contrôle d'accès basé sur les rôles (RBAC)

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Sommaire

contrôle d’accès basé sur les rôles (RBAC)

En savoir plus sur le RBAC des outils ONTAP

Le contrôle d’accès basé sur les rôles (RBAC) est un cadre de sécurité permettant de contrôler l’accès aux ressources au sein d’une organisation. Le RBAC simplifie l’administration en définissant des rôles avec des niveaux d’autorité spécifiques pour effectuer des actions, au lieu d’attribuer des autorisations à chaque utilisateur. Les rôles définis sont attribués aux utilisateurs, ce qui contribue à réduire le risque d’erreur et simplifie la gestion du contrôle d’accès dans toute votre organisation.

Le modèle standard RBAC comprend plusieurs technologies ou phases d’implémentation de complexité croissante. Le résultat est que les déploiements RBAC réels, basés sur les besoins des éditeurs de logiciels et de leurs clients, peuvent différer et aller de relativement simples à très complexes.

Composants RBAC

De manière générale, plusieurs composants sont inhérents à toute implémentation RBAC. Ces composants sont liés entre eux de différentes manières afin de définir les processus d’autorisation.

Privileges

Un privilège est une action ou une capacité qui peut être autorisée ou refusée. Il peut s’agir d’une action simple, comme la possibilité de lire un fichier, ou d’une opération plus abstraite, spécifique à un système logiciel donné. Privileges peuvent également être définis pour restreindre l’accès aux points de terminaison REST API et aux commandes CLI. Chaque implémentation RBAC inclut des privilèges prédéfinis et peut également permettre aux administrateurs de créer des privilèges personnalisés.

Rôles

Un rôle est un conteneur regroupant un ou plusieurs privilèges. Les rôles sont généralement définis en fonction de tâches ou de fonctions spécifiques. Lorsqu’un rôle est attribué à un utilisateur, celui-ci reçoit tous les privilèges contenus dans ce rôle. À l’instar des privilèges, 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 par les privilèges sont exécutées sur ou avec les objets associés. Selon l’implémentation, les privilèges peuvent être accordés à un type d’objet ou à une instance d’objet spécifique.

Utilisateurs et groupes

Les utilisateurs sont affectés ou associés à un rôle appliqué après l’authentification. Certaines implémentations de RBAC n’autorisent qu’un seul rôle par utilisateur, tandis que d’autres permettent plusieurs rôles par utilisateur, avec éventuellement un seul rôle actif à la fois. L’attribution de rôles à des groupes peut encore simplifier l’administration de la sécurité.

Autorisations

Une permission est une définition qui associe un utilisateur ou un groupe, ainsi qu’un rôle, à un objet. Les permissions peuvent être utiles dans un modèle d’objet hiérarchique où elles peuvent éventuellement être héritées par les éléments enfants de la hiérarchie.

Deux environnements RBAC

Il existe deux environnements RBAC distincts à prendre en compte lors de l'utilisation des ONTAP tools for VMware vSphere 10. ONTAP tools for VMware vSphere 10 requiert des privilèges spécifiques à la fois dans vCenter et dans ONTAP pour effectuer ses opérations. Bien que les ONTAP tools automatisent les tâches de gestion du stockage, ils ne créent pas de comptes utilisateur ni dans vCenter ni dans ONTAP. Les comptes de service doivent être créés par un administrateur vSphere selon les besoins. Cette documentation fournit des instructions aux administrateurs pour attribuer les rôles et autorisations nécessaires à une gestion efficace des ONTAP tools.

Serveur VMware vCenter

L'implémentation RBAC dans VMware vCenter Server est utilisée pour restreindre l'accès aux objets exposés via l'interface utilisateur du client vSphere. Dans le cadre de l'installation des ONTAP tools for VMware vSphere 10, l'environnement RBAC est étendu pour inclure des objets supplémentaires représentant les capacités des ONTAP tools. L'accès à ces objets est fourni via le plug-in distant. Voir "vCenter Server environnement RBAC" pour plus d'informations.

Cluster ONTAP

ONTAP tools for VMware vSphere 10 se connecte à un cluster ONTAP via l'API REST ONTAP pour effectuer des opérations liées au stockage. L'accès aux ressources de stockage est contrôlé par un rôle ONTAP associé à l'utilisateur ONTAP fourni lors de l'authentification. Voir "Environnement RBAC ONTAP" pour plus d'informations.

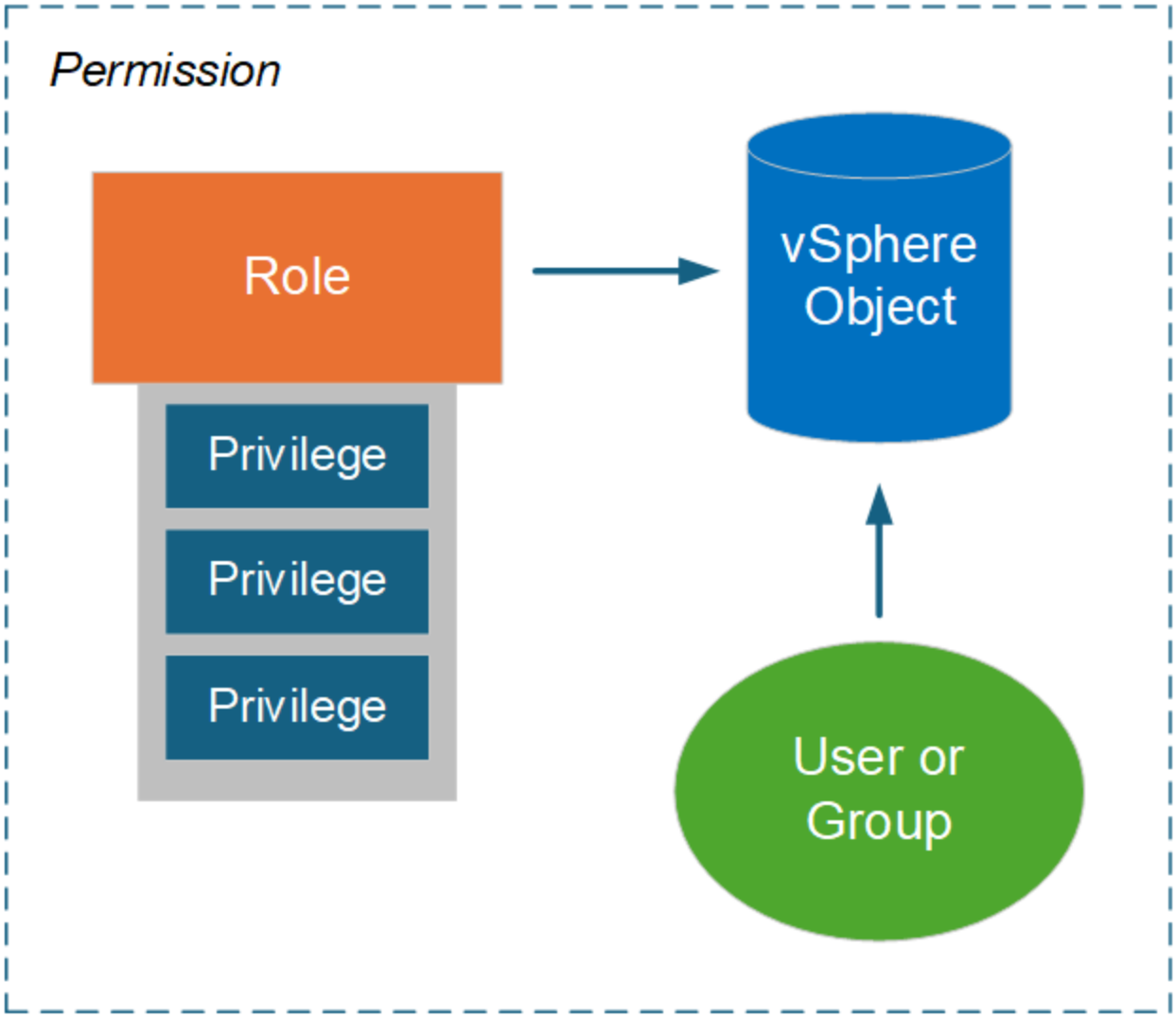
RBAC avec VMware vSphere

Comment le contrôle d'accès basé sur les rôles (RBAC) du serveur vCenter fonctionne avec les outils ONTAP

VMware vCenter Server offre 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 de vCenter.

Illustration d'une autorisation de serveur vCenter

Une autorisation est la base pour appliquer le 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 de l'autorisation. Une illustration de haut niveau d'une autorisation vCenter est présentée dans la figure ci-dessous.



Composants d'une autorisation de serveur vCenter

Une autorisation vCenter Server est un ensemble de plusieurs composants qui sont liés entre eux lors de la création de l'autorisation.

vSphere objets

Les autorisations sont associées à des objets vSphere, tels que le serveur vCenter, les hôtes ESXi, les machines virtuelles, les banques de données, les centres de données et les dossiers. En fonction des autorisations attribuées à l'objet, le serveur vCenter détermine les actions ou tâches que chaque utilisateur ou groupe peut effectuer sur cet objet. Pour les tâches spécifiques à ONTAP tools for VMware vSphere, toutes les autorisations sont attribuées et validées au niveau racine ou au niveau du dossier racine du serveur vCenter. Voir "Utilisez le contrôle d'accès basé sur les rôles (RBAC) avec le serveur vCenter" pour plus d'informations.

Privileges et rôles

Il existe deux types de privilèges vSphere utilisés avec les ONTAP tools for VMware vSphere 10. Pour simplifier le travail avec le contrôle d'accès basé sur les rôles (RBAC) dans cet environnement, ONTAP tools fournit des rôles contenant les privilèges natifs et personnalisés requis. Les privilèges incluent :

- Privilèges natifs du serveur vCenter

  Voici les privilèges fournis par le serveur vCenter.

- Privilèges spécifiques aux outils ONTAP

  Ce sont des privilèges personnalisés propres aux ONTAP tools for VMware vSphere.

Utilisateurs et groupes

Vous pouvez définir des utilisateurs et des groupes à l'aide d'Active Directory ou de l'instance locale du serveur vCenter. 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 des privilèges du rôle associé. Notez que les rôles ne sont pas attribués directement aux utilisateurs isolément. Au contraire, les utilisateurs et les groupes obtiennent l'accès à un objet via les privilèges de rôle dans le cadre de l'autorisation du serveur vCenter plus large.

vCenter Server : considérations RBAC pour les ONTAP tools

Plusieurs aspects de l'implémentation RBAC des ONTAP tools for VMware vSphere 10 avec vCenter Server doivent être pris en compte avant de les utiliser dans un environnement de production.

vCenter rôles et le compte administrateur

Vous n'avez besoin de définir et d'utiliser les rôles serveur vCenter personnalisés que si vous souhaitez limiter l'accès aux objets vSphere et aux tâches d'administration associées. Si la limitation de l'accès n'est pas requise, vous pouvez utiliser un compte administrateur à la place. Chaque compte administrateur est défini avec le rôle Administrateur au niveau supérieur de la hiérarchie des objets. Cela fournit un accès complet aux objets vSphere, y compris ceux ajoutés par ONTAP tools for VMware vSphere 10.

hiérarchie des objets vSphere

L'inventaire des objets vSphere est organisé de manière hiérarchique. Par exemple, vous pouvez parcourir la hiérarchie comme suit :

`vCenter Server` → `Datacenter` → `Cluster` → `ESXi host` → `Virtual Machine`

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 ONTAP tools for VMware vSphere 10

Pour simplifier le travail avec le contrôle d'accès basé sur les rôles (RBAC) du serveur vCenter, ONTAP tools for VMware vSphere fournit des rôles prédéfinis adaptés à diverses tâches administratives.

> Vous pouvez créer des rôles personnalisés si nécessaire. Pour ce faire, clonez l'un des rôles existants des ONTAP tools et modifiez-le selon vos besoins. Après avoir effectué les modifications de configuration, les utilisateurs clients vSphere concernés doivent se déconnecter puis se reconnecter pour activer les changements.

Pour afficher les rôles ONTAP tools for VMware vSphere, sélectionnez **Menu** en haut du client vSphere, puis cliquez sur **Administration** et ensuite sur **Rôles** à gauche. Les privilèges suivants doivent être inclus dans le rôle attribué à l'utilisateur vCenter responsable du déploiement ou de l'intégration du serveur vCenter.

Assurez-vous que ces privilèges sont configurés comme prérequis au processus de déploiement ou d'intégration.

- Alarmes
  - Accuser réception de l'alarme
- Bibliothèque de contenu
  - Ajouter un élément de bibliothèque
  - Vérifier dans un modèle
  - Consultez un modèle
  - Télécharger les fichiers
  - Importer le stockage
  - Stockage de lecture
  - Synchroniser l'élément de bibliothèque
  - Synchroniser la bibliothèque abonnée
  - Afficher les paramètres de configuration
- Magasin de données
  - Allouer de l'espace
  - Parcourir le datastore
  - opérations de fichiers de bas niveau
  - Supprimer le fichier
  - Mettre à jour les fichiers de la machine virtuelle
  - Mise à jour des métadonnées de la machine virtuelle
- Gestionnaire d'agents ESX
  - View
- Dossier
  - Créer un dossier
- Hôte
  - Configuration
    - Paramètres avancés
    - Modifier les paramètres
    - Configuration réseau
    - Ressources système
    - Configuration du démarrage automatique de la machine virtuelle
  - Opérations locales
    - Créer une machine virtuelle
    - Supprimer la machine virtuelle
    - Reconfigurer la machine virtuelle
- Réseau

    - Attribuer un réseau
    - Configurer
- OvfManager
    - OvfConsumer Accès
- Profil de l’hôte
    - View
- Ressource
    - Affecter une machine virtuelle au pool de ressources
- Tâche planifiée
    - Créer des tâches
    - Modifier la tâche
    - Exécuter la tâche
- Tâches
    - Créer une tâche
    - Tâche de mise à jour
- vApp
    - Ajouter une machine virtuelle
    - Affecter un pool de ressources
    - Attribuer vApp
    - Créer
    - Importer
    - Déplacer
    - Mise hors tension
    - Mise sous tension
    - Récupérer depuis l’URL
    - Afficher l’environnement OVF
- machine virtuelle
    - Modifier la configuration
        - Ajouter un disque existant
        - Ajouter un nouveau disque
        - Ajouter ou supprimer un appareil
        - Configuration avancée
        - Modifier le nombre de CPU
        - Changer la mémoire
        - Modifier les paramètres
        - Modifier la ressource
        - Étendre le disque virtuel

        - Modifier les paramètres de l’appareil
        - Retirer le disque
        - Réinitialiser les informations invité
        - Mise à niveau de la compatibilité des machines virtuelles
    - Modifier l’inventaire
        - Créer à partir de l’existant
        - Créer nouveau
        - Déplacer
        - S’inscrire
        - Retirer
        - Annuler l’enregistrement
    - Interaction
        - Opération de sauvegarde sur machine virtuelle
        - Configurer le support CD
        - Configurer le support de disquette
        - Connectez des appareils
        - Interaction avec la console
        - Gestion du système d’exploitation invité par l’API VIX
        - Mise hors tension
        - Mise sous tension
        - Réinitialiser
        - Suspendre
    - Provisionnement
        - Autoriser l’accès au disque
        - Cloner le modèle
        - Personnaliser l’invité
        - Déployer le modèle
        - Modifier la spécification de personnalisation
        - Lire les spécifications de personnalisation
    - Gestion des instantanés
        - Créer un instantané
        - Supprimer l’instantané
        - Renommer le snapshot
        - Rétablir l’instantané

Il existe trois rôles prédéfinis, décrits ci-dessous.

Administrateur de NetApp ONTAP tools for VMware vSphere

Fournit tous les privilèges natifs du serveur vCenter et les privilèges spécifiques aux outils ONTAP requis pour

effectuer les tâches principales d'administrateur des ONTAP tools for VMware vSphere.

NetApp ONTAP tools for VMware vSphere en lecture seule

Fournit un accès en lecture seule aux outils ONTAP. Ces utilisateurs ne peuvent effectuer aucune action des outils ONTAP pour VMware vSphere soumise à un contrôle d'accès.

NetApp ONTAP tools pour VMware vSphere Provision

Fournit certains des privilèges natifs du serveur vCenter et des privilèges spécifiques aux outils ONTAP qui sont nécessaires au provisionnement du stockage. Vous pouvez effectuer les tâches suivantes :

- Créer de nouveaux datastores
- Gérer les datastores

vSphere objets et backends de stockage ONTAP

Les deux environnements RBAC fonctionnent de concert. Lors de l'exécution d'une tâche dans l'interface client vSphere, les rôles des outils ONTAP définis pour le serveur vCenter sont vérifiés en premier. Si l'opération est autorisée par vSphere, alors les privilèges du rôle ONTAP sont examinés. Cette seconde étape est effectuée en fonction du rôle ONTAP attribué à l'utilisateur lors de la création et de la configuration du stockage principal.

Utilisation du contrôle d'accès basé sur les rôles (RBAC) du serveur vCenter

Il y a quelques éléments à prendre en compte lors de la gestion des privilèges et des autorisations du serveur vCenter.

Privilèges requis

Pour accéder à l'interface utilisateur ONTAP tools for VMware vSphere 10, vous devez disposer du privilège *View* spécifique à ONTAP tools. Si vous vous connectez à vSphere sans ce privilège et 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'attribution dans la hiérarchie des objets vSphere détermine les parties de l'interface utilisateur auxquelles vous pouvez accéder. L'attribution du privilège « View » à l'objet racine vous permet d'accéder aux ONTAP tools for VMware vSphere en cliquant sur l'icône NetApp.

Vous pouvez également attribuer le privilège d'affichage à un niveau d'objet vSphere inférieur. Cependant, cela limitera les menus des ONTAP tools for VMware vSphere auxquels vous pouvez accéder et utiliser.

Attribution des autorisations

Vous devez utiliser les autorisations du serveur vCenter si vous souhaitez limiter l'accès aux objets et tâches vSphere. L'endroit où vous attribuez l'autorisation dans la hiérarchie des objets vSphere détermine les tâches ONTAP tools for VMware vSphere 10 que les utilisateurs peuvent effectuer.

Sauf si vous devez définir un accès plus restrictif, il est généralement conseillé d'attribuer les autorisations au niveau de l'objet racine ou du dossier racine.

Les autorisations disponibles avec ONTAP tools for VMware vSphere 10 s'appliquent aux objets non-vSphere personnalisés, tels que les systèmes de stockage. Dans la mesure du possible, vous devez attribuer ces autorisations à l'objet racine ONTAP tools for VMware vSphere, car il n'existe aucun objet vSphere auquel vous pouvez les attribuer. Par exemple, toute autorisation incluant le privilège « Ajouter/Modifier/Supprimer des systèmes de stockage » d'ONTAP tools for VMware vSphere doit être attribuée au niveau de l'objet racine.

Lors de la définition d'une autorisation à un niveau supérieur de la hiérarchie des objets, vous pouvez configurer l'autorisation pour qu'elle soit transmise et héritée par les objets enfants. Si nécessaire, vous pouvez attribuer aux objets enfants des autorisations supplémentaires qui remplacent celles héritées du parent.

Vous pouvez modifier une autorisation à tout moment. Si vous modifiez l'un des privilèges au sein d'une autorisation, les utilisateurs associés à l'autorisation doivent se déconnecter de vSphere puis se reconnecter pour que la modification soit prise en compte.

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.