en charge. Si la machine virtuelle dispose d'un snapshot avec mémoire, la machine virtuelle n'est pas prise en compte pour la protection.

Vous ne pouvez pas non plus protéger les machines virtuelles non protégées qui disposent d'un instantané de

mémoire. Pour cette version, vous devez supprimer l'instantané de mémoire avant d'activer la protection de la machine virtuelle.

Pour les machines virtuelles Windows avec type de stockage ASA r2, lorsque vous prenez un instantané de la machine virtuelle, il s'agira d'un instantané en lecture seule. Lorsqu'un appel de puissance est lancé pour la machine virtuelle, le fournisseur VASA crée un LUN à l'aide du snapshot en lecture seule, puis l'active pour les IOPS. Lors de la demande de mise hors tension, VASA Provider supprime le LUN qui a été créé, puis désactive les IOPS.

Migrer des machines virtuelles avec des banques de données NFS et VMFS vers des banques de données vVols

Vous pouvez migrer des machines virtuelles depuis des banques de données NFS et VMFS vers des banques de données Virtual Volumes (vVols) pour tirer parti de la gestion des machines virtuelles basée sur des stratégies et d'autres fonctionnalités vVols . Les banques de données vVols vous permettent de répondre à des exigences de charge de travail accrues.

Avant de commencer

Assurez-vous que VASA Provider n'est en cours d'exécution sur aucune des machines virtuelles que vous prévoyez de migrer. Si vous migrez une machine virtuelle exécutant VASA Provider vers une banque de données vVols , vous ne pouvez effectuer aucune opération de gestion, y compris la mise sous tension des machines virtuelles qui se trouvent sur les banques de données vVols .

À propos de cette tâche

Lorsque vous migrez d'une banque de données NFS et VMFS vers une banque de données vVols , vCenter Server utilise les déchargements vStorage API for Array Integration (VAAI) lors du déplacement de données à partir de banques de données VMFS, mais pas à partir d'un fichier NFS VMDK. Les déchargements VAAI réduisent normalement 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**, puis sélectionnez **Suivant**.
3. Sélectionnez un format de disque virtuel, une stratégie de stockage de machine virtuelle et une banque de données vVol qui correspondent aux fonctionnalités de la banque de données que vous migrez.
4. Vérifiez les paramètres et sélectionnez **Terminer**.

Nettoyage VASA

Suivez les étapes de cette section pour effectuer le nettoyage VASA.

> Il est recommandé de supprimer toutes les banques de données vVols avant d'effectuer 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 vCenter Server.
3. Arrêtez les ONTAP tools for VMware vSphere VM.

4. Supprimer les ONTAP tools for VMware vSphere VM.

Attacher ou détacher un disque de données d'une machine virtuelle

Attacher un disque de données à une machine virtuelle

Attachez un disque de données à une machine virtuelle pour étendre la capacité de stockage.

Étapes

1. Connectez-vous au client vSphere.
2. Cliquez avec le bouton droit sur une machine virtuelle dans l'inventaire et sélectionnez **Modifier les paramètres**.
3. Dans l'onglet **Matériel virtuel**, sélectionnez **Disque dur existant**.
4. Sélectionnez la machine virtuelle sur laquelle se trouve le disque.
5. Sélectionnez le disque que vous souhaitez connecter et sélectionnez **OK**

Résultat

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

Détacher un disque de données de la machine virtuelle

Vous pouvez détacher un disque de données attaché à une machine virtuelle lorsqu'il n'est plus nécessaire. Lorsque vous détachez le disque de la machine virtuelle, il n'est pas automatiquement supprimé ; il reste sur le système de stockage ONTAP .

Étapes

1. Connectez-vous au client vSphere.
2. Cliquez avec le bouton droit sur une machine virtuelle dans l'inventaire et sélectionnez **Modifier les paramètres**.
3. Déplacez votre pointeur sur le disque et sélectionnez **Supprimer**.

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

Informations 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

Lorsque vous exécutez pour la première fois les ONTAP tools for VMware vSphere dans un client vSphere, les outils ONTAP découvrent les hôtes ESXi, leurs LUN et exportations NFS, ainsi que les systèmes de stockage NetApp qui possèdent ces LUN et exportations.

Avant de commencer

- Tous les hôtes ESXi doivent être sous tension et connectés.

- Toutes les machines virtuelles de stockage (SVM) à découvrir doivent être en cours d'exécution et chaque nœud de cluster doit avoir au moins un LIF de données configuré 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 informations sur les systèmes de stockage existants pour obtenir les dernières informations de capacité et de configuration à tout moment. Vous pouvez également modifier les informations d'identification que les ONTAP tools for VMware vSphere utilisent pour se connecter aux systèmes de stockage.

Lors de la découverte des systèmes de stockage, les ONTAP tools for VMware vSphere collectent des informations auprès des hôtes ESXi gérés par l'instance vCenter Server.

Étapes

1. Depuis la page d'accueil de vSphere Client, sélectionnez **Hôtes et clusters**.
2. Cliquez avec le bouton droit sur le centre de données requis et sélectionnez * Outils NetApp ONTAP * > * Mettre à jour les données de l'hôte * .

   Dans la boîte de dialogue **Confirmer**, confirmez votre choix.

3. Sélectionnez les contrôleurs de stockage découverts qui ont le statut `Authentication Failure` et sélectionnez **Actions** > **Modifier**.
4. Remplissez les informations requises dans la boîte de dialogue **Modifier le système de stockage**.
5. Répétez les étapes 4 et 5 pour tous les contrôleurs de stockage avec `Authentication Failure` statut.

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

- Utilisez les ONTAP tools for VMware vSphere pour configurer les paramètres d'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.
- Fournissez les informations d'identification du système de stockage.

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

Vous pouvez utiliser le tableau de bord des ONTAP tools for VMware vSphere pour modifier les paramètres de votre hôte ESXi.

Avant de commencer

S'il y a un problème avec les paramètres de votre hôte ESXi, le problème s'affiche dans le portlet des systèmes hôtes ESXi du tableau de bord. Vous pouvez sélectionner le problème pour afficher le nom d'hôte ou l'adresse IP de l'hôte ESXi qui présente le problème.

Étapes

1. Connectez-vous au client vSphere.
2. Dans la page des raccourcis, sélectionnez * Outils NetApp ONTAP * sous la section plug-ins.
3. Accédez au portlet **Conformité de l'hôte ESXi** dans la présentation (tableau de bord) du plug-in ONTAP tools for VMware vSphere .

4. Sélectionnez le lien **Appliquer les paramètres recommandés**.
5. Dans la fenêtre **Appliquer les paramètres d'hôte recommandés**, sélectionnez les hôtes que vous souhaitez conformer aux paramètres d'hôte recommandés par NetApp et sélectionnez **Suivant**.

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

6. Dans la page des paramètres, sélectionnez les valeurs recommandées 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 d'outils ONTAP

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

Étapes

1. Lancez le gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les informations d'identification d'administrateur des ONTAP tools for VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez l'icône **administrateur** dans le coin supérieur droit de l'écran et sélectionnez **Modifier le mot de passe**.
4. Dans la fenêtre contextuelle de modification du mot de passe, saisissez l'ancien mot de passe et les détails du nouveau mot de passe. La contrainte de modification du mot de passe est affichée sur l'écran de l'interface utilisateur.
5. Sélectionnez **Modifier** pour appliquer les modifications.

Réinitialiser le mot de passe du gestionnaire d'outils ONTAP

Si vous avez oublié le mot de passe du gestionnaire des outils ONTAP , vous pouvez réinitialiser les informations d'identification de l'administrateur à l'aide du jeton généré par la console de maintenance des ONTAP tools for VMware vSphere .

Étapes

1. Lancez le gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Sur l'écran de connexion, sélectionnez l'option **Réinitialiser le mot de passe**.

   Pour réinitialiser le mot de passe du gestionnaire, vous devez générer le jeton de réinitialisation à l'aide de la console de maintenance des ONTAP tools for VMware vSphere .

   a. Depuis le serveur vCenter, ouvrez la console de maintenance

b. Entrez « 2 » pour sélectionner l'option de configuration du système

c. Entrez « 3 » pour modifier le mot de passe de l'utilisateur « maint ».

3. Dans la fenêtre contextuelle de modification du mot de passe, saisissez le jeton de réinitialisation du mot de passe, le nom d'utilisateur et les détails du nouveau mot de passe.
4. Sélectionnez **Réinitialiser** pour appliquer les modifications. Une fois le mot de passe réinitialisé avec succès, vous pouvez utiliser un nouveau mot de passe pour vous connecter.

Réinitialiser le mot de passe de l'utilisateur de l'application

Le mot de passe utilisateur de l'application est utilisé pour l'enregistrement du fournisseur SRA et VASA auprès de vCenter Server.

Étapes

1. Lancez le gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les informations d'identification d'administrateur des ONTAP tools for VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **Paramètres** dans la barre latérale.
4. Dans l'écran **Informations d'identification VASA/SRA**, sélectionnez **Réinitialiser le mot de passe**.
5. Fournissez un nouveau mot de passe et confirmez les nouvelles entrées de mot de passe.
6. Sélectionnez **Réinitialiser** pour appliquer les modifications.

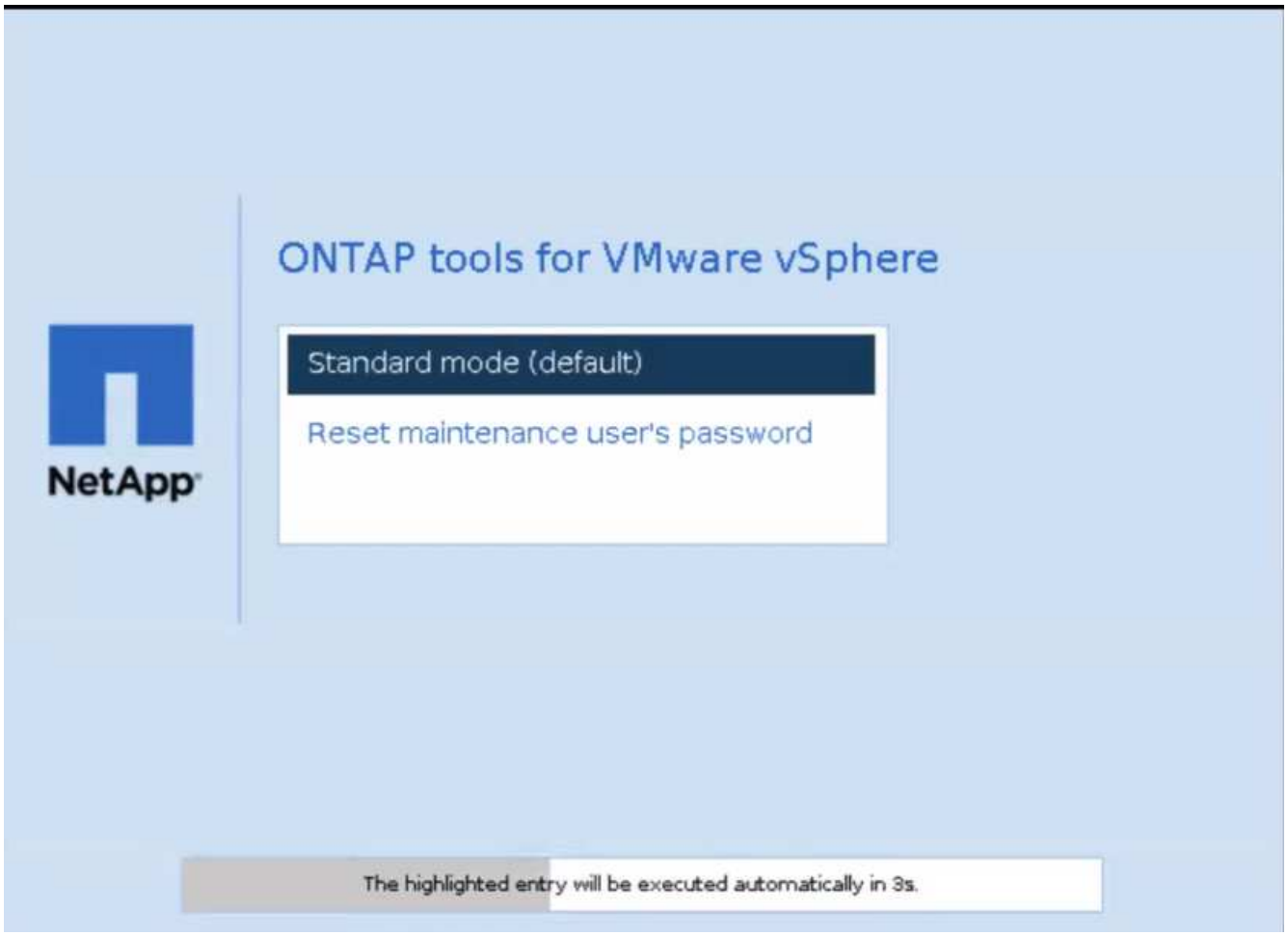
Réinitialiser le mot de passe utilisateur de la console de maintenance

Lors du redémarrage du système d'exploitation invité, le menu GRUB affiche une option permettant de réinitialiser le mot de passe de l'utilisateur de la console de maintenance. Cette option permet de mettre à jour le mot de passe de l'utilisateur de la console de maintenance présent sur la machine virtuelle correspondante. Une fois la réinitialisation terminée, la machine virtuelle redémarre pour définir le nouveau mot de passe. Dans un scénario de déploiement haute disponibilité, après le redémarrage de la machine virtuelle, le mot de passe est automatiquement mis à jour sur les deux autres machines virtuelles.

> Pour les ONTAP tools for VMware vSphere HA, vous devez modifier le mot de passe de l'utilisateur de la console de maintenance sur le premier nœud, qui est node1.

Étapes

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



Vous avez 5 secondes pour choisir votre option. Appuyez sur n'importe quelle touche pour arrêter la progression et geler le menu GRUB.

3. Sélectionnez l'option **Réinitialiser le mot de passe de l'utilisateur de maintenance**. La console de maintenance s'ouvre.
4. Dans la console, saisissez les détails du nouveau mot de passe. Le nouveau mot de passe et les détails du nouveau mot de passe doivent correspondre pour réinitialiser le mot de passe avec succès. Vous avez trois chances de saisir le mot de passe correct. Le système redémarre après avoir saisi avec succès le nouveau mot de passe.
5. Appuyez sur Entrée pour continuer. Le mot de passe est mis à jour sur la VM.

> Le même menu GRUB apparaît également lors de la mise sous tension de la VM. Cependant, vous ne devez utiliser l'option de réinitialisation du mot de passe qu'avec l'option **Redémarrer le système d'exploitation invité**.

Gérer la protection du cluster d'hôtes

Modifier le cluster d'hôtes protégé

Vous pouvez effectuer les tâches suivantes dans le cadre de la protection contre les modifications. Vous pouvez effectuer toutes les modifications dans le même flux de travail.

- Ajoutez de nouveaux magasins de données ou hôtes au cluster protégé.
- Ajoutez de nouvelles relations SnapMirror aux paramètres de protection.
- Supprimez les relations SnapMirror existantes des paramètres de protection.
- Modifier une relation SnapMirror existante.

Surveiller la protection du cluster d'hôtes

Utilisez cette procédure pour surveiller l'état de la protection du cluster hôte. Vous pouvez surveiller chaque cluster d'hôtes protégé ainsi que son état de protection, les relations SnapMirror , les banques de données et l'état SnapMirror correspondant.

Étapes

1. Connectez-vous au client vSphere.
2. Accédez à * Outils NetApp ONTAP * > **Protection** > **Relations entre clusters d'hôtes**.

   L'icône sous la colonne de protection indique l'état de la protection

3. Passez la souris sur l'icône pour voir plus de détails.

Ajouter de nouveaux magasins de données ou hôtes

Utilisez cette procédure pour protéger les banques de données ou les hôtes nouvellement ajoutés. Vous pouvez ajouter de nouveaux hôtes au cluster protégé ou créer de nouvelles banques de données sur le cluster hôte à l'aide de l'interface utilisateur native de vCenter.

Étapes

1. Connectez-vous au client vSphere.
2. Pour modifier les propriétés d'un cluster protégé, vous pouvez soit
   a. Accédez à * Outils NetApp ONTAP * > * Protection * > * Relations entre les clusters d'hôtes *, sélectionnez le menu à points de suspension en regard du cluster et sélectionnez * Modifier * ou
   b. Cliquez avec le bouton droit sur un cluster hôte et sélectionnez * Outils NetApp ONTAP * > * Protéger le cluster *.
3. Si vous avez créé une banque de données dans l'interface utilisateur native de vCenter, cette banque de données est affichée comme non protégée. L'interface utilisateur affiche tous les magasins de données du cluster et leur état de protection dans une boîte de dialogue. Sélectionnez le bouton **Protéger** pour activer une protection complète.
4. Si vous avez ajouté un nouvel hôte ESXi, l'état de protection s'affiche comme partiellement protégé. Sélectionnez le menu points de suspension sous les paramètres SnapMirror et sélectionnez **Modifier** pour définir la proximité de l'hôte ESXi nouvellement ajouté.

   > Dans le cas d'une relation de type asynchrone, la modification n'est pas prise en charge, car il est impossible d'ajouter la SVM cible du site tertiaire à la même instance des outils ONTAP . Cependant, vous pouvez utiliser le gestionnaire système ou l'interface de ligne de commande de la SVM cible pour modifier la configuration de la relation.

5. Sélectionnez **Enregistrer** après avoir effectué les modifications nécessaires.
6. Vous pouvez voir les modifications dans la fenêtre **Protéger le cluster**.

Une tâche vCenter est créée et vous pouvez suivre la progression dans le panneau **Tâche récente**.

Ajouter une nouvelle relation SnapMirror

Étapes

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

   Vous pouvez voir les modifications dans la fenêtre **Protéger le cluster**.

Une tâche vCenter est créée et vous pouvez suivre la progression dans le panneau **Tâche récente**.

Supprimer une relation SnapMirror existante

Pour supprimer une relation SnapMirror asynchrone, le site secondaire SVM ou le cluster doit être ajouté comme backend de stockage sur les ONTAP tools for VMware vSphere. Vous ne pouvez pas supprimer toutes les relations SnapMirror . Lorsque vous supprimez une relation, la relation correspondante sur le cluster ONTAP est également supprimée. Lorsque vous supprimez une relation AutomatedFailOverDuplex SnapMirror , les banques de données sur la destination ne sont pas mappées et le groupe de cohérence, les LUN, les volumes et les igroups sont supprimés du cluster ONTAP de destination.

La suppression de la relation déclenche une nouvelle analyse sur le site secondaire pour supprimer le LUN non mappé en tant que chemin actif des hôtes.

Étapes

1. Connectez-vous au client vSphere.
2. Pour modifier les propriétés d'un cluster protégé, vous pouvez soit
   a. Accédez à * Outils NetApp ONTAP * > * Protection * > * Relations entre les clusters d'hôtes *, sélectionnez le menu à points de suspension en regard du cluster et sélectionnez * Modifier * ou
   b. Cliquez avec le bouton droit sur un cluster hôte et sélectionnez * Outils NetApp ONTAP * > * Protéger le cluster *.
3. Sélectionnez le menu points de suspension sous les paramètres de SnapMirror et sélectionnez **Supprimer**.

Une tâche vCenter est créée et vous pouvez suivre la progression dans le panneau **Tâche récente**.

Modifier une relation SnapMirror existante

Pour modifier une relation SnapMirror asynchrone, le site secondaire SVM ou le cluster doit être ajouté comme backend de stockage sur les ONTAP tools for VMware vSphere. S'il s'agit d'une relation SnapMirror AutomatedFailOverDuplex, vous pouvez modifier la proximité de l'hôte en cas de configuration uniforme et l'accès de l'hôte en cas de configuration non uniforme. Vous ne pouvez pas échanger les types de stratégie Asynchronous et AutomatedFailOverDuplex. Vous pouvez définir la proximité ou l'accès des hôtes nouvellement découverts sur le cluster.

Vous ne pouvez pas modifier une relation SnapMirror asynchrone existante.

Étapes

1. Connectez-vous au client vSphere.
2. Pour modifier les propriétés d'un cluster protégé, vous pouvez soit
   a. Accédez à * Outils NetApp ONTAP * > * Protection * > * Relations entre les clusters d'hôtes *, sélectionnez le menu à points de suspension en regard du cluster et sélectionnez * Modifier * ou
   b. Cliquez avec le bouton droit sur un cluster hôte et sélectionnez * Outils NetApp ONTAP * > * Protéger le cluster *.
3. Si le type de stratégie AutomatedFailOverDuplex est sélectionné, ajoutez les détails de proximité ou d'accès à l'hôte.
4. Sélectionnez le bouton **Protéger**.

Une tâche vCenter est créée et vous pouvez suivre la progression dans le panneau **Tâche récente**.

Supprimer la protection du cluster hôte

Lorsque vous supprimez la protection du cluster hôte, les banques de données deviennent non protégées.

Étapes

1. Pour afficher les clusters d'hôtes protégés, accédez à * Outils NetApp ONTAP * > **Protection** > **Relations entre les clusters d'hôtes**.

   Sur cette page, vous pouvez surveiller les clusters d'hôtes protégés ainsi que leur état de protection, leur relation SnapMirror et leur statut SnapMirror correspondant.

2. Dans la fenêtre **Protection du cluster hôte**, sélectionnez le menu à points de suspension en regard du cluster, puis sélectionnez **Supprimer la protection**.

Désactiver AutoSupport

Lors de la première configuration de votre système de stockage, AutoSupport est activé par défaut. Il envoie des messages au support technique 24 heures après son activation. Lorsque vous désactivez AutoSupport, vous ne bénéficierez plus d'une assistance et d'une surveillance proactives.

Il est recommandé de garder AutoSupport activé. Cela permet d'accélérer la détection et la résolution des problèmes. Le système collecte les informations AutoSupport et les stocke localement, même lorsqu'il est désactivé. Cependant, il n'envoie le rapport à aucun réseau.

Étapes

1. Lancez le gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous avec les informations d'identification d'administrateur des ONTAP tools for VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez l'option **Paramètres** > **Télémétrie** > **Modifier**.

4. Désélectionnez l'option * AutoSupport* et enregistrez les modifications.

Mettre à jour l'URL du proxy AutoSupport

Mettez à jour l'URL du proxy AutoSupport pour garantir le bon fonctionnement de la fonctionnalité AutoSupport dans les scénarios où un serveur proxy est utilisé pour le contrôle d'accès au réseau ou les mesures de sécurité. Il permet aux données AutoSupport d'être acheminées via le proxy approprié, permettant une transmission sécurisée et une conformité.

Étapes

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

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

Ajouter des serveurs NTP

Saisissez les détails du serveur NTP pour synchroniser les horloges de l'appliance des outils ONTAP .

Étapes

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

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

Créer une sauvegarde et récupérer la configuration des outils ONTAP

À partir des ONTAP tools for VMware vSphere 10.3, l'appliance utilise un provisionneur de stockage dynamique, vous ne pouvez pas atteindre un RPO nul. Cependant, vous pouvez atteindre un RPO proche de zéro. Pour atteindre un RPO proche de zéro, vous devez créer une sauvegarde de la configuration et la restaurer sur une nouvelle machine virtuelle.

Pour migrer vers HA lorsque la sauvegarde non HA est activée, désactivez d'abord la sauvegarde et réactivez-la après la migration.

Créer une sauvegarde et télécharger le fichier de sauvegarde

Étapes

1. Depuis vCenter Server, ouvrez la console de maintenance.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrer `4` pour sélectionner **Support et Diagnostics**.
4. Entrer `3` pour sélectionner l'option **Activer la sauvegarde du système**.
5. En cas de non-HA, saisissez les informations d'identification vCenter sur lesquelles la machine virtuelle des outils ONTAP est déployée.
6. Entrez la valeur de fréquence de sauvegarde entre 5 et 60 minutes.
7. Appuyez sur **Entrée**

   Cela crée la sauvegarde et pousse la sauvegarde vers la banque de données de la machine virtuelle à intervalles réguliers.

8. Pour accéder à la sauvegarde, accédez à la section stockage et sélectionnez le magasin de données de la machine virtuelle
9. Sélectionnez la section **Fichiers**.

   Dans la section fichier, vous pouvez voir le répertoire. Le nom du répertoire sera l'adresse IP des outils ONTAP où les points (.) sont remplacés par des traits de soulignement, suffixés par *backup*.

10. Pour plus d'informations sur la sauvegarde, téléchargez le fichier backup_info.txt depuis **Fichiers** > **Télécharger**.

Récupérer

Pour récupérer la configuration, mettez hors tension la machine virtuelle existante et déployez une nouvelle machine virtuelle à l'aide de l'OVA qui a été utilisé dans le déploiement initial.

Vous devez utiliser la même adresse IP des outils ONTAP pour la nouvelle machine virtuelle et la configuration du système, telle que les services activés, la taille du nœud et le mode HA, doit être identique à celle du déploiement initial.

Effectuez les étapes suivantes pour récupérer la configuration à partir du fichier de sauvegarde.

1. Depuis vCenter Server, ouvrez la console de maintenance.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrer `4` pour sélectionner **Support et Diagnostics**.
4. Entrer `2` pour sélectionner l'option **Activer l'accès au diagnostic à distance** et créer un nouveau mot de passe pour l'accès au diagnostic.
5. Sélectionnez une sauvegarde dans le répertoire téléchargé. Le nom du dernier fichier de sauvegarde est enregistré dans le fichier *backup_info.txt*.
6. Exécutez la commande ci-dessous pour copier la sauvegarde sur la nouvelle machine virtuelle et entrez le

mot de passe de diagnostic lorsque vous y êtes invité.

```
scp <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.

7. Une fois le fichier de sauvegarde copié, connectez-vous au shell de diagnostic et exécutez la commande suivante :

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

Les journaux sont enregistrés dans le fichier */var/log/post-deploy-upgrade.log*.

8. Après une récupération réussie, les services et les objets vCenter sont restaurés.

Désinstaller les ONTAP tools for VMware vSphere

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

Étapes

1. Supprimez ou déplacez toutes les machines virtuelles des ONTAP tools for VMware vSphere .
   - Pour supprimer les machines virtuelles, reportez-vous à "Supprimer et réenregistrer les machines virtuelles et les modèles de machines virtuelles"
   - Pour les déplacer vers un magasin de données non géré, reportez-vous à "Comment migrer votre machine virtuelle avec Storage vMotion"
2. "Supprimer les banques de données"créé sur les ONTAP tools for VMware vSphere.
3. Si vous avez activé le fournisseur VASA, sélectionnez **Paramètres** > **Paramètres du fournisseur VASA** > **Désinscrire** dans les outils ONTAP pour désinscrire les fournisseurs VASA de tous les serveurs vCenter.
4. Dissociez tous les backends de stockage de l'instance vCenter Server. "Dissocier les backends de stockage de l'instance vCenter Server" .
5. Supprimez tous les backends de stockage. "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 du dispositif VMware Live Site Recovery à l'aide du port 5480.
   b. Sélectionnez **Adaptateurs de réplication de stockage**.
   c. Sélectionnez la carte SRA appropriée et, 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 aux ONTAP tools for VMware vSphere. "Gérer les instances de vCenter Server" .
8. Mettez hors tension les ONTAP tools for VMware vSphere à partir de vCenter Server et supprimez les

machines virtuelles.

Quelle est la prochaine étape ?

"Supprimer les volumes FlexVol"

Supprimer les volumes FlexVol

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

Étapes

1. Déterminez les ONTAP tools for VMware vSphere à partir du premier nœud de machine virtuelle.

   cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocole

   S'il s'agit d'un déploiement iSCSI, vous devez également supprimer les igroups.

2. Obtenez la liste des volumes FlexVol .

   kubectl décrit les volumes persistants | grep internalName | awk -F'=' '{print $2}'

3. Supprimez les machines virtuelles du vCenter Server. Se référer à "Supprimer et réenregistrer les machines virtuelles et les modèles de machines virtuelles" .
4. Supprimer les volumes FlexVol . Se référer à "Supprimer un FlexVol volume" . Dans la commande CLI pour supprimer un volume, indiquez le nom exact des volumes FlexVol .
5. Supprimez les groupes SAN du système de stockage ONTAP en cas de déploiement iSCSI. Se référer à "Afficher et gérer les initiateurs et les groupes SAN" .

Mettre à niveau les ONTAP tools for VMware vSphere

Mise à niveau des ONTAP tools for VMware vSphere 10.x vers 10.4

Vous pouvez effectuer une mise à niveau des ONTAP tools for VMware vSphere 10.2 ou 10.3 vers 10.4. Cependant, la mise à niveau directe des outils ONTAP 10.0 ou 10.1 vers 10.4 n'est pas prise en charge.

NOTE:

- Dans les systèmes ASA r2, vous devez effectuer une mise à niveau vers les ONTAP tools for VMware vSphere 10.4 avec ONTAP 9.16.1 avant d'ajouter d'autres zones de disponibilité de stockage (SAZ).
- Si la mise à niveau des ONTAP tools for VMware vSphere 10.2 ou 10.3 vers la version 10.4 échoue, la restauration n'est pas prise en charge. Pour récupérer la configuration, utilisez RPO pour les ONTAP tools for VMware vSphere 10.2 et RPO proche de zéro ou récupération de snapshot pour les ONTAP tools for VMware vSphere 10.3.

Avant de commencer

Pour une mise à niveau non HA, mettez hors tension la machine virtuelle des outils ONTAP et pour une mise à niveau HA, mettez hors tension le premier nœud avant d'apporter les modifications suivantes aux paramètres de la machine virtuelle (VM).

Si vous effectuez une mise à niveau depuis les ONTAP tools for VMware vSphere 10.2 ou 10.3, vous devez suivre les étapes suivantes avant de procéder à la mise à niveau : * Ajouter un disque dur supplémentaire de 100 Go à chaque nœud, car les données de service sont stockées localement sur la machine virtuelle. * Modifier le processeur et la mémoire de la machine virtuelle hors tension en fonction de votre déploiement. Activer le plug-in à chaud pour le processeur et la RAM.

+

Type de déploiement	CPU (cœur) par nœud	Mémoire (Go) par nœud	Espace disque (Go) par nœud	CPU total (cœur)	Mémoire (Go)	Espace disque total (Go)
Non-HA Petit	9	18	350	9	18	350
Milieu sans HA	13	26	350	13	26	350
HA Petit	9	18	350	27	54	1050
HA Moyen	13	26	350	39	78	1050
HA Grand	17	34	350	51	102	1050

- Allumez la machine virtuelle une fois les modifications effectuées et attendez que les services passent à un état d'exécution.
- En cas de déploiement HA, effectuez les modifications des ressources, activez le plug-in à chaud pour le processeur et la RAM, et ajoutez également des disques durs de 100 Go pour le deuxième et le troisième nœud. Il n'est pas nécessaire de redémarrer ces nœuds.

- Si l'appliance a été déployée en tant que chemin local (déploiement facile) avec les outils ONTAP 10.2, vous devez prendre un instantané de mise au repos avant la mise à niveau.

Si vous effectuez une mise à niveau des ONTAP tools for VMware vSphere 10.0 vers 10.1, vous devez effectuer les étapes suivantes avant de procéder à la mise à niveau : **Activer les diagnostics**

1. Depuis vCenter Server, ouvrez une console sur les outils ONTAP .
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Saisissez **4** pour sélectionner **Support et diagnostics**.
4. Saisissez **2** pour sélectionner **Activer l'accès au diagnostic à distance**.
5. Entrez **y** pour définir le mot de passe de votre choix.
6. Connectez-vous à l'adresse IP de la VM à partir du terminal/putty avec l'utilisateur « diag » et le mot de passe défini à l'étape précédente.

Faites une sauvegarde de MongoDB

Exécutez les commandes suivantes pour effectuer une sauvegarde de MongoDB :

- kn exec -it ntv-mongodb-0 sh - kn est un alias de kubectl -n ntv-system.
- Exécutez la commande *env | grep MONGODB_ROOT_PASSWORD* à l'intérieur du pod.
- Exécutez la commande *exit* pour sortir du pod.
- Exécutez la commande *kn exec ntv-mongodb-0 --mongodump -u root -p MONGODB_ROOT_PASSWORD --archive=/tmp/mongodb-backup.gz --gzip* pour remplacer le MONGO_ROOT_PASSWORD défini à partir de la commande ci-dessus.
- Exécutez la commande *kn cp ntv-mongodb-0:/tmp/mongodb-backup.gz ./mongodb-backup.gz* pour copier la sauvegarde mongodb créée à l'aide de la commande ci-dessus du pod vers l'hôte.

Prenez un instantané quasi instantané de tous les volumes

- Exécutez la commande « kn get pvc » et enregistrez la sortie de la commande.
- Prenez des instantanés de tous les volumes un par un en utilisant l'une des méthodes suivantes :
  - Depuis l'interface de ligne de commande, exécutez la commande *volume snapshot create -vserver <vserver_name> -volume <volume_name> -snapshot <snapshot_name>*
  - Depuis l'interface utilisateur d' ONTAP System Manager, recherchez le volume par son nom dans la barre de recherche, puis ouvrez ce volume en sélectionnant le nom. Accédez à l'instantané et ajoutez l'instantané de ce volume.

Prenez l'instantané des ONTAP tools for VMware vSphere dans vCenter (3 machines virtuelles en cas de déploiement HA, 1 machine virtuelle en cas de déploiement non HA)

- Dans l'interface utilisateur du client vSphere, sélectionnez la machine virtuelle.
- Accédez à l'onglet Instantanés et sélectionnez le bouton **Prendre un instantané**. Prenez un instantané inactif de la machine virtuelle. Se référer à "Prendre un instantané d'une machine virtuelle" pour plus de détails.

Avant d'effectuer la mise à niveau, supprimez les pods terminés du bundle de journaux avec le préfixe « generate-support-bundle-job ». Si la génération du bundle de support est en cours, attendez qu'elle soit terminée, puis supprimez le pod.

Pour tout type de mise à niveau, vous devez ajouter un disque dur (HDD) supplémentaire de 100 Go. Pour ajouter un disque dur, effectuez la tâche suivante.

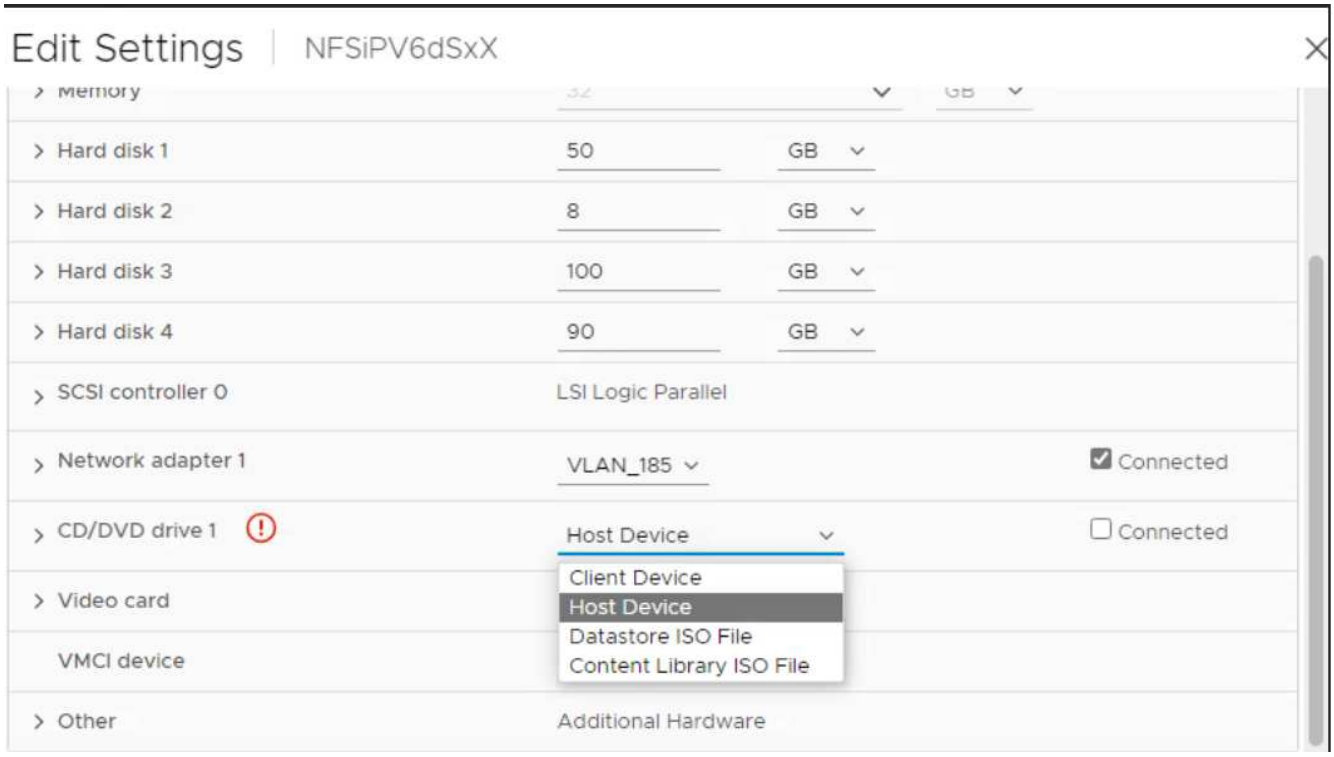
1. Sélectionnez la machine virtuelle dans une configuration à nœud unique ou les trois machines virtuelles dans une configuration HA.
2. Faites un clic droit sur la ou les machines virtuelles et sélectionnez **Ajouter un nouveau périphérique** > **Disque dur**
3. Ajoutez un disque dur de 100 Go dans le champ **Nouveau disque dur**.
4. Sélectionnez **Appliquer**

Après avoir ajouté le disque dur, mettez à jour les ressources de la machine virtuelle pour les configurations respectives et redémarrez la machine virtuelle principale.

Un nouveau disque dur sera créé. Le provisionneur de stockage dynamique utilise ce disque dur pour générer ou répliquer les volumes.

Étapes

1. Téléchargez les ONTAP tools for VMware vSphere vers la bibliothèque de contenu.
2. Dans la page principale de la machine virtuelle, sélectionnez **Actions** > **Modifier les paramètres**
3. Sélectionnez le fichier ISO de la bibliothèque de contenu dans la fenêtre des paramètres d'édition sous le champ **Lecteur CD/DVD**.
4. Sélectionnez le fichier ISO et sélectionnez **OK**. Cochez la case connectée dans le champ **Lecteur CD/DVD**.



5. Depuis vCenter Server, ouvrez une console sur les outils ONTAP .
6. Connectez-vous en tant qu'utilisateur de maintenance.
7. Entrez **3** pour sélectionner le menu Configuration système.
8. Entrez **7** pour sélectionner l'option de mise à niveau.

9. Lors de la mise à niveau, les actions suivantes sont effectuées automatiquement :
    a. Mise à niveau du certificat
    b. Mise à niveau du plug-in à distance

Après la mise à niveau vers les ONTAP tools for VMware vSphere 10.4, vous pouvez :

- Désactiver 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.
- En cas de mise à niveau non HA, redémarrez la machine virtuelle des outils ONTAP pour refléter les modifications. En cas de mise à niveau HA, redémarrez le premier nœud pour refléter les modifications sur le nœud.

Quelle est la prochaine étape

Après avoir effectué une mise à niveau à partir des versions précédentes des ONTAP tools for VMware vSphere vers la version 10.4, analysez à nouveau les adaptateurs SRA pour vérifier que les détails sont mis à jour sur la page Adaptateurs de réplication de stockage VMware Live Site Recovery.

Une fois la mise à niveau réussie, supprimez manuellement les volumes Trident d' ONTAP en suivant la procédure suivante :

> Ces étapes ne sont pas requises si les ONTAP tools for VMware vSphere 10.1 ou 10.2 se trouvaient dans des configurations non HA de petite ou moyenne taille (chemin local).

1. Depuis vCenter Server, ouvrez une console sur les outils ONTAP .
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Saisissez **4** pour sélectionner le menu **Support et diagnostics**.
4. Saisissez **1** pour sélectionner l'option **Shell de diagnostic d'accès**.
5. Exécutez la commande suivante

```
sudo python3 /home/maint/scripts/ontap_cleanup.py
```

6. Entrez le nom d'utilisateur et le mot de passe ONTAP

Cela supprime tous les volumes Trident dans ONTAP utilisés dans les ONTAP tools for VMware vSphere 10.1/10.2.

Informations connexes

"Migrer des ONTAP tools for VMware vSphere 9.xx vers 10.4"

Codes d'erreur de mise à niveau

Vous pouvez 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 chiffres représentant le script qui a rencontré le problème et les trois derniers

chiffres représentant le flux de travail spécifique dans ce script.

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

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

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

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

Code d'erreur de mise à niveau	Flux de travail	Résolution
052	L'ISO peut être la même que la version actuelle ou deux versions au-dessus de la version actuelle.	Utilisez une version ISO compatible pour effectuer une mise à niveau à partir de votre version actuelle.
068	La restauration des paquets Debian a échoué	Utilisez une récupération basée sur un RPO zéro ou un snapshot et réessayez la mise à niveau.
069	Échec de la restauration des fichiers	Utilisez une récupération basée sur un RPO zéro ou un snapshot 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	Vérifiez le fichier /var/log/upgrade-run.log et réessayez la mise à niveau.
075	Les pré-vérifications de mise à niveau ont échoué	Réessayez la mise à niveau.

Code d’erreur de mise à niveau	Flux de travail	Résolution
076	La mise à niveau du registre a échoué	Utilisez une récupération basée sur un RPO zéro ou un snapshot et réessayez la mise à niveau.
077	La restauration du registre a échoué	Utilisez une récupération basée sur un RPO zéro ou un snapshot et réessayez la mise à niveau.
078	La mise à niveau de l’opérateur a échoué	Utilisez une récupération basée sur un RPO zéro ou un snapshot et réessayez la mise à niveau.
079	La restauration de l’opérateur a échoué	Utilisez une récupération basée sur un RPO zéro ou un snapshot et réessayez la mise à niveau.
080	La mise à niveau des services a échoué	Utilisez une récupération basée sur un RPO zéro ou un snapshot et réessayez la mise à niveau.
081	La restauration des services a échoué	Utilisez une récupération basée sur un RPO zéro ou un snapshot et réessayez la mise à niveau.
082	La suppression des anciennes images du conteneur a échoué	Utilisez une récupération basée sur un RPO zéro ou un snapshot et réessayez la mise à niveau.
083	La suppression de la sauvegarde a échoué	Utilisez une récupération basée sur un RPO zéro ou un snapshot et réessayez la mise à niveau.
084	Le retour du JobManager en mode Production a échoué	Suivez les étapes ci-dessous pour récupérer/terminer la mise à niveau. 1. Activer le shell de diagnostic 2. Exécutez la commande : *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 3. Consultez les journaux dans /var/log/post-deploy-upgrade.log
087	Les étapes de post-mise à niveau ont échoué.	Effectuez les étapes suivantes pour récupérer/terminer la mise à niveau. 1. Activer le shell de diagnostic 2. Exécutez la commande *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 3. Consultez les journaux dans /var/log/post-deploy-upgrade.log

Code d'erreur de mise à niveau	Flux de travail	Résolution
088	La configuration de la rotation du journal pour journald a échoué	Vérifiez les paramètres réseau de la VM compatibles avec l'hôte sur lequel la VM est hébergée. Vous pouvez essayer de migrer la VM vers un autre hôte et de redémarrer.
089	La modification de la propriété 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 pour la mise à niveau du système d'exploitation. Les services des outils ONTAP sont mis à niveau et de nouveaux pods seront exécutés.
096	Installer un provisionneur de stockage dynamique	Vérifiez les journaux de mise à niveau et réessayez la mise à niveau.
097	La désinstallation des services pour la mise à niveau a échoué	Utilisez un RPO nul ou une récupération basée sur un instantané et réessayez la mise à niveau.
098	la copie du secret dockercred du système ntv vers l'espace de noms du provisionneur de stockage dynamique a échoué	Vérifiez les journaux de mise à niveau et réessayez la mise à niveau.
099	Échec de la validation du nouvel ajout de disque dur	Ajoutez le nouveau disque dur à tous les nœuds en cas de déploiement HA et à un nœud en cas de déploiement non HA.
108	Échec du script d'amorçage	-
109	la sauvegarde des données du volume persistant a échoué	Vérifiez 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 basée sur un RPO zéro ou un snapshot et réessayez la mise à niveau.
111	La mise à jour des paramètres de délai d'expiration etcd pour RKE2 a échoué	Vérifiez 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	Vérifiez les journaux de mise à niveau et réessayez la mise à niveau.

Code d'erreur de mise à niveau	Flux de travail	Résolution
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	Vérifiez les journaux de mise à niveau et réessayez la mise à niveau.
056	la suppression de la sauvegarde de migration a échoué	N / A

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

En savoir plus sur "Comment restaurer les ONTAP tools for VMware vSphere en cas d'échec de la mise à niveau de la version 10.0 vers la version 10.1"

Migrer les ONTAP tools for VMware vSphere 9.xx vers 10.4

Migrer des ONTAP tools for VMware vSphere 9.xx vers 10.4

Le déplacement des outils NetApp ONTAP tools for VMware vSphere de la version 9.xx vers la version 10.x nécessite un processus de migration en raison des mises à jour et des améliorations importantes du produit entre les versions.

Vous pouvez migrer des ONTAP tools for VMware vSphere 9.12D1, 9.13D2 et 9.13P2 vers les ONTAP tools for VMware vSphere 10.4.

Si vous disposez de banques de données NFS et VMFS et d'aucune banque de données vVols dans votre configuration, désinstallez simplement les outils ONTAP 9.xx et déployez les outils ONTAP 10.x. Cependant, si votre configuration contient des magasins de données vVols , vous devrez suivre un processus de migration du fournisseur VASA et du SRA.

Le tableau suivant décrit le processus de migration dans ces deux scénarios différents.

*Si la configuration dispose de magasins de données vVols *	Si la configuration contient uniquement des banques de données NFS et VMFS
Étapes : 1. "Migrer le fournisseur VASA" 2. "Créer des politiques de stockage de machines virtuelles"	Étapes : 1. Supprimez les outils ONTAP 9.xx de votre environnement. Se référer à "Comment supprimer OTV 9.xx de votre environnement" Article de la base de connaissances NetApp . 2. "Déployer et configurer les ONTAP tools for VMware vSphere 10.4" 3. "Mettre à jour le SRA" 4. "Créer des politiques de stockage de machines virtuelles"

Après la migration des ONTAP tools for VMware vSphere 9.xx vers 10.4, les banques de données vVols utilisant le protocole NVMe/FC deviennent non opérationnelles car les outils ONTAP 10.4 prennent en charge le protocole NVMe-oF uniquement avec les banques de données VMFS.

Migrer le fournisseur VASA et mettre à jour le SRA

Étapes pour migrer le fournisseur VASA

1. Pour activer Derby PORT 1527 sur les ONTAP tools for VMware vSphere, activez l'utilisateur root et connectez-vous à la CLI via SSH. Ensuite, exécutez la commande suivante :

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. Déployez les ONTAP tools for VMware vSphere 10.4.
3. Ajoutez l'instance vCenter Server que vous souhaitez migrer vers les ONTAP tools for VMware vSphere 10.4. Consultez "Ajouter une instance de vCenter Server" pour plus d'informations.

4. Intégrez le backend de stockage localement à partir des API du serveur vCenter pour le plug-in des outils ONTAP .
5. Émettez l'API suivante depuis Swagger ou dans Postman pour migrer.

   curl -X POST `https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migration-jobs`

   Vous pouvez accéder à Swagger via cette URL : `https://$FQDN_IP_PORT/', for example: `\https://10.67.25.33:8443 .

   Méthode HTTP et point de terminaison

   Cet appel d'API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
POSTE	/api/v1

   Type de traitement

   Asynchrone

   Exemple de boucle

   curl -X POST'https://<OTV-NG-IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-jobs' \ --header 'x-auth: <auth_token>' \ --header 'Content-Type: application/json' \ --data '{ "otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "username": "xxxxx", "password": "" }, "database_password": "" }'

   Corps de la demande pour une autre migration de version :

   { "otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "username": "xxxxx", "password": "*" } }

   Exemple de sortie JSON

   Un objet de travail est renvoyé. Vous devez enregistrer l'identifiant du travail pour l'utiliser à l'étape suivante.

   { "id": 123, "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "status": "running" }

6. 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`
   ```

   Une fois le travail terminé, examinez le rapport de migration. Ce rapport est inclus dans les données du travail et est accessible à partir de la réponse au travail.

7. Ajoutez les ONTAP tools for VMware vSphere au vCenter Server et"Enregistrer le fournisseur VASA" avec les ONTAP tools for VMware vSphere.
8. "Activer le fournisseur VASA"service sur les ONTAP tools for VMware vSphere 10.4.
9. Arrêtez les ONTAP tools for VMware vSphere 9.10/9.11/9.12/9.13 à partir de la console de maintenance.

   Ne supprimez pas le fournisseur VASA.

   Après l'arrêt de l'ancien fournisseur VASA, vCenter Server bascule vers les ONTAP tools for VMware vSphere. Tous les datastores et machines virtuelles deviennent accessibles et sont gérés par les ONTAP tools for VMware vSphere.

10. Les banques de données NFS et VMFS migrées à partir des ONTAP tools for VMware vSphere 9.xxx sont visibles dans les ONTAP tools for VMware vSphere 10.4 uniquement après le déclenchement de la tâche de découverte de banque de données, ce qui peut prendre jusqu'à 30 minutes. Vérifiez que les banques de données sont visibles sur la page de présentation de la page d'interface utilisateur des outils ONTAP pour le plug-in VMware vSphere.
11. 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

Exemple de boucle

curl -X PATCH
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/84dr73bd-9173-65r7-w345-8ufdbb887d43`

Exemple de sortie JSON

Un objet de travail est renvoyé. Vous devez enregistrer l'identifiant du travail pour l'utiliser à l'étape suivante.

{ "id": 123, "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "status": "running" }

Le corps de la requête est vide pour l'opération de correctif.

> L'UUID est l'UUID de migration renvoyé en réponse à l'API post-migration.

Après avoir exécuté l'API de migration de correctifs, toutes les machines virtuelles sont conformes à la politique de stockage.

Quelle est la prochaine étape

Après avoir terminé la migration et enregistré les outils ONTAP 10.4 sur vCenter Server, suivez ces étapes :

- Attendez que **Discovery** soit terminé, les certificats seront actualisés automatiquement sur tous les hôtes.
- Prévoyez un délai suffisant avant de lancer les opérations sur la banque de données et les machines virtuelles. Le délai d'attente requis varie en fonction du nombre d'hôtes, de banques de données et de machines virtuelles dans la configuration. Un manque d'attente peut entraîner des pannes opérationnelles intermittentes.

Après la mise à niveau, si l'état de conformité de la machine virtuelle est obsolète, réappliquez la stratégie de stockage en procédant comme suit :

1. Accédez au magasin de données et sélectionnez **Résumé** > **Stratégies de stockage VM**.

   L'état de conformité sous **Conformité à la politique de stockage VM** indique **Obsolète**.

2. Sélectionnez la politique de machine virtuelle de stockage et la machine virtuelle correspondante
3. Sélectionnez **Appliquer**

   L'état de conformité sous **Conformité à la politique de stockage VM** est désormais affiché comme conforme.

Informations connexes

- "En savoir plus sur les ONTAP tools for VMware vSphere 10 RBAC"
- "Mise à niveau des ONTAP tools for VMware vSphere 10.x vers 10.4"

Étapes pour mettre à jour l'adaptateur de réplication de stockage (SRA)

Avant de commencer

Dans le plan de récupération, le site protégé désigne l'emplacement où les machines virtuelles sont actuellement exécutées, tandis que le site de récupération désigne l'emplacement où elles seront restaurées. L'interface SRM affiche l'état du plan de récupération, avec des détails sur les sites protégé et de récupération. Dans le plan de récupération, les boutons **CleanupP** et **Reprotect** sont désactivés, tandis que les boutons TEST et EXÉCUTER restent activés. Cela indique que le site est prêt pour la récupération des données. Avant de migrer le SRA, vérifiez qu'un site est en état protégé et l'autre en état de récupération.

> Ne commencez pas la migration si le basculement a été effectué mais que la reprotection est en attente. Assurez-vous que le processus de reprotection est terminé avant de procéder à la migration. Si un basculement de test est en cours, nettoyez le basculement de test et démarrez la migration.

1. Suivez ces étapes pour supprimer l'adaptateur SRA des outils ONTAP pour VMware vSphere 9.xx dans VMware Site Recovery :
   a. Accéder à la page de gestion de la configuration de VMware Live Site Recovery
   b. Accédez à la section **Adaptateur de réplication de stockage**.
   c. Dans le menu à points de suspension, sélectionnez **Réinitialiser la configuration**.
   d. Dans le menu à points de suspension, sélectionnez **Supprimer**.
2. Effectuez ces étapes sur les sites de protection et de récupération.
   a. "Activer les ONTAP tools for VMware vSphere"

b. Installez les ONTAP tools for VMware vSphere 10.4 SRA en suivant les étapes décrites dans"Configurer SRA sur le dispositif VMware Live Site Recovery" .

c. Sur la page de l'interface utilisateur de VMware Live Site Recovery, effectuez les opérations **Discover Arrays** et **Discover Devices** et confirmez que les périphériques s'affichent comme avant la migration.

Automatiser à l'aide de l'API REST

En savoir plus sur les ONTAP tools for VMware vSphere 10

Les ONTAP tools for VMware vSphere 10 sont un ensemble d'outils pour la gestion du cycle de vie des machines virtuelles. Il comprend une API REST robuste que vous pouvez utiliser dans le cadre de vos processus d'automatisation.

Fondation des services Web REST

Representational State Transfer (REST) est un style de création d'applications Web distribuées, y compris la conception d'API de services Web. Il établit un ensemble de technologies permettant d'exposer les ressources basées sur le serveur et de gérer leurs états.

Ressources et représentation de l'État

Les ressources sont les composants fondamentaux d'une application de services Web REST. Il y a deux tâches initiales importantes lors de la conception d'une API REST :

- Identifier les ressources système ou basées sur le serveur
- Définir les états des ressources et les opérations de transition d'état associées

Les applications clientes peuvent afficher et modifier les états 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 des services Web pour échanger des messages sur les ressources. Il suit le modèle CRUD basé sur les opérations génériques de création, de lecture, de mise à jour et de suppression. Le protocole HTTP comprend des en-têtes de demande et de réponse ainsi que des codes d'état de réponse.

Formatage des données JSON

Bien qu'il existe plusieurs formats de messages 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 utilisée pour transférer des informations d'état décrivant les ressources et les actions souhaitées.

Sécurité

La sécurité est un aspect important d'une API REST. Outre le protocole TLS (Transport Layer Security) utilisé pour protéger le trafic HTTP sur le réseau, les ONTAP tools for VMware vSphere 10 utilisent également des jetons d'accès pour l'authentification. Vous devez acquérir un jeton d'accès et l'utiliser lors des appels d'API ultérieurs.

Prise en charge des requêtes asynchrones

Les ONTAP tools for VMware vSphere 10 exécutent la plupart des requêtes de manière synchrone, renvoyant un code d'état une fois l'opération terminée. Il prend également en charge le traitement asynchrone pour les tâches qui nécessitent un temps d'exécution plus long.

Environnement du gestionnaire d'outils ONTAP

Il y a 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 sur une machine virtuelle distincte.

Adresse IP des outils ONTAP

Les ONTAP tools for VMware vSphere 10 exposent une adresse IP unique qui fournit une passerelle vers les capacités de la machine virtuelle. Vous devez fournir l'adresse lors de la configuration initiale et elle est attribuée à un composant d'équilibrage de charge interne. L'adresse est utilisée par l'interface utilisateur du gestionnaire d'outils ONTAP ainsi que pour accéder directement à la page de documentation Swagger et à l'API REST.

Deux API REST

En plus des ONTAP tools for VMware vSphere 10, le cluster ONTAP dispose de sa propre API REST. ONTAP Tools Manager utilise l'API REST ONTAP comme 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 des ONTAP tools for VMware vSphere 10

Bien que REST établisse un ensemble commun de technologies et de bonnes pratiques, l'implémentation exacte de chaque API peut varier en fonction des choix de conception. Vous devez être familiarisé avec la conception des ONTAP tools for VMware vSphere 10 avant de l'utiliser.

L'API REST comprend plusieurs catégories de ressources telles que les vCenters et les agrégats. Passez en revue le"Référence API" pour plus d'informations.

Comment accéder à l'API REST

Vous pouvez accéder aux ONTAP tools for VMware vSphere 10 via l'adresse IP des outils ONTAP ainsi que le port. L'URL complète comprend 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 cohérente pour chaque instance des ONTAP tools for VMware vSphere 10 ; seules la catégorie de ressource et la ressource spécifique changent entre les points de terminaison.

> Les valeurs d'adresse IP et de port dans les exemples ci-dessous sont fournies à titre d'illustration uniquement. Vous devez modifier ces valeurs pour votre environnement.

Exemple d'accès aux services d'authentification

```
https://10.61.25.34:8443/virtualization/api/v1/auth/login
```

Cette URL peut être utilisée pour demander un jeton d'accès à l'aide de la méthode POST.

Exemple 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 utilisent HTTP et les paramètres associés pour agir sur les instances et les collections de ressources. Les détails de l'implémentation HTTP sont présentés ci-dessous.

Méthodes HTTP

Les méthodes ou verbes HTTP pris en charge par l'API REST sont présentés dans le tableau ci-dessous.

Méthode	CRUD	Description
OBTENIR	Lire	Récupère les propriétés d'objet pour une instance de ressource ou une collection. Ceci est considéré comme une opération de liste lorsqu'il est utilisé avec une collection.
POSTE	Créer	Crée une nouvelle instance de ressource en fonction des paramètres d'entrée.
METTRE	Mise à jour	Met à jour une instance de ressource entière avec le corps de requête JSON fourni. Les valeurs clés non modifiables par l'utilisateur sont conservées.
CORRECTIF	Mise à jour	Demande qu'un ensemble de modifications sélectionnées dans la demande soit appliqué à l'instance de ressource.
SUPPRIMER	Supprimer	Supprime une instance de ressource existante.

En-têtes de demande et de réponse

Le tableau suivant résume 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` .
authentification x	Demande	Contient un jeton d'accès identifiant l'utilisateur émettant la demande via l'application cliente.
Type de contenu	Réponse	Renvoyé par le serveur en fonction de la `Accept` en-tête de 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.
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 demande a réussi bien qu'aucun contenu n'ait été renvoyé.
400	Mauvaise demande	La demande d'entrée 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	Non trouvé	La ressource référencée dans la demande n'existe pas.
409	Conflit	Une 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 est effectuée à l'aide d'un jeton d'accès. Les caractéristiques pertinentes du jeton et du processus d'authentification incluent :

- Le client doit demander un jeton à l'aide des informations d'identification d'administrateur du gestionnaire des outils ONTAP (nom d'utilisateur et mot de passe).
- Les jetons sont formatés sous forme de jeton Web JSON (JWT).
- Chaque jeton expire après 60 minutes.
- Les requêtes API d'un client doivent inclure le jeton dans le `x-auth` en-tête de requête.

Se référer à"Votre premier appel d'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 s'exécutent donc de manière synchrone. Autrement dit, ils renvoient un code d'état (par exemple 200) une fois la demande terminée. Les requêtes qui prennent plus de temps à exécuter s'exécutent de manière asynchrone à l'aide d'une tâche en arrière-plan.

Après avoir émis un appel API qui s'exécute de manière asynchrone, le serveur renvoie un code d'état HTTP 202. Cela indique que la demande a été acceptée mais pas encore terminée. Vous pouvez interroger la tâche en arrière-plan pour déterminer son statut, notamment sa réussite ou son échec.

Le traitement asynchrone est utilisé pour plusieurs types d'opérations de longue durée, notamment les opérations de stockage de données et vVol. Reportez-vous à la catégorie Gestionnaire de tâches de l'API REST sur la page Swagger pour plus d'informations.

Votre premier appel d'API REST ONTAP tools for VMware vSphere 10

Vous pouvez émettre un appel d'API à l'aide de curl pour démarrer avec les ONTAP tools for VMware vSphere 10.

Avant de commencer

Vous devez vérifier les informations et les paramètres requis dans les exemples de boucles.

Informations requises

Vous avez besoin des éléments suivants :

- ONTAP tools for VMware vSphere 10 Adresse IP ou FQDN ainsi que le port
- Informations d'identification pour l'administrateur du gestionnaire d'outils ONTAP (nom d'utilisateur et mot de passe)

Paramètres et variables

Les exemples curl présentés ci-dessous incluent des variables de style Bash. Vous pouvez définir ces variables dans l'environnement Bash ou les mettre à jour manuellement avant d'émettre les commandes. Si vous définissez les variables, le shell remplacera les valeurs dans chaque commande avant son exécution. Les variables sont décrites dans le tableau ci-dessous.

Variable	Description
$FQDN_IP_PORT	Le nom de domaine complet ou l'adresse IP du gestionnaire d'outils ONTAP ainsi que le numéro de port.
$MYUSER	Nom d'utilisateur pour le compte ONTAP Tools Manager.
$MONMOT DE PASSE	Mot de passe associé au nom d'utilisateur du gestionnaire d'outils ONTAP .
$ACCESS_TOKEN	Le jeton d'accès émis par le gestionnaire d'outils ONTAP .

Les commandes et la sortie suivantes sur la CLI Linux illustrent comment une variable peut être définie et affichée :

```
FQDN_IP_PORT=172.14.31.224:8443
echo $FQDN_IP
172.14.31.224:8443
```

Étape 1 : Acquérir un jeton d'accès

Vous devez acquérir un jeton d'accès pour utiliser l'API REST. Un exemple de procédure de demande d'un jeton d'accès est présenté ci-dessous. Vous devez remplacer les valeurs 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 d’API REST

Une fois que vous disposez d’un jeton d’accès, vous pouvez utiliser curl pour émettre un appel d’API REST. Inclure le jeton d’accès acquis à la première étape.

Exemple de boucle

```
curl --request GET \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/vcenters" \
--header "Accept: */*" \
--header "x-auth: $ACCESS_TOKEN"
```

La réponse JSON inclut une liste des instances VMware vCenter configurées sur le gestionnaire d’outils ONTAP .

Référence API pour les ONTAP tools for VMware vSphere 10 REST API

La référence de l’API REST des ONTAP tools for VMware vSphere 10 contient des détails sur tous les appels d’API. Cette référence est utile lors du développement d’applications d’automatisation.

Vous pouvez accéder à la documentation 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 nom de domaine complet des ONTAP tools for VMware vSphere 10 ainsi que du port.

Étapes

1. Tapez l’URL suivante dans votre navigateur en remplaçant la combinaison appropriée d’adresse IP et de port par la variable et appuyez sur **Entrée**.

   `https://$FQDN_IP_PORT/`

   Exemple

   `https://10.61.25.33:8443/`

2. À titre d’exemple d’appel d’API individuel, faites défiler 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 déposées, aux brevets et bien plus encore.

Copyright

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

Marques de commerce

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

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

Brevets

Une liste actuelle des brevets détenus par NetApp est disponible à l'adresse suivante :

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

Politique de confidentialité

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

Open source

Les fichiers d'avis fournissent des informations sur les droits d'auteur et les licences tiers utilisés dans les logiciels NetApp .

"Avis concernant les ONTAP tools for VMware vSphere 10.4"

Informations sur le copyright

Copyright © 2025 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.