RBAC avec VMware vSphere

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Sommaire

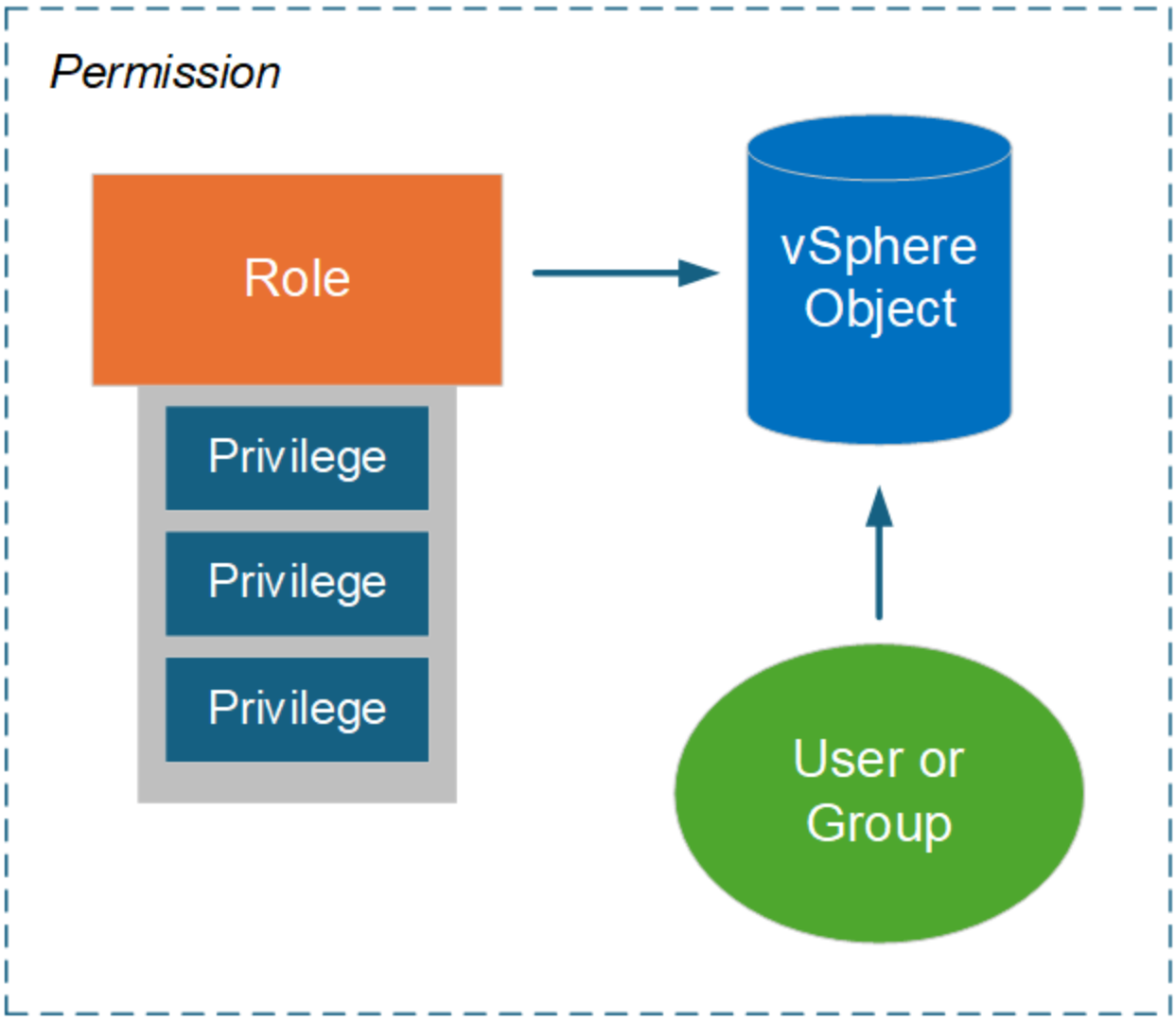
RBAC avec VMware vSphere

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.

Informations sur le copyright

Informations sur les marques commerciales