



RBAC avec ONTAP

ONTAP tools for VMware vSphere 10

NetApp
November 04, 2025

Sommaire

RBAC avec ONTAP	1
Environnement ONTAP RBAC avec ONTAP tools for VMware vSphere 10	1
Aperçu des options administratives	1
Travailler avec les rôles REST ONTAP	2
Utiliser ONTAP RBAC avec les ONTAP tools for VMware vSphere 10	2
Aperçu du processus de configuration.....	2
Configurer le rôle à l'aide du Gestionnaire système	3

RBAC avec ONTAP

Environnement ONTAP RBAC avec ONTAP tools for VMware vSphere 10

ONTAP fournit un environnement RBAC robuste et extensible. Vous pouvez utiliser la fonctionnalité RBAC pour contrôler l'accès aux opérations de stockage et système telles qu'exposées via l'API REST et la CLI. Il est utile de se familiariser avec l'environnement avant de l'utiliser avec un déploiement ONTAP tools for VMware vSphere 10.

Aperçu des options administratives

Plusieurs options sont disponibles lors de l'utilisation ONTAP RBAC en fonction de votre environnement et de vos objectifs. Un aperçu des principales décisions administratives est présenté ci-dessous. Voir aussi "[ONTAP Automation : 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 d'autorisations explicites, telles que celles utilisées 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 :

- REPOS

Les rôles REST ont été introduits avec ONTAP 9.6 et sont généralement appliqués 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 ONTAP et aux actions associées.

- Traditionnel

Il s'agit des rôles hérités inclus avant ONTAP 9.6. Ils continuent d'être un aspect fondamental du RBAC. Les privilèges sont définis en termes d'accès aux commandes CLI ONTAP .

Bien que les rôles REST aient été introduits plus récemment, les rôles traditionnels présentent certains avantages. Par exemple, des paramètres de requête supplémentaires peuvent éventuellement être inclus afin que les privilèges définissent plus précisément les objets auxquels ils sont appliqués.

Portée

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

Définitions des rôles

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

Travailler avec les rôles REST ONTAP

Plusieurs éléments doivent être pris en compte lors de l'utilisation des rôles ONTAP REST inclus avec les ONTAP tools for VMware vSphere 10.

Cartographie des rôles

Que vous utilisez un rôle traditionnel ou REST, toutes les décisions d'accès ONTAP sont prises en fonction de la commande CLI sous-jacente. Mais comme les priviléges d'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 en parallèle.

Définition d'un rôle REST à l'aide des privilèges CLI

Étant donné ONTAP utilise toujours les commandes CLI pour déterminer l'accès à un niveau de base, il est possible d'exprimer un rôle REST à l'aide des priviléges de commande CLI au lieu des points de terminaison 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 avec l'interface de ligne de commande ONTAP et l'API REST. Cependant, il est plus pratique d'utiliser l'interface du gestionnaire système avec le fichier JSON disponible via le gestionnaire d'outils ONTAP . Voir "[Utiliser ONTAP RBAC avec les ONTAP tools for VMware vSphere 10](#)" pour plus d'informations.

Utiliser ONTAP RBAC avec les ONTAP tools for VMware vSphere 10

Il existe plusieurs aspects des ONTAP tools for VMware vSphere 10 avec ONTAP que vous devez prendre en compte avant de l'utiliser dans un environnement de production.

Aperçu du processus de configuration

Les ONTAP tools for VMware vSphere 10 incluent 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 télécharger sur le cluster ONTAP . Vous pouvez créer l'utilisateur et personnaliser le rôle en fonction de votre environnement et de vos besoins de sécurité.

Les principales étapes de configuration sont décrites à un niveau élevé ci-dessous. Se référer à "["Configurer les rôles et priviléges des utilisateurs ONTAP"](#)" pour plus de détails.

1. Préparer

Vous devez disposer des informations d'identification administratives pour le gestionnaire d'outils ONTAP et le cluster ONTAP .

2. Télécharger le fichier de définition JSON

Après vous être connecté à l'interface utilisateur du gestionnaire d'outils ONTAP , vous pouvez télécharger le fichier JSON contenant les définitions RBAC.

3. Créer un utilisateur ONTAP avec un rôle

Après vous être connecté au Gestionnaire système, vous pouvez créer l'utilisateur et le rôle :

1. Sélectionnez **Cluster** sur la gauche puis **Paramètres**.
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 téléchargez-le.

4. Configurer le rôle

Dans le cadre de la définition du rôle, vous devez prendre plusieurs décisions administratives. Voir [Configurer le rôle à l'aide du Gestionnaire système](#) pour plus de détails.

Configurer le rôle à l'aide du Gestionnaire système

Une fois que vous avez commencé à créer un nouvel utilisateur et un nouveau 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 des utilisateurs et des rôles principaux

Les définitions RBAC sont regroupées sous forme de plusieurs fonctionnalités de produit, notamment des combinaisons de VSC, VASA Provider et SRA. Vous devez sélectionner l'environnement ou les environnements dans lesquels 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 à distance, sélectionnez VSC. Vous devez également choisir le nom d'utilisateur et le mot de passe associé.

Privileges

Les priviléges de rôle sont organisés en quatre ensembles en fonction du niveau d'accès nécessaire au stockage ONTAP . Les priviléges sur lesquels sont basés les rôles incluent :

- Découverte

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

- Créer un espace de stockage

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

- Modifier le stockage

Ce rôle vous permet de modifier le stockage. Il inclut également tous les priviléges associés à la découverte et à la création de rôles de stockage.

- Détruire le stockage

Ce rôle vous permet de détruire le stockage. Il inclut également tous les priviléges associés à la découverte, à la création de stockage et à 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 »)
- Capacité du produit que vous avez sélectionnée
- Liste des ensembles de priviléges.

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 © 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 JOUSSANCE, 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.