



Concepts

ONTAP tools for VMware vSphere 10

NetApp

November 17, 2025

This PDF was generated from <https://docs.netapp.com/fr-fr/ontap-tools-vmware-vsphere-103/concepts/ontap-tools-overview.html> on November 17, 2025. Always check docs.netapp.com for the latest.

Sommaire

- Concepts 1
 - Présentation des outils ONTAP pour VMware vSphere 1
 - Concepts et termes clés 1
 - Contrôle d'accès basé sur des rôles 4
 - Découvrez les outils ONTAP pour VMware vSphere 10 RBAC 4
 - RBAC avec VMware vSphere 5
 - RBAC avec ONTAP 9
 - Haute disponibilité des outils ONTAP pour VMware vSphere 12
 - AutoSupport 12
 - Interface utilisateur du Gestionnaire d'outils ONTAP 13

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.

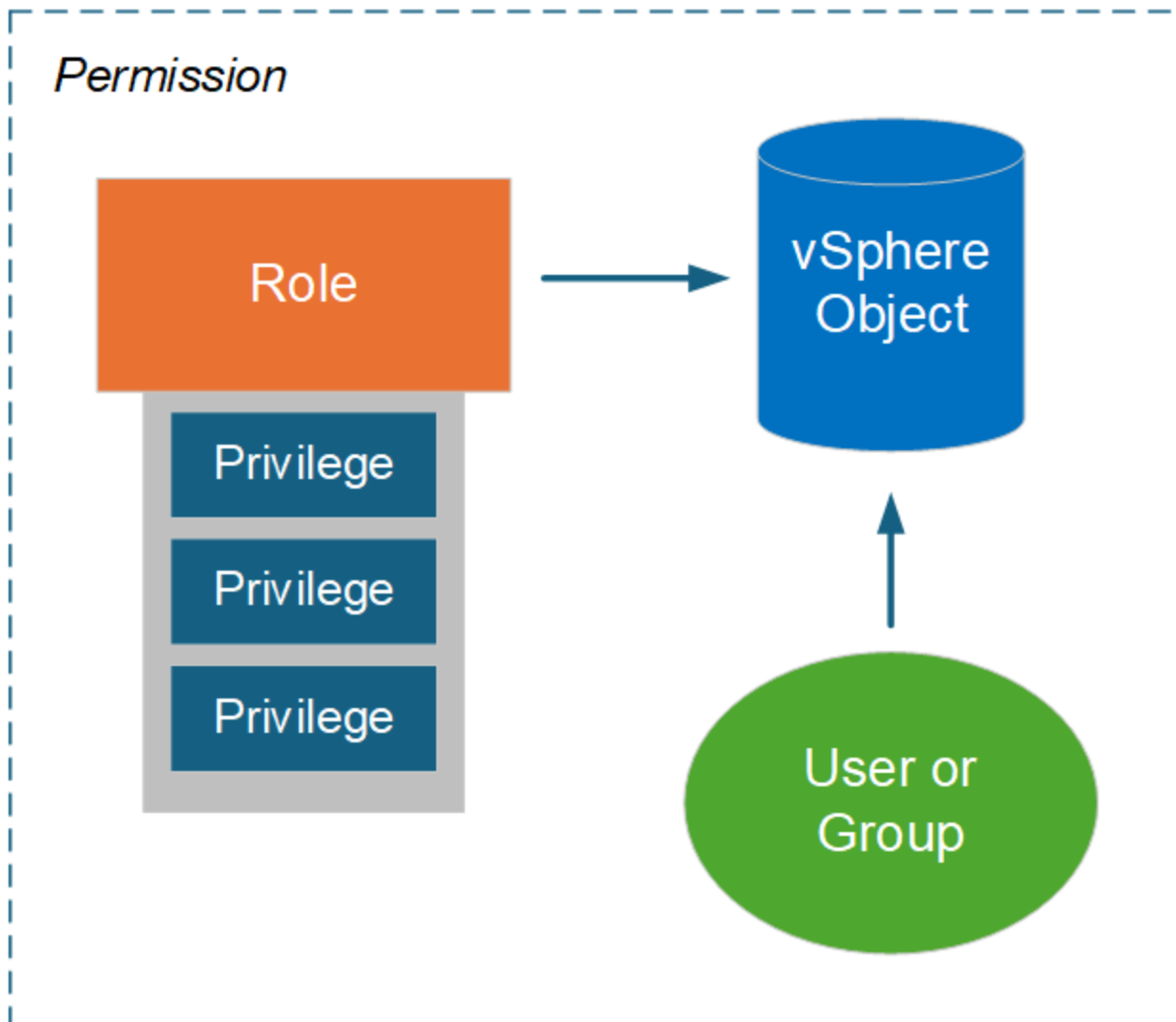
RBAC avec VMware vSphere

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.

ONTAP tools Manager

Administrator

Overview

Alerts

Jobs

Storage backends

vCenters

Log bundles

Certificates

Settings

Overview

EDIT APPLIANCE SETTINGS

Appliance

Healthy

Size: Small
HA: Enabled
VASA provider: Enabled
SRA: Enabled

VIEW DETAILS

Alerts

3
Error

2
Warning

5
Info

VIEW ALL ALERTS (43)

ONTAP tools nodes

nodename_01
 Online
demo_vm1

VIEW DETAILS

nodename_02
 Online
demo_vm2

VIEW DETAILS

nodename_03
 Online
demo_vm3

VIEW DETAILS

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.

14

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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