



Concepts

ONTAP tools for VMware vSphere 9.10

NetApp
January 18, 2024

Sommaire

- Concepts 1
 - Présentation des outils ONTAP 1
 - Configurations de VASA Provider pour vvol 2
 - Configurer la configuration de la reprise après incident 4
 - Contrôle d'accès basé sur des rôles 4
 - Configuration de la haute disponibilité des outils ONTAP 13
 - Configurations MetroCluster prises en charge par les outils ONTAP 15

Concepts

Présentation des outils ONTAP

Les outils ONTAP pour VMware vSphere offrent une gestion du cycle de vie de bout en bout des ordinateurs virtuels dans des environnements VMware qui utilisent des systèmes de stockage NetApp. Il simplifie la gestion des données et du stockage des environnements VMware en permettant aux administrateurs de gérer directement le stockage au sein du serveur vCenter.

Avec vSphere 6.5, VMware a introduit un nouveau client basé sur HTML5 appelé vSphere client. Les versions 9.6 et ultérieures des outils ONTAP ne prennent en charge que le client vSphere. Les outils ONTAP s'intègrent au client vSphere et vous permettent d'utiliser des services SSO. Dans un environnement comportant plusieurs instances vCenter Server, chaque instance vCenter Server à gérer doit disposer de sa propre instance enregistrée de VSC.

Chaque composant des outils ONTAP offre des fonctionnalités qui vous aident à gérer votre stockage plus efficacement.

Virtual Storage Console (VSC).

VSC vous permet d'effectuer les tâches suivantes :

- Ajoutez des contrôleurs de stockage, attribuez des informations d'identification et configurez les autorisations pour les contrôleurs de stockage VSC, que SRA et VASA Provider peuvent exploiter
- Provisionner les datastores
- Surveiller les performances des datastores et des machines virtuelles de l'environnement vCenter Server
- Contrôler l'accès de l'administrateur aux objets vCenter Server à l'aide du contrôle d'accès basé sur des rôles (RBAC) à deux niveaux :

- Objets vSphere, tels que des machines virtuelles et des datastores

Ces objets sont gérés à l'aide du RBAC de vCenter Server.

- Le stockage ONTAP

Les systèmes de stockage sont gérés à l'aide du RBAC de ONTAP.

- Afficher et mettre à jour les paramètres d'hôte des hôtes ESXi connectés au système de stockage NetApp

Les opérations de provisionnement VSC tirent parti du plug-in NFS pour les API VMware vStorage for Array Integration (VAAI). Le plug-in NFS pour VAAI est une bibliothèque logicielle qui intègre les bibliothèques de disques virtuels VMware installées sur l'hôte ESXi. Le package VMware VAAI permet de décharger certaines tâches des hôtes physiques vers la baie de stockage. Vous pouvez effectuer des tâches telles que le provisionnement fin et l'accélération matérielle au niveau de la baie afin de réduire la charge de travail sur les hôtes ESXi. La fonctionnalité de déchargement de copies et de réservation d'espace améliorent les performances des opérations VSC.

Le plug-in NetApp NFS pour VAAI n'est pas fourni avec VSC. Vous pouvez cependant télécharger le pack d'installation du plug-in et obtenir les instructions d'installation du plug-in sur le site de support NetApp.

Vasa Provider

Vasa Provider pour ONTAP utilise les API VMware vSphere pour Storage Awareness (VASA) pour envoyer des informations sur le stockage utilisé par VMware vSphere vers vCenter Server. Vasa Provider est intégré aux outils ONTAP. Vasa Provider permet d'effectuer les tâches suivantes :

- Provisionnez les datastores VMware Virtual volumes (vvols)
- Créez des profils de capacité de stockage qui définissent différents objectifs de niveau de service (SLO) pour votre environnement
- Vérifiez la conformité entre les datastores et les profils de capacité de stockage
- Définissez des alarmes pour vous avertir lorsque les volumes et les agrégats approchent des limites de seuil
- Surveillez les performances des disques virtuels (VMDK) et des machines virtuelles créées dans les datastores vvols

Si vous utilisez ONTAP 9.6 ou une version antérieure, VASA Provider communique avec vCenter Server à l'aide des API VASA et communique avec ONTAP à l'aide d'API NetApp appelées ZAPI. Pour afficher le tableau de bord vvols pour ONTAP 9.6 et les versions antérieures, vous devez avoir installé et enregistré les services API OnCommand dans votre serveur vCenter. Si vous utilisez ONTAP 9.7 et versions ultérieures, vous n'avez pas besoin d'enregistrer les services d'API OnCommand avec VASA Provider pour afficher le tableau de bord vvols.



Pour ONTAP 9.6 et versions antérieures, VASA Provider requiert une instance dédiée des services d'API OnCommand. Une instance de services d'API OnCommand ne peut pas être partagée avec plusieurs instances de VASA Provider.

Storage Replication adapter (SRA)

Lorsque SRA est activé et utilisé conjointement avec VMware Site Recovery Manager (SRM), vous pouvez restaurer les datastores vCenter Server et les machines virtuelles en cas de défaillance. SRA vous permet d'utiliser la réplication basée sur les baies (ABR) pour les sites protégés et les sites de reprise après incident en cas de défaillance.

Informations connexes

["Support NetApp"](#)

Configurations de VASA Provider pour vvols

Vous pouvez utiliser VASA Provider pour ONTAP pour créer et gérer des volumes virtuels VMware (vvols). Vous pouvez provisionner, modifier, monter et supprimer un datastore vvols. Vous pouvez également ajouter du stockage au datastore vvols ou supprimer du stockage du datastore vvols. pour plus de flexibilité. Vous pouvez provisionner et gérer chaque machine virtuelle et le VMDK associé.

Un datastore vvols est constitué d'un ou plusieurs volumes FlexVol au sein d'un container de stockage (également appelé « sauvegarde de stockage »). Une machine virtuelle peut être répartie entre un datastore vvols ou plusieurs datastores vvols.

Vous pouvez créer un datastore vvols comprenant plusieurs volumes FlexVol. Toutefois, tous les volumes

FlexVol du conteneur de stockage doivent utiliser le même protocole (NFS, iSCSI ou FCP) et les mêmes serveurs virtuels de stockage (SVM).

Vous ne devez pas avoir de connaissances détaillées sur le stockage sous-jacent. Par exemple, vous n'avez pas besoin d'identifier un volume FlexVol spécifique pour contenir le stockage. Une fois que vous avez ajouté des volumes FlexVol dans le datastore vvol, le conteneur de stockage gère les exigences de stockage et prévient toutes les situations lors du provisionnement de machines virtuelles, où VMware a provisionné dans un volume de sauvegarde sans capacité.



Il est recommandé d'inclure plusieurs volumes FlexVol dans un datastore vvol pour davantage de performances et de flexibilité. Les volumes FlexVol étant soumis à des restrictions de nombre de LUN qui limitent le nombre de machines virtuelles, y compris plusieurs volumes FlexVol, vous pouvez stocker davantage de machines virtuelles dans votre datastore vVols.

Dans le cadre du processus de configuration, vous devez spécifier un profil de capacité de stockage pour le datastore vvol que vous créez. Vous pouvez sélectionner un ou plusieurs profils de capacité de stockage VASA Provider pour un datastore vvol. Vous pouvez également spécifier un profil de capacité de stockage par défaut pour tous les datastores vvol qui sont automatiquement créés dans ce conteneur de stockage.

Vasa Provider crée différents types de vvol lors du provisionnement de machine virtuelle ou de la création de VMDK, selon les besoins.

- **Config**

VMware vSphere utilise ce datastore vvol pour stocker des informations de configuration.

Dans les implémentations SAN (bloc), le stockage correspond à une LUN de 4 Go.

Dans une implémentation NFS, il s'agit d'un répertoire contenant les fichiers de configuration de VM tels que le fichier vmx et les pointeurs vers d'autres datastores vVols.

- **Données**

Ce vVols contient des informations sur le système d'exploitation et des fichiers utilisateur.

Dans les implémentations SAN, il s'agit d'une LUN de la taille du disque virtuel.

Dans une implémentation NFS, il s'agit d'un fichier de la taille du disque virtuel.

Pour chaque volume de données NFS vvol provisionné sur les clusters ONTAP versions 9.8 et ultérieures, tous les fichiers VMDK sont enregistrés à des fins de surveillance des metrics de performance tels que les IOPS, le débit et la latence.

- **Permuter**

Ce vvol est créé lorsque la machine virtuelle est mise sous tension et est supprimé lors de la mise hors tension de la machine virtuelle.

Dans les implémentations SAN, il s'agit d'une LUN de la taille de la mémoire virtuelle.

Dans une implémentation NFS, il s'agit d'un fichier de la taille de la mémoire virtuelle.

- **Mémoire**

Ce vVols est créé si l'option snapshots de mémoire est sélectionnée lors de la création de snapshots de

VM.

Dans les implémentations SAN, il s'agit d'une LUN de la taille de la mémoire virtuelle.

Dans une implémentation NFS, il s'agit d'un fichier de la taille de la mémoire virtuelle.

Configurer la configuration de la reprise après incident

Vous pouvez créer et gérer la configuration de la reprise après incident dans vCenter Server avec SRM (site Recovery Manager) de VMware.

Vasa Provider intègre désormais les fonctionnalités de Storage Replication adapter (SRA). Si vous avez configuré des datastores vvol dans votre datacenter, alors pour la restauration de datastores vvol, il n'est pas nécessaire d'installer SRA séparément pour la reprise après incident. Dans site Recovery Manager (SRM), vous devez coupler les sites protégés et de reprise. Une fois le couplage du site effectué, la partie suivante de la configuration SRM implique la configuration d'une paire de matrices qui permet à SRM de communiquer avec le système de stockage pour détecter les périphériques et la réplication des périphériques. Avant de pouvoir configurer la paire de matrices, vous devez d'abord créer une paire de sites dans SRM.

Cette version des outils ONTAP vous offre la possibilité d'utiliser la configuration SnapMirror synchrone pour la reprise après incident.



VMware site Recovery Manager (SRM) n'utilise pas SRA pour la gestion de la reprise après incident des datastores vVols. Au contraire, VASA Provider est utilisé pour la réplication et le contrôle de basculement des datastores vvol sur des clusters ONTAP 9.7 et versions ultérieures.

["Activez Storage Replication adapter"](#)

Contrôle d'accès basé sur des rôles

Présentation du contrôle d'accès basé sur des rôles dans les outils ONTAP

vCenter Server fournit un contrôle d'accès basé sur des rôles (RBAC) qui vous permet de contrôler l'accès aux objets vSphere. Dans les outils ONTAP® pour VMware vSphere, vCenter Server RBAC fonctionne avec le RBAC ONTAP pour déterminer quelles tâches VSC un utilisateur spécifique peut effectuer sur des objets d'un système de stockage spécifique.

Pour réussir une tâche, vous devez disposer des autorisations appropriées pour le contrôle d'accès basé sur les rôles du serveur vCenter. Lors d'une tâche, VSC vérifie les autorisations vCenter Server d'un utilisateur avant de vérifier les privilèges ONTAP de l'utilisateur.

Vous pouvez définir les autorisations de vCenter Server sur l'objet racine (également appelé dossier racine). Vous pouvez ensuite affiner la sécurité en limitant les entités enfants qui n'ont pas besoin de ces autorisations.

Composants des autorisations de vCenter Server

vCenter Server reconnaît les autorisations et non les privilèges. Chaque autorisation vCenter Server comprend trois composants.

VCenter Server dispose des composants suivants :

- Un ou plusieurs privilèges (le rôle)

Les privilèges définissent les tâches qu'un utilisateur peut effectuer.

- Un objet vSphere

L'objet est la cible des tâches.

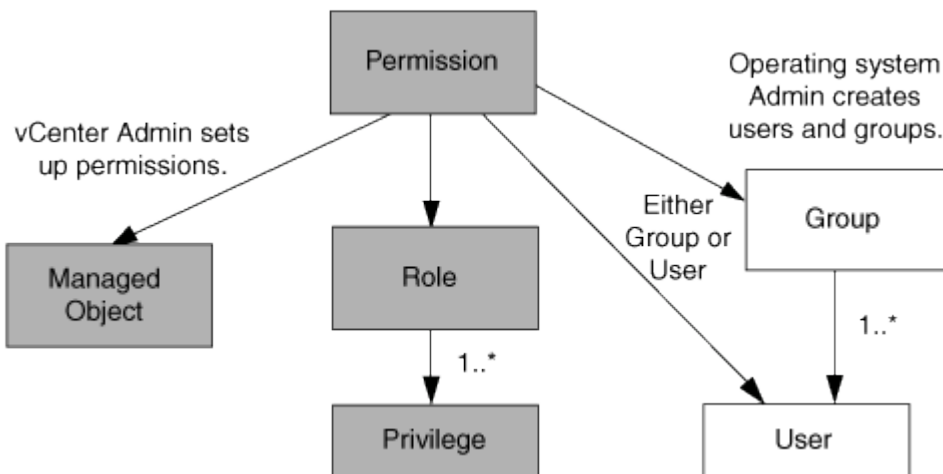
- Un utilisateur ou un groupe

L'utilisateur ou le groupe définit qui peut effectuer la tâche.

Comme le montre le diagramme suivant, vous devez disposer des trois éléments pour avoir une autorisation.



Dans ce diagramme, les cases grises indiquent les composants qui existent dans vCenter Server et les cases blanches indiquent les composants qui existent dans le système d'exploitation où le serveur vCenter est exécuté.



Privilèges

Deux types de privilèges sont associés aux outils ONTAP pour VMware vSphere :

- Privilèges de serveur vCenter natif

Ces privilèges sont fournis avec vCenter Server.

- Privilèges spécifiques à VSC

Ces privilèges sont définis pour des tâches VSC spécifiques. Ils sont uniques à VSC.

Les tâches VSC requièrent à la fois des privilèges spécifiques à VSC et des privilèges natifs vCenter Server. Ces privilèges constituent le « rôle » pour l'utilisateur. Une autorisation peut avoir plusieurs privilèges. Ces privilèges concernent un utilisateur connecté à vCenter Server.



Pour simplifier l'utilisation du contrôle d'accès basé sur des rôles vCenter Server, VSC fournit plusieurs rôles standard contenant tous les privilèges natifs et spécifiques de VSC requis pour effectuer des tâches VSC.

Si vous modifiez les privilèges dans une autorisation, l'utilisateur associé à cette autorisation doit se déconnecter, puis se connecter pour activer l'autorisation mise à jour.

Privilège	Rôles	Tâches
Console des outils NetApp ONTAP > Afficher	<ul style="list-style-type: none">Administrateur VSCProvisionnement VSCVSC en lecture seule	Toutes les tâches spécifiques à VSC et VASA Provider requièrent le privilège View.
NetApp Virtual Storage Console > gestion basée sur des règles > gestion ou <code>privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label > gestion</code>	Administrateur VSC	Tâches VSC et VASA Provider associées aux profils de fonctionnalité de stockage et aux paramètres de seuil.

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. Vous pouvez attribuer des autorisations à n'importe quel objet vSphere. En fonction de l'autorisation attribuée à un objet vSphere, vCenter Server détermine qui peut effectuer les tâches sur cet objet. Pour les tâches VSC spécifiques, les autorisations sont attribuées et validées uniquement au niveau du dossier racine (vCenter Server) et non sur toute autre entité. Sauf pour le fonctionnement du plug-in VAAI, où les autorisations sont validées par rapport à l'ESXi concerné.

Utilisateurs et groupes

Vous pouvez utiliser Active Directory (ou la machine vCenter Server locale) pour configurer des utilisateurs et des groupes d'utilisateurs. Vous pouvez ensuite utiliser les autorisations de vCenter Server pour accorder l'accès à ces utilisateurs ou groupes afin de leur permettre d'effectuer des tâches VSC spécifiques.



Ces autorisations vCenter Server s'appliquent aux utilisateurs de VSC vCenter, et non aux administrateurs VSC. Par défaut, les administrateurs VSC disposent d'un accès complet au produit et ne requièrent pas l'autorisation qui leur est attribuée.

Les utilisateurs et les groupes n'ont pas de rôles qui leur sont attribués. Ils ont accès à un rôle en faisant partie de l'autorisation vCenter Server.

Points clés concernant l'attribution et la modification des autorisations pour vCenter Server

Lorsque vous travaillez avec des autorisations vCenter Server, vous devez garder à l'esprit plusieurs points clés. La réussite d'une tâche d'outils ONTAP pour VMware vSphere peut dépendre de l'endroit où vous avez attribué une autorisation ou des actions qu'un utilisateur a effectuées après la modification d'une autorisation.

Attribution d'autorisations

Vous n'avez besoin de configurer les autorisations vCenter Server que si vous souhaitez limiter l'accès aux objets et aux tâches vSphere. Sinon, vous pouvez vous connecter en tant qu'administrateur. Cette connexion vous permet automatiquement d'accéder à tous les objets vSphere.

L'endroit où vous attribuez une autorisation détermine les tâches VSC que l'utilisateur peut effectuer.

Parfois, pour assurer la réalisation d'une tâche, vous devez attribuer l'autorisation à un niveau supérieur, tel que l'objet racine. C'est le cas lorsqu'une tâche nécessite un privilège qui ne s'applique pas à un objet vSphere spécifique (par exemple, le suivi de la tâche) ou lorsqu'un privilège requis s'applique à un objet non vSphere (par exemple, un système de stockage).

Dans ce cas, vous pouvez configurer une autorisation de sorte qu'elle soit héritée par les entités enfants. Vous pouvez également attribuer d'autres autorisations aux entités enfants. La permission attribuée à une entité enfant remplace toujours l'autorisation héritée de l'entité parent. Cela signifie que vous pouvez autoriser une entité enfant pour restreindre la portée d'une autorisation qui a été attribuée à un objet racine et héritée par l'entité enfant.



À moins que les règles de sécurité de votre entreprise ne nécessitent des autorisations plus restrictives, il est conseillé d'attribuer des autorisations à l'objet racine (également appelé dossier racine).

Autorisations et objets non vSphere

L'autorisation que vous créez est appliquée à un objet non vSphere. Par exemple, un système de stockage n'est pas un objet vSphere. Si un privilège s'applique à un système de stockage, vous devez attribuer l'autorisation contenant ce privilège à l'objet racine VSC car aucun objet vSphere ne peut être affecté.

Par exemple, toute autorisation incluant un privilège tel que le privilège VSC « Add/Modify/Skip Storage Systems » doit être attribuée au niveau de l'objet racine.

Modification des autorisations

Vous pouvez modifier une autorisation à tout moment.

Si vous modifiez les privilèges dans une autorisation, l'utilisateur associé à cette autorisation doit se déconnecter puis se reconnecter pour activer l'autorisation mise à jour.

Rôles standard fournis avec les outils ONTAP

Pour simplifier la utilisation des privilèges vCenter Server et du contrôle d'accès basé sur des rôles (RBAC), Virtual Storage Console (VSC) propose des rôles VSC standard qui vous permettent d'effectuer des tâches VSC clés. Il existe également un rôle en lecture seule qui vous permet de consulter les informations de VSC, mais ne pas effectuer de tâches.

Les rôles VSC standard disposent à la fois des privilèges spécifiques à VSC et des privilèges vCenter Server natifs requis pour que les utilisateurs puissent effectuer des tâches VSC. En outre, les rôles sont configurés de manière à disposer des privilèges requis pour toutes les versions prises en charge de vCenter Server.

En tant qu'administrateur, vous pouvez attribuer ces rôles aux utilisateurs selon les besoins.



Lorsque vous mettez à niveau VSC vers la dernière version, les rôles standard sont automatiquement mis à niveau pour fonctionner avec la nouvelle version de VSC.

Vous pouvez afficher les rôles standard VSC en cliquant sur **Rôles** sur la page d'accueil du client vSphere.

Les rôles décrits dans VSC vous permettent d'effectuer les tâches suivantes :

Rôle	Description
Administrateur VSC	Fournit tous les privilèges vCenter Server natifs et les privilèges spécifiques à VSC requis pour effectuer toutes les tâches VSC.
VSC en lecture seule	Fournit un accès en lecture seule à VSC. Ces utilisateurs ne peuvent pas effectuer d'actions VSC contrôlées par l'accès.
Provisionnement VSC	Fournit tous les privilèges vCenter Server natifs et les privilèges spécifiques à VSC requis pour le provisionnement du stockage. Vous pouvez effectuer les tâches suivantes : <ul style="list-style-type: none">• Créer de nouveaux datastores• Détruire les datastores• Afficher des informations sur les profils de capacité de stockage

Instructions d'utilisation des rôles standard VSC

Lorsque vous utilisez les outils ONTAP standard pour les rôles VMware vSphere, vous devez suivre certaines directives.

Vous ne devez pas modifier directement les rôles standard. Si vous le faites, VSC remplacera vos modifications à chaque fois que vous mettez à niveau VSC. À chaque mise à niveau de VSC, le programme d'installation met à jour les définitions de rôles standard. Vous êtes ainsi assuré que les rôles sont à jour pour votre version de VSC et pour toutes les versions prises en charge de vCenter Server.

Vous pouvez toutefois utiliser les rôles standard pour créer des rôles adaptés à votre environnement. Pour ce faire, vous devez copier le rôle standard VSC, puis modifier le rôle copié. En créant un nouveau rôle, vous pouvez le conserver même lorsque vous redémarrez ou mettez à niveau le service Windows VSC.

Les rôles standard de VSC comme vous le souhaitez peuvent être utilisés comme suit :

- Utilisation des rôles standard VSC pour toutes les tâches VSC.

Dans ce scénario, les rôles standard fournissent tous les privilèges dont l'utilisateur a besoin pour effectuer les tâches VSC.

- Associer des rôles pour développer les tâches qu'un utilisateur peut effectuer.

Si les rôles standard VSC fournissent une granularité trop importante pour votre environnement, vous pouvez développer les rôles en créant des groupes de niveau supérieur contenant plusieurs rôles.

Si un utilisateur doit effectuer d'autres tâches non VSC qui nécessitent des privilèges vCenter Server natifs supplémentaires, vous pouvez créer un rôle qui fournit ces privilèges et l'ajouter au groupe également.

- Créer des rôles plus précis.

Si votre entreprise exige que vous implémentiez des rôles plus restrictifs que les rôles VSC standard, vous pouvez utiliser les rôles VSC pour créer de nouveaux rôles.

Dans ce cas, vous clonez les rôles VSC nécessaires, puis modifiez le rôle cloné de sorte que celui-ci dispose uniquement des privilèges dont l'utilisateur a besoin.

Privilèges requis pour les tâches VSC

Les différents outils ONTAP pour les tâches VMware vSphere requièrent différentes combinaisons de privilèges spécifiques à Virtual Storage Console (VSC) et vCenter Server natif.

Pour plus d'informations sur les privilèges requis pour les tâches VSC, consultez l'article 1032542 de la base de connaissances NetApp.

["Comment configurer le RBAC pour Virtual Storage Console"](#)

Privilège au niveau du produit requis par les outils ONTAP pour VMware vSphere

Pour accéder aux outils ONTAP pour l'interface utilisateur graphique VMware vSphere, vous devez disposer du privilège de vue spécifique au produit (VSC) attribué au niveau de l'objet vSphere correct. Si vous vous connectez sans ce privilège, VSC affiche un message d'erreur lorsque vous cliquez sur l'icône NetApp et vous empêche d'accéder à VSC.

Les informations suivantes décrivent le privilège VSC Product-Level View :

Privilège	Description	Niveau d'affectation
Afficher	Vous pouvez accéder à l'interface graphique de VSC. Ce privilège ne vous permet pas d'effectuer des tâches dans VSC. Pour effectuer toutes les tâches VSC, vous devez disposer des privilèges vCenter Server natifs et spécifiques à VSC pour ces tâches.	<p>Le niveau d'affectation détermine les parties de l'interface utilisateur que vous pouvez voir. L'attribution du privilège View (View) à l'objet racine (dossier) vous permet d'entrer dans VSC en cliquant sur l'icône NetApp.</p> <p>Vous pouvez attribuer le privilège View à un autre niveau d'objets vSphere. Toutefois, vous pouvez limiter les menus VSC que vous pouvez voir et utiliser.</p> <p>L'objet racine est l'endroit recommandé pour attribuer une autorisation contenant le privilège d'affichage.</p>

Autorisations pour les systèmes de stockage ONTAP et les objets vSphere

Le contrôle d'accès basé sur des rôles (RBAC) de ONTAP vous permet de contrôler l'accès aux systèmes de stockage spécifiques et de contrôler les actions qu'un utilisateur peut effectuer sur ces systèmes. Dans les outils ONTAP® pour VMware vSphere, le contrôle d'accès basé sur les rôles (RBAC) de ONTAP fonctionne avec vCenter Server RBAC pour déterminer quelles tâches VSC (Virtual Storage Console) un utilisateur spécifique peut effectuer sur les objets d'un système de stockage spécifique.

VSC utilise les identifiants (nom d'utilisateur et mot de passe) que vous configurez dans VSC afin d'authentifier chaque système de stockage et de déterminer les opérations de stockage pouvant être effectuées sur ce système de stockage. VSC utilise un ensemble d'identifiants pour chaque système de stockage. Ces identifiants déterminent quelles tâches VSC peuvent être effectuées sur ce système de stockage. En d'autres termes, les identifiants sont utilisés pour VSC et non pour un utilisateur VSC.

Le contrôle d'accès basé sur des rôles (RBAC) ONTAP ne s'applique qu'à l'accès aux systèmes de stockage et aux tâches VSC liées au stockage, comme le provisionnement de machines virtuelles. Si vous ne disposez pas des privilèges ONTAP RBAC appropriés pour un système de stockage spécifique, vous ne pouvez pas effectuer de tâches sur un objet vSphere hébergé sur ce système de stockage. Vous pouvez utiliser le contrôle d'accès basé sur des rôles ONTAP associé aux privilèges spécifiques de VSC afin de contrôler les tâches VSC que un utilisateur peut effectuer :

- Surveillance et configuration d'objets de stockage ou vCenter Server résidant sur un système de stockage
- Provisionnement d'objets vSphere résidant sur un système de stockage

L'utilisation du contrôle d'accès basé sur des rôles (RBAC) ONTAP avec les privilèges spécifiques de VSC fournit une couche de sécurité orientée stockage que l'administrateur du stockage peut gérer. Par conséquent, le contrôle d'accès est plus granulaire que ce que vous ne pouvez prendre en charge que le RBAC ONTAP seul ou le RBAC vCenter Server. Par exemple, avec le RBAC de vCenter Server, vous pouvez permettre à vCenter UserB de provisionner un datastore sur le stockage NetApp tout en empêchant vCenter UserA de provisionner des datastores. Si les informations d'identification du système de stockage pour un système de stockage spécifique ne prennent pas en charge la création de stockage, ni vCenter UserB ni vCenter UserA ne peuvent provisionner un datastore sur ce système de stockage.

Lorsque vous lancez une tâche VSC, VSC vérifie d'abord si vous disposez de l'autorisation vCenter Server appropriée pour cette tâche. Si l'autorisation de vCenter Server n'est pas suffisante pour vous permettre d'effectuer la tâche, VSC n'a pas besoin de vérifier les privilèges ONTAP de ce système de stockage car vous n'avez pas réussi le contrôle de sécurité initial du serveur vCenter. Dans ce cas, vous ne pouvez pas accéder au système de stockage.

Si l'autorisation vCenter Server est suffisante, VSC vérifie alors les privilèges RBAC ONTAP (votre rôle ONTAP) associés aux informations d'identification du système de stockage (nom d'utilisateur et mot de passe) Pour déterminer si vous disposez de privilèges suffisants pour exécuter les opérations de stockage requises par la tâche VSC sur ce système de stockage. Si vous disposez des privilèges ONTAP appropriés, vous pouvez accéder au système de stockage et effectuer la tâche VSC. Les rôles ONTAP déterminent les tâches VSC que vous pouvez effectuer sur le système de stockage.

Chaque système de stockage dispose d'un ensemble de privilèges ONTAP qui lui sont associés.

L'utilisation de RBAC ONTAP et du RBAC vCenter Server offre les avantages suivants :

- Sécurité

L'administrateur peut déterminer les utilisateurs qui peuvent effectuer les tâches au niveau objet précis de vCenter Server et au niveau du système de stockage.

- Informations d'audit

Dans de nombreux cas, VSC fournit une piste d'audit sur le système de stockage, qui vous permet de suivre les événements vers l'utilisateur vCenter Server qui a effectué les modifications du stockage.

- Facilité d'utilisation

Vous pouvez conserver toutes les informations d'identification du contrôleur en un seul emplacement.

Rôles ONTAP recommandés pour l'utilisation des outils ONTAP pour VMware vSphere

Vous pouvez configurer plusieurs rôles ONTAP recommandés pour utiliser les outils ONTAP® pour VMware vSphere et le contrôle d'accès basé sur les rôles (RBAC). Ces rôles disposent des privilèges ONTAP requis pour effectuer les opérations de stockage requises exécutées par les tâches Virtual Storage Console (VSC).

Pour créer de nouveaux rôles utilisateur, vous devez vous connecter en tant qu'administrateur sur les systèmes de stockage exécutant ONTAP. Vous pouvez créer des rôles ONTAP à l'aide de l'une des options suivantes :

- ONTAP System Manager 9.8P1 ou version ultérieure

["Configurez les rôles et privilèges utilisateur"](#)

- Créateur d'utilisateurs RBAC pour l'outil ONTAP (si vous utilisez ONTAP 9.6 ou une version antérieure)

Chaque rôle ONTAP est associé à un nom d'utilisateur et une paire de mots de passe qui constituent les identifiants du rôle. Si vous ne vous connectez pas à l'aide de ces informations d'identification, vous ne pouvez pas accéder aux opérations de stockage associées au rôle.

Par mesure de sécurité, les rôles ONTAP spécifiques à VSC sont classés par ordre hiérarchique. Le premier rôle est donc le rôle le plus restrictif et ne dispose que de privilèges associés à un ensemble d'opérations de stockage VSC de base. Le rôle suivant inclut à la fois ses propres privilèges et tous les privilèges associés au rôle précédent. Chaque rôle supplémentaire est moins restrictif en termes de limites au niveau des opérations de stockage prises en charge.

Voici certains des rôles RBAC ONTAP recommandés lors de l'utilisation de VSC. Une fois ces rôles créés, vous pouvez attribuer les rôles aux utilisateurs qui doivent effectuer des tâches associées au stockage, par exemple le provisionnement de machines virtuelles.

1. Détection

Il permet donc d'ajouter des systèmes de stockage.

2. Créer un stockage

Grâce à ce rôle, vous pouvez créer du stockage. Ce rôle inclut également l'ensemble des privilèges associés au rôle découverte.

3. Modifier le stockage

Ce rôle vous permet de modifier le stockage. Ce rôle inclut également tous les privilèges associés au rôle découverte et au rôle Créer un stockage.

4. Détruire le stockage

Vous pouvez ainsi détruire le stockage. Ce rôle inclut également tous les privilèges associés au rôle découverte, au rôle Créer un stockage et au rôle Modifier le stockage.

Si vous utilisez VASA Provider pour ONTAP, vous devez également définir un rôle de gestion basée sur des règles (PBM). Il permet de gérer le stockage à l'aide de règles de stockage. Ce rôle requiert également que vous ayez défini le rôle « questions à poser ».

Configuration du contrôle d'accès basé sur des rôles ONTAP pour les outils ONTAP pour VMware vSphere

Vous devez configurer le contrôle d'accès basé sur des rôles (RBAC) ONTAP sur le système de stockage si vous souhaitez utiliser le contrôle d'accès basé sur des rôles avec les outils ONTAP pour VMware vSphere. Vous pouvez créer un ou plusieurs comptes utilisateur personnalisés avec des privilèges d'accès limités grâce à la fonction RBAC ONTAP.

VSC et SRA peuvent accéder aux systèmes de stockage au niveau du cluster ou de la machine virtuelle de stockage (SVM)SVM. Si vous ajoutez des systèmes de stockage au niveau du cluster, vous devez fournir les identifiants de l'utilisateur admin pour fournir toutes les fonctionnalités requises. Si vous ajoutez des systèmes de stockage en ajoutant directement des détails SVM, vous devez savoir que l'utilisateur « vsadmin » n'a pas tous les rôles et les fonctionnalités nécessaires pour effectuer certaines tâches.

Vasa Provider ne peut accéder aux systèmes de stockage qu'au niveau du cluster. Si VASA Provider est requis pour un contrôleur de stockage spécifique, le système de stockage doit être ajouté à VSC au niveau du cluster, même si vous utilisez VSC ou SRA.

Pour créer un nouvel utilisateur et connecter un cluster ou un SVM aux outils ONTAP, il faut effectuer les opérations suivantes :

- Créer un administrateur de cluster ou un rôle d'administrateur SVM



Pour créer ces rôles, vous pouvez utiliser l'une des méthodes suivantes :

- ONTAP System Manager 9.8P1 ou version ultérieure

["Configurez les rôles et privilèges utilisateur"](#)

- Créateur d'utilisateurs RBAC pour l'outil ONTAP (si vous utilisez ONTAP 9.6 ou une version antérieure)
- Créez des utilisateurs avec le rôle attribué et le jeu d'applications approprié à l'aide de ONTAP

Ces identifiants sont nécessaires pour configurer les systèmes de stockage pour VSC. Vous pouvez configurer les systèmes de stockage pour VSC en saisissant les identifiants dans VSC. Chaque fois que vous vous connectez à un système de stockage avec ces identifiants, vous disposez d'autorisations pour accéder aux fonctions VSC que vous avez configurées dans ONTAP lors de la création des identifiants.

- Ajoutez le système de stockage à VSC et fournissez les identifiants de l'utilisateur que vous venez de créer

Rôles VSC

VSC classe les privilèges ONTAP en fonction de l'ensemble des rôles VSC suivants :

- Détection

Permet la détection de tous les contrôleurs de stockage connectés

- Créer un stockage

Création de volumes et de LUN

- Modifier le stockage

Permet le redimensionnement et la déduplication des systèmes de stockage

- Détruire le stockage

Permet la destruction de volumes et de LUN

Rôles de VASA Provider

Vous pouvez créer uniquement une gestion basée sur des règles au niveau du cluster. Ce rôle permet la gestion du stockage basée sur des règles à l'aide de profils de fonctions de stockage.

Rôles SRA

SRA classe les privilèges d'ONTAP en rôle SAN ou NAS au niveau du cluster ou des SVM. Les utilisateurs peuvent ainsi exécuter des opérations SRM.

Lors de l'ajout du cluster à VSC, VSC procède à une validation initiale des rôles RBAC ONTAP. Si vous avez ajouté une adresse IP de stockage SVM directe, VSC n'effectue pas la validation initiale. VSC vérifie et applique les privilèges plus tard dans le flux de travail des tâches.

Configuration de la haute disponibilité des outils ONTAP

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

Les outils ONTAP s'appuient sur la fonction haute disponibilité de VMware vSphere et sur la fonction tolérance aux pannes (FT) de vSphere pour assurer une haute disponibilité. La solution haute disponibilité permet une reprise rapide en cas de panne provoquée par :

- Défaillance d'hôte
- 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 que les outils ONTAP assurent la haute disponibilité. Seuls les hôtes vCenter Server et ESXi doivent être configurés à l'aide de la fonction HA de VMware vSphere ou de la fonction FT de vSphere en fonction de leurs besoins. La haute disponibilité et la tolérance de défaillance nécessitent des hôtes en cluster associés au stockage partagé. FT a des exigences et des limites supplémentaires.

Outre la solution haute disponibilité VMware vSphere et la solution FT vSphere, les outils ONTAP permettent également de garantir le fonctionnement continu des services des outils ONTAP. Le processus de surveillance

des outils ONTAP surveille régulièrement les trois services et les redémarre automatiquement en cas de défaillance. Ainsi, il est possible d'éviter les défaillances des applications.



vCenter HA n'est pas pris en charge par les outils ONTAP.

Haute disponibilité VMware vSphere

Vous pouvez configurer votre environnement vSphere sur lequel les outils ONTAP pour VMware vSphere sont déployés pour la haute disponibilité (HA). La fonction de haute disponibilité de VMware offre une protection contre les défaillances matérielles et les défaillances du système d'exploitation dans les environnements virtuels.

La fonction VMware HA surveille les machines virtuelles afin de détecter les défaillances du système d'exploitation et du matériel. Lorsqu'une défaillance est détectée, la fonction VMware HA redémarre les machines virtuelles sur les autres serveurs physiques du pool de ressources. Une intervention manuelle n'est pas requise lorsqu'une défaillance de serveur est détectée.

La procédure de configuration de VMware HA dépend de la version de votre serveur vCenter. Par exemple, vous pouvez utiliser le lien de référence suivant et sélectionner la version de vCenter Server requise pour afficher les étapes de configuration de VMware HA.

["Documentation VMware vSphere : création et utilisation de clusters vSphere HA"](#)

Tolérance aux pannes VMware vSphere

La fonction VMware vSphere Fault Tolerance (FT) offre une haute disponibilité (HA) à un niveau plus élevé et permet de protéger les machines virtuelles sans perte de données ni de connexions. Vous devez activer ou désactiver les outils vSphere FT pour ONTAP à partir de votre serveur vCenter.

Assurez-vous que votre licence vSphere prend en charge FT avec le nombre de CPU virtuels requis pour les outils ONTAP dans votre environnement (au moins 2 CPU virtuels ; 4 CPU virtuels pour les environnements à grande échelle).

vSphere FT permet aux machines virtuelles de fonctionner en continu, même en cas de panne de serveur. Lorsque vSphere FT est activé sur une machine virtuelle, une copie de la machine virtuelle principale est automatiquement créée sur un autre hôte (la machine virtuelle secondaire) sélectionné par Distributed Resource Scheduler (DRS). Si DRS n'est pas activé, l'hôte cible est sélectionné à partir des hôtes disponibles. vSphere FT exploite la machine virtuelle principale et la machine virtuelle secondaire en mode parallèle, chaque mise en miroir de l'état d'exécution de la machine virtuelle principale vers la machine virtuelle secondaire.

En cas de défaillance matérielle causant la défaillance de la machine virtuelle principale, la machine virtuelle secondaire reprend immédiatement l'endroit où la machine virtuelle principale est arrêtée. La machine virtuelle secondaire continue de fonctionner sans perte de connexions réseau, de transactions ou de données.

Votre système doit répondre aux exigences du processeur, aux exigences de limite des machines virtuelles et aux exigences de licence pour la configuration de vSphere FT pour votre instance vCenter Server.

La procédure de configuration de HA dépend de la version de votre serveur vCenter. Par exemple, vous pouvez utiliser le lien de référence suivant et sélectionner la version de vCenter Server requise pour afficher les étapes de configuration de HA.

["Documentation VMware vSphere : exigences en matière de tolérance aux pannes, limites et licences"](#)

Configurations MetroCluster prises en charge par les outils ONTAP

Les outils ONTAP pour VMware vSphere prennent en charge les environnements qui utilisent les configurations MetroCluster IP et FC pour ONTAP. La majeure partie de ce support est automatique. Toutefois, vous remarquerez peut-être quelques différences si vous utilisez un environnement MetroCluster avec VSC et VASA Provider.



SRA ne prend pas en charge les configurations MetroCluster.

Les configurations MetroCluster et VSC

Vous devez vous assurer que VSC détecte les contrôleurs du système de stockage sur le site principal et sur le site secondaire. En général, VSC détecte automatiquement les contrôleurs de stockage. Si vous utilisez une LIF de gestion de cluster, il est recommandé de vérifier que VSC a détecté les clusters sur les deux sites. Vous pouvez également ajouter manuellement les contrôleurs de stockage à VSC. Vous pouvez également modifier les paires de noms d'utilisateur et de mots de passe que VSC utilise pour se connecter aux contrôleurs de stockage.

Lorsqu'un basculement se produit, les SVM sur le site secondaire prennent le contrôle. Ces SVM ont le suffixe «-mc» ajouté à leurs noms. En cas de basculement lorsque vous effectuez des opérations telles que le provisionnement d'un datastore, le nom de la SVM où réside le datastore est modifié afin d'inclure le suffixe «-mc». Ce suffixe est supprimé lorsque le rétablissement se produit, et que les SVM du contrôle de reprise sur le site principal.



Si vous avez ajouté des SVM directs avec la configuration MetroCluster à VSC, la modification du nom du SVM (l'ajout du suffixe «-mc») n'est pas reflétée. Toutes les autres opérations de basculement continuent à s'exécuter normalement.

En cas de basculement ou de rétablissement, VSC peut prendre quelques minutes pour détecter et détecter automatiquement les clusters. Si cela se produit pendant l'exécution d'une opération VSC comme le provisionnement d'un datastore, vous risquez de rencontrer un retard.

Configurations MetroCluster et VASA Provider

Vasa Provider prend automatiquement en charge les environnements qui utilisent les configurations MetroCluster. Le basculement est transparent dans les environnements VASA Provider. Vous ne pouvez pas ajouter de SVM directs à VASA Provider.



Vasa Provider n'ajoute pas le suffixe «-mc» aux noms des SVM sur le site secondaire après un basculement.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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