



Contrôle d'accès basé sur des rôles

ONTAP tools for VMware vSphere 10

NetApp

September 30, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/ontap-tools-vmware-vsphere-100/concepts/concept_vcenter_server_role_based_access_control_features_in_vsc_for_vmware_vsphere.html on September 30, 2025. Always check docs.netapp.com for the latest.

Sommaire

- Contrôle d'accès basé sur des rôles 1
 - Présentation du contrôle d'accès basé sur des rôles dans les outils ONTAP 1
 - Points clés sur l'attribution et la modification de rôles pour vCenter Server 2
 - Rôles standard fournis avec les outils ONTAP 2
 - Autorisations pour les systèmes ONTAP back-end et les objets vSphere 2
 - Rôles ONTAP recommandés pour l'utilisation des outils ONTAP pour VMware vSphere 3

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. VCenter Server fournit des services d'authentification et d'autorisation centralisés à différents niveaux de son inventaire, en utilisant des droits d'utilisateur et de groupe avec des rôles et des privilèges. VCenter Server comprend cinq composants principaux pour la gestion du RBAC :

Composants	Description
Privilèges	Un privilège active ou refuse l'accès pour effectuer des actions dans vSphere.
Rôles	Un rôle contient un ou plusieurs privilèges système où chaque privilège définit un droit administratif à un objet ou un type d'objet donné dans le système. En attribuant un rôle à un utilisateur, celui-ci hérite des fonctionnalités des privilèges définis dans ce rôle.
Utilisateurs et groupes	Les utilisateurs et les groupes sont utilisés dans les autorisations pour attribuer des rôles à partir d'Active Directory (AD) ou d'utilisateurs/groupes Windows potentiellement locaux (non recommandé)
Autorisations	Les autorisations vous permettent d'attribuer des privilèges aux utilisateurs ou aux groupes pour effectuer certaines actions et modifier les objets dans vCenter Server. Les autorisations vCenter Server affectent uniquement les utilisateurs qui se connectent à vCenter Server plutôt que les utilisateurs qui se connectent directement à un hôte ESXi.
Objet	Entité sur laquelle les actions sont exécutées. Les objets VMware vCenter sont des data centers, des dossiers, des pools de ressources, des clusters, des hôtes, et machines virtuelles

Pour effectuer correctement une tâche, vous devez disposer des rôles RBAC vCenter Server appropriés. Au cours d'une tâche, les outils ONTAP vérifient les rôles du serveur vCenter d'un utilisateur avant de vérifier les privilèges ONTAP de l'utilisateur.



Les rôles de serveur vCenter s'appliquent aux utilisateurs vCenter des outils ONTAP, et non aux administrateurs. Par défaut, les administrateurs disposent d'un accès complet au produit et n'ont pas besoin de rôles qui leur sont attribués.

Les utilisateurs et les groupes peuvent accéder à un rôle en faisant partie d'un rôle vCenter Server.

Points clés sur l'attribution et la modification de rôles pour vCenter Server

Vous n'avez besoin de configurer des rôles 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'emplacement où vous attribuez un rôle détermine les tâches des outils ONTAP qu'un utilisateur peut effectuer. Vous pouvez modifier un rôle à tout moment. Si vous modifiez les privilèges d'un rôle, l'utilisateur associé à ce rôle doit se déconnecter, puis se reconnecter pour activer le rôle mis à jour.

Rôles standard fournis avec les outils ONTAP

Pour simplifier l'utilisation des privilèges vCenter Server et du contrôle d'accès basé sur des rôles, les outils ONTAP fournissent des rôles d'outils ONTAP standard qui vous permettent d'effectuer les tâches clés des outils ONTAP. Il existe également un rôle en lecture seule qui vous permet d'afficher les informations, mais pas d'effectuer des tâches.

Vous pouvez afficher les rôles standard des outils ONTAP en cliquant sur **Rôles** sur la page d'accueil du client vSphere. Les rôles fournis par les outils ONTAP vous permettent d'effectuer les tâches suivantes :

Rôle	Description
Administrateur des outils NetApp ONTAP	Fournit tous les privilèges du serveur vCenter natif et les privilèges spécifiques aux outils ONTAP requis pour effectuer certaines tâches des outils ONTAP.
Outils NetApp ONTAP en lecture seule	Accès en lecture seule aux outils ONTAP. Ces utilisateurs ne peuvent pas effectuer d'actions d'outils ONTAP contrôlées par l'accès.
Provisionnement des outils NetApp ONTAP	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

Le rôle admin de l'interface utilisateur Manager n'est pas enregistré dans vCenter. Ce rôle est spécifique à l'interface utilisateur du gestionnaire.

Si votre entreprise exige que vous mettiez en œuvre des rôles plus restrictifs que les rôles standard pour les outils ONTAP, vous pouvez utiliser les rôles des outils ONTAP pour créer de nouveaux rôles.

Dans ce cas, vous allez cloner les rôles d'outils ONTAP nécessaires, puis modifier le rôle cloné de sorte qu'il ne dispose que des privilèges dont votre utilisateur a besoin.

Autorisations pour les systèmes ONTAP back-end et les objets vSphere

Si l'autorisation vCenter Server est suffisante, les outils ONTAP vérifient ensuite les privilèges RBAC ONTAP (votre rôle ONTAP) associés aux informations d'identification du système back-end de stockage (le nom d'utilisateur et le mot de passe). pour déterminer si vous disposez de privilèges suffisants pour effectuer les opérations de stockage requises par la tâche d'outils ONTAP sur ce back-end de stockage. Si vous disposez des privilèges ONTAP appropriés, vous pouvez accéder au Effectuez les tâches associées au stockage back-

end et aux outils ONTAP. Les rôles ONTAP déterminent les tâches des outils ONTAP que vous pouvez effectuer sur le back-end de stockage.

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

Vous pouvez définir plusieurs rôles ONTAP recommandés pour l'utilisation des outils ONTAP pour VMware vSphere et le contrôle d'accès basé sur des rôles (RBAC). Ces rôles contiennent les privilèges ONTAP requis pour effectuer les opérations de stockage requises qui sont exécutées par les tâches des outils ONTAP.

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 ONTAP System Manager 9.8P1 ou version ultérieure. Voir "[Liste des privilèges minimaux requis pour les utilisateurs du cluster dont le périmètre global n'est pas défini sur admin](#)" pour en savoir plus.

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.

À titre de mesure de sécurité, les rôles ONTAP spécifiques aux outils ONTAP sont classés de manière hiérarchique. Cela signifie que le premier rôle est le rôle le plus restrictif et ne dispose que des privilèges associés à l'ensemble le plus basique d'opérations de stockage des outils ONTAP. 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 quelques-uns des rôles ONTAP RBAC recommandés lors de l'utilisation d'outils ONTAP. 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 ».

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.