Contrôle d'accès basé sur les rôles (RBAC) avec ONTAP

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/ontap-tools-vmware-vsphere-105/concepts/rbac-ontap-environment.html on July 24, 2026. Always check docs.netapp.com for the latest.

Sommaire

Contrôle d’accès basé sur les rôles (RBAC) avec ONTAP

Fonctionnement du contrôle d’accès basé sur les rôles (RBAC) ONTAP avec les ONTAP tools

ONTAP offre un environnement RBAC robuste et extensible. Vous pouvez utiliser la fonctionnalité RBAC pour contrôler l’accès au stockage et aux opérations système exposées via l’API REST et le CLI. Il est utile de bien connaître l’environnement avant de l’utiliser avec un déploiement ONTAP tools for VMware vSphere 10.

Aperçu des options administratives

Plusieurs options s’offrent à vous lors de l’utilisation de ONTAP RBAC, selon votre environnement et vos objectifs. Un aperçu des principales décisions d’administration est présenté ci-dessous. Voir aussi "Automatisation ONTAP : aperçu de la sécurité RBAC" pour plus d’informations.

> ONTAP RBAC est conçu spécifiquement pour les environnements de stockage et est plus simple que l’implémentation RBAC fournie avec vCenter Server. Avec ONTAP, vous attribuez directement un rôle à l’utilisateur. La configuration explicite des autorisations, comme celle utilisée avec vCenter Server, n’est pas nécessaire avec ONTAP RBAC.

Types de rôles et de privilèges

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

- REST

  Les rôles REST ont été introduits avec ONTAP 9.6 et s’appliquent généralement aux utilisateurs accédant à ONTAP via l’API REST. Les privilèges inclus dans ces rôles sont définis en termes d’accès aux points de terminaison de l’API REST d’ONTAP et aux actions associées.

- Traditionnel

  Il s’agit des rôles hérités antérieurs à ONTAP 9.6. Ils demeurent un élément fondamental du RBAC. Les privilèges sont définis en termes d’accès aux commandes CLI ONTAP.

Bien que les rôles REST soient plus récents, les rôles traditionnels présentent certains avantages. Par exemple, des paramètres de requête supplémentaires peuvent être inclus afin de permettre aux Privileges de définir plus précisément les objets auxquels ils s’appliquent.

Portée

Les rôles ONTAP peuvent être définis avec l’une des deux étendues différentes. Ils peuvent être appliqués à une SVM de données spécifique (niveau SVM) ou à l’ensemble du cluster ONTAP (niveau cluster).

Définitions des rôles

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

Travailler avec les rôles REST ONTAP

Plusieurs points sont à prendre en compte lors de l'utilisation des rôles ONTAP REST inclus avec ONTAP tools for VMware vSphere 10.

Cartographie des rôles

Que vous utilisiez un rôle traditionnel ou REST, toutes les décisions d'accès ONTAP sont prises en fonction de la commande CLI sous-jacente. Mais comme les privilèges dans un rôle REST sont définis en termes de points de terminaison de l'API REST, ONTAP doit créer un rôle traditionnel *mappé* pour chacun des rôles REST. Par conséquent, chaque rôle REST correspond à un rôle traditionnel sous-jacent. Cela permet à ONTAP de 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 parallèles.

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

Comme ONTAP utilise systématiquement les commandes CLI pour déterminer les accès de base, il est possible d'exprimer un rôle REST à l'aide des privilèges des commandes CLI plutôt que des points de terminaison REST. Un avantage de cette approche est la granularité supplémentaire offerte par les rôles traditionnels.

Interface d'administration lors de la définition des rôles ONTAP

Vous pouvez créer des utilisateurs et des rôles avec l'interface de ligne de commande ONTAP (CLI) et l'API REST ONTAP. Cependant, il est plus pratique d'utiliser l'interface System Manager ainsi que le fichier JSON disponible via ONTAP tools Manager. Voir "Utilisez ONTAP RBAC avec les ONTAP tools for VMware vSphere 10" pour plus d'informations.

Considérations RBAC ONTAP pour les outils ONTAP

Plusieurs aspects de la mise en œuvre du contrôle d'accès basé sur les rôles (RBAC) des ONTAP tools for VMware vSphere 10 avec ONTAP doivent être pris en compte avant de l'utiliser dans un environnement de production.

Aperçu du processus de configuration

ONTAP tools for VMware vSphere inclut la prise en charge de la création d'un utilisateur ONTAP avec un rôle personnalisé. Les définitions sont regroupées dans un fichier JSON que vous pouvez importer dans le cluster ONTAP. Vous pouvez créer l'utilisateur et adapter le rôle à votre environnement et à vos besoins en matière de sécurité.

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

1. Préparer

Vous devez disposer d'identifiants d'administrateur à la fois pour ONTAP tools Manager et pour le cluster ONTAP.

2. Téléchargez le fichier de définition JSON

Après vous être connecté à l'interface utilisateur de ONTAP tools Manager, vous pouvez télécharger le fichier JSON contenant les définitions RBAC.

3. Créez un utilisateur ONTAP avec un rôle

Après vous être connecté à System Manager, vous pouvez créer l'utilisateur et le rôle :

1. Sélectionnez **Cluster** à gauche, puis **Settings**.
2. Faites défiler vers le bas jusqu'à **Utilisateurs et rôles** et cliquez −→.
3. Sélectionnez **Ajouter** sous **Utilisateurs** et sélectionnez **Virtualization products**.
4. Sélectionnez le fichier JSON sur votre poste de travail local et téléversez-le.

4. Configurer le rôle

Pour définir ce 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 nouvel 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 principale des utilisateurs et des rôles

Les définitions RBAC sont intégrées à plusieurs fonctionnalités produit, notamment des combinaisons de VSC, VASA Provider et SRA. Vous devez sélectionner l'environnement ou les environnements où vous avez besoin de la prise en charge RBAC. Par exemple, si vous souhaitez que les rôles prennent en charge la fonctionnalité de plug-in distant, sélectionnez VSC. Vous devez également choisir le nom d'utilisateur et le mot de passe associé.

Privileges

Les privilèges des rôles sont organisés en quatre ensembles en fonction du niveau d'accès requis pour le stockage ONTAP. Les privilèges sur lesquels les rôles sont basés comprennent :

- Découverte

  Ce rôle vous permet d'ajouter des systèmes de stockage.

- Créer un stockage

  Ce rôle vous permet de créer du stockage. Il inclut également tous les privilèges associés au rôle de découverte.

- Modifier le stockage

  Ce rôle vous permet de modifier le stockage. Il inclut également tous les privilèges associés aux rôles de découverte et de création de stockage.

- Détruire le stockage

  Ce rôle vous permet de supprimer du stockage. Il inclut également tous les privilèges associés aux rôles de découverte, de création et de modification de stockage.

Générez l'utilisateur avec un rôle

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

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

Exemple

```
OTV_10_VSC_Discovery_Create
```

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

Informations sur le copyright

Copyright © 2026 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.