RBAC avec VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
November 04, 2025

Sommaire

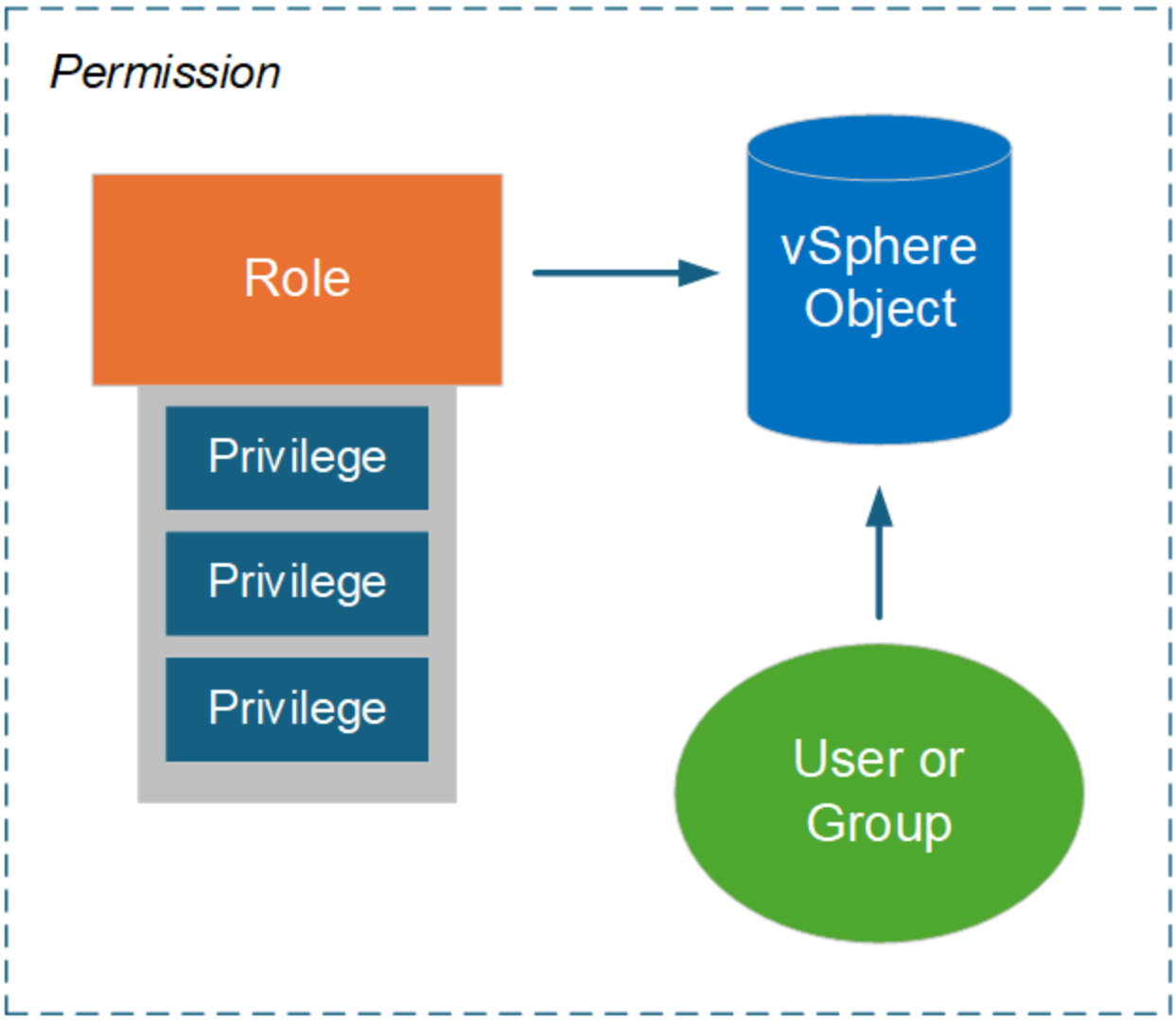
RBAC avec VMware vSphere

Environnement vCenter Server RBAC avec ONTAP tools for VMware vSphere 10

VMware vCenter Server fournit une fonctionnalité RBAC qui vous permet de contrôler l'accès aux objets vSphere. Il s'agit d'un élément important des services de sécurité d'authentification et d'autorisation centralisés de vCenter.

Illustration d'une autorisation vCenter Server

Une autorisation constitue la base de l'application du contrôle d'accès dans l'environnement vCenter Server. Il est appliqué à un objet vSphere avec un utilisateur ou un groupe inclus dans la définition d'autorisation. Une illustration de haut niveau d'une autorisation vCenter est fournie dans la figure ci-dessous.



Composants d’une autorisation vCenter Server

Une autorisation vCenter Server est un package de plusieurs composants qui sont liés entre eux 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 banques de données, les centres de données et les dossiers. En fonction des autorisations attribuées à l’objet, vCenter Server détermine quelles actions ou tâches peuvent être effectuées sur l’objet par chaque utilisateur ou groupe. Pour les tâches spécifiques aux ONTAP tools for VMware vSphere, toutes les autorisations sont attribuées et validées au niveau de la racine ou du dossier racine de vCenter Server. Voir "Utiliser 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 RBAC dans cet environnement, les outils ONTAP fournissent des rôles contenant les privilèges natifs et personnalisés requis. Les privilèges comprennent :

- Privilèges natifs du serveur vCenter

  Ce sont les privilèges fournis par vCenter Server.

- Privilèges spécifiques aux outils ONTAP

  Il s’agit de privilèges personnalisés propres aux ONTAP tools for 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.

Utiliser vCenter Server RBAC avec les ONTAP tools for VMware vSphere 10

Il existe plusieurs aspects des ONTAP tools for 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 devez uniquement définir et utiliser les rôles vCenter Server personnalisés 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 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 les ONTAP tools for VMware vSphere 10.

Hiérarchie des objets vSphere

L'inventaire des objets vSphere est organisé dans une hiérarchie. 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 les ONTAP tools for VMware vSphere 10

Pour simplifier l'utilisation de vCenter Server RBAC, les ONTAP tools for 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 selon vos besoins. Après avoir effectué les modifications de configuration, les utilisateurs du client vSphere concernés doivent se déconnecter et se reconnecter pour activer les modifications.

Pour afficher les ONTAP tools for VMware vSphere , sélectionnez **Menu** en haut du client vSphere et cliquez sur **Administration**, puis sur **Rôles** sur la gauche. Il existe trois rôles prédéfinis comme décrit ci-dessous.

ONTAP tools for VMware vSphere NetApp ONTAP pour VMware vSphere Administrator

Fournit tous les privilèges natifs de vCenter Server et les privilèges spécifiques aux outils ONTAP requis pour effectuer les tâches d'administrateur des ONTAP tools for VMware vSphere .

Outils NetApp ONTAP tools for VMware vSphere en lecture seule

Fournit un accès en lecture seule aux outils ONTAP . Ces utilisateurs ne peuvent pas exécuter d' ONTAP tools for VMware vSphere dont l'accès est contrôlé.

ONTAP tools for VMware vSphere NetApp ONTAP pour VMware vSphere Provision

Fournit certains des privilèges natifs de vCenter Server et des privilèges spécifiques aux outils ONTAP requis pour provisionner le stockage. Vous pouvez effectuer les tâches suivantes :

- Créer de nouveaux magasins de données
- Gérer les magasins de données

Objets vSphere et backends 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 sur vCenter Server sont vérifiés en premier. Si l'opération est autorisée par vSphere, les privilèges du rôle ONTAP sont examinés. Cette deuxième étape est effectuée en fonction du rôle ONTAP attribué à l'utilisateur lors de la création et de la configuration du backend de stockage.

Travailler avec vCenter Server RBAC

Il y a quelques éléments à prendre en compte lorsque vous travaillez avec les privilèges et autorisations de vCenter Server.

Privilèges requis

Pour accéder à l'interface utilisateur des ONTAP tools for VMware vSphere 10, vous devez disposer du privilège *View* spécifique aux outils ONTAP . Si vous vous connectez à vSphere sans ce privilège et cliquez sur l'icône NetApp , les ONTAP tools for VMware vSphere affichent un message d'erreur et vous empêchent 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 Affichage 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 Affichage à un autre niveau d'objet vSphere inférieur. Cependant, cela limitera les ONTAP tools for VMware vSphere auxquels vous pouvez accéder et que vous pouvez utiliser.

Attribution des autorisations

Vous devez utiliser les autorisations vCenter Server 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 ONTAP tools for VMware vSphere 10 que les utilisateurs peuvent effectuer.

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 ONTAP tools for VMware vSphere 10 s'appliquent aux objets non vSphere personnalisés, tels que les systèmes de stockage. Si possible, vous devez attribuer ces autorisations aux ONTAP tools for VMware vSphere, car il n'existe aucun objet vSphere auquel vous pouvez les attribuer. Par exemple, toute autorisation qui inclut un privilège « Ajouter/Modifier/Supprimer des systèmes de stockage » des 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 dans la hiérarchie des objets, vous pouvez configurer l'autorisation afin 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'un des privilèges d'une autorisation, les utilisateurs associés à l'autorisation doivent se déconnecter de vSphere et se reconnecter pour activer la modification.

Informations sur le copyright

Informations sur les marques commerciales