RBAC avec VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
August 25, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/ontap-tools-vmware-vsphere-10/concepts/rbac-vcenter-environment.html on August 25, 2025. Always check docs.netapp.com for the latest.

Sommaire

RBAC avec VMware vSphere . . . 1
Environnement RBAC du serveur vCenter avec les outils ONTAP pour VMware vSphere 10 . . . 1
Illustration d’une autorisation vCenter Server . . . 1
Composants d’une autorisation vCenter Server . . . 2
Utilisez vCenter Server RBAC avec les outils ONTAP pour VMware vSphere 10 . . . 2
Rôles vCenter et compte administrateur . . . 2
Hiérarchie des objets vSphere . . . 3
Rôles inclus avec les outils ONTAP pour VMware vSphere 10 . . . 3
Objets vSphere et systèmes back-end de stockage ONTAP . . . 3
Utilisation de vCenter Server RBAC . . . 3

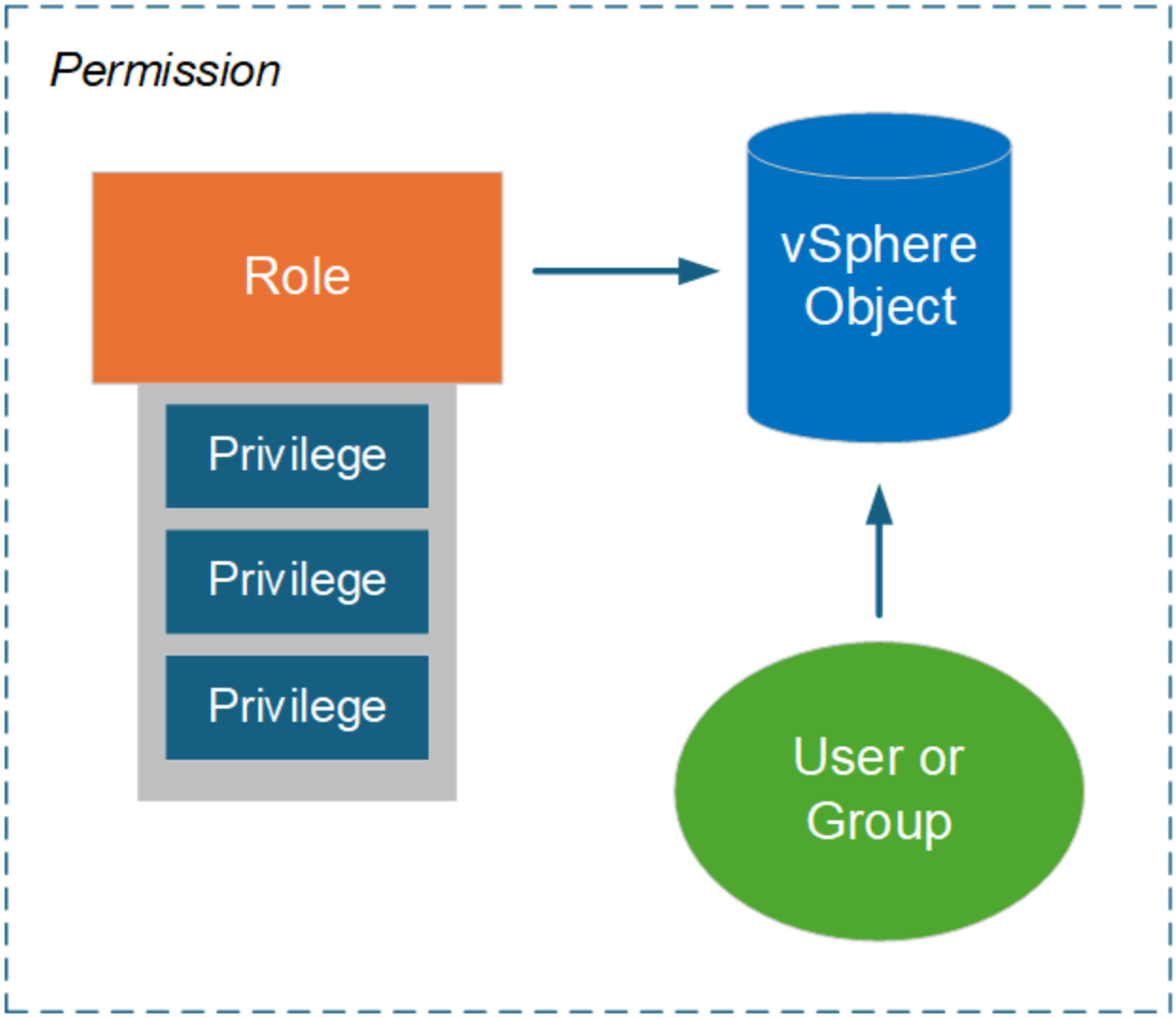
RBAC avec VMware vSphere

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

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.

Informations sur le copyright

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

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

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

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

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

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

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

Informations sur les marques commerciales

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