Documentation sur les outils ONTAP pour VMware vSphere

ONTAP tools for VMware vSphere 10.3

NetApp
April 11, 2025

Sommaire

Documentation sur les outils ONTAP pour VMware vSphere

Notes de mise à jour

Notes de mise à jour

Découvrez les nouveautés et les améliorations disponibles dans les outils ONTAP pour VMware vSphere 10.3.

Pour obtenir la liste complète des nouvelles fonctionnalités et améliorations, reportez-vous à Nouveautés des outils ONTAP pour VMware vSphere 10.3la section .

Pour savoir si la migration à partir des outils ONTAP pour VMware vSphere 9 vers les outils ONTAP 10.3 est adaptée à votre déploiement, reportez-vous à la Comparaison des fonctionnalités des outils ONTAP pour VMware vSphere 9 et des outils ONTAP pour VMware vSphere 10. La migration est prise en charge à partir des outils ONTAP pour VMware vSphere 9.12-D et des versions 9.13-D vers les outils ONTAP pour VMware vSphere 10.3.

Pour plus d'informations, reportez-vous au "Notes de version des outils ONTAP pour VMware vSphere 10.3" . Vous devez vous connecter avec votre compte NetApp ou créer un compte pour accéder aux notes de version.

Nouveautés des outils ONTAP pour VMware vSphere 10.3

Découvrez les nouvelles fonctionnalités disponibles dans les outils ONTAP pour VMware vSphere 10.3.

Mise à jour	Description
Prise en charge de nouvelles versions de plate-forme et d'applications	Les outils ONTAP pour VMware vSphere 10.3 prennent désormais en charge les versions de plateforme et d'application suivantes : • ONTAP 9.16.0 et versions ultérieures • VMware vSphere 8.0 U3 • VMware Live site Recovery 9.0
Facilité de déploiement	Vous pouvez désormais déployer les outils ONTAP pour VMware vSphere 10.3 avec une configuration minimale requise sur un cluster à un seul nœud, puis les mettre à jour vers un déploiement haute disponibilité ou à plusieurs nœuds.
Provisionnement et configuration transparents	Les outils ONTAP pour VMware vSphere 10.3 ont supprimé les dépendances associées à Trident et utilisent désormais le provisionnement de stockage dynamique pour permettre un provisionnement et une configuration transparents.
Sécurité renforcée pour l'authentification par API REST	Les outils ONTAP pour VMware vSphere 10.3 s'appuient désormais sur des certificats signés par l'autorité de certification pour les API REST et l'interface utilisateur des outils ONTAP afin d'améliorer la sécurité.

Mise à jour	Description
Prise en charge des systèmes ASA r2	Les outils ONTAP pour VMware vSphere 10.3 prennent en charge le provisionnement de datastores VMFS sur les systèmes ASA r2 afin de protéger les datastores VMFS avec la synchronisation active SnapMirror et SRA/VMware Live site Recovery.
Observabilité améliorée	Les outils ONTAP pour VMware vSphere 10.3 étendent la prise en charge des metrics d'observabilité pour les datastores VMFS et vVol et leurs machines virtuelles respectives.

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

Découvrez si la migration à partir des outils ONTAP pour VMware vSphere 9 vers les outils ONTAP pour VMware vSphere 10.1 ou version ultérieure est adaptée à vos besoins. Pour obtenir les informations les plus récentes sur la compatibilité, reportez-vous àla section "Matrice d'interopérabilité NetApp".

Fonction	Outils ONTAP 9.13	Outils ONTAP 10.1	Outils ONTAP à partir de 10.2
Proposition de valeur clé	Rationalisez et simplifiez les opérations du premier au deuxième jour grâce à des fonctionnalités améliorées de sécurité, de conformité et d'automatisation	Évolution des outils ONTAP 10.x vers la parité 9.x tout en augmentant les limites de haute disponibilité, de performances et d'évolutivité	Prise en charge étendue pour inclure FC pour VMFS et vVols et NVMe-of/FC, NVMe-of/TCP pour VMFS uniquement. La facilité d'utilisation de NetApp SnapMirror, la configuration simple des clusters de stockage vSphere Metro et la prise en charge de VMware Live site Recovery sur trois sites
Qualification de la version ONTAP	ONTAP 9.9.1 à ONTAP 9.15.1	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 et 9.16.0 pour les outils ONTAP 10.3.
Prise en charge de la version de 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
Protocoles pris en charge	Datastores NFS et VMFS : datastores NFS (v3 et v4.1), VMFS (iSCSI et FCP) vVols : iSCSI, FCP, NVMe/FC, NFS v3	Datastores NFS et VMFS : NFS (v3 et v4.1), VMFS (iSCSI) vVols datastores : iSCSI, NFS v3	Datastores NFS et VMFS : datastores NFS (v3 et v4.1), VMFS (iSCSI/FCP/NVMe-of) avec vVols : iSCSI, FCP, NFS v3

Fonction	Outils ONTAP 9.13	Outils ONTAP 10.1	Outils ONTAP à partir de 10.2
Évolutivité	Hôtes et machines virtuelles : 300 hôtes, jusqu'à 10 000 datastores de machines virtuelles : 600 NFS, jusqu'à 50 VMFS, jusqu'à 250 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 sur les performances, la capacité et la conformité des hôtes Rapports dynamiques sur les machines virtuelles et les datastores	Mise à jour des tableaux de bord sur les performances, la capacité et la conformité des hôtes Rapports sur les VM et datastores dynamiques	Mise à jour des tableaux de bord sur les performances, la capacité et la conformité des hôtes Rapports sur les VM et datastores dynamiques
Protection des données	Réplication SRA pour VMFS et NFS FlexVols pour l'intégration de vVols SCV et interopérable pour la sauvegarde	SRA pour la réplication des datastores iSCSI VMFS et NFS v3	Réplication SRA pour les datastores iSCSI VMFS et NFS v3 protection trois sites combinant SMAS et VMware Live site Recovery.
Prise en charge de VASA Provider	VASA 4,0	VASA 3,0	VASA 3,0

Concepts

Présentation des outils ONTAP pour VMware vSphere

Les outils ONTAP pour VMware vSphere sont un ensemble d'outils de gestion du cycle de vie des machines virtuelles. Il s'intègre à l'écosystème VMware pour faciliter le provisionnement des datastores et assurer une protection de base des machines virtuelles.

Les outils ONTAP pour VMware vSphere sont un ensemble de microservices évolutifs horizontalement, pilotés par les événements et déployés en tant qu'appliance virtuelle ouverte (OVA). Cette version intègre l'API REST avec ONTAP.

Les outils ONTAP pour VMware vSphere comprennent les éléments suivants :

- Des fonctionnalités de machine virtuelle telles que la protection de base et la reprise après incident
- Vasa Provider pour la gestion granulaire des VM
- Gestion du stockage basée sur des règles
- Storage Replication adapter (SRA)
- Synchronisation active SnapMirror (SMAS)

Concepts et termes clés

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

Systèmes ASA r2

Les nouveaux systèmes NetApp ASA r2 apportent une solution matérielle et logicielle unifiée qui simplifie l'expérience et répond parfaitement aux besoins des clients SAN. "En savoir plus sur les systèmes de stockage ASA r2".

Autorité de certification (CA)

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

Groupe de cohérence

Un groupe de cohérence est un ensemble de volumes gérés comme une seule unité. Dans ONTAP, les groupes de cohérence simplifient la gestion et garantissent la protection d'une charge de travail applicative couvrant plusieurs volumes. En savoir plus sur "groupe de cohérence".

Double pile

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

Haute disponibilité (HA)

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

Numéro d'unité logique (LUN)

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

Espace de noms et sous-système NVMe

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

Gestionnaire d'outils ONTAP

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

Appliance virtuelle ouverte (OVA)

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

Objectif de point de récupération

Le RPO mesure la fréquence de sauvegarde ou de réplication des données. Elle représente le moment dans lequel les données doivent être restaurées après une panne afin de reprendre les activités de l'entreprise. Par exemple, si une entreprise a un objectif de point de récupération de 4 heures, elle peut tolérer la perte de 4 heures de données en cas d'incident.

Synchronisation active SnapMirror (SMAS)

La synchronisation active SnapMirror assure la continuité des services, même en cas de défaillance complète d'un site. Les applications peuvent ainsi basculer en toute transparence au moyen d'une copie secondaire. Une intervention manuelle, ainsi que des scripts personnalisés sont requis pour déclencher un basculement avec la synchronisation active SnapMirror. Lear en savoir plus sur "Synchronisation active SnapMirror".

Systèmes back-end

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

Storage Replication adapter (SRA)

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

SVM (Storage Virtual machine)

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

Configuration uniforme et non uniforme

- **Accès uniforme à l'hôte** signifie que les hôtes des deux sites sont connectés à tous les chemins vers les clusters de stockage sur les deux sites. Les chemins intersites sont étirés sur toute la distance.
- **Accès hôte non uniforme** signifie que les hôtes de chaque site sont connectés uniquement au cluster du même site. Les chemins intersites et les chemins étendus ne sont pas connectés.

> Un accès uniforme à l'hôte est pris en charge pour tout déploiement SnapMirror à synchronisation active. L'accès non uniforme à l'hôte n'est pris en charge que pour les déploiements actif-actif symétriques.

VMFS (Virtual machine File System)

VMFS est un système de fichiers en cluster spécialement conçu pour le stockage de 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. Elle présente plusieurs avantages et offre une alternative à l'utilisation d'un LUN classique. Un datastore vVol est généralement associé à une seule LUN qui agit comme un conteneur pour les vVols.

Stratégie de stockage de VM

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

Restauration de site en direct VMware

VMware Live site Recovery assure la continuité de l'activité, la reprise après incident, la migration de site et des fonctionnalités de test sans interruption pour les environnements virtuels VMware.

API VMware vSphere pour la sensibilisation du stockage (VASA)

Vasa est un ensemble d'API qui intègre les baies de stockage à vCenter Server pour la gestion et l'administration. L'architecture repose sur plusieurs composants, notamment le 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 vers la baie. VAAI permet d'améliorer considérablement les performances des tâches consommatrices de stockage.

Cluster de stockage vSphere Metro

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

Datastore vVols

Le datastore vVols est une représentation logique d'un conteneur vVols créée et gérée par un fournisseur VASA.

RPO nul

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

Contrôle d'accès basé sur des rôles

Découvrez les outils ONTAP pour VMware vSphere 10 RBAC

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

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

Composants RBAC

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

Privilèges

Un *privilège* est une action ou une capacité qui peut être autorisée ou refusée. Il peut s'agir d'une opération simple telle que la capacité de lire un fichier ou une opération plus abstraite spécifique à un système logiciel donné. Vous pouvez également définir Privileges pour limiter l'accès aux terminaux de l'API REST et aux commandes de l'interface de ligne de commande. Chaque implémentation de RBAC inclut une Privileges prédéfinie et peut également permettre aux administrateurs de créer une Privileges personnalisée.

Rôles

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

Objets

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

Utilisateurs et groupes

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

Autorisations

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

Deux environnements RBAC

Il existe deux environnements RBAC distincts que vous devez prendre en compte lorsque vous utilisez les outils ONTAP pour VMware vSphere 10.

Serveur VMware vCenter

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

Groupe ONTAP

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

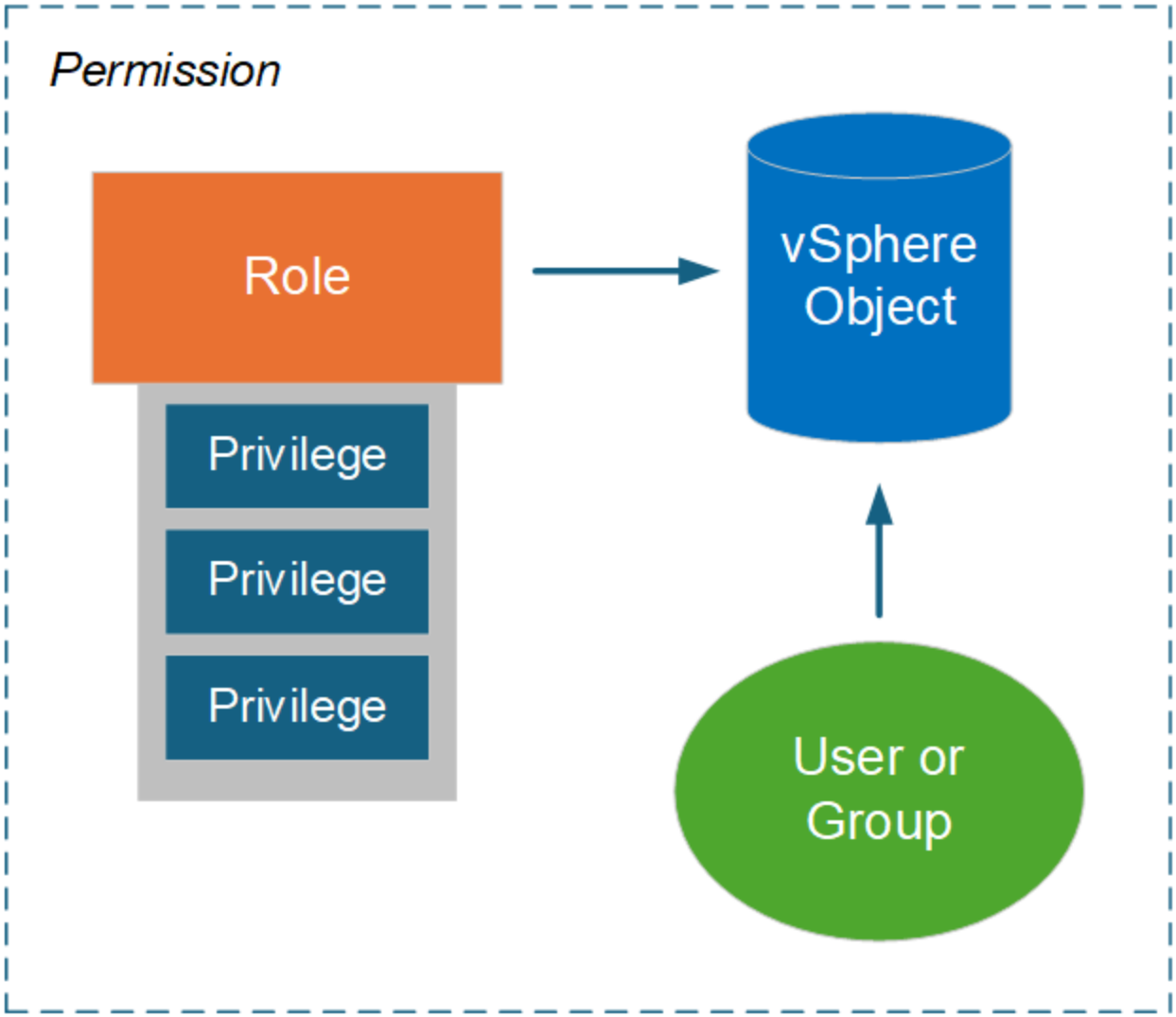
RBAC avec VMware vSphere

Environnement RBAC du serveur vCenter avec les outils ONTAP pour VMware vSphere 10

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

Illustration d'une autorisation vCenter Server

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



Composants d'une autorisation vCenter Server

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

Objets vSphere

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

Privileges et rôles

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

- Privilèges de serveur vCenter natif

  Il s'agit du Privileges fourni par vCenter Server.

- Privilèges spécifiques aux outils ONTAP

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

Utilisateurs et groupes

Vous pouvez définir des utilisateurs et des groupes à l'aide d'Active Directory ou de l'instance vCenter Server locale. Associé à un rôle, vous pouvez créer une autorisation sur un objet dans la hiérarchie d'objets vSphere. L'autorisation accorde l'accès en fonction du Privileges dans le rôle associé. Notez que les rôles ne sont pas attribués directement aux utilisateurs isolés. Les utilisateurs et les groupes peuvent accéder à un objet via le rôle Privileges, dans le cadre de l'autorisation serveur vCenter plus importante.

Utilisez vCenter Server RBAC avec les outils ONTAP pour VMware vSphere 10

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

Rôles vCenter et compte administrateur

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

Hiérarchie des objets vSphere

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

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

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

Rôles inclus avec les outils ONTAP pour VMware vSphere 10

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

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

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

Outils NetApp ONTAP pour VMware vSphere Administrator

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

Outils NetApp ONTAP pour VMware vSphere en lecture seule

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

Outils NetApp ONTAP pour le provisionnement VMware vSphere

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

- Créer de nouveaux datastores
- Gérer les datastores

Objets vSphere et systèmes back-end de stockage ONTAP

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

Utilisation de vCenter Server RBAC

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

Privilèges requis

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

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

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

Attribution d'autorisations

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

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

Les autorisations disponibles avec les outils ONTAP pour VMware vSphere 10 s'appliquent aux objets non vSphere personnalisés, tels que les systèmes de stockage. Si possible, vous devez attribuer ces autorisations

aux outils ONTAP pour l'objet racine VMware vSphere car il n'y a pas d'objet vSphere auquel vous pouvez l'affecter. Par exemple, toute autorisation qui inclut un privilège « Ajout/modification/Suppression de systèmes de stockage » des outils ONTAP pour VMware vSphere doit être attribuée au niveau de l'objet racine.

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

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

RBAC avec ONTAP

Environnement ONTAP RBAC avec les outils ONTAP pour VMware vSphere 10

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

Présentation des options administratives

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

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

Types de rôles et de Privileges

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

- REPOS

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

- Traditionnel

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

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

Portée

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

Définitions de rôle

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

Utilisation des rôles REST ONTAP

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

Mappage de rôles

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

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

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

Interface d'administration lors de la définition des rôles ONTAP

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

Utilisez ONTAP RBAC avec les outils ONTAP pour VMware vSphere 10

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

Présentation du processus de configuration

Les outils ONTAP pour VMware vSphere 10 incluent la prise en charge de la création d'un utilisateur ONTAP avec un rôle personnalisé. Ces définitions sont fournies dans un fichier JSON que vous pouvez télécharger vers le cluster ONTAP. Vous pouvez créer l'utilisateur et adapter le rôle à vos besoins en matière d'environnement et de sécurité.

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

1. Préparation

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

2. Téléchargez le fichier de définition JSON

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

3. Créez un utilisateur ONTAP avec un rôle

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

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

4. Configurez le rôle

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

Configurez le rôle à l'aide de System Manager

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

Configuration de l'utilisateur principal et du rôle

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

Privilèges

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

- Détection

  Il permet donc d'ajouter des systèmes de stockage.

- Créer du stockage

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

- Modifier le stockage

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

- Détruire le stockage

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

Générer l'utilisateur avec un rôle

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

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

Exemple

```
OTV_10_VSC_Discovery_Create
```

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

Haute disponibilité des outils ONTAP pour VMware vSphere

Les outils ONTAP pour VMware vSphere prennent en charge une configuration haute disponibilité afin d'assurer la continuité de l'activité des outils ONTAP pour VMware vSphere en cas de défaillance.

La solution haute disponibilité permet une reprise rapide en cas de panne provoquée par :

- Défaillance d'hôte

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

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

Aucune configuration supplémentaire n'est requise pour les outils ONTAP pour VMware vSphere en vue d'assurer la haute disponibilité.

Les outils ONTAP pour VMware vSphere ne prennent pas en charge vCenter HA.

Pour activer la fonction de haute disponibilité, l'ajout à chaud de processeur et la connexion à chaud de mémoire doivent être activés pendant le déploiement ou plus tard dans les outils ONTAP pour les paramètres de machine virtuelle VMware vSphere.

AutoSupport

AutoSupport est un mécanisme qui surveille de manière proactive l'état de votre système et envoie automatiquement des messages au support technique NetApp, à votre organisation de support interne et à un partenaire de support.

L'option AutoSupport est activée par défaut lorsque vous configurez votre système de stockage pour la première fois. L'AutoSupport envoie des messages au support technique sous 24 heures après l'activation de AutoSupport.

Vous pouvez désactiver AutoSupport à l'aide de l'option **Configuration de l'application** > **Désactiver AutoSupport** de la console de maintenance. Il est recommandé de le laisser activé. L'activation de AutoSupport accélère la détection des problèmes et accélère la résolution des problèmes. Le système collecte les informations AutoSupport et les stocke localement, même lorsque le AutoSupport est désactivé. Cependant, il n'envoie pas le rapport à aucun réseau. Vous devez fournir l'url du proxy à l'aide de la console de maintenance de la première machine virtuelle. Utilisez l'option **Configuration de l'application** > **mettre à jour l'URL du proxy AutoSupport** pour entrer l'URL du proxy.

Interface utilisateur du Gestionnaire d'outils ONTAP

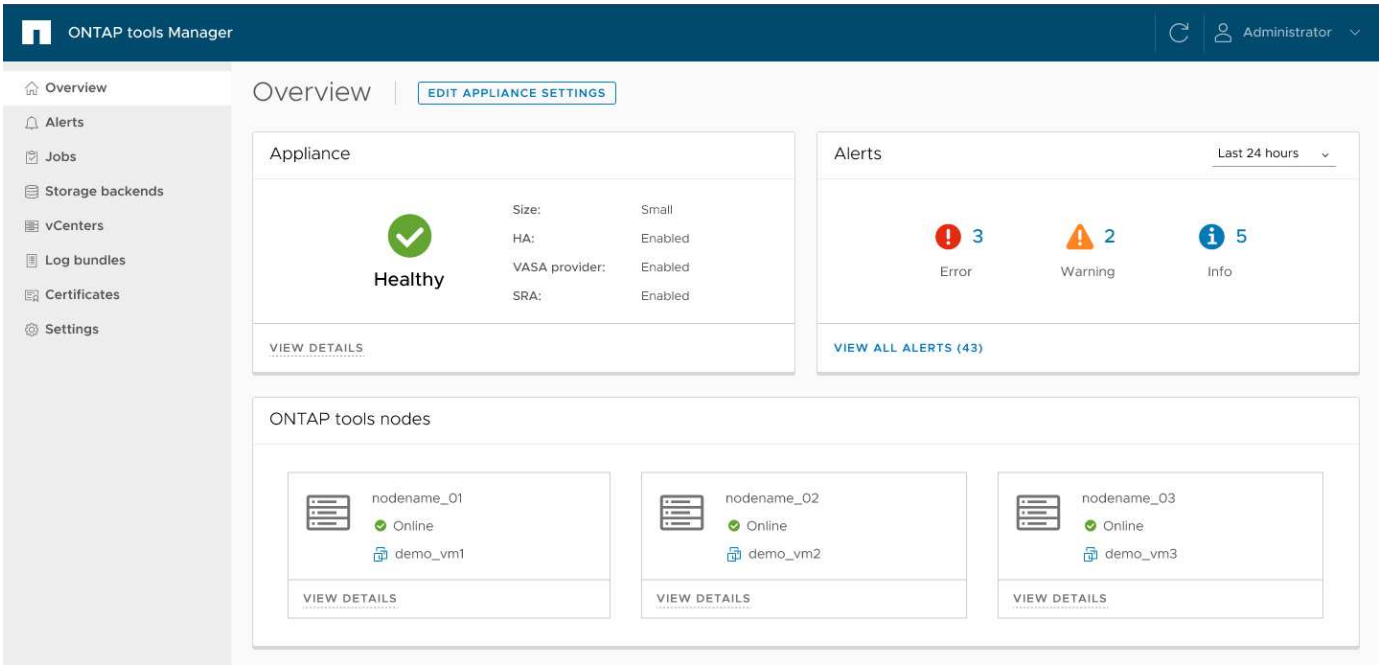
Les outils ONTAP pour VMware vSphere sont un système mutualisé capable de gérer plusieurs instances de vCenter Server. ONTAP Tools Manager offre davantage de contrôle aux outils ONTAP pour l'administrateur VMware vSphere sur les instances vCenter Server gérées et les systèmes back-end de stockage intégrés.

ONTAP Tools Manager vous aide à :

- Gestion des instances vCenter Server : permet d'ajouter et de gérer des instances vCenter Server aux outils ONTAP.
- Gestion du stockage back-end : ajoutez et gérez des clusters de stockage ONTAP aux outils ONTAP pour VMware vSphere et mappez-les vers des instances vCenter Server intégrées à l'échelle mondiale.
- Téléchargements de bundles de journaux : permet de collecter des fichiers journaux pour les outils ONTAP pour VMware vSphere.
- Gestion des certificats : remplacez le certificat auto-signé par un certificat AC personnalisé et renouvelez ou actualisez tous les certificats du fournisseur VASA et des outils ONTAP.
- Gestion des mots de passe : permet de 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/`-le à partir du navigateur et connectez-vous à l'aide des informations d'identification d'administrateur ONTAP Tools for VMware vSphere que vous avez fournies lors du déploiement.

La section Présentation du gestionnaire d'outils ONTAP vous aide à gérer la configuration des appliances, notamment la gestion des services, la montée en charge de la taille des nœuds et l'activation de la haute disponibilité. Vous pouvez également surveiller les informations globales des outils ONTAP liés au(x) nœud(s), telles que l'état, les détails du réseau et les alertes.



Carte	Description
Carte d'appareil	La carte de l'appliance indique l'état général de l'appliance ONTAP Tools. Il affiche les détails de la configuration de l'appliance et l'état des services activés. Pour plus d'informations sur l'appliance ONTAP Tools, cliquez sur le lien **Afficher les détails**. Lorsqu'un travail d'action de modification de paramètre d'appliance est en cours, le portlet de l'appliance affiche l'état et les détails du travail.
Carte d'alertes	La carte alertes répertorie les alertes des outils ONTAP par type, y compris les alertes de haute disponibilité au niveau du nœud. Vous pouvez afficher la liste des alertes en sélectionnant dans le texte de comptage (hyperlien). Le lien vous dirige vers la page d'affichage des alertes filtrée en fonction du type sélectionné.
Carte des nœuds des 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 relatives au réseau. Vous pouvez sélectionner sur **Afficher les détails** pour afficher les détails supplémentaires liés au nœud sélectionné. [REMARQUE] dans une configuration non HA, un seul nœud est affiché. En configuration haute disponibilité, trois nœuds sont illustrés.

Déployez les outils ONTAP pour VMware vSphere

Démarrage rapide des outils ONTAP pour VMware vSphere

La mise en route des outils ONTAP pour VMware vSphere comprend quelques étapes. Ce démarrage rapide vous guide tout au long de la configuration initiale des outils ONTAP pour VMware vSphere.

Dans un premier temps, vous déploierez les outils ONTAP pour VMware vSphere sous forme de configuration à un seul nœud de petite taille qui fournit des services de base pour la prise en charge des datastores NFS et VMFS. Si vous devez étendre votre configuration pour utiliser le datastore vVols et la haute disponibilité (HA), vous le ferez une fois ce workflow terminé. Pour plus d'informations, reportez-vous au "Workflow de déploiement de la HAUTE DISPONIBILITÉ".

Planification du déploiement

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

Assurez-vous que vCenter Server est installé et accessible.

- "Matrice d'interopérabilité"
- "Conditions préalables au déploiement des outils ONTAP pour VMware vSphere"
- "Avant de commencer"

Déployez les outils ONTAP pour VMware vSphere

Dans un premier temps, vous allez déployer les outils ONTAP pour VMware vSphere sous forme de configuration à un seul nœud de petite taille qui fournit des services de base pour la prise en charge des datastores NFS et VMFS. Si vous prévoyez d'étendre votre configuration pour utiliser les datastores vVols et la haute disponibilité (HA), vous le ferez une fois ce workflow terminé. Pour réussir l'extension vers une configuration haute disponibilité, vous devez vous assurer que les options d'ajout à chaud de CPU et de mémoire hot-plug sont activées.

- "Déployez les outils ONTAP pour VMware vSphere"

Ajouter des instances vCenter Server

Ajoutez une ou plusieurs instances de vCenter Server aux outils ONTAP pour VMware vSphere pour configurer, gérer et protéger vos datastores virtuels dans votre environnement vCenter Server.

- "Ajouter des instances vCenter Server"

Configurez les rôles d'utilisateur ONTAP et Privileges

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

- "Configurer les rôles et privilèges des utilisateurs ONTAP"

Configuration des systèmes back-end

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

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

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

Mettez à niveau les certificats si vous travaillez avec plusieurs serveurs vCenter

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

- "Gérer les certificats"

(Facultatif) activez la protection SRA

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

- "Configurez SRA sur l'appliance VMware Live site Recovery"

(Facultatif) Activer la protection de synchronisation active SnapMirror

Configurez les outils ONTAP pour VMware vSphere afin de gérer la protection des clusters hôtes pour la synchronisation active SnapMirror. Couplez les clusters source et destination et le SVM pour SnapMirror actif Sync. Cela s'applique uniquement aux datastores VMFS.

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

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

Planifiez des sauvegardes de vos outils ONTAP pour la configuration de VMware vSphere que vous pouvez utiliser pour restaurer la configuration en cas de défaillance.

- "Créer une sauvegarde et restaurer l'installation des outils ONTAP"

Workflow de déploiement de la haute disponibilité (HA

Si vous utilisez des datastores vVols, vous devez étendre le déploiement initial des outils ONTAP à une configuration haute disponibilité et activer les services VASA Provider.

1 **Scale-up du déploiement**

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

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

2 **Activation des services**

Pour configurer le datastore vVols, vous devez activer le service VASA Provider. Enregistrez le fournisseur VASA dans vCenter et vérifiez que vos règles de stockage répondent aux exigences de haute disponibilité, y compris les configurations réseau et de stockage appropriées.

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

- "Activation des services VASA Provider et SRA"

3 **Mettre à niveau les certificats**

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

- "Gérer les certificats"

Conditions préalables au déploiement des outils ONTAP pour VMware vSphere

Avant de déployer les outils ONTAP pour VMware vSphere, vous devez connaître l'espace requis pour le package de déploiement ainsi que certaines exigences de base en matière de système hôte.

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

Configuration minimale requise

- **Espace requis pour le package d'installation par nœud**
  - 15 Go pour les installations à provisionnement fin
  - 348 Go pour les installations à provisionnement lourd

- **Exigences de dimensionnement du système hôte** la mémoire recommandée selon la taille du déploiement est comme indiqué dans le tableau ci-dessous :

Type de déploiement	CPU	Mémoire (Go)	Espace disque (Go) thick provisionné
Non HA petit	9	18	350
Support non HA	13	26	350
HAUTE DISPONIBILITÉ faible (trois nœuds au total)	27	54	1050
Support HAUTE DISPONIBILITÉ (trois nœuds au total)	39	78	1050
HAUTE DISPONIBILITÉ ÉLEVÉE (trois nœuds au total)	51	102	1050

Exigences minimales en matière de stockage et d'applications

Stockage, hôte et applications	Configuration minimale requise pour la version
ONTAP	9.14.1, 9.15.1 et 9.16.0. FAS, ASA A-Series, ASA C-Series, AFF A-Series, AFF C-Series et ASA r2.
Hôtes ESXi	ESXi 7.0.3
Serveur vCenter	VCenter 7.0U3
Vasa Provider	3.0
Application OVA	10,3

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

"Matrice d'interopérabilité"

Limites de configuration pour le déploiement des outils ONTAP pour VMware vSphere

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

Déploiement	Type	Nombre de vVols	Nombre d'hôtes
Non HA	Petit (S)	~12 KO	32
Non HA	Moyen (M)	~24 KO	64
Haute-disponibilité	Petit (S)	~24 KO	64
Haute-disponibilité	Moyen (M)	environ 50 000	128

Haute-disponibilité	Grand (L)	environ 100 000	256 [REMARQUE] le nombre d'hôtes dans le tableau indique le nombre total d'hôtes provenant de plusieurs vCenters.

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

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

Taille du déploiement vCenter	Petit	Moyen
Nombre total de machines virtuelles configurées pour la protection à l'aide de la réplication basée sur les baies	2000	5000
Nombre total de groupes de protection de réplication basés sur les baies	250	250
Nombre total de groupes de protection par plan de reprise d'activité	50	50
Nombre de datastores répliqués	255	255
Nombre de VM	4000	7000

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

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

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

Configuration requise pour les ports

Le tableau suivant présente les ports réseau utilisés par NetApp ainsi que leurs fonctions. Assurez-vous que ces ports sont ouverts et accessibles pour faciliter le bon fonctionnement et la communication dans le système. Assurez-vous que les configurations réseau nécessaires sont en place pour permettre au trafic sur ces ports de fonctionner correctement pour les 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	Description

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 utilisateur de maintenance, les messages d'état et la mise à jour des valeurs sur les trois nœuds en cas de configuration haute disponibilité.
443 (TCP)	Il s'agit du port pass-through pour les communications entrantes du service VASA Provider. Le certificat auto-signé Vasa Provider 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 de l'interface utilisateur Manager.
2379 (TCP)	Il s'agit du port par défaut pour les demandes client telles que obtenir, mettre, supprimer ou surveiller les clés dans le magasin de valeurs de clé etcd.
2380 (TCP)	Il s'agit du port par défaut pour la communication 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 de service de metrics prometheus.
7946 (TCP+UDP)	Ce port est utilisé pour la détection du réseau de conteneurs 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 SNMP trap Packets.
6443 (TCP)	Source : nœuds agents RKE2. Destination : nœuds de serveur REK2. Description : API Kubernetes
9345 (TCP)	Source : nœuds agents RKE2. Destination : nœuds de serveur REK2. Description : API superviseur REK2
8472 (TCP+UDP)	Tous les nœuds doivent pouvoir atteindre d'autres nœuds sur 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 : mesures 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.

Avant de commencer…

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

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

Fiche technique de déploiement

Pour le déploiement d'un seul nœud

Utilisez la fiche suivante pour rassembler les informations requises pour le déploiement initial des outils ONTAP pour VMware vSphere : pour le déploiement initial des outils ONTAP pour VMware vSphere :

Conditions requises	Votre valeur
Adresse IP de l'application ONTAP Tools	
Adresse IP d'interconnexion de nœud pour la communication entre nœuds	
Nom d'hôte DNS du premier nœud	

Conditions requises	Votre valeur
Serveur DNS principal	
Serveur DNS secondaire	
Domaine de recherche DNS	
Adresse IPv4 du nœud principal	
Masque de sous-réseau de l'adresse IPv4	
Passerelle par défaut pour l'adresse IPv4	
Adresse IPv6 (facultatif)	
Longueur du préfixe IPv6 (facultatif)	
Passerelle pour l'adresse IPv6 (facultatif)	

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

Pour les déploiements haute disponibilité (HA)

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

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

Configuration du pare-feu réseau

Ouvrez les ports requis pour les adresses IP de votre pare-feu réseau. Les outils ONTAP doivent pouvoir atteindre cette LIF sur le port 443. Reportez-vous "Configuration requise pour les ports"à pour connaître les dernières mises à jour.

Déployez les outils ONTAP pour VMware vSphere

Les outils ONTAP pour l'appliance VMware vSphere sont déployés sous forme de nœud unique de petite taille avec des services de base pour prendre en charge les datastores NFS et VMFS.

Avant de commencer

Une bibliothèque de contenu dans VMware est un objet conteneur qui stocke les modèles de machine virtuelle, les modèles vApp et d'autres types de fichiers. Le déploiement avec la bibliothèque de contenu vous offre une expérience transparente car il ne dépend pas de la connectivité réseau.

Vous devez stocker la bibliothèque de contenu sur un datastore partagé 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 en configuration haute disponibilité. Ne supprimez pas le modèle de bibliothèque de contenu après le déploiement.

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

Si vous ne disposez pas d'une bibliothèque de contenu, procédez comme suit pour en créer une :

Créer une bibliothèque de contenu dans vous prévoyez d'utiliser uniquement un déploiement à un seul nœud, la création d'une bibliothèque de contenu n'est pas nécessaire.

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

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

Avant de procéder au déploiement, définissez le DRS (Distributed Resource Scheduler) du cluster sur l'inventaire sur « conservateur ». Cela permet de s'assurer que les machines virtuelles ne sont pas migrées lors de l'installation.

Les outils ONTAP pour VMware vSphere sont initialement déployés sous forme de configuration non HA. Pour évoluer vers le déploiement haute disponibilité, vous devez activer le plug-in CPU hot plug et mémoire hot plug. 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 `.zip` fichier contenant les binaires (*.ova*) et les certificats signés pour les outils ONTAP pour 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 où vous avez l'intention de déployer l'OVA.

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

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

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

5. Dans le champ **Sélectionner un nom et un dossier**, entrez le nom de la machine virtuelle et choisissez son emplacement.
   - Si vous utilisez la version de vCenter Server 8.0.3, sélectionnez l'option **Personnaliser le matériel de cette machine virtuelle**, qui activera une étape supplémentaire appelée **Personnaliser le matériel** avant de passer à la fenêtre **prêt à terminer**.
   - Si vous utilisez la version de vCenter Server 7.0.3, suivez les étapes de la section **Qu'est-ce qui suit ?** à la fin du déploiement.
6. Sélectionnez une ressource d'ordinateur et sélectionnez **Suivant**. Si vous le souhaitez, cochez la case **mettre automatiquement sous tension la machine virtuelle déployée**.
7. Passez en revue les détails du modèle et sélectionnez **Suivant**.
8. Lisez et acceptez le contrat de licence et sélectionnez **Suivant**.
9. Sélectionnez le stockage pour la configuration et le format du disque, puis sélectionnez **Suivant**.
10. Sélectionnez le réseau de destination pour chaque réseau source et sélectionnez **Suivant**.
11. Dans la fenêtre **Personnaliser le modèle**, remplissez les champs requis et sélectionnez **Suivant**.
    - Les informations sont validées lors de l'installation. En cas de divergence, un message d'erreur s'affiche sur la console Web et vous êtes invité à le corriger.
    - Les noms d'hôte doivent comporter des lettres (A-Z, a-z), des chiffres (0-9) et des tirets (-). Pour configurer la double pile, spécifiez le nom d'hôte mappé sur l'adresse IPv6.

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

12. Lorsque vous utilisez la version de vCenter Server 8.0.3, dans la fenêtre **Personnaliser le matériel**, activez les options **CPU hot add** et **Memory hot plug** pour permettre la fonctionnalité HA.
13. Consultez les détails dans la fenêtre **prêt à terminer**, sélectionnez **Terminer**.

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

14. Mettez le serveur virtuel sous tension une fois la tâche terminée.

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

Si le formulaire OVF contient des incohérences, une boîte de dialogue vous invite à prendre des mesures correctives. Utilisez le bouton Tab pour naviguer, apporter les modifications nécessaires et sélectionner « OK. Vous avez trois tentatives pour résoudre les problèmes. Si les problèmes persistent après trois tentatives, le processus d'installation s'arrête et il est conseillé de réessayer l'installation sur une nouvelle machine virtuelle.

Et la suite ?

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

1. Connectez-vous au client vCenter
2. Accédez aux outils ONTAP pour la machine virtuelle VMware vSphere sous **inventaires** et sélectionnez l'option **Modifier les paramètres**.
3. Sous les options **CPU**, cochez la case **Activer l'ajout à chaud de CPU**
4. Sous les options **Memory**, cochez la case **Enable** par rapport à **Memory hot plug**.

Codes d'erreur de déploiement

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

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

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

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

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

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

Code d'erreur de déploiement	Workflow	Résolution
050	Échec de la génération de la clé SSH	Redémarrez la machine virtuelle (VM) principale.

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

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

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

Configuration des outils ONTAP pour VMware vSphere

Ajouter des instances vCenter Server

Ajoutez des instances de vCenter Server aux outils ONTAP pour VMware vSphere pour configurer, gérer et protéger vos datastores virtuels dans votre environnement vCenter Server.

À propos de cette tâche

Grâce à l'intégration à vCenter, les outils ONTAP vous permettent d'effectuer des tâches de stockage telles que le provisionnement, les copies Snapshot et la protection des données directement depuis le client vSphere. Vous n'avez plus besoin de passer à des consoles de gestion du stockage distinctes.

Étapes

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

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

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

Enregistrez le fournisseur VASA avec une instance vCenter Server

Vous pouvez enregistrer le fournisseur VASA dans une instance de serveur vCenter à l'aide des outils ONTAP pour VMware vSphere. La section Paramètres du fournisseur VASA affiche l'état d'enregistrement du fournisseur VASA pour le serveur vCenter sélectionné.

Étapes

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Sélectionnez **raccourcis** > **Outils NetApp ONTAP** dans la section modules externes.
3. Sélectionnez **Paramètres** > **VASA Paramètres fournisseur**. L'état d'enregistrement du fournisseur VASA s'affiche comme non enregistré.
4. Sélectionnez le bouton **Register** pour enregistrer le fournisseur VASA.

5. Entrez un nom pour le fournisseur VASA et fournissez les informations d'identification de l'utilisateur de l'application VMware vSphere pour les outils ONTAP, puis sélectionnez **Register**.
6. Une fois l'enregistrement et l'actualisation de la page réussis, l'état, le nom et la version du fournisseur VASA enregistré s'affichent. Après l'enregistrement, l'action de désinscription est activée.

Après la fin

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

Étapes

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

Installez le plug-in NFS VAAI

Le plug-in NFS vStorage API for Array Integration (NFS VAAI) est un composant logiciel qui intègre les baies de stockage VMware vSphere et NFS. Installez le plug-in NFS VAAI à l'aide des outils ONTAP pour VMware vSphere afin de tirer parti des fonctionnalités avancées de votre baie de stockage NFS et de 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" package d'installation.
- Assurez-vous que vous disposez du correctif ou des versions ultérieures de l'hôte ESXi 7.0U3 et de ONTAP 9.14.1 ou versions ultérieures.
- Monter un datastore NFS.
- Définissez les valeurs des paramètres de l'hôte DataMover.HardwareAcceleratedMove, DataMover.HardwareAcceleratedInit et VMFS3.HardwareAcceleratedLoking sur "1". Pour définir automatiquement ces valeurs, appliquez les paramètres recommandés de l'hôte EXSi. Reportez-vous à la "Configurer les paramètres de chemins d'accès multiples et de délai d'attente du serveur ESXi".
- Activez l'option vstorage sur la machine virtuelle de stockage (SVM) en utilisant la commande vserver nfs modify -vserver_name -vstorage Enabled.
- Assurez-vous de disposer des dernières versions de correctifs de vSphere 7.0U3.
- VSphere 8.x est pris en charge par le plug-in NetApp NFS VAAI 2.0.1 (build 16).

Étapes

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Sélectionnez **raccourcis** > **Outils NetApp ONTAP** dans la section modules externes.
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, cliquez sur le bouton **Upload**.
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 tâches récentes du client Web vSphere.

7. Vous devez redémarrer manuellement l'hôte ESXi une fois l'installation terminée.

   Lorsque l'administrateur VMware redémarre l'hôte VMware ESXi, les outils ONTAP pour VMware vSphere détectent et active automatiquement le plug-in NFS VAAI.

Et la suite ?

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

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

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

Informations associées

"Prise en charge de VMware vStorage over NFS"

"Activer ou désactiver NFSv4.0"

"Prise en charge de ONTAP pour NFSv4.2"

Configurer les paramètres de l'hôte ESXi

La configuration des paramètres de chemins d'accès multiples et de temporisation du serveur ESXi garantit la haute disponibilité et l'intégrité des données en permettant un basculement transparent vers un chemin de stockage de sauvegarde en cas de défaillance d'un chemin principal.

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

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

À propos de cette tâche

Selon votre configuration et la charge du système, ce processus peut prendre un certain temps. La progression de la tâche s'affiche dans le panneau tâches récentes.

Étapes

1. Sur la page d'accueil du client Web VMware vSphere, sélectionnez **hosts and clusters**.
2. Cliquez avec le bouton droit de la souris sur un hôte et sélectionnez **NetApp ONTAP Tools** > **Update host data**.
3. Sur la page des raccourcis du client Web VMware vSphere, sélectionnez **NetApp ONTAP Tools** dans la section des plug-ins.
4. Accédez à la carte **ESXi Host Compliance** 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.
8. Dans le volet récapitulatif, vérifiez les valeurs et sélectionnez **Terminer**. Vous pouvez suivre la progression dans le panneau des tâches récentes.

Définissez les valeurs de l'hôte ESXi

À l'aide des outils ONTAP pour VMware vSphere, vous pouvez définir des délais d'expiration et d'autres valeurs sur les hôtes VMware ESXi afin de garantir des performances optimales et un basculement réussi. Les outils ONTAP pour les ensembles VMware vSphere sont basés sur des tests NetApp internes.

Vous pouvez définir les valeurs suivantes sur un hôte ESXi :

Paramètres de l'adaptateur HBA/CNA

Définit les paramètres de délai d'expiration de HBA recommandés pour les systèmes de stockage NetApp.

Paramètres	Définir cette valeur sur…
Disk.QFullSampleSize	32 pour toutes les configurations. La définition de cette valeur permet d'éviter les erreurs d'E/S.
Disk.QFullThreshold	8 pour toutes les configurations. La définition de cette valeur permet d'éviter les erreurs d'E/S.
Délais d'expiration de la carte HBA FC Emulex	Valeur par défaut.
Délais de connexion HBA FC QLogic	Valeur par défaut.

Paramètres MPIO

Les paramètres MPIO définissent les chemins de prédilection pour les systèmes de stockage NetApp. Ils déterminent quels 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 un seul datastore LUN, pensez à modifier le paramètre d'équilibrage de charge de la règle de sélection de chemin (PSP) de Round Robin (VMW_PSP_RR) du paramètre d'IOPS par défaut de 1000 à une valeur de 1.

Paramètres NFS

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

Configurer les rôles et privilèges des utilisateurs ONTAP

Vous pouvez configurer de nouveaux rôles et privilèges utilisateur pour la gestion des systèmes back-end de stockage à l'aide du fichier JSON fourni avec les outils ONTAP pour VMware vSphere et ONTAP System Manager.

Avant de commencer

- Vous devez avoir téléchargé le fichier de privilèges ONTAP depuis les outils ONTAP pour VMware vSphere à l'aide de *https://<loadbalancerIP>:8443/Virtualization/user-Privileges/Users_roles.zip*.
- Vous devez avoir téléchargé le fichier privilèges ONTAP à partir des outils ONTAP à l'aide de `https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip`.

> La création d'utilisateurs s'effectue au niveau du cluster ou directement au niveau des SVM. Vous pouvez également créer des utilisateurs sans utiliser le fichier user_roles.json et, si c'est le cas, vous devez disposer d'un ensemble minimal de privilèges au niveau du SVM.

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

Étapes

1. Extrayez le fichier téléchargé *https://<loadbalancerIP>:8443/Virtualization/user-Privileges/Users_roles.zip*.
2. Accédez à ONTAP System Manager à l'aide de l'adresse IP de gestion du cluster.
3. Connectez-vous au cluster avec admin Privileges. Pour configurer un utilisateur, effectuez les opérations suivantes :
   a. Pour configurer l'utilisateur des outils ONTAP du cluster, sélectionnez **Cluster** > **Paramètres** > **utilisateurs et rôles**.
   b. Pour configurer l'utilisateur des outils ONTAP du SVM, sélectionner **SVM de stockage** > **Paramètres** > volet **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 de privilèges ONTAP.

Le champ produit est renseigné automatiquement.

f. Sélectionnez la fonctionnalité requise dans le menu déroulant Product Capability.

Le champ **role** est renseigné automatiquement en fonction de la fonctionnalité de produit sélectionnée.

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

h. Sélectionnez le rôle Privileges (découverte, création de stockage, modification du stockage, destruction du stockage, NAS/SAN) requis pour l'utilisateur, puis sélectionnez **Ajouter**.

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

Exigences de mappage des agrégats du SVM

Pour utiliser les identifiants utilisateur SVM pour provisionner les datastores, les outils ONTAP internes pour VMware vSphere créent des volumes sur l'agrégat spécifié dans l'API POST des datastores. La ONTAP ne permet pas la création de volumes sur des agrégats non mappés sur un SVM à l'aide des informations d'identification utilisateur du SVM. Pour résoudre ce problème, vous devez mapper les SVM avec les agrégats à l'aide de l'API REST ou de l'interface de ligne de commandes de ONTAP comme décrit dans cette section.

API REST :

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

Interface de ligne de commande ONTAP :

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

Créez manuellement un utilisateur et un rôle ONTAP

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 admin Privileges.
   a. Pour configurer les rôles des outils ONTAP du cluster, sélectionnez **Cluster** > **Paramètres** > **utilisateurs et rôles**.
   b. Pour configurer les rôles des outils ONTAP du SVM du cluster, sélectionner le volet **SVM de stockage** > **Paramètres** > **utilisateurs et rôles**
3. Créer des rôles :
   a. Sélectionnez **Ajouter** dans la table **rôles**.

b. Entrez les détails **nom de rôle** et **attributs de rôle**.

   Ajoutez le **REST API Path** et l'accès correspondant dans le menu déroulant.

c. Ajoutez toutes les API nécessaires et enregistrez les modifications.

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

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

Les privilèges minimaux requis pour l'utilisateur de cluster avec périmètre global non-admin créé sans utiliser le fichier JSON d'utilisateurs sont répertoriés dans cette section. Si un cluster est ajouté au périmètre local, il est recommandé d'utiliser le fichier JSON pour créer les utilisateurs, car les outils ONTAP pour VMware vSphere requièrent bien plus que les privilèges de lecture pour le provisionnement sur ONTAP.

À l'aide d'API :

API	Niveau d'accès	Utilisé pour
/api/cluster	Lecture seule	Découverte de la configuration du cluster
/api/cluster/licences/licences	Lecture seule	Contrôle de licence 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/stockage/agrégats	Lecture seule	Vérification de l'espace de l'agrégat lors du provisionnement des datastores/volumes
/api/stockage/cluster	Lecture seule	Pour obtenir les données d'espace et d'efficacité au niveau du cluster
/api/stockage/disques	Lecture seule	Pour obtenir les disques associés dans un agrégat
/api/stockage/qos/politiques	Lire/Créer/Modifier	Gestion de la QoS et de la stratégie des machines virtuelles
/api/svm/svm	Lecture seule	Pour obtenir la configuration SVM au cas où le Cluster est ajouté localement.

/api/network/ip/interfaces	Lecture seule	Add Storage back-end : pour identifier le périmètre de la LIF de gestion, il s'agit de Cluster/SVM

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

Vous avez besoin de la découverte, de la création, de la modification et de la destruction de Privileges pour effectuer des opérations de CORRECTIFS et une restauration automatique en cas de défaillance sur les datastores. Le manque de ces Privileges ensemble entraîne des interruptions de flux de travail et des problèmes de nettoyage.

Création des outils ONTAP pour VMware vSphere utilisateur basé sur l'API ONTAP avec détection, création de stockage, modification de stockage, destruction de stockage Privileges permet de lancer des découvertes et de gérer les flux de production des outils ONTAP.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
services/name-mappings -access readonly

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Pour créer un utilisateur SVM scoped avec tout le Privileges, lancer 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>
```

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

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

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

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

Exemple :

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

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

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

Exemple :

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

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

Si l'utilisateur des outils ONTAP pour VMware vSphere 10.1 est un utilisateur dont la portée est définie en cluster et créé à l'aide du fichier json, exécutez les commandes suivantes sur l'interface de ligne de commande ONTAP en utilisant l'utilisateur admin pour effectuer la mise à niveau vers la version 10.3.

Pour les fonctionnalités du produit :

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

Cluster Privileges :

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

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

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

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

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

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

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

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

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

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

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

Si l'utilisateur disposant des outils ONTAP pour VMware vSphere 10.1 est un utilisateur avec périmètre SVM créé à l'aide du fichier json, exécuter les commandes suivantes sur l'interface de ligne de commande ONTAP en utilisant l'utilisateur admin pour effectuer la mise à niveau vers la version 10.3.

SVM Privileges :

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

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

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

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

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

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

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

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

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

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

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

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
```

Ajout d'un système back-end

L'ajout d'un système back-end de stockage vous permet d'intégrer un cluster ONTAP.

À propos de cette tâche

Pour ajouter un système back-end de stockage à un cluster dont le périmètre est global dans une architecture mutualisée, ajoutez le système back-end de stockage à l'aide du gestionnaire d'outils ONTAP. Après avoir ajouté le système back-end de stockage au cluster global, vous devez associer le cluster aux locataires vCenter souhaités. Le locataire vCenter doit intégrer les machines virtuelles de stockage (SVM) souhaitées. Cela permet à un utilisateur SVM de provisionner le datastore vVols. Vous pouvez ajouter du stockage dans vCenter à l'aide de la SVM.

Pour ajouter un système back-end de stockage à un cluster dont le périmètre est local, ajoutez vos systèmes ONTAP directement à l'aide du plug-in ONTAP Tools sur le serveur vCenter.

Utilisation du Gestionnaire d'outils ONTAP

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

Étapes

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

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

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

Lorsque vous ajoutez un back-end de stockage via l'interface utilisateur client vSphere, le datastore vVols ne prend pas en charge l'ajout direct d'un utilisateur SVM.

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

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

Et la suite ?

La liste est actualisée et le système back-end de stockage ajouté apparaît dans la liste.

Associer un back-end de stockage à une instance vCenter Server

Associez un système back-end de stockage à vCenter Server pour créer un mappage global entre le système back-end de stockage et l'instance vCenter Server intégrée.

Étapes

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

3. Sélectionnez vCenter dans la barre latérale.
4. Sélectionnez les ellipses verticales par rapport à l'instance vCenter Server que vous souhaitez associer aux systèmes back-end de stockage.
5. Sélectionnez le back-end de stockage dans la liste déroulante pour associer l'instance vCenter Server au back-end de stockage requis.

Configurer l'accès au réseau

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

Étapes

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

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

4. Sélectionnez **Enregistrer**.

Créer un datastore

Lorsque vous créez un datastore au niveau du cluster hôte, le datastore est créé et monté sur tous les hôtes de destination. Vous pouvez voir cette option uniquement si vous avez le Privileges requis.

- Vous pouvez uniquement créer des datastores VMFS sur un cluster protégé. Lorsque vous ajoutez un datastore VMFS à un cluster protégé, le datastore est automatiquement protégé.
- Vous ne pouvez pas créer de datastore sur un data Center qui possède un ou plusieurs clusters hôtes protégés.
- Vous ne pouvez pas créer de datastore sur l'hôte si le cluster hôte parent est protégé par une relation de type de stratégie Automated Failover Duplex (configuration uniforme/non uniforme).
- Vous pouvez créer un datastore VMFS sur un hôte, uniquement s'il possède une relation asynchrone.

Créer un datastore vVols

Vous pouvez créer un datastore vVols avec de nouveaux volumes ou des volumes existants. Vous ne pouvez pas créer de datastore vVols avec la combinaison de volumes existants et nouveaux.

Cette option permet de vérifier que les agrégats racine ne sont pas mappés sur un SVM.

Depuis les outils ONTAP pour VMware vSphere 10.3, vous pouvez créer un datastore vVols à l'aide du type de stockage ONTAP ASA r2. Le datastore vVols créé sur les systèmes ASA r2 est doté d'un gain d'espace sous la forme thin.vVol. Vasa Provider crée un conteneur et les terminaux de protocole souhaités lors du workflow de création de datastore vVol. Ce conteneur n'aura pas de volumes de sauvegarde.

Avant de commencer

- Assurez-vous que VASA Provider est enregistré avec le vCenter sélectionné.
- Pour l'utilisateur SVM du système de stockage ASA r2, le SVM doit être mappé sur l'agrégat

Étapes

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Cliquez avec le bouton droit de la souris sur un système hôte, un cluster hôte ou un centre de données et sélectionnez **NetApp ONTAP Tools** > **Create datastore**.
3. Dans le volet **Type**, sélectionnez vVols dans **Type de datastore**.
4. Dans le volet **Nom et Protocole**, indiquez **nom du datastore** et **Protocole**.

   Le type de stockage ASA r2 prend uniquement en charge les protocoles iSCSI et FC pour les vVols.

5. Dans le volet **Storage**, sélectionnez la machine virtuelle de stockage où vous souhaitez créer le datastore. Dans la section **Options avancées**, sélectionnez une règle d'export personnalisée (pour le protocole NFS) ou un nom de groupe initiateur personnalisé (pour le protocole iSCSI amd FC), le cas échéant.

   Dans le SVM de type de stockage ASA r2, les unités de stockage (LUN/namespace) ne sont pas créées, car le datastore n'est qu'un conteneur logique.

6. Dans le volet **attributs de stockage**, vous pouvez créer de nouveaux volumes ou utiliser les volumes existants. Lors de la création d'un volume, vous pouvez activer la QoS sur le datastore. Cette étape ne s'applique pas aux datastores vVols utilisant un stockage ONTAP de type ASA r2 car le datastore vVol ne possède pas de volumes de sauvegarde. Par défaut, un volume est créé sur chaque demande de création de LUN.
7. Vérifiez votre sélection dans le volet **Résumé** et sélectionnez **Terminer**. Le datastore vVols est créé et monté sur tous les hôtes.

Créer un datastore NFS

Un datastore VMware Network File System (NFS) utilise le protocole NFS pour connecter les hôtes ESXi à un périphérique de stockage partagé via un réseau. Les datastores NFS sont généralement utilisés dans les environnements VMware vSphere et offrent plusieurs avantages, tels que la simplicité et la flexibilité.

Étapes

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Cliquez avec le bouton droit de la souris sur un système hôte, un cluster hôte ou un centre de données et sélectionnez **NetApp ONTAP Tools** > **Create datastore**.
3. Dans le volet **Type**, sélectionnez NFS dans **Type de datastore**.
4. Dans le volet **Nom et protocole**, entrez le nom, la taille et les informations de protocole du datastore. Dans les options avancées, sélectionnez **datastore cluster** et **Kerberos Authentication**.

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

5. Dans le volet **Storage**, sélectionnez **Platform** et **Storage VM**. Vous pouvez sélectionner **Custom Export Policy** dans la section **Advanced option**.
   - **Le bouton bascule asymétrique** n'est visible que si la performance ou la capacité est sélectionnée dans la liste déroulante plate-forme.
   - **Toute option** dans le menu déroulant de la plate-forme vous permet de voir tous les SVM faisant partie de vCenter indépendamment de la plate-forme ou de l'indicateur asymétrique.
6. Dans le volet **attributs de stockage**, sélectionnez l'agrégat pour la création du volume. Dans les options avancées, choisissez **Réserve d'espace** et **Activer QoS** selon les besoins.
7. Vérifiez les sélections dans le volet **Résumé** et sélectionnez **Terminer**.

Le datastore NFS est créé et monté sur tous les hôtes.

Créer un datastore VMFS

VMFS (Virtual machine File System) est un système de fichiers en cluster spécialement conçu pour le stockage de fichiers de machines virtuelles dans des environnements VMware vSphere. Elle permet à plusieurs hôtes ESXi d'accéder simultanément aux mêmes fichiers de machine virtuelle, ce qui permet d'utiliser des fonctionnalités telles que vMotion et haute disponibilité.

Avant de commencer

Vérifier les éléments suivants avant de continuer :

- Pour chaque protocole côté stockage ONTAP, les services et LIF respectifs doivent être activés.
- Pour l'utilisateur SVM du système de stockage ASA r2, le SVM doit être mappé sur l'agrégat
- Si vous utilisez le protocole NVMe/TCP, effectuez les étapes suivantes pour configurer l'hôte ESXi :
  a. Examinez le "Guide de compatibilité VMware"

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

  b. Vérifiez si le fournisseur de la carte d'interface réseau (NIC) prend en charge la carte réseau ESXi avec le protocole NVMe/TCP.
  c. Configurez la carte réseau ESXi pour NVMe/TCP conformément aux spécifications du fournisseur de la carte réseau.
  d. Si vous utilisez VMware vSphere 7, suivez les instructions qui s'affichent sur le site VMware "Configurez la liaison VMkernel pour l'adaptateur NVMe over TCP" pour configurer la liaison du port NVMe/TCP. Si vous utilisez VMware vSphere 8, suivez "Configuration de NVMe over TCP

sur ESXi"la procédure pour configurer la liaison du port NVMe/TCP.

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

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

- Si vous utilisez le protocole NVME/FC, effectuez les étapes suivantes pour configurer l'hôte ESXi :

a. Activez NVMe over Fabrics (NVMe-of) sur vos hôtes ESXi.

b. Segmentation SCSI complète.

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

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

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

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

Étapes

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Cliquez avec le bouton droit de la souris sur un système hôte, un cluster hôte ou un centre de données et sélectionnez **NetApp ONTAP Tools** > **Create datastore**.
3. Sélectionnez le type de datastore VMFS.
4. Entrez le nom, la taille et les informations de protocole du datastore dans le volet **Nom et Protocole**. Si vous choisissez d'ajouter le nouveau datastore à un cluster de datastore VMFS existant, sélectionnez le sélecteur de cluster datastore sous **Advanced Options**.
5. Sélectionnez Storage VM dans le volet **Storage**. Indiquez le **Nom du groupe initiateur** personnalisé dans la section **Options avancées** du volet (facultatif). Vous pouvez choisir un groupe initiateur existant pour le datastore ou créer un nouveau groupe initiateur avec un nom personnalisé.

   Lorsque le protocole est sélectionné comme NVMe/FC ou NVMe/TCP, un nouveau sous-système d'espace de noms est créé et utilisé pour le mappage de l'espace de noms. Par défaut, le sous-système d'espace de noms est créé à l'aide du nom généré automatiquement, y compris le nom du datastore. Vous pouvez renommer le sous-système d'espace de noms dans le champ **custom namespace subsystem name** des options avancées du volet **Storage**.

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

   a. Sélectionnez **aggregate** dans le menu déroulant.

   Pour les systèmes de stockage ASA r2, l'option **aggregate** n'est pas requise, car le stockage ASA r2 est désagrégée. Lorsque vous choisissez un SVM de type ASA r2, la page des attributs de stockage affiche les options d'activation de la QoS.

b. Selon le protocole sélectionné, une unité de stockage (LUN/namespace) est créée avec une réserve d'espace de type Thin.

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

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

Pour la création de datastores VMFS avec le protocole NVMe/FC ou NVMe/TCP, vous ne pouvez pas utiliser le volume existant, vous devez créer un nouveau volume.

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

Si vous créez le datastore sur un cluster protégé, un message en lecture seule s'affiche : « le datastore est en cours de montage sur un cluster protégé ». Le datastore VMFS est créé et monté sur tous les hôtes.

Protection des datastores et des machines virtuelles

Protégez à l'aide de la protection de cluster hôte

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

Avant de commencer

Assurez-vous que les conditions préalables suivantes sont remplies :

- Le cluster hôte ne dispose que de datastores d'un SVM.
- Le datastore monté sur le cluster hôte ne doit pas être monté sur un hôte extérieur au cluster.
- Tous les datastores montés sur le cluster hôte doivent être des datastores VMFS avec protocole iSCSI/FC. Les datastores vVols, NFS ou VMFS avec protocoles NVMe/FC et NVMe/TCP ne sont pas pris en charge.
- Les FlexVol/LUN formant des datastores montés sur le cluster hôte ne doivent pas faire partie d'un groupe de cohérence existant.
- Les FlexVol/LUN formant des datastores montés sur le cluster hôte ne doivent pas faire partie d'une relation SnapMirror existante.
- Le cluster hôte doit comporter au moins un datastore.

Étapes

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Cliquez avec le bouton droit de la souris sur un cluster hôte et sélectionnez **NetApp ONTAP Tools** > **Protect Cluster**.
3. Dans la fenêtre protéger le cluster, le type de datastore et les détails de la machine virtuelle de stockage source sont renseignés automatiquement. Sélectionnez le lien datastores pour afficher les datastores protégés.
4. Entrez le **nom du groupe de cohérence**.
5. Sélectionnez **Ajouter une relation**.
6. Dans la fenêtre **Ajouter une relation SnapMirror**, sélectionnez **VM de stockage cible** et le type **Stratégie**.

   Le type de règle peut être asynchrone ou automatique FailOverDuplex.

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

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

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

8. Sélectionnez **Ajouter**.
9. Dans la fenêtre **Protect cluster**, vous ne pouvez pas modifier le cluster protégé pendant l'opération de création. Vous pouvez supprimer et ajouter une protection à nouveau. Pendant l'opération de modification de la protection du cluster hôte, l'option d'édition est disponible. Vous pouvez modifier ou supprimer les relations à l'aide des options du menu points de suspension.
10. Sélectionnez le bouton **protéger**.

    Une tâche vCenter est créée avec les détails de l'ID du travail et sa progression est affichée dans le panneau 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 **NetApp ONTAP Tools** > **protection** > **Host cluster relations**.

Protégez à l'aide de la protection SRA

Activez SRA pour protéger les datastores

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

Avant de commencer

- Vous devez avoir configuré votre instance vCenter Server et votre hôte ESXi.
- Vous devez avoir déployé des outils ONTAP pour VMware vSphere.
- Vous devez avoir téléchargé le `.tar.gz` fichier de l'adaptateur SRA à partir du "Site de support NetApp".
- Les clusters ONTAP source et destination doivent avoir la même planification SnapMirror personnalisée que celle créée avant d'exécuter les workflows SRA.

Étapes

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

Configurez 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.

Configurez SRA pour les environnements SAN

Avant de commencer

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

- Restauration de site en direct VMware

La documentation relative à l'installation de VMware Live site Recovery se trouve 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 du site protégé.
2. Vérifiez que LES LUN sont dans des igroups qui ont `ostype` Option définie sur *VMware* sur le système de stockage principal.
3. Vérifier que les hôtes ESXi sur le site de reprise 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 en vérifiant que les hôtes ESXi disposent de LUN locales connectées au SVM ou au `iscsi show initiators` Commande sur les SVM.
   Vérifiez l'accès aux LUN mappées sur l'hôte ESXi pour vérifier la connectivité iSCSI.

Configurez SRA pour les environnements NAS

Avant de commencer

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

- Restauration de site en direct VMware

  La documentation relative à 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 sur le serveur SRA.

Étapes

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

Configurez SRA pour les environnements hautement évolutifs

Vous devez configurer les intervalles de délai d'expiration du stockage conformément aux

paramètres recommandés pour Storage Replication adapter (SRA) afin de garantir des performances optimales dans des environnements hautement évolutifs.

Paramètres du fournisseur de stockage

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

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

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

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

Paramètres de stockage

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

> L'intervalle de temporisation spécifié est la valeur maximale. Il n'est pas nécessaire d'attendre que le délai maximum soit atteint. La plupart des commandes se terminent dans l'intervalle maximal défini de temps d'attente.

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

Configurez SRA sur l'appliance VMware Live site Recovery

Une fois l'appliance VMware Live site Recovery déployée, vous devez configurer SRA sur l'appliance VMware Live site Recovery. La configuration réussie de SRA permet à l'appliance VMware Live site Recovery de communiquer avec SRA pour la gestion de la reprise après incident. Vous devez stocker les outils ONTAP pour les informations d'identification VMware vSphere (adresse IP) sur l'appliance VMware Live site Recovery pour permettre la communication entre l'appliance VMware Live site Recovery et SRA.

Avant de commencer

Vous devez avoir téléchargé le fichier *tar.gz* à partir de "Site de support NetApp".

À propos de cette tâche

La configuration de SRA sur l'appliance VMware Live site Recovery stocke les informations d'identification SRA sur l'appliance VMware Live site Recovery.

Étapes

1. Sur l'écran de l'appliance VMware Live site Recovery, sélectionnez **Storage Replication adapter** > **New adapter**.
2. Chargez le fichier *.tar.gz* dans VMware Live site Recovery.
3. Connectez-vous à l'aide d'un compte administrateur à l'appliance VMware Live site Recovery à l'aide de putty.
4. Basculer vers l'utilisateur root à l'aide de la commande : `su root`
5. Exécutez la commande `cd /var/log/vmware/srm` pour accéder au répertoire de journaux.
6. À l'emplacement du journal, entrez la commande pour obtenir l'ID docker utilisé par SRA : `docker ps -l`
7. Pour vous connecter à l'ID de conteneur, entrez la commande : `docker exec -it -u srm <container id> sh`
8. Configurer VMware Live site Recovery avec les outils ONTAP pour l'adresse IP et le mot de passe 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>'`

   Vous devez fournir la valeur du mot de passe entre guillemets pour vous assurer que le script Perl ne lit pas les caractères spéciaux du mot de passe comme délimiteur de l'entrée.

   Le nom d'utilisateur et le mot de passe de l'application sont définis lors du déploiement des outils ONTAP. Cette opération est nécessaire pour l'enregistrement du fournisseur VASA/SRA.

9. Relancez la recherche des adaptateurs pour vérifier que les détails sont mis à jour sur la page adaptateurs de réplication de stockage de VMware Live site Recovery.

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

Mettez à jour les informations d'identification SRA

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

Avant de commencer

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

Étapes

1. Exécutez les commandes suivantes pour supprimer le dossier de la machine de restauration de site direct VMware Outils ONTAP mis en cache nom d'utilisateur mot de passe :

   a. `sudo su <enter root password>`

b. `docker ps`

c. `docker exec -it <container_id> sh`

d. `cd conf/`

e. `rm -rf *`

2. Exécutez la commande Perl pour configurer SRA avec les nouvelles informations d'identification :

a. `cd ..`

b. `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>` Vous devez avoir un devis unique autour de la valeur du mot de passe.

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

Configuration des sites protégés et de reprise après incident

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

Configuration des groupes de protection

Avant de commencer

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

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

Étapes

1. Connectez-vous à vCenter Server, puis sélectionnez **site Recovery** > **protection Groups**.
2. Dans le volet **groupes de protection**, sélectionnez **Nouveau**.
3. Spécifiez un nom et une description pour le groupe de protection, Direction et sélectionnez **Suivant**.
4. Dans le champ **Type**, sélectionnez l'option de champ **Type…** en tant que groupes de datastores (réplication basée sur la baie) pour les datastores NFS et VMFS.
Le domaine de panne n'est rien d'autre que les SVM avec la réplication activée. Les SVM qui ont uniquement mis en œuvre le peering et qui ne présentent aucun problème sont affichés.
5. Dans l'onglet Replication Groups, sélectionnez la paire de matrices activée ou les groupes de réplication sur lesquels la machine virtuelle est configurée, puis sélectionnez **Next**.

Toutes les machines virtuelles du groupe de réplication sont ajoutées au groupe de protection.

6. Sélectionnez le plan de reprise existant ou créez un nouveau plan en sélectionnant **Ajouter au nouveau plan de reprise**.
7. Dans l'onglet prêt à terminer, vérifiez les détails du groupe de protection que vous avez créé, puis

sélectionnez **Terminer**.

Protection par paires et sites de reprise après incident

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

Avant de commencer

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

Étapes

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

Résultat

Les sites protégés et de restauration s'affichent dans la boîte de dialogue objets.

Configuration des ressources protégées et du site de reprise

Configurer les mappages du 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 afin de pouvoir mapper chaque ressource du site protégé à la ressource appropriée sur le site de reprise.

Vous devez effectuer les configurations de ressources suivantes :

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

Avant de commencer

Vous devez avoir connecté les sites protégés et de reprise.

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **site Recovery** > **sites**.
2. Sélectionnez votre site protégé et sélectionnez **gérer**.
3. Sélectionnez **mappages réseau** > **Nouveau** dans l'onglet gérer pour créer un nouveau mappage réseau.

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

Résultat

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

Configurer les mappages de dossiers

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

Avant de commencer

Vous devez avoir connecté les sites protégés et de reprise.

Étapes

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

Résultat

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

Configurer les mappages de ressources

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

Avant de commencer

Vous devez avoir connecté les sites protégés et de reprise.

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

Étapes

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

Résultat

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

Configurez les datastores à espace réservé

Vous devez configurer un datastore de marque de réservation pour qu'il garde un emplacement dans l'inventaire vCenter sur le site de reprise pour la machine virtuelle protégée (VM). Le datastore réservé n'a pas besoin d'être volumineux car les machines virtuelles de substitution sont petites et n'utilisent que quelques centaines de kilo-octets ou moins.

Avant de commencer

- Vous devez avoir connecté les sites protégés et de reprise.
- Vous devez 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 **Placeholder datastores** > **New** dans l'onglet gérer pour créer un nouveau datastore de marque de réservation.
4. Sélectionnez le datastore approprié et sélectionnez **OK**.

   Les datastores à espace réservé peuvent être locaux ou distants et ne doivent pas être répliqués.

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

Configurez SRA à l'aide du gestionnaire de baies

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

Avant de commencer

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

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

Étapes

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

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

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

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

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

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

   d. Si vous vous connectez à un cluster, entrez le nom du SVM dans le champ **SVM name**.

      Vous pouvez également laisser ce champ vide.

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

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

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

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

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

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

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

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

Vérification des systèmes de stockage répliqués

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

Avant de commencer

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

Étapes

1. Connectez-vous à votre serveur vCenter.
2. Accédez à **site Recovery** > **Array Based Replication**.
3. Sélectionnez la paire de matrices requise et vérifiez les détails correspondants.

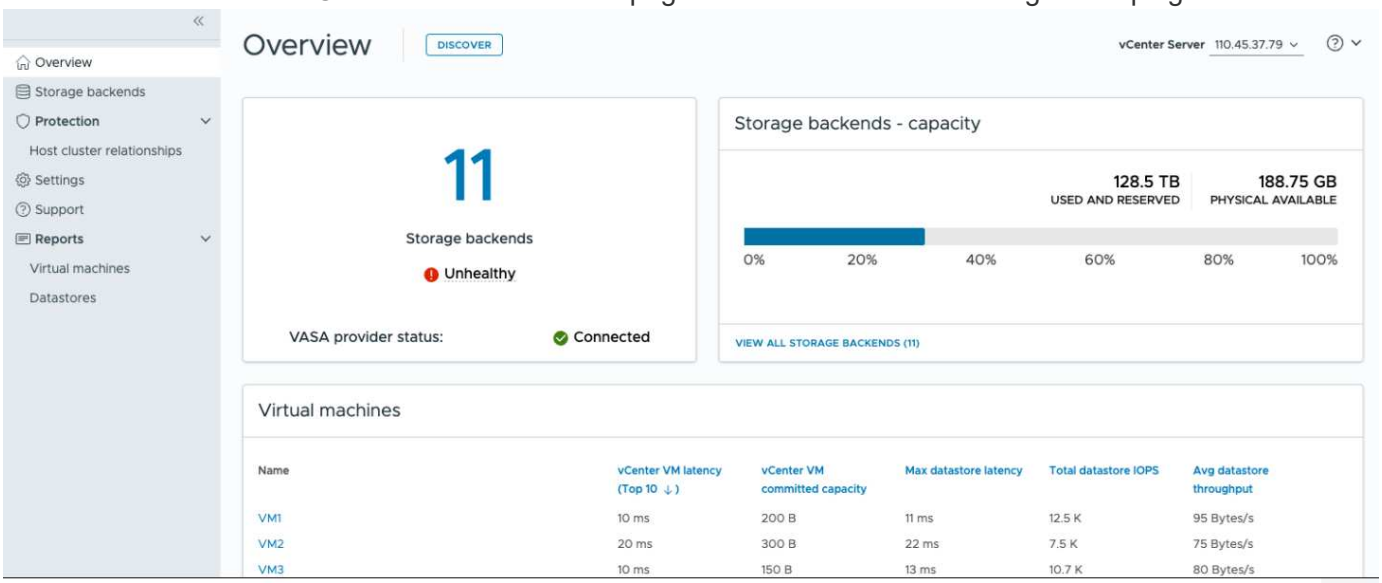
   Les systèmes de stockage doivent être découverts sur le site protégé et le site de reprise dont le statut est « activé ».

Gérez les outils ONTAP pour VMware vSphere

Présentation du tableau de bord des outils ONTAP pour VMware vSphere

Lorsque vous sélectionnez l'icône du plug-in ONTAP Tools for VMware vSphere dans la section des raccourcis du client vCenter, l'interface utilisateur accède à la page de présentation. Cette page fonctionne comme le tableau de bord qui fournit le résumé du plug-in ONTAP Tools for VMware vSphere.

Dans le cas de la configuration ELM (Enhanced Linked mode Setup), le menu déroulant de sélection de vCenter Server apparaît et vous pouvez sélectionner un serveur vCenter pour afficher les données qui lui sont pertinentes. Cette liste déroulante est disponible pour toutes les autres vues de liste du plug-in.
La sélection du serveur vCenter effectuée sur une page est conservée dans les onglets du plug-in.



À partir de la page de présentation, vous pouvez exécuter l'action **Discovery**. L'action de détection exécute la détection au niveau de vCenter pour détecter les éventuels systèmes back-end de stockage, hôtes, datastores, état/relations de protection récemment ajoutés ou mis à jour. Vous pouvez exécuter une découverte à la demande des entités sans avoir à attendre la découverte planifiée.

Le bouton action ne sera activé que si vous disposez du 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 tâches récentes.

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

Carte	Description

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

Interface utilisateur du Gestionnaire d’outils ONTAP

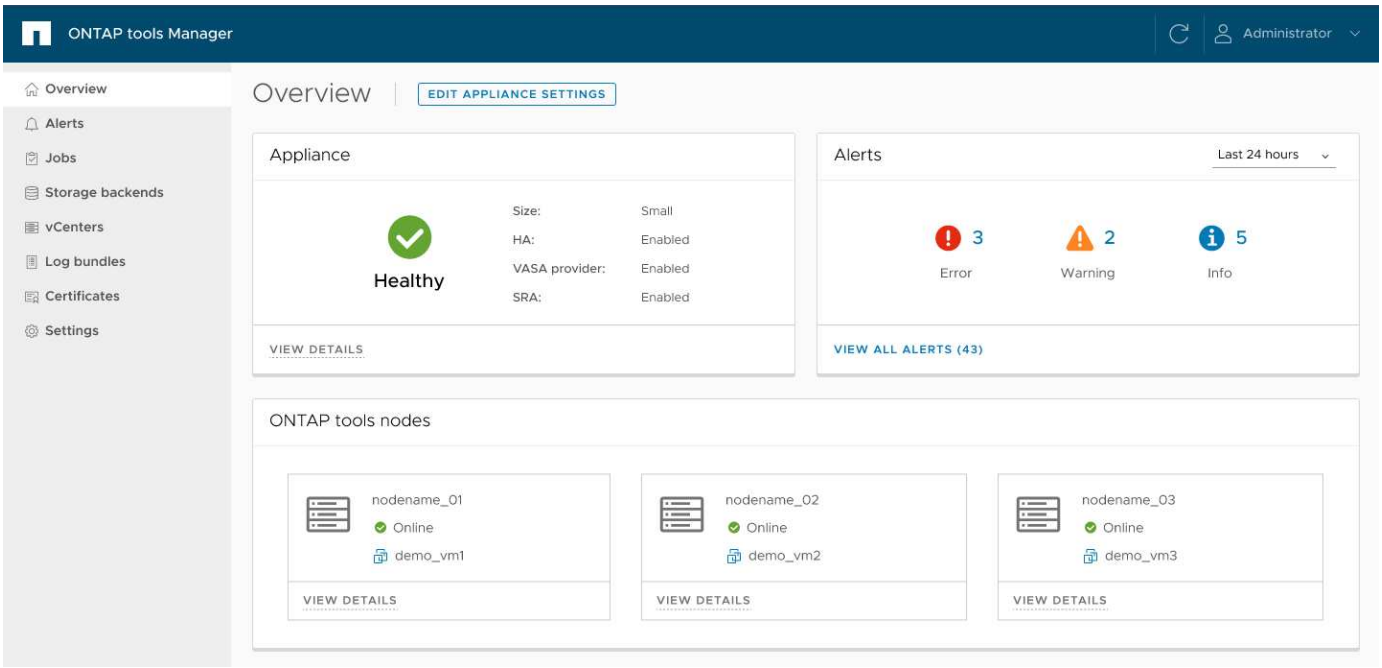
Les outils ONTAP pour VMware vSphere sont un système mutualisé capable de gérer plusieurs instances de vCenter Server. ONTAP Tools Manager offre davantage de contrôle aux outils ONTAP pour l’administrateur VMware vSphere sur les instances vCenter Server gérées et les systèmes back-end de stockage intégrés.

ONTAP Tools Manager vous aide à :

- Gestion des instances vCenter Server : permet d’ajouter et de gérer des instances vCenter Server aux outils ONTAP.
- Gestion du stockage back-end : ajoutez et gérez des clusters de stockage ONTAP aux outils ONTAP pour VMware vSphere et mappez-les vers des instances vCenter Server intégrées à l’échelle mondiale.
- Téléchargements de bundles de journaux : permet de collecter des fichiers journaux pour les outils ONTAP pour VMware vSphere.
- Gestion des certificats : remplacez le certificat auto-signé par un certificat AC personnalisé et renouvelez ou actualisez tous les certificats du fournisseur VASA et des outils ONTAP.
- Gestion des mots de passe : permet de 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/`-le à partir du navigateur et connectez-vous à l’aide des informations d’identification d’administrateur ONTAP Tools for VMware vSphere que vous avez fournies lors du déploiement.

La section Présentation du gestionnaire d’outils ONTAP vous aide à gérer la configuration des appliances, notamment la gestion des services, la montée en charge de la taille des nœuds et l’activation de la haute disponibilité. Vous pouvez également surveiller les informations globales des outils ONTAP liés au(x) nœud(s), telles que l’état, les détails du réseau et les alertes.



Carte	Description
Carte d'appareil	La carte de l'appliance indique l'état général de l'appliance ONTAP Tools. Il affiche les détails de la configuration de l'appliance et l'état des services activés. Pour plus d'informations sur l'appliance ONTAP Tools, cliquez sur le lien **Afficher les détails**. Lorsqu'un travail d'action de modification de paramètre d'appliance est en cours, le portlet de l'appliance affiche l'état et les détails du travail.
Carte d'alertes	La carte alertes répertorie les alertes des outils ONTAP par type, y compris les alertes de haute disponibilité au niveau du nœud. Vous pouvez afficher la liste des alertes en sélectionnant dans le texte de comptage (hyperlien). Le lien vous dirige vers la page d'affichage des alertes filtrée en fonction du type sélectionné.
Carte des nœuds des 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 relatives au réseau. Vous pouvez sélectionner sur **Afficher les détails** pour afficher les détails supplémentaires liés au nœud sélectionné. [REMARQUE] dans une configuration non HA, un seul nœud est affiché. En configuration haute disponibilité, trois nœuds sont illustrés.

Activez les outils ONTAP pour les services VMware vSphere

Gestionnaire pour activer des services tels que VASA Provider, importation de la configuration vVols et reprise après incident (SRA) à l'aide du gestionnaire d'outils ONTAP.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **Modifier les paramètres de l'appareil** dans la section Présentation.
4. Dans la section **Services**, vous pouvez activer des services facultatifs tels que VASA Provider, importer la configuration vVols et SRA (Disaster Recovery) selon vos besoins.

   Lors de la première activation des services, vous devez créer les informations d'identification du fournisseur VASA et SRA. Ils permettent d'enregistrer ou d'activer les services VASA Provider et SRA sur le serveur vCenter.

   Avant de désactiver les services optionnels, 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 active la migration des données vVols des outils ONTAP 9.x vers les outils ONTAP 10.3.

Modification des outils ONTAP pour la configuration de VMware vSphere

À l'aide du gestionnaire d'outils ONTAP faites évoluer verticalement les outils ONTAP de la configuration VMware vSphere pour augmenter le nombre de nœuds dans le déploiement ou modifier la configuration en configuration haute disponibilité (HA). Les outils ONTAP pour l'appliance VMware vSphere sont initialement déployés dans une configuration non HA à nœud unique.

Avant de commencer

- Assurez-vous que votre modèle OVA possède la même version OVA que le nœud 1. Le nœud 1 est le nœud par défaut sur lequel les outils ONTAP pour VMware vSphere OVA sont initialement déployés.
- Assurez-vous que l'ajout à chaud du processeur et la connexion à chaud de la mémoire sont activés.

Étapes

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

   Lorsque les outils ONTAP sont en configuration haute disponibilité, 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 outils ONTAP pour VMware vSphere, vous êtes uniquement autorisé à augmenter la taille des nœuds ; vous ne pouvez pas réduire la taille des nœuds. Dans une configuration non HA, seule une configuration de taille moyenne est prise en charge. Dans une configuration haute disponibilité, les moyennes et grandes configurations sont prises en charge.

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

   Une fois la configuration haute disponibilité activée, vous ne pouvez plus revenir à une configuration à nœud unique non HA.

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

   > La plupart des options d'entrée sont pré-remplies avec les détails réseau du nœud 1 pour faciliter le flux de travail. Toutefois, vous pouvez modifier les données d'entrée avant d'accéder à la page finale de l'assistant. Vous pouvez entrer 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 chaque fois que vous passez à la fenêtre suivante.

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

Et la suite ?

La page **vue d'ensemble** affiche l'état du déploiement. À l'aide de l'ID de tâche, vous pouvez également suivre l'état du travail de modification des paramètres de l'appliance depuis la vue travaux.

En cas d'échec du déploiement de la haute disponibilité et si l'état du nouveau nœud indique « Nouveau », supprimez la nouvelle machine virtuelle dans vCenter avant de réessayer d'activer l'opération de haute disponibilité.

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

Gérer les datastores

Montez des datastores NFS et VMFS

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

Description de la tâche

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

Étapes

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

Et la suite ?

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

Démontez les datastores NFS et VMFS

L'action de démontage du datastore démonte un datastore NFS ou VMFS des hôtes ESXi. L'action démonter le datastore est activée pour les datastores NFS et VMFS découverts ou gérés par les outils ONTAP pour VMware vSphere.

Étapes

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Cliquez avec le bouton droit de la souris sur un objet datastore NFS ou VMFS et sélectionnez **Unmount datastore**.

   Une boîte de dialogue s'ouvre et répertorie les hôtes ESXi sur lesquels le datastore est monté. Lorsque l'opération est effectuée sur un datastore protégé, un message d'avertissement s'affiche à l'écran.

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

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

4. Sélectionnez le bouton **Unmount**.

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

> Si le datastore protégé est démonté, le paramètre de protection de sortie peut entraîner une protection partielle. Reportez-vous "Modifier le cluster hôte protégé"à pour activer une protection complète.

Et la suite ?

Vous pouvez suivre la progression dans le panneau tâches récentes.

Montez un datastore vvols

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

Étapes

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

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

Redimensionner les datastores NFS et VMFS

Le redimensionnement d'un datastore vous permet d'augmenter le stockage des fichiers de votre machine virtuelle. Vous pouvez modifier la taille d'un datastore en fonction de l'évolution des exigences de votre infrastructure.

À propos de cette tâche

Vous pouvez uniquement augmenter la taille des datastores NFS et VMFS. Un volume FlexVol faisant partie d'un datastore NFS et VMFS ne peut pas se réduire en dessous de la taille existante, mais peut croître de 120 % au maximum.

Étapes

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

Développez le datastore vVols

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

L'opération étendre le datastore vVols ne s'applique pas au datastore vVols basé sur ASA r2.

Étapes

1. Sur la page d'accueil de vSphere client, sélectionnez **hosts and clusters**.
2. Dans le volet de navigation, sélectionnez le centre de données qui contient le datastore.
3. Cliquez avec le bouton droit de la souris sur le datastore et sélectionnez **NetApp ONTAP Tools** > **Add Storage to datastore**.
4. Dans la fenêtre **create ou Select volumes**, vous pouvez créer de nouveaux volumes ou choisir parmi les volumes existants. L'interface utilisateur est intuitive. Suivez les instructions de votre choix.
5. Dans la fenêtre **Résumé**, examinez les sélections et sélectionnez **développer**. Vous pouvez suivre la progression dans le panneau tâches récentes.

Réduire le datastore vVols

L'action Supprimer le datastore supprime le datastore lorsqu'il n'y a pas de vVols sur le datastore sélectionné.

L'opération de réduction du datastore vVols n'est pas prise en charge pour le datastore vVols basé sur ASA r2.

Étapes

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

   L'option de sélection du volume sur lequel réside les vVols est désactivée.

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

Supprimer les datastores

L'action Supprimer le stockage du datastore est prise en charge sur tous les outils ONTAP pour les datastores VMware vSphere découverts ou gérés vVols du serveur vCenter. Cette action permet de supprimer des volumes du datastore vVols.

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

La suppression d'une tâche de datastore des outils ONTAP pour VMware vSphere dans vCenter Server effectue les opérations suivantes :

- Démonte le conteneur vVol.
- Nettoie le groupe initiateur. Si igroup n'est pas utilisé, supprime iqn du igroup.
- Supprime le conteneur Vvol.
- Laisse les volumes Flex sur la baie de stockage.

Pour supprimer un datastore NFS, VMFS ou vvol des outils ONTAP du serveur vCenter, procédez comme suit :

Étapes

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Cliquez avec le bouton droit de la souris sur un système hôte, un cluster hôte ou un centre de données et sélectionnez **NetApp ONTAP Tools** > **Delete datastore**.

   Vous ne pouvez pas supprimer les datastores si des machines virtuelles utilisent ce datastore. Vous devez déplacer les machines virtuelles vers un autre datastore avant de supprimer le datastore. Vous ne pouvez pas cocher la case de suppression de volume si le datastore appartient à un cluster hôte protégé.

   a. Dans le cas d'un datastore NFS ou VMFS, une boîte de dialogue s'affiche avec la liste des machines virtuelles qui utilisent le datastore.
   b. Si le datastore VMFS est créé sur des systèmes ASA r2 et s'il fait partie de la protection, vous devez annuler la protection du datastore avant de le supprimer.
   c. Dans le cas d'un datastore vVols, l'action Supprimer le datastore supprime le datastore uniquement s'il n'y a aucun vVols associé. La boîte de dialogue Supprimer le datastore permet de supprimer des

volumes du cluster ONTAP.

d. Dans le cas d'un datastore vVols basé 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 d'un datastore VMFS faisant partie du cluster hôte protégé.

Vues de stockage ONTAP pour les datastores

Les outils ONTAP pour VMware vSphere affichent la vue côté stockage ONTAP des datastores et de leurs volumes dans l'onglet configurer.

Étapes

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

Type de datastore	Information disponible
Datastore NFS	La page **Détails du stockage** contient des informations sur les systèmes back-end de stockage, les agrégats et les volumes. La page de détails NFS contient des données relatives au datastore NFS.
Datastores VMFS	La page **Storage details** contient des informations sur le back-end de stockage, l'agrégat et le volume. La page **LUN details** contient des données relatives à la LUN. La page **Namespace details** contient des données relatives à l'espace de noms lorsque le datastore VMFS utilise le protocole NVMe/TCP ou NVMe/FC. Les détails des volumes et des agrégats ne sont pas affichés pour les datastores basés sur le système de stockage ASA r2.
Datastores vVols	Répertorie tous les volumes. Vous pouvez développer ou supprimer du stockage à partir du volet de stockage ONTAP. Cette vue n'est pas prise en charge pour le datastore vVols système ASA r2.

Vue du stockage des machines virtuelles

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

> Cette vue s'applique à la machine virtuelle sur laquelle au moins un disque associé aux outils ONTAP pour le datastore VMware vSphere Managed vVols est monté.

Étapes

1. À partir du client vSphere, accédez à la machine virtuelle.
2. Sélectionnez l'onglet **Monitor** dans le volet de droite.
3. Sélectionnez **NetApp ONTAP Tools** > **Storage**. Les détails **Storage** apparaissent dans le volet de droite. Vous pouvez voir la liste des vVols présents sur la machine virtuelle.

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

Gérer les seuils de stockage

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

Étapes :

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Dans la page raccourcis, sélectionnez **NetApp ONTAP Tools** dans la section modules externes.
3. Dans le volet gauche des outils ONTAP, accédez à **Paramètres** > **Paramètres de seuil** > **Modifier**.
4. Dans la fenêtre **Modifier le seuil**, indiquez les valeurs souhaitées dans les champs **presque plein** et **plein** et sélectionnez **Enregistrer**. Vous pouvez réinitialiser les chiffres sur les valeurs recommandées, soit 80 pour presque plein et 90 pour plein.

Gestion des systèmes back-end

Les systèmes back-end de stockage sont des systèmes que les hôtes ESXi utilisent pour le stockage des données.

Découverte du stockage

Vous pouvez exécuter la détection d'un système back-end de stockage à la demande sans attendre une découverte planifiée pour mettre à jour les détails du stockage.

Suivez les étapes ci-dessous pour découvrir les systèmes back-end.

Étapes

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Dans la page raccourcis, sélectionnez **NetApp ONTAP Tools** dans la section modules externes.
3. Dans le volet gauche des outils ONTAP, accédez à **systèmes back-end de stockage** et sélectionnez un système back-end de stockage.
4. Sélectionnez le menu des ellipses verticales et sélectionnez **découvrir le stockage**

Vous pouvez suivre la progression dans le panneau tâches récentes.

Modification des systèmes back-end de stockage

Suivez les étapes de cette section pour modifier un système back-end de stockage.

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`

2. Dans la page raccourcis, sélectionnez **NetApp ONTAP Tools** dans la section modules externes.
3. Dans le volet gauche des outils ONTAP, accédez à **systèmes back-end de stockage** et sélectionnez un système back-end de stockage.
4. Sélectionnez le menu des ellipses verticales et sélectionnez **Modifier** pour modifier les informations d'identification ou le nom du port. Vous pouvez suivre la progression dans le panneau tâches récentes.

Vous pouvez effectuer l'opération Modifier 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 à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez les systèmes back-end de stockage dans la barre latérale.
4. Sélectionnez le back-end de stockage à modifier.
5. Sélectionnez le menu ellipses verticales et sélectionnez **Modifier**.
6. Vous pouvez modifier les informations d'identification ou le port. Entrez **Nom d'utilisateur** et **Mot de passe** pour modifier le backend de stockage.

Suppression des systèmes back-end

Vous devez supprimer tous les datastores connectés au système back-end de stockage avant de supprimer le système back-end. Suivez les étapes ci-dessous pour supprimer un système back-end de stockage.

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Dans la page raccourcis, sélectionnez **NetApp ONTAP Tools** dans la section modules externes.
3. Dans le volet gauche des outils ONTAP, accédez à **systèmes back-end de stockage** et sélectionnez un système back-end de stockage.
4. Sélectionnez le menu ellipses verticales et sélectionnez **Supprimer**. Assurez-vous que le système back-end de stockage ne contient aucun datastore. Vous pouvez suivre la progression dans le panneau tâches récentes.

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

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **systèmes back-end de stockage** dans la barre latérale.
4. Sélectionnez le système back-end de stockage à supprimer
5. Sélectionnez le menu ellipses verticales et sélectionnez **Supprimer**.

Vue détaillée du système back-end de stockage

La page back-end de stockage répertorie tous les systèmes back-end. Vous pouvez détecter le stockage, modifier et supprimer les opérations sur les systèmes back-end que vous avez ajoutés, et non sur la SVM

enfant individuelle sous le cluster.

Lorsque vous sélectionnez le cluster parent ou l'enfant sous le système back-end de stockage, vous pouvez afficher le récapitulatif global du composant. Lorsque vous sélectionnez le cluster parent, vous disposez de la liste déroulante actions à partir de laquelle vous pouvez effectuer les opérations de découverte de stockage, de modification et de suppression.

La page de résumé fournit les détails suivants :

- État du système back-end de stockage
- Informations sur la capacité
- Informations de base sur la machine virtuelle
- Informations réseau telles que l'adresse IP et le port du réseau. Pour la SVM enfant, les informations seront les mêmes que le back-end de stockage parent.
- Privilèges autorisés et limités pour le système back-end de stockage. Pour la SVM enfant, les informations seront les mêmes que le back-end de stockage parent. Les privilèges ne s'affichent que sur les systèmes back-end de stockage basés sur le cluster. Si vous ajoutez SVM en tant que système back-end de stockage, les informations relatives aux privilèges ne seront pas affichées.
- La vue détaillée du cluster ASA r2 n'inclut pas l'onglet niveaux locaux lorsque la propriété désagrégée est définie sur « true » pour le SVM ou le cluster.
- Pour les systèmes SVM ASA r2, le portlet capacité n'est pas affiché. Le portail de capacité n'est requis que lorsque la propriété désagrégée est définie comme « true » pour le SVM ou le cluster.
- Pour les systèmes ASA r2 SVM, la section informations de base présente le type de plateforme.

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

L'onglet niveaux locaux fournit des informations détaillées sur la liste des agrégats.

Gestion des instances vCenter Server

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

Dissociez les systèmes back-end de stockage de l'instance vCenter Server

La page de liste vCenter Server affiche le nombre de systèmes back-end de stockage associés. Chaque instance de vCenter Server peut être associée ou dissociée à un système back-end de stockage.

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez l'instance vCenter Server requise dans la barre latérale.
4. Sélectionnez les ellipses verticales par rapport au serveur vCenter que vous souhaitez associer ou dissocier avec les systèmes back-end de stockage.
5. Sélectionnez **dissocier le backend de stockage**.

Modifier une instance de vCenter Server

Suivez les étapes ci-dessous pour modifier des instances de vCenter Server.

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

Supprimer une instance de vCenter Server

Vous devez supprimer tous les systèmes back-end associés au serveur vCenter avant de le supprimer.

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez les instances vCenter Server applicables dans la barre latérale
4. Sélectionnez les ellipses verticales par rapport au serveur vCenter que vous souhaitez supprimer et sélectionnez **Supprimer**.

> Une fois que vous avez supprimé des instances vCenter Server, elles ne seront plus gérées par l'application.

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

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

Gérer les certificats

Par défaut, lors du déploiement, un certificat auto-signé est généré pour les outils ONTAP et VASA Provider. 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 d'autorité de certification personnalisée sont obligatoires dans un déploiement multi-vCenter.

Avant de commencer

- Le nom de domaine sur lequel le certificat est émis doit être mappé sur 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 de l'équilibreur de charge.

> Une adresse IP de l'équilibreur de charge doit être mappée sur un nom de domaine complet (FQDN). Les certificats doivent contenir le même nom de domaine complet mappé à l'adresse IP de l'équilibreur de charge dans les autres noms d'objet ou d'objet.

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

Certificat de mise à niveau des outils ONTAP

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

Étapes

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

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

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

4. Pour mettre à niveau le certificat auto-signé vers un certificat CA personnalisé, sélectionnez **certificats** > **ONTAP Tools** > **mettre à niveau vers CA** option.
   a. Dans la fenêtre contextuelle, téléchargez le certificat du serveur, la clé privée du certificat du serveur, le certificat de l'autorité de certification racine et les fichiers de certificat intermédiaires.
   b. Entrez le nom de domaine pour lequel vous avez généré ce certificat et mettez à niveau le certificat.

      Le système sera hors ligne jusqu'à la fin de la mise à niveau et vous serez déconnecté de l'interface du Gestionnaire d'outils ONTAP.

Mettre à niveau le certificat VASA Provider

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

Étapes

1. Lancez le Gestionnaire d'outils ONTAP à partir d'un navigateur Web : `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Connectez-vous à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.
3. Sélectionnez **certificats** > **VASA Provider** ou **ONTAP Tools** > **Renew** pour renouveler les certificats.
4. Sélectionnez **certificats** > **VASA Provider** ou **ONTAP Tools** > **mettre à niveau vers CA** pour mettre à niveau le certificat auto-signé vers un certificat CA personnalisé.
   a. Dans la fenêtre contextuelle, téléchargez le certificat du serveur, la clé privée du certificat du serveur, le certificat de l'autorité de certification racine et les fichiers de certificat intermédiaires.

b. Entrez le nom de domaine pour lequel vous avez généré ce certificat et mettez à niveau le certificat.

Le système sera hors ligne jusqu'à la fin de la mise à niveau et vous serez déconnecté de l'interface du Gestionnaire d'outils ONTAP.

Accès aux outils ONTAP pour la console de maintenance VMware vSphere

Présentation des outils ONTAP pour la console de maintenance VMware vSphere

Vous pouvez gérer les configurations de votre application, de votre système et de votre 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 offres de support, définir différents niveaux de journal, afficher et gérer les configurations TLS et démarrer les diagnostics à distance.

Vous devez avoir installé les outils VMware après avoir déployé les outils ONTAP pour VMware vSphere pour accéder à la console de maintenance. Vous devez utiliser `maint` En tant que nom d'utilisateur et mot de passe que vous avez configurés pendant le déploiement pour vous connecter à la console de maintenance des outils ONTAP. Vous devez utiliser **nano** pour modifier les fichiers dans la console de maintenance ou de connexion racine.

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

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

Menu Console	Options
Configuration de l'application	1. Afficher le récapitulatif de l'état du serveur 2. Modifier le niveau du JOURNAL pour les services VASA Provider et SRA 3. Désactivez AutoSupport 4. Mettre à jour l'URL du proxy AutoSupport

Configuration du système	1. Redémarrez la machine virtuelle 2. Arrêter la machine virtuelle 3. Modifier le mot de passe utilisateur « familiariser » 4. Modifier le fuseau horaire 5. Ajouter un nouveau serveur NTP 6. Augmentation de la taille des disques de prison (/prison) 7. Mise à niveau 8. Installez VMware Tools
Configuration du réseau	1. Afficher les paramètres d'adresse IP 2. Afficher les paramètres de recherche du nom de domaine 3. Modifier les paramètres de recherche du nom de domaine 4. Afficher les routes statiques 5. Modifier les routes statiques 6. Valider les modifications 7. Envoyez une requête ping à un hôte 8. Restaurez les paramètres par défaut
Support et diagnostics	1. Accéder au shell de diagnostic 2. Activer l'accès aux diagnostics à distance 3. Fournir les informations d'identification vCenter pour la sauvegarde 4. Effectuer des sauvegardes

Configurer l'accès aux diagnostics à distance

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

Avant de commencer

L'extension VASA Provider 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 limites suivantes :

- Vous n'avez droit qu'à un seul compte de connexion par activation de SSH.
- L'accès SSH au compte utilisateur diag est désactivé lorsque l'une des conditions suivantes se produit :
  - Le délai expire.

La session de connexion reste valide jusqu'à minuit le lendemain.

- Vous vous connectez à nouveau en tant qu'utilisateur diag à l'aide de SSH.

Étapes

1. Depuis vCenter Server, ouvrez une console vers VASA Provider.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrez `4` Pour sélectionner support et Diagnostics.
4. Entrez `2` pour sélectionner Activer l'accès aux diagnostics à distance.
5. Entrez `y` Dans la boîte de dialogue Confirmation pour activer l'accès au diagnostic à distance.
6. Saisissez un mot de passe pour l'accès au diagnostic à distance.

Démarrez SSH sur les autres nœuds

Vous devez démarrer SSH sur les autres nœuds avant la mise à niveau.

Avant de commencer

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

À propos de cette tâche

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

Étapes

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

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

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

Avant de commencer

Vous devez disposer des informations d'identification de l'utilisateur de maintenance.

À propos de cette tâche

Si vous avez modifié les informations d'identification du serveur vCenter, du ONTAP ou de la LIF de données 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 vers VASA Provider.

2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrez `2` pour sélectionner le menu de configuration du système.
4. Entrez `9` pour modifier les informations d'identification ONTAP.
5. Entrez `10` pour modifier les informations d'identification de vCenter.

Rapports sur les outils ONTAP

Le plug-in ONTAP Tools for VMware vSphere fournit des rapports pour les machines virtuelles et les datastores. Lorsque vous sélectionnez l'icône du plug-in NetApp ONTAP Tools for VMware vSphere dans la section des raccourcis du client vCenter, l'interface utilisateur accède à la page Présentation. Sélectionnez l'onglet Rapports pour afficher la machine virtuelle et le rapport datastores.

Le rapport machines virtuelles affiche la liste des machines virtuelles découvertes (au moins un disque doit être issu des datastores basés sur le stockage ONTAP) avec des mesures de performances. Lorsque vous développez l'enregistrement de la machine virtuelle, toutes les informations relatives au datastore relatives au disque s'affichent.

Le rapport datastores affiche la liste des outils ONTAP détectés ou reconnus pour les datastores gérés VMware vSphere provisionnés à partir du back-end de stockage ONTAP de tous types avec des metrics de performances.

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

Collectez les fichiers journaux

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

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

Étapes

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

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

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

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

Étapes

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Depuis la page d'accueil de vSphere client, accédez à **support** > **Log bundle** > **Generate**.
3. Indiquez l'étiquette de l'ensemble de journaux et générez l'ensemble de journaux.
   Vous pouvez voir l'option de téléchargement lorsque les fichiers sont générés. Le téléchargement peut prendre un certain temps.

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

Gérer des machines virtuelles

Considérations relatives à la migration ou au clonage de machines virtuelles

Lors de la migration de machines virtuelles existantes dans votre data Center, vous devez prendre en compte certaines considérations.

Migrer des machines virtuelles protégées

Vous pouvez migrer les machines virtuelles protégées vers :

- Même datastore vVvols dans un autre hôte ESXi
- Il existe un autre datastore compatible vVvols dans le même hôte ESXi
- Il existe un autre datastore compatible vVvols dans un hôte VMware ESXi différent

Si la machine virtuelle est migrée vers un autre volume FlexVol, 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 VMware ESXi mais un même stockage, le fichier de métadonnées du volume FlexVol sous-jacent ne sera pas modifié.

Machines virtuelles protégées par des clones

Vous pouvez cloner des machines virtuelles protégées à plusieurs méthodes :

- Même conteneur du même volume FlexVol à l'aide du groupe de réplication

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

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

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

- Il existe un autre conteneur ou datastore vvols

  Volume FlexVol sur lequel la machine virtuelle clonée est placée, le fichier de métadonnées est mis à jour

les informations relatives à la machine virtuelle.

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

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

Voir "Création d'une machine virtuelle pour le clonage" pour plus de détails.

Snapshots de machine virtuelle

Actuellement, seuls les snapshots de machine virtuelle sans mémoire sont pris en charge. Si la machine virtuelle possède une copie Snapshot de la mémoire, la machine virtuelle n'est pas prise en compte pour sa protection.

Vous ne pouvez pas non plus protéger les machines virtuelles non protégées qui disposent d'une mémoire Snapshot. Pour cette version, vous devez supprimer l'instantané de mémoire avant d'activer la protection de la machine virtuelle.

Pour une machine virtuelle Windows avec un type de stockage ASA r2, lorsque vous créez un snapshot de la machine virtuelle, il s'agit d'un snapshot en lecture seule. Lorsqu'un appel de mise sous tension est lancé pour la machine virtuelle, le fournisseur VASA crée un LUN à l'aide du snapshot en lecture seule, puis il 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.

Migrez les machines virtuelles avec les datastores NFS et VMFS vers les datastores vVols

Vous pouvez migrer des machines virtuelles des datastores NFS et VMFS vers des datastores Virtual volumes (vVols) pour tirer parti de la gestion des machines virtuelles basée sur des règles et d'autres fonctionnalités vVols. Les datastores vvols vous permettent de répondre à de plus en plus de besoins de charge de travail.

Avant de commencer

Assurez-vous que VASA Provider ne s'exécute sur aucune des machines virtuelles que vous prévoyez de migrer. Si vous migrez une machine virtuelle qui exécute VASA Provider dans un datastore vvols, vous ne pouvez pas effectuer d'opérations de gestion, y compris la mise sous tension des machines virtuelles qui se trouvent sur des datastores vvols.

À propos de cette tâche

Lorsque vous migrez d'un datastore NFS et VMFS vers un datastore vVols, vCenter Server utilise les API vStorage APIs for Array Integration (VAAI) pour décharger les données lors du déplacement de datastores VMFS, mais pas à partir d'un fichier VMDK NFS. VAAI réduit généralement la charge sur l'hôte.

Étapes

1. Cliquez avec le bouton droit de la souris sur la machine virtuelle à migrer et sélectionnez **migrer**.
2. Sélectionnez **changer stockage uniquement**, puis **Suivant**.
3. Sélectionnez un format de disque virtuel, une stratégie de stockage VM et un datastore vVol correspondant aux fonctionnalités du datastore que vous migrez.
4. Vérifiez les paramètres et sélectionnez **Terminer**.

Nettoyage de Vasa

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

> Il est recommandé de supprimer tous les datastores vVols avant d'effectuer le nettoyage de VASA.

Étapes

1. Annulez l'enregistrement du plug-in en accédant à https://OTV_IP:8143/Register.html
2. Vérifiez que le plug-in n'est plus disponible sur vCenter Server.
3. Fermez les outils ONTAP pour VMware vSphere VM.
4. Supprimez les outils ONTAP pour VMware vSphere VM.

Découverte des systèmes et des hôtes de stockage

Lors de la première exécution des outils ONTAP pour VMware vSphere dans un client vSphere, les outils ONTAP permettent de détecter les hôtes ESXi, leurs LUN et leurs exportations NFS, ainsi que les systèmes de stockage NetApp qui possèdent ces LUN et ces exportations.

Avant de commencer

- Tous les hôtes ESXi doivent être sous tension et connectés.
- Tous les SVM à découvrir doivent être en cours d'exécution, et chaque nœud de cluster doit disposer d'au moins une LIF de données configurée pour le protocole de stockage utilisé (NFS ou iSCSI).

À propos de cette tâche

Vous pouvez détecter de nouveaux systèmes de stockage ou mettre à jour les informations concernant les systèmes de stockage existants afin d'obtenir à tout moment les informations les plus récentes sur leur capacité et leur configuration. Vous pouvez également modifier les informations d'identification utilisées par les outils ONTAP pour VMware vSphere pour vous connecter aux systèmes de stockage.

Lors de la découverte des systèmes de stockage, les outils ONTAP pour VMware vSphere collectent des informations à partir des hôtes ESXi gérés par l'instance vCenter Server.

Étapes

1. Sur la page d'accueil de vSphere client, sélectionnez **hosts and clusters**.
2. Cliquez avec le bouton droit de la souris sur le centre de données requis et sélectionnez **NetApp ONTAP Tools** > **Update Host Data** .

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

3. Sélectionnez les contrôleurs de stockage détectés qui ont l'état `Authentication Failure` et sélectionnez **actions** > **Modifier**.
4. Renseignez les informations requises dans la boîte de dialogue **Modifier le système de stockage**.
5. Répétez les étapes 4 et 5 pour tous les contrôleurs de stockage avec `Authentication Failure` état.

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

- Utilisez les outils ONTAP pour VMware vSphere pour configurer les paramètres de l'hôte VMware ESXi pour les hôtes qui affichent l'icône d'alerte dans la colonne des paramètres de l'adaptateur, dans la colonne des paramètres MPIO ou dans la colonne des paramètres NFS.
- Indiquez les informations d'identification du système de stockage.

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

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

Avant de commencer

En cas de problème avec vos paramètres d'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 présentant le problème.

Étapes

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Dans la page raccourcis, sélectionnez **NetApp ONTAP Tools** dans la section modules externes.
3. Accédez au portlet **ESXi Host Compliance** dans la Présentation (tableau de bord) du plug-in ONTAP Tools for VMware vSphere.
4. Sélectionnez le lien **appliquer les paramètres recommandés**.
5. Dans la fenêtre **appliquer les paramètres d'hôte recommandés**, sélectionnez les hôtes que vous souhaitez respecter avec les 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.
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 à l'aide des outils ONTAP pour les informations d'identification d'administrateur VMware vSphere que vous avez fournies lors du déploiement.

3. Sélectionnez l'icône **Administrator** 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, entrez l'ancien mot de passe et les détails du nouveau mot de passe. La contrainte de modification du mot de passe s'affiche sur l'écran de l'interface utilisateur.
5. Sélectionnez **Modifier** pour appliquer les modifications.

Réinitialisez le mot de passe du gestionnaire d'outils ONTAP

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

   a. Dans vCenter Server, ouvrez la console de maintenance
   b. Entrez « 2 » pour sélectionner l'option de configuration du système
   c. Saisissez « 3 » pour modifier le mot de passe utilisateur « maint ».
3. Dans la fenêtre contextuelle de modification du mot de passe, entrez 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, vous pouvez utiliser le nouveau mot de passe pour vous connecter.

Réinitialiser le mot de passe utilisateur de l'application

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

Étapes

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

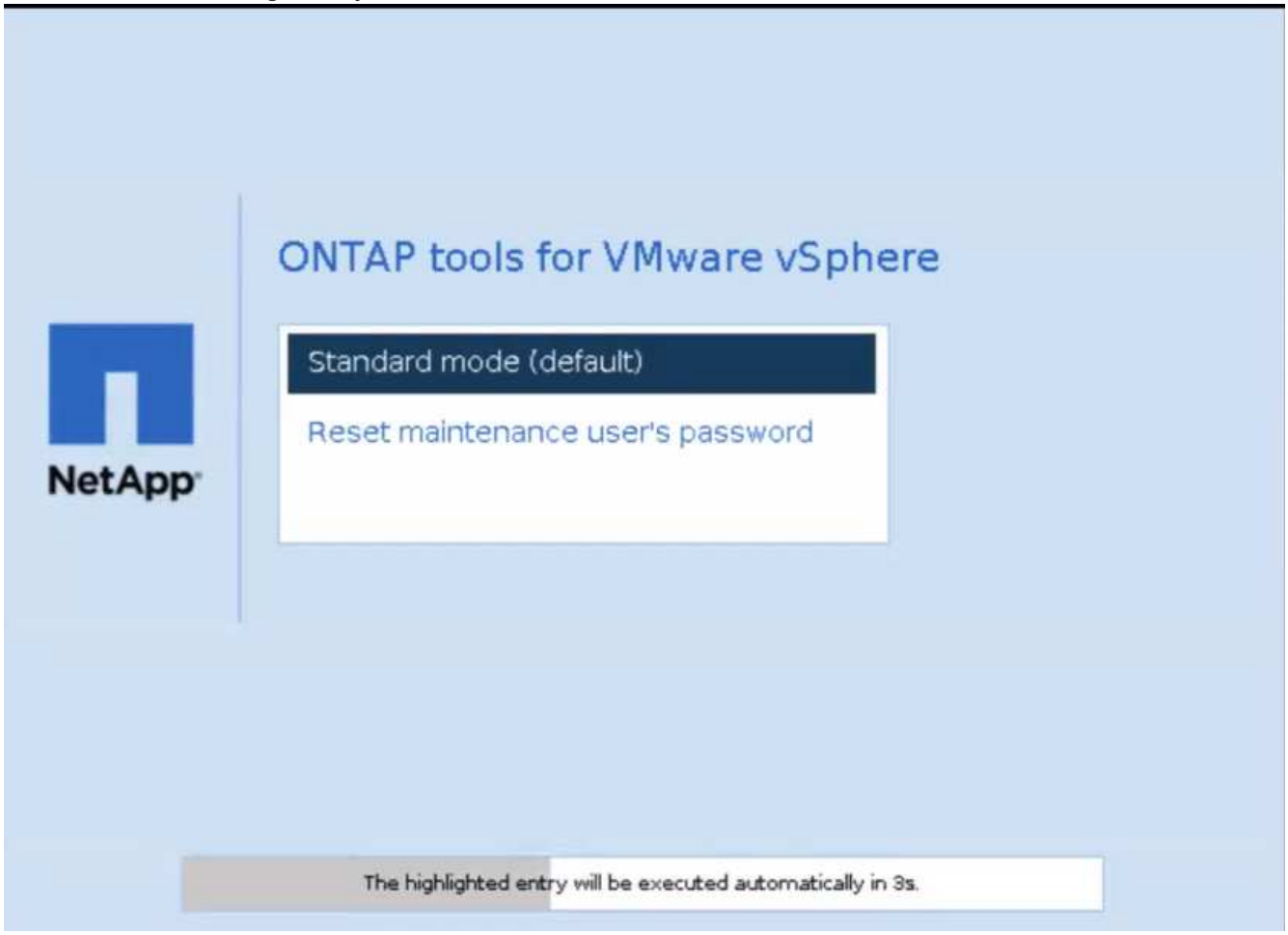
Réinitialiser le mot de passe utilisateur de la console de maintenance

Lors du redémarrage du système d'exploitation invité, le menu GRUB affiche une option permettant de réinitialiser le mot de passe utilisateur de la console de maintenance. Cette option permet de mettre à jour le mot de passe utilisateur de la console de maintenance présent sur la machine virtuelle correspondante. Une fois le mot de passe réinitialisé, la machine virtuelle redémarre pour définir le nouveau mot de passe. Dans le cas d'un 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 le déploiement des outils ONTAP pour VMware vSphere HA, vous devez modifier le mot de passe utilisateur de la console de maintenance sur le nœud principal, c'est-à-dire le nœud 1.

Étapes

1. Connectez-vous à votre serveur vCenter
2. Cliquez avec le bouton droit de la souris sur la machine virtuelle et sélectionnez **Power** > **Restart Guest OS**
   Pendant le redémarrage du système, l'écran suivant s'affiche :



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

3. Sélectionnez l'option **Réinitialiser le mot de passe de l'utilisateur de maintenance**. La console de maintenance s'ouvre.

4. Dans la console, entrez 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 la saisie du nouveau mot de passe.
5. Appuyez sur entrée pour continuer.
Le mot de passe est mis à jour sur la machine virtuelle.

> Le même menu GRUB s'affiche également pendant la mise sous tension de la machine virtuelle. Cependant, vous devez utiliser l'option de réinitialisation du mot de passe uniquement avec l'option **redémarrer le système d'exploitation invité**.

Gestion de la protection des clusters hôtes

Modifier le cluster hôte protégé

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

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

Surveillez la protection des clusters hôtes

Utilisez cette procédure pour surveiller l'état de la protection du cluster hôte. Vous pouvez contrôler chaque cluster hôte protégé ainsi que son état de protection, ses relations SnapMirror, ses datastores et l'état de SnapMirror correspondant.

Étapes

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Accédez à **NetApp ONTAP Tools** > **protection** > **Host cluster Relationships**.

   L'icône située sous la colonne protection indique l'état de la protection
3. Passez la souris sur l'icône pour afficher plus de détails.

Ajoutez de nouveaux datastores ou hôtes

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

Étapes

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Pour modifier les propriétés d'un cluster protégé, vous pouvez l'un ou l'autre
   a. Accédez à **NetApp ONTAP Tools** > **protection** > **Host cluster Relationships**, sélectionnez le menu points de suspension en regard du cluster et sélectionnez **Edit** or

b. Cliquez avec le bouton droit de la souris sur un cluster hôte et sélectionnez **NetApp ONTAP Tools** > **Protect Cluster**.

3. Si vous avez créé un datastore dans l'interface utilisateur vCenter native, ce datastore s'affiche comme non protégé. L'interface utilisateur affiche tous les datastores du cluster et leur état de protection dans une boîte de dialogue. Sélectionnez le bouton **Protect** pour activer la protection complète.
4. Si vous avez ajouté un nouvel hôte ESXi, l'état de protection est 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, l'action de modification n'est pas prise en charge, car vous ne pouvez pas ajouter le SVM cible pour le site tertiaire à la même instance d'outils ONTAP. Cependant, vous pouvez utiliser le system Manager ou l'interface de ligne de commandes du SVM cible pour modifier la configuration des relations.

5. Sélectionnez **Enregistrer** après avoir effectué les modifications nécessaires.
6. Vous pouvez voir les modifications dans la fenêtre **Protect 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 à l'aide de `https://<vcenterip>/<ui>`
2. Pour modifier les propriétés d'un cluster protégé, vous pouvez l'un ou l'autre
   a. Accédez à **NetApp ONTAP Tools** > **protection** > **Host cluster Relationships**, sélectionnez le menu points de suspension en regard du cluster et sélectionnez **Edit** or
   b. Cliquez avec le bouton droit de la souris sur un cluster hôte et sélectionnez **NetApp ONTAP Tools** > **Protect Cluster**.
3. Sélectionnez **Ajouter une relation**.
4. Ajoutez une nouvelle relation en tant que type de stratégie **Asynchronous** ou **AutomatedFailOverDuplex**.
5. Sélectionnez **protéger**.

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

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

Supprimez une relation SnapMirror existante

Pour supprimer une relation SnapMirror asynchrone, un serveur SVM ou un cluster de site secondaire doit être ajouté en tant que système back-end de stockage dans les outils ONTAP pour VMware vSphere. Vous ne pouvez pas supprimer toutes les relations SnapMirror. Lorsque vous supprimez une relation, la relation respective sur le cluster ONTAP est également supprimée. Lorsque vous supprimez une relation SnapMirror AutomatedFailOverDuplex, les datastores sur la destination ne sont pas mappés 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 la LUN non mappée en tant que chemin actif des hôtes.

Étapes

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Pour modifier les propriétés d'un cluster protégé, vous pouvez l'un ou l'autre
   a. Accédez à **NetApp ONTAP Tools** > **protection** > **Host cluster Relationships**, sélectionnez le menu points de suspension en regard du cluster et sélectionnez **Edit** or
   b. Cliquez avec le bouton droit de la souris sur un cluster hôte et sélectionnez **NetApp ONTAP Tools** > **Protect Cluster**.
3. Sélectionnez le menu points de suspension sous les paramètres 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, un serveur SVM ou un cluster de site secondaire doit être ajouté en tant que système back-end de stockage dans les outils ONTAP pour 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 à l'hôte en cas de configuration non uniforme. Vous ne pouvez pas échanger des types de stratégie asynchrone et AutomatedFailOverDuplex. Vous pouvez définir la proximité ou l'accès des hôtes récemment découverts sur le cluster.

Vous ne pouvez pas modifier une relation SnapMirror asynchrone existante.

Étapes

1. Connectez-vous au client vSphere à l'aide de `https://<vcenterip>/<ui>`
2. Pour modifier les propriétés d'un cluster protégé, vous pouvez l'un ou l'autre
   a. Accédez à **NetApp ONTAP Tools** > **protection** > **Host cluster Relationships**, sélectionnez le menu points de suspension en regard du cluster et sélectionnez **Edit** or
   b. Cliquez avec le bouton droit de la souris sur un cluster hôte et sélectionnez **NetApp ONTAP Tools** > **Protect Cluster**.
3. Si le type de stratégie AutomatedFailOverDuplex est sélectionné, ajoutez des détails sur la proximité de l'hôte ou l'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**.

Retirez la protection du cluster hôte

Lorsque vous supprimez la protection du cluster hôte, les datastores deviennent non protégés.

Étapes

1. Pour afficher les clusters d'hôtes protégés, accédez à **NetApp ONTAP Tools** > **protection** > **Host cluster relations**.

   Dans cette page, vous pouvez surveiller les clusters hôtes protégés ainsi que l'état de protection, la relation SnapMirror et l'état de SnapMirror correspondant.

2. Dans la fenêtre **Host Cluster protection**, sélectionnez le menu points de suspension correspondant au

cluster, puis sélectionnez **Remove protection**.

Désactivez 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 recevrez plus de support et de surveillance proactifs.

Il est recommandé de conserver AutoSupport activé. Elle accélère la détection et la résolution des problèmes. Le système collecte les informations AutoSupport et les stocke localement, même lorsqu'elles sont désactivées.

Étapes

1. Dans vCenter Server, ouvrez la console de maintenance.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrez 1 pour sélectionner **Configuration de l'application**.
4. Entrez 3 pour sélectionner **Désactiver AutoSupport**.
5. Entrez y dans la boîte de dialogue de confirmation.

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 cas où un serveur proxy est utilisé pour le contrôle d'accès au réseau ou les mesures de sécurité. Il permet de router les données AutoSupport via le proxy approprié, ce qui garantit une transmission et une conformité sécurisées.

Étapes

1. Dans vCenter Server, ouvrez la console de maintenance.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrez 1 pour sélectionner **Configuration de l'application**.
4. Entrez 4 pour sélectionner **mettre à jour URL proxy AutoSupport**.
5. Entrez l'URL du proxy.

Créez une sauvegarde et restaurez la configuration

Étant donné que les outils ONTAP pour VMware vSphere 10.3 utilisent le provisionnement de stockage dynamique, vous ne pouvez pas atteindre un RPO nul. Toutefois, 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.

Créez une sauvegarde et téléchargez le fichier de sauvegarde

Étapes

1. Dans vCenter Server, ouvrez la console de maintenance.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrez `4` pour sélectionner **support et diagnostic**.
4. Entrez `3` pour sélectionner l'option **Activer la sauvegarde du système**.
5. Dans le cas d'une configuration non HA, entrez les informations d'identification vCenter sur lesquelles la machine virtuelle ONTAP Tools est déployée.
6. Entrez la valeur de fréquence de sauvegarde entre 5-60 min.
7. Appuyez sur **entrée**

   Cela crée la sauvegarde et la transmet au datastore de la machine virtuelle à intervalles réguliers.

8. Pour accéder à la sauvegarde, accédez à la section stockage et sélectionnez le datastore 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, avec le suffixe *backup*.

10. Pour plus d'informations sur la sauvegarde, téléchargez le fichier backup_info.txt à partir de **Files** > **Download**.

Reprise après incident

Pour restaurer la configuration, mettez la machine virtuelle existante hors tension et déployez une nouvelle machine virtuelle à l'aide de l'OVA qui a été utilisée lors du déploiement initial.

Vous devez utiliser la même adresse IP d'outil ONTAP (IP d'équilibreur de charge) pour la nouvelle machine virtuelle, et la configuration système telle que les services activés, la taille du nœud et le mode haute disponibilité doit être identique au déploiement initial.

Procédez comme suit pour restaurer la configuration à partir du fichier de sauvegarde.

1. Dans vCenter Server, ouvrez la console de maintenance.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrez `4` pour sélectionner **support et diagnostic**.
4. Entrez `2` pour sélectionner l'option **Activer l'accès au diagnostic à distance** et créer un nouveau mot de passe pour l'accès au diagnostic.
5. Sélectionnez une sauvegarde dans le répertoire téléchargé. Le nom du dernier fichier de sauvegarde est enregistré dans *backup_info.txt* file.
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 de 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. Une fois la restauration effectuée, les services et les objets vCenter sont restaurés.

Désinstallez les outils ONTAP pour VMware vSphere

La désinstallation des outils ONTAP pour VMware vSphere supprime toutes les données contenues dans les outils.

Étapes

1. Supprimez ou déplacez toutes les machines virtuelles des outils ONTAP pour les datastores gérés VMware vSphere.
   - Pour supprimer les machines virtuelles, reportez-vous à la section "Supprimez et réenregistrez les machines virtuelles et les modèles de machines virtuelles"
   - Pour les déplacer vers un datastore non géré, reportez-vous à la section "Stockage vMotion"
2. "Supprimer les datastores" Créé sur les outils ONTAP pour VMware vSphere.
3. Si vous avez activé le fournisseur VASA, sélectionnez **Paramètres** > **VASA Provider settings** > **Unregister** dans les outils ONTAP pour désenregistrer les fournisseurs VASA de tous les serveurs vCenter.
4. Dissociez tous les systèmes back-end de l'instance vCenter Server. Reportez-vous à la "Dissociez les systèmes back-end de stockage de l'instance vCenter Server".
5. Suppression de tous les systèmes back-end Reportez-vous à la "Gestion des systèmes back-end".
6. Supprimez l'adaptateur SRA de VMware Live site Recovery :
   a. Connectez-vous en tant qu'administrateur à l'interface de gestion de l'appliance VMware Live site Recovery à l'aide du port 5480.
   b. Sélectionnez **Storage Replication Adapters**.
   c. Sélectionnez la carte SRA appropriée et, dans le menu déroulant, sélectionnez **Supprimer**.
   d. Confirmez que vous connaissez les résultats de la suppression de la carte et sélectionnez **Supprimer**.
7. Supprimez les instances de serveur vCenter intégrées aux outils ONTAP pour VMware vSphere. Reportez-vous à la "Gestion des instances vCenter Server".
8. Mettez hors tension les outils ONTAP pour les machines virtuelles VMware vSphere à partir du serveur vCenter et supprimez les machines virtuelles.

Et la suite ?

"Supprimez les volumes FlexVol"

Supprimez les volumes FlexVol

L'utilisation d'un cluster ONTAP dédié aux outils ONTAP pour le déploiement VMware crée de nombreux volumes FlexVol inutilisés. Après avoir supprimé les outils ONTAP pour VMware vSphere, vous devez supprimer les volumes FlexVol afin d'éviter tout impact sur les performances.

Étapes

1. Déterminer le type de déploiement des outils ONTAP pour VMware vSphere à partir de la machine virtuelle du nœud principal.

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

3. Supprimez les machines virtuelles du serveur vCenter. Reportez-vous à la "Supprimez et réenregistrez les machines virtuelles et les modèles de machines virtuelles".
4. Supprimez des volumes FlexVol du Gestionnaire système ONTAP. Reportez-vous à la "Supprime un volume FlexVol". Dans la commande CLI permettant de supprimer un volume, donnez le nom exact des volumes FlexVol.
5. Supprimez les igroups SAN du système de stockage ONTAP en cas de déploiement iSCSI. Reportez-vous à la "Affichez et gérez les initiateurs SAN et igroups".

Mettez à niveau les outils ONTAP pour VMware vSphere

Mise à niveau des outils ONTAP pour VMware vSphere 10.x vers la version 10.3

Cette mise à niveau est prise en charge pour les déploiements haute disponibilité et non haute disponibilité. Les chemins de mise à niveau pris en charge sont les suivants :

À partir des outils ONTAP pour la configuration VMware vSphere 10.1 et 10.2	Aux outils ONTAP pour la configuration VMware vSphere 10.3
Non HA petit	Non HA et avancé petit
Support non HA	Non HA et support avancé
Avancé petit	Non HA et avancé petit
Support avancé	Non HA et support avancé
HA petit	HA petit
HA moyen	HA moyen
HAUTE disponibilité	HAUTE disponibilité

Les mises à niveau à partir des outils ONTAP pour VMware vSphere 10.1 et 10.2 vers 10.3 sont prises en charge. Les mises à niveau directes des outils ONTAP 10.0 à 10.3 ne sont pas prises en charge.

Avant de commencer

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

- Ajoutez un disque dur supplémentaire de 100 Go à chaque nœud, car les données de service sont stockées localement sur la machine virtuelle.
- Modifiez le processeur et la mémoire de la machine virtuelle mise hors tension en fonction du type de votre déploiement. Activez le plug-in actif pour le processeur et la RAM.

10.3 Type de déploiement	CPU (Core) par nœud	Mémoire (Go) par nœud	Espace disque (Go) par nœud	Total CPU (cœur)	Mémoire (Go)	Espace disque total (Go)
Non HA petit	9	18	350	9	18	350
Non HA Moyen	13	26	350	13	26	350
HA petit	9	18	350	27	54	1050
HA Moyen	13	26	350	39	78	1050

10.3 Type de déploiement	CPU (Core) par nœud	Mémoire (Go) par nœud	Espace disque (Go) par nœud	Total CPU (cœur)	Mémoire (Go)	Espace disque total (Go)
HAUTE disponibilité	17	34	350	51	102	1050

- Mettez la machine virtuelle sous tension une fois les modifications effectuées et attendez que les services soient en cours d'exécution.
- En cas de déploiement haute disponibilité, apportez les modifications nécessaires aux ressources, activez le plug-in à chaud pour le processeur et la RAM, et ajoutez des disques durs de 100 Go pour le deuxième et le troisième nœuds. 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 10.1 ou 10.2, vous devez arrêter la copie Snapshot avant de procéder à la mise à niveau.

Si vous effectuez une mise à niveau à partir des outils ONTAP pour VMware vSphere 10.0 vers la version 10.1, vous devez effectuer les étapes suivantes avant de procéder à la mise à niveau :

Activer les diagnostics

1. À partir du serveur vCenter, ouvrez une console pour accéder aux outils ONTAP.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrez **4** pour sélectionner **support et diagnostic**.
4. Entrez **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 machine virtuelle à partir du terminal/de la putty avec l'utilisateur comme 'diag' et le mot de passe défini à l'étape précédente.

Prendre 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 système ntv.
- Exécutez la commande *env | grep MONGODB_ROOT_PASSWORD* dans le pod.
- Exécutez la commande *exit* pour sortir du pod.
- Exécutez *kn exec ntv-mongodb-0 --mongodump -u root -p MONGODB_ROOT_PASSWORD --archive=/tmp/mongodb-backup.gz --gzip* command pour remplacer le jeu MONGO_ROOT_PASSWORD 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 l'instantané de tous les volumes

- Exécutez la commande « kn Get pvc » et enregistrez la sortie de la commande.
- Prenez des snapshots de tous les volumes une par une à l'aide de l'une des méthodes suivantes :
  - Depuis l'interface de ligne de commande, lancer la commande *volume snapshot create -vserver <vserver_name> -volume <volume_name> -snapshot <snapshot_name>*
  - Dans l'interface utilisateur du Gestionnaire système ONTAP, recherchez le volume par son nom dans

la barre de recherche, puis ouvrez ce volume en sélectionnant son nom. Accédez à l'instantané et ajoutez l'instantané de ce volume.

Prendre le snapshot des outils ONTAP pour les machines virtuelles 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 instantané**. Prendre un snapshot suspendu de la machine virtuelle. Voir "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'il soit terminé, puis supprimez le pod.

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

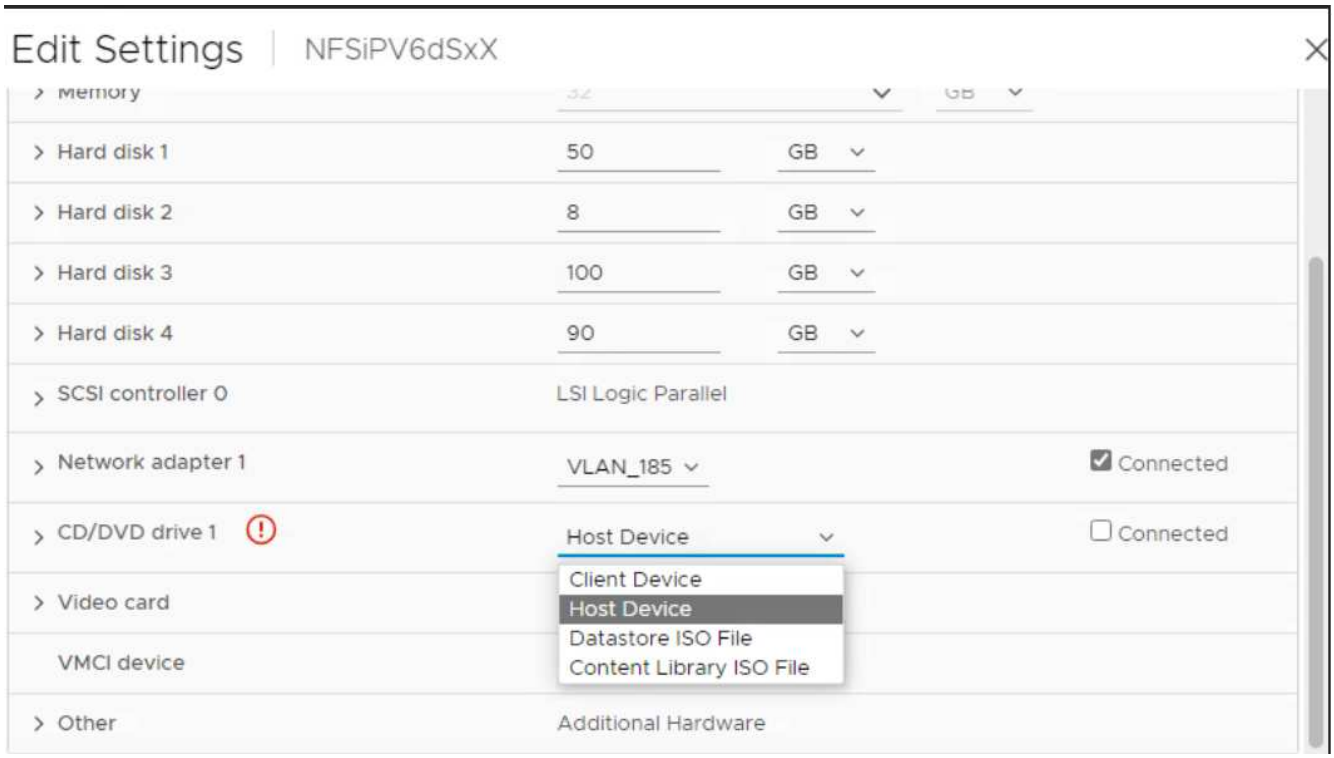
1. Sélectionnez la VM en configuration à un seul nœud ou les trois VM en configuration haute disponibilité.
2. Cliquez avec le bouton droit de la souris sur la ou les machines virtuelles et sélectionnez **Ajouter un nouveau périphérique** > **disque dur**
3. Ajoutez un disque dur de 100 Go dans le champ **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 mécanisme de provisionnement du stockage dynamique utilise ce disque dur pour générer ou répliquer les volumes.

Étapes

1. Télécharger les outils ONTAP pour VMware vSphere, mettez à niveau ISO vers la bibliothèque de contenu.
2. Sur la page VM principale, sélectionnez **actions** > **Modifier les paramètres**
3. Sélectionnez le fichier ISO de la bibliothèque de contenu dans la fenêtre de modification des paramètres sous le champ **lecteur de CD/DVD**.
4. Sélectionnez le fichier ISO et sélectionnez **OK**. Cochez la case connecté dans le champ **lecteur de CD/DVD**.



5. À partir du serveur vCenter, ouvrez une console pour accéder aux outils ONTAP.
6. Connectez-vous en tant qu'utilisateur de maintenance.
7. Entrez **3** pour sélectionner le menu Configuration du système.
8. Entrez **7** pour sélectionner l'option de mise à niveau.
9. Lorsque vous effectuez une mise à niveau, les actions suivantes sont automatiquement exécutées :
   a. Mise à niveau du certificat
   b. Mise à niveau du plug-in à distance

Après avoir effectué la mise à niveau vers les outils ONTAP pour VMware vSphere 10.3, vous pouvez :

- Désactivez les services à partir de l'interface utilisateur Manager
- Passez d'une configuration non HA à une configuration haute disponibilité
- Évolution verticale petite configuration non HA de moyen ou de grand format non HA.
- En cas de mise à niveau non HA, redémarrez la machine virtuelle d'outils ONTAP pour refléter les modifications. Dans le cas d'une mise à niveau HA, redémarrez le premier nœud pour refléter les modifications sur le nœud.

Après la fin

Après la mise à niveau des versions précédentes des outils ONTAP pour VMware vSphere vers la version 10.3, relancez l'analyse des adaptateurs SRA pour vérifier que les informations sont mises à jour sur la page adaptateurs de réplication du stockage de VMware Live site Recovery.

Une fois la mise à niveau effectuée, supprimez manuellement les volumes Trident de ONTAP en procédant comme suit :

Ces étapes ne sont pas nécessaires si les outils ONTAP pour VMware vSphere 10.1 ou 10.2 se trouvent dans des configurations de petite ou moyenne haute disponibilité (chemin local).

1. À partir du serveur vCenter, ouvrez une console pour accéder aux outils ONTAP.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrez **4** pour sélectionner le menu **support et diagnostic**.
4. Entrez **1** pour sélectionner l'option **Access diagnostics shell**.
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

Cette opération supprime tous les volumes Trident dans ONTAP utilisés dans les outils ONTAP pour VMware vSphere 10.1/10.2.

Informations connexes

"Migrez des outils ONTAP pour VMware vSphere 9.x vers la version 10.3"

Codes d'erreur de mise à niveau

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

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

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

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

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

07	firstboot-deploy-otv-ng.pl, mise à niveau, non HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

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

Mettre à niveau le code d'erreur	Workflow	Résolution
068	Échec de la restauration des paquets Debian	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
069	Échec de la restauration des fichiers	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
070	Échec de la suppression de la sauvegarde	-
071	Cluster Kubernetes défectueux	-
074	Echec du montage ISO	Vérifiez le fichier /var/log/upgrade-run.log et réessayez la mise à niveau.
075	Échec des pré-vérifications de mise à niveau	Réessayez la mise à niveau.
076	Échec de la mise à niveau du Registre	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
077	Échec de la restauration du registre	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
078	La mise à niveau de l'opérateur a échoué	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
079	Echec du retour arrière de l'opérateur	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
080	La mise à niveau des services a échoué	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
081	Échec de la restauration des services	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
082	Échec de la suppression des anciennes images du conteneur	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.

083	La suppression de la sauvegarde a échoué	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
084	Echec de la remise en production du JobManager	Suivez les étapes ci-dessous pour récupérer/terminer la mise à niveau. 1. Activer le shell de diagnostic 2. Exécutez la commande : *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 3. Vérifiez les journaux dans /var/log/post-deploy-upgrade.log
087	Échec des étapes post-mise à niveau.	Procédez comme suit pour récupérer/terminer la mise à niveau. 1. Activer le shell de diagnostic 2. Exécutez *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* command 3. Vérifiez les journaux dans /var/log/post-deploy-upgrade.log
088	La configuration de la rotation du journal pour journald a échoué	Vérifiez les paramètres réseau de la machine virtuelle compatibles avec l'hôte sur lequel la machine virtuelle est hébergée. Vous pouvez essayer de migrer la machine virtuelle vers un autre hôte et redémarrer.
089	La modification de la propriété du fichier de configuration de rotation du journal de synthèse a échoué	Réessayez la mise à niveau.
093	La mise à niveau du provisionnement de stockage dynamique a échoué	Réessayez la mise à niveau.
094	Échec de la restauration du mécanisme de provisionnement du stockage dynamique	Réessayez la mise à niveau.
095	Échec de la mise à niveau du se	Aucune récupération pour la mise à niveau du système d'exploitation. Les services d'outils ONTAP sont mis à niveau et de nouveaux pods seront en cours d'exécution.
096	Installer le provisionneur de stockage dynamique	Consultez les journaux de mise à niveau et réessayez la mise à niveau.

097	La désinstallation des services pour la mise à niveau a échoué	Utilisez un RPO nul ou une restauration basée sur des snapshots et réessayez la mise à niveau.
098	échec de la copie du secret dockercred du système ntv vers l'espace de noms du mécanisme de provisionnement de stockage dynamique	Consultez les journaux de mise à niveau et réessayez la mise à niveau.
099	Impossible de valider l'ajout de nouveau disque dur	Ajout du nouveau disque dur à tous les nœuds en cas de haute disponibilité et à un nœud en cas de déploiement non HA
108	Echec du script d'amorçage	-
109	la sauvegarde des données du volume persistant a échoué	Consultez les journaux de mise à niveau et réessayez la mise à niveau.
110	échec de la restauration des données du volume persistant	Utilisez une restauration basée sur des snapshots ou un RPO nul et réessayez la mise à niveau.
111	Échec de la mise à jour des paramètres de délai d'attente d'ETCD pour le RKE2	Consultez les journaux de mise à niveau et réessayez la mise à niveau.
112	La désinstallation du provisionnement de stockage dynamique a échoué	-
113	L'actualisation des ressources sur les nœuds secondaires a échoué	Consultez les journaux de mise à niveau et réessayez la mise à niveau.

Les outils ONTAP pour VMware vSphere 10.3 prennent en charge un RPO nul.

En savoir plus sur "Restauration des outils ONTAP pour VMware vSphere en cas d'échec de la mise à niveau de la version 10.0 vers la version 10.1"

Migrez des outils ONTAP pour VMware vSphere 9.x vers la version 10.3

Lors de la migration des données de stockage, les systèmes back-end sont intégrés manuellement via des API REST. Lors de la migration des données VASA Provider, les données sont exportées de la base de données Derby existante et importées dans la base de données MongoDB.

Vous ne devez migrer les outils ONTAP pour la configuration de VMware vSphere 9.xx que si la configuration gère uniquement la fonctionnalité VASA Provider.

Après la migration des outils ONTAP pour VMware vSphere 9.x vers 10.3, les datastores vVols avec le protocole NVMe/FC ne fonctionnent pas, car les outils ONTAP 10.3 prennent uniquement en charge NVMe-of avec les datastores VMFS.

À propos de cette tâche

Vous pouvez effectuer la migration à partir des outils ONTAP pour VMware vSphere 9.12D1 et 9.13D2 vers la version 10.3.

Vous devez effectuer la sauvegarde OVA de votre version actuelle avant de procéder à la mise à niveau vers les versions de correctifs.

Étapes de migration courantes

1. Déploiement des outils OVA pour ONTAP pour VMware vSphere 10.3.
2. Ajoutez l'instance vCenter Server que vous souhaitez migrer vers les outils ONTAP pour VMware vSphere 10.3. Voir "Ajouter des instances vCenter Server".
3. Intégration locale du système back-end de stockage à partir des outils ONTAP pour les API de serveur vCenter du plug-in VMware vSphere. Ajoutez du stockage en tant que stockage local délimité pour la migration.
4. Les datastores NFS et VMFS migrés depuis les outils ONTAP pour VMware vSphere 9.xx ne sont visibles dans les outils ONTAP pour VMware vSphere 10.3 qu'après le déclenchement de la procédure de détection des datastores, qui peut prendre jusqu'à 30 minutes. Vérifiez si les datastores sont visibles sur la page Présentation des outils ONTAP de la page de l'interface utilisateur du plug-in VMware vSphere.

Étapes de migration SRA

Avant de commencer

Avant la migration, assurez-vous que l'un des sites est protégé et que l'autre est en état de récupération.

Ne migrez pas si le basculement vient d'être terminé et si la protection est en attente. Terminez la re-protection, puis effectuez la migration. Une fois le test du plan de reprise terminé, nettoyez le test de restauration et démarrez la migration.

1. Effectuez les étapes suivantes pour supprimer les outils ONTAP pour VMware vSphere 9.xx version SRA

adapter dans l'interface utilisateur de VMware Live site Recovery :

a. Accédez à la page de gestion de la configuration de VMware Live site Recovery
b. Accédez à la section **Storage Replication adapter**
c. Sélectionnez le menu points de suspension et sélectionnez **Réinitialiser la configuration**
d. Sélectionnez le menu points de suspension et sélectionnez **Supprimer**

Effectuez ces étapes sur les sites de protection et de reprise d'activité.

2. Installez les outils ONTAP pour l'adaptateur VMware vSphere 10.3 SRA sur les sites de protection et de reprise en suivant la procédure décrite à la section "Configurez SRA sur l'appliance VMware Live site Recovery"
3. Sur la page de l'interface utilisateur de VMware Live site Recovery, exécutez les opérations **Discover Arrays** et **Discover Devices** et vérifiez que les périphériques s'affichent comme ils l'étaient avant la migration.

Étapes de migration de VASA Provider

1. Activez le PORT Derby 1527 sur les outils ONTAP existants pour VMware vSphere. Pour activer le port, connectez-vous à l'interface de ligne de commande avec l'utilisateur root et exécutez la commande suivante :

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. Déploiement d'OVA pour les outils ONTAP pour VMware vSphere 10.3.
3. Ajoutez l'instance vCenter Server que vous souhaitez migrer vers les outils ONTAP pour VMware vSphere 10.3. Voir "Ajoutez une instance de vCenter Server".
4. Intégration locale du système back-end de stockage à partir des API de serveur vCenter du plug-in distant. Ajoutez le stockage en tant que périmètre local pour la migration.
5. Émettez l'appel d'API suivant pour migrer :

Méthode HTTP et noeud final

Cet appel d'API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
POST	/api/v1

Type de traitement

Asynchrone

Exemple Curl

/api/v1/vcenters/{vcguid}/migration-jobs

Exemple d'entrée JSON
Corps de la demande pour la migration depuis 9.12 et 9.13 :

{
« otv_ip » : « 10.12.13.45 »,
« vasa_provider_credentials » : {
"username": "vasauser",
"mot de passe" : "**« **
}
"mot_de_passe_base_de_données" : "«
}

Corps de la demande pour une autre migration de version :

{
« otv_ip » : « 10.12.13.45 »,
« vasa_provider_credentials » : {
"username": "vasauser",
"mot de passe" : "** «
}
}

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 »,
« etat » : « en cours »
}

6. Utilisez l'URI suivant pour vérifier l'état :

```
https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobID>?
includeSubJobsAndTasks=true
```

Une fois le travail terminé, validez le rapport de migration. Le rapport fait partie des données du travail et peut être vu à partir de la réponse du travail.

7. Ajoutez les outils ONTAP pour le fournisseur de stockage VMware vSphere au serveur vCenter et "Enregistrez le fournisseur VASA avec une instance vCenter Server".
8. Arrêtez les outils ONTAP du fournisseur de stockage VMware vSphere 9.10/9.11/9.12/9.13 le service VASA Provider depuis la console de maintenance.

   Ne supprimez pas VASA Provider.

   Une fois l'ancien fournisseur VASA arrêté, le serveur vCenter bascule vers les outils ONTAP pour VMware vSphere. Tous les datastores et machines virtuelles sont accessibles et servis à partir des outils ONTAP pour VMware vSphere.

9. Effectuez la migration des correctifs à l'aide de l'API suivante :

Méthode HTTP et noeud final

Cet appel d'API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
CORRECTIF	/api/v1

Type de traitement

Asynchrone

Exemple Curl

PATCH "/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/84dr73bd-9173-65r7-w345-8ufdbb887d43

Exemple d'entrée JSON

{
« id » : 123,
« migration_id » : « d50073ce-35b4-4c51-9d2e-4ce66f802c35 »,
« etat » : « en cours »
}

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 »,
« etat » : « en cours »
}

Le corps de la demande est vide pour l'opération de patch.

uuid est l'uuid de migration renvoyé en réponse à l'API post-migration.

Une fois l'API de migration des correctifs exécutée, toutes les machines virtuelles sont conformes à la stratégie de stockage.

Une fois la migration réussie et après avoir enregistré les outils ONTAP 10.3 sur le serveur vCenter, procédez comme suit :

- Actualisez le certificat sur tous les hôtes.
- Attendez un certain temps avant d'effectuer des opérations de datastore (DS) et de machine virtuelle (VM). Le temps d'attente dépend du nombre d'hôtes, de DS et de VM dans la configuration. Si vous n'attendez pas, les opérations peuvent échouer par intermittence.

Après la fin

Après la mise à niveau, si l'état de conformité de la machine virtuelle est obsolète, réappliquez la stratégie de stockage de la machine virtuelle en procédant comme suit :

1. Naviguez jusqu'au datastore et sélectionnez **Summary** > **VM Storage policies**.

   Sous **conformité de la stratégie de stockage VM**, vous pouvez voir l'état de conformité. Il s'affiche sous la forme **dépassé**

2. Sélectionnez la stratégie Storage VM et la VM correspondante
3. Sélectionnez **appliquer**

   L'état de conformité sous **conformité de la stratégie de stockage VM** est maintenant indiqué comme conforme.

Informations connexes

"Mise à niveau des outils ONTAP pour VMware vSphere 10.x vers la version 10.3"

Automatisation à l’aide de l’API REST

En savoir plus sur les outils ONTAP pour l’API REST VMware vSphere 10

Les outils ONTAP pour VMware vSphere 10 sont un ensemble d’outils destinés à la gestion du cycle de vie des machines virtuelles. Elle comprend une API REST robuste que vous pouvez utiliser dans le cadre de vos processus d’automatisation.

Base de services Web REST

Representational State Transfer (REST) est un style permettant de créer des applications Web distribuées, y compris la conception d’API de services Web. Il établit un ensemble de technologies permettant d’exposer les ressources basées sur les serveurs et de gérer leur état.

Ressources et représentation d’état

Les ressources sont les composants de base d’une application de services Web REST. Lors de la conception d’une API REST, deux tâches initiales sont importantes :

- Identifier les ressources système ou serveur
- Définissez les États de ressource et les opérations de transition d’état associées

Les applications client peuvent afficher et modifier les États de ressources via des flux de messages bien définis.

Messages HTTP

HTTP (HyperText Transfer Protocol) est le protocole utilisé par le client et le serveur de services Web pour échanger des messages sur les ressources. Il suit le modèle CRUD basé sur les opérations génériques de création, lecture, mise à jour et suppression. Le protocole HTTP comprend des en-têtes de requête et de réponse ainsi que des codes d’état de réponse.

Formatage des données JSON

Bien qu’il existe plusieurs formats de message disponibles, l’option la plus populaire est JavaScript Object notation (JSON). JSON est une norme industrielle pour la représentation de structures de données simples en texte brut et sert à transférer des informations d’état décrivant les ressources et les actions souhaitées.

Sécurité

La sécurité est un aspect important des API REST. Outre le protocole TLS (transport Layer Security) utilisé pour protéger le trafic HTTP sur le réseau, les outils ONTAP pour l’API REST VMware vSphere 10 utilisent également des jetons d’accès pour l’authentification. Vous devez acquérir un jeton d’accès et l’utiliser lors des appels API suivants.

Prise en charge des requêtes asynchrones

Les outils ONTAP pour l’API REST VMware vSphere 10 effectuent la plupart des requêtes de manière synchrone, en renvoyant un code d’état une fois l’opération terminée. Il prend également en charge le traitement asynchrone pour les tâches qui nécessitent plus de temps.

Environnement ONTAP Tools Manager

L’environnement ONTAP Tools Manager comporte plusieurs aspects à prendre en compte.

Ordinateur virtuel

Les outils ONTAP pour VMware vSphere 10 sont déployés à l'aide de l'architecture du plug-in à distance vSphere. Le logiciel, y compris la prise en charge de l'API REST, s'exécute sur une machine virtuelle distincte.

Adresse IP des outils ONTAP

Les outils ONTAP pour VMware vSphere 10 exposent une adresse IP unique qui fournit une passerelle vers les fonctionnalités de la machine virtuelle. Vous devez fournir cette adresse lors de la configuration initiale et l'attribuer à un composant d'équilibrage de charge interne. L'adresse est utilisée par l'interface utilisateur du Gestionnaire d'outils ONTAP ainsi que pour accéder directement à la page de documentation swagger et à l'API REST.

Deux API REST

Outre les outils ONTAP pour l'API REST de VMware vSphere 10, le cluster ONTAP dispose de sa propre API REST. Le gestionnaire d'outils ONTAP utilise l'API REST ONTAP en tant que client pour effectuer des tâches liées au stockage. Il est important de garder à l'esprit que ces deux API sont distinctes. Pour plus d'informations, reportez-vous "Automatisation ONTAP"à .

Détails de mise en œuvre des outils ONTAP pour l'API REST VMware vSphere 10

Même si REST établit un ensemble commun de technologies et de bonnes pratiques, l'implémentation exacte de chaque API peut varier en fonction des choix de conception. Vous devez vous familiariser avec la conception préalable des outils ONTAP pour l'API REST VMware vSphere 10.

L'API REST comprend plusieurs catégories de ressources telles que les instances vCenter et les agrégats. Consultez le "Référence API" pour plus d'informations.

Comment accéder à l'API REST

Vous pouvez accéder aux outils ONTAP pour l'API REST VMware vSphere 10 via l'adresse IP de l'équilibreur de charge des outils ONTAP et le port. L'URL complète comprend plusieurs parties, notamment :

- Adresse IP et port des outils ONTAP
- Version API
- Catégorie de ressource
- Ressource spécifique

Vous devez configurer l'adresse IP lors de la configuration initiale et le port est toujours 8443. Par ailleurs, pour une instance spécifique d'outils ONTAP pour VMware vSphere 10, la première partie de l'URL est constante. Seule la catégorie de ressource et la ressource spécifique varient sur les noeuds finaux.

Les valeurs d'adresse IP et de port indiquées dans les exemples ci-dessous sont fournies à titre d'illustration uniquement. Vous devez modifier ces valeurs pour votre environnement.

Exemple d'accès aux services d'authentification

```
https://10.61.25.34:8443/virtualization/api/v1/auth/login
```

Cette URL peut être utilisée pour demander un jeton d'accès à l'aide de la méthode POST.

Exemple de liste des serveurs vCenter

```
https://10.61.25.34:8443/virtualization/api/v1/vcenters
```

Cette URL peut être utilisée pour demander une liste des instances de serveur vCenter définies à l'aide de LA méthode GET.

Détails d'HTTP

Les outils ONTAP pour l'API REST VMware vSphere 10 utilisent le protocole HTTP et les paramètres associés pour agir sur les instances et les collections de ressources. Les détails de l'implémentation HTTP sont présentés ci-dessous.

Méthodes HTTP

Les méthodes HTTP ou verbes pris en charge par l'API REST sont présentées dans le tableau ci-dessous.

Méthode	CRUD	Description
OBTENEZ	Lecture	Récupère les propriétés d'un objet pour une instance ou une collection de ressources. Cette opération est considérée comme une opération de liste lorsqu'elle est utilisée avec une collection.
POST	Créer	Crée une nouvelle instance de ressource basée sur les paramètres d'entrée.
EN	Mise à jour	Met à jour une instance de ressource entière avec le corps de demande JSON fourni. Les valeurs clés qui ne peuvent pas être modifiées par l'utilisateur sont conservées.
CORRECTIF	Mise à jour	Demande l'application d'un ensemble de modifications sélectionnées dans la demande à l'instance de ressource.
SUPPRIMER	Supprimer	Supprime une instance de ressource existante.

En-têtes de demande et de réponse

Le tableau suivant récapitule les en-têtes HTTP les plus importants utilisés avec l'API REST.

En-tête	Type	Remarques sur l'utilisation
Accepter	Demande	Il s'agit du type de contenu que l'application client peut accepter. Les valeurs valides incluent '*/*' ou `application/json`.
x-auth	Demande	Contient un jeton d'accès identifiant l'utilisateur qui émet la demande via l'application client.
Type de contenu	Réponse	Renvoyé par le serveur en fonction de l' `Accept`en-tête de la requête.

Codes d'état HTTP

Les codes d'état HTTP utilisés par l'API REST sont décrits ci-dessous.

Code	Signification	Description
200	OK	Indique la réussite des appels qui ne créent pas une 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 un travail en arrière-plan a été créé pour exécuter la demande.
204	Aucun contenu	La demande a réussi bien qu'aucun contenu n'ait été renvoyé.
400	Demande incorrecte	L'entrée de la demande n'est pas reconnue ou est inappropriée.
401	Non autorisé	L'utilisateur n'est pas autorisé et doit s'authentifier.
403	Interdit	L'accès est refusé en raison d'une erreur d'autorisation.
404	Introuvable	La ressource mentionnée dans la demande n'existe pas.
409	Conflit	La tentative de création d'un objet a échoué car celui-ci existe déjà.
500	Erreur interne	Une erreur interne générale s'est produite sur le serveur.

Authentification

L'authentification d'un client sur l'API REST s'effectue à l'aide d'un jeton d'accès. Les caractéristiques pertinentes du token et du processus d'authentification sont les suivantes :

- Le client doit demander un jeton à l'aide des informations d'identification de l'administrateur du Gestionnaire d'outils ONTAP (nom d'utilisateur et mot de passe).
- Les tokens sont formatés en tant que jeton Web JSON (JWT).
- Chaque jeton expire au bout de 60 minutes.
- Les requêtes API d'un client doivent inclure le token dans l' `x-auth`en-tête de la requête.

Reportez-vous à la "Votre premier appel de l'API REST" pour un exemple de demande et d'utilisation d'un jeton d'accès.

Demandes synchrones et asynchrones

La plupart des appels d'API REST s'effectuent rapidement et s'exécutent donc de manière synchrone. C'est-à-dire qu'ils renvoient un code d'état (tel que 200) après qu'une demande a été traitée. Les requêtes qui prennent plus de temps à effectuer s'exécutent de manière asynchrone à l'aide d'une tâche en arrière-plan.

Après avoir émis un appel API qui s'exécute de manière asynchrone, le serveur renvoie un code d'état HTTP 202. Cela indique que la demande a été acceptée mais pas encore terminée. Vous pouvez interroger le travail en arrière-plan pour déterminer son état, y compris sa réussite ou son échec.

Le traitement asynchrone est utilisé pour plusieurs types d'opérations longues à réaliser, notamment les opérations de datastore et vVol. Pour plus d'informations, reportez-vous à la catégorie Gestionnaire de travaux de l'API REST à la page swagger.

Votre premier appel concernant les outils ONTAP pour l'API REST VMware vSphere 10

Vous pouvez émettre un appel d'API à l'aide de CURL pour commencer à utiliser les outils ONTAP pour l'API REST VMware vSphere 10.

Avant de commencer

Vous devez consulter les informations et les paramètres requis dans les exemples de boucles.

Informations requises

Il faut les éléments suivants :

- Outils ONTAP pour l'adresse IP ou le nom de domaine complet de VMware vSphere 10 ainsi que le port
- Informations d'identification de l'administrateur du Gestionnaire d'outils ONTAP (nom d'utilisateur et mot de passe)

Paramètres et variables

Les exemples de boucles présentés ci-dessous incluent des variables de style Bash. Vous pouvez définir ces variables dans l'environnement Bash ou les mettre à jour manuellement avant d'exécuter les commandes. Si vous définissez les variables, le shell substituera les valeurs dans chaque commande avant de l'exécuter. Les variables sont décrites dans le tableau ci-dessous.

Variable	Description
$FQDN_IP_PORT	Nom de domaine complet ou adresse IP du gestionnaire d'outils ONTAP avec le numéro de port.
$MONUTILISATEUR	Nom d'utilisateur du compte Gestionnaire d'outils ONTAP.
$MYPASSWORD	Mot de passe associé au nom d'utilisateur du Gestionnaire d'outils ONTAP.
$ACCESS_TOKEN	Jeton d'accès émis par le gestionnaire d'outils ONTAP.

Les commandes et résultats suivants au niveau de l'interface de ligne de commande Linux illustrent comment une variable peut être définie et affichée :

```
FQDN_IP_PORT=172.14.31.224:8443
echo $FQDN_IP
172.14.31.224:8443
```

Étape 1 : acquérir un jeton d'accès

Vous devez acquérir un jeton d'accès pour utiliser l'API REST. Un exemple de demande de jeton d'accès est présenté ci-dessous. Vous devez remplacer les valeurs appropriées pour votre environnement.

```
curl --request POST \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/login” \
--header "Content-Type: application/json" \
--header "Accept: */*" \
-d "{"username": "$MYUSER", "password": "$MYPASSWORD"}"
```

Copiez et enregistrez le jeton d’accès fourni dans la réponse.

Étape 2 : lancez l’appel de l’API REST

Après avoir un jeton d’accès, vous pouvez utiliser curl pour émettre un appel API REST. Incluez le jeton d’accès acquis dans la première étape.

Exemple de boucle

```
curl --request GET \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/vcenters" \
--header "Accept: */*" \
--header "x-auth: $ACCESS_TOKEN"
```

La réponse JSON inclut une liste des instances VMware vCenter configurées pour le gestionnaire d’outils ONTAP.

Référence des API pour les outils ONTAP pour l’API REST VMware vSphere 10

La référence des outils ONTAP pour l’API REST VMware vSphere 10 contient des détails sur tous les appels d’API. Cette référence est utile lors du développement d’applications d’automatisation.

Vous pouvez accéder à la documentation en ligne des outils ONTAP pour l’API REST de VMware vSphere 10 via l’interface utilisateur swagger. Vous avez besoin de l’adresse IP ou du nom de domaine complet des outils ONTAP pour le service de passerelle VMware vSphere 10 ainsi que du port.

Étapes

1. Tapez l’URL suivante dans votre navigateur en remplaçant l’adresse IP et la combinaison de ports appropriés par la variable et appuyez sur **entrée**.

   `https://$FQDN_IP_PORT/`

   Exemple

   `https://10.61.25.33:8443/`

2. Comme exemple d’appel d’API individuel, faites défiler jusqu’à la catégorie **vCenters** et sélectionnez **OBTENIR** en regard du noeud final `/virtualization/api/v1/vcenters`

Mentions légales

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

Droits d’auteur

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

Marques déposées

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

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

Brevets

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

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

Politique de confidentialité

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

Source ouverte

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

"Avis concernant les outils ONTAP pour VMware vSphere 10.3"

Informations sur le copyright

Informations sur les marques commerciales