Contrôle d'accès basé sur des rôles

ONTAP tools for VMware vSphere 10.1

NetApp
June 21, 2024

Sommaire

Contrôle d’accès basé sur des rôles

Présentation du contrôle d’accès basé sur des rôles dans les outils ONTAP pour VMware vSphere

VCenter Server fournit un contrôle d’accès basé sur des rôles (RBAC) qui vous permet de contrôler l’accès aux objets vSphere. VCenter Server fournit des services d’authentification et d’autorisation centralisés à différents niveaux de son inventaire, en utilisant des droits d’utilisateur et de groupe avec des rôles et des privilèges. VCenter Server comprend cinq composants principaux pour la gestion du RBAC :

Composants	Description
Privilèges	Un privilège active ou refuse l’accès pour effectuer des actions dans vSphere.
Rôles	Un rôle contient un ou plusieurs privilèges système où chaque privilège définit un droit administratif à un objet ou un type d’objet donné dans le système. En attribuant un rôle à un utilisateur, celui-ci hérite des fonctionnalités des privilèges définis dans ce rôle.
Utilisateurs et groupes	Les utilisateurs et les groupes sont utilisés dans les autorisations pour attribuer des rôles à partir d’Active Directory (AD). VCenter Server dispose de ses propres utilisateurs et groupes locaux que vous pouvez utiliser.
Autorisations	Les autorisations vous permettent d’attribuer des privilèges aux utilisateurs ou aux groupes pour effectuer certaines actions et modifier les objets dans vCenter Server. Les autorisations vCenter Server affectent uniquement les utilisateurs qui se connectent à vCenter Server plutôt que les utilisateurs qui se connectent directement à un hôte ESXi.
Objet	Entité sur laquelle les actions sont exécutées. Les objets VMware vCenter sont des data centers, des dossiers, des pools de ressources, des clusters, des hôtes, et machines virtuelles

Pour effectuer correctement une tâche, vous devez disposer des rôles RBAC vCenter Server appropriés. Au cours d’une tâche, les outils ONTAP pour VMware vSphere vérifient les rôles du serveur vCenter d’un utilisateur avant de vérifier les privilèges ONTAP de l’utilisateur.

Les rôles de serveur vCenter s’appliquent aux outils ONTAP pour les utilisateurs de VMware vSphere vCenter, et non aux administrateurs. Par défaut, les administrateurs disposent d’un accès complet au produit et n’ont pas besoin de rôles qui leur sont attribués.

Les utilisateurs et les groupes peuvent accéder à un rôle en faisant partie d’un rôle vCenter Server.

Points clés sur l'attribution et la modification de rôles pour vCenter Server

Vous n'avez besoin de configurer des rôles vCenter Server que si vous souhaitez limiter l'accès aux objets et aux tâches vSphere. Sinon, vous pouvez vous connecter en tant qu'administrateur. Cette connexion vous permet automatiquement d'accéder à tous les objets vSphere.

L'affectation d'un rôle détermine les outils ONTAP pour les tâches VMware vSphere qu'un utilisateur peut effectuer. Vous pouvez modifier un rôle à tout moment. Si vous modifiez les privilèges d'un rôle, l'utilisateur associé à ce rôle doit se déconnecter, puis se reconnecter pour activer le rôle mis à jour.

Rôles standard fournis avec les outils ONTAP pour VMware vSphere

Pour simplifier l'utilisation des privilèges vCenter Server et du contrôle d'accès basé sur des rôles, les outils ONTAP pour VMware vSphere fournissent des outils ONTAP standard pour les rôles VMware vSphere, qui vous permettent d'exécuter les principaux outils ONTAP pour les tâches VMware vSphere. Il existe également un rôle en lecture seule qui vous permet d'afficher les informations, mais pas d'effectuer des tâches.

Vous pouvez afficher les outils ONTAP pour les rôles standard VMware vSphere en cliquant sur **Roles** sur la page d'accueil de vSphere client. Les rôles fournis par les outils ONTAP pour VMware vSphere vous permettent d'effectuer les tâches suivantes :

Rôle	Description
Outils NetApp ONTAP pour VMware vSphere Administrator	Fournit tous les privilèges vCenter Server natifs et les privilèges spécifiques aux outils ONTAP requis pour exécuter certains outils ONTAP pour les tâches VMware vSphere.
Outils NetApp ONTAP pour VMware vSphere en lecture seule	Accès en lecture seule aux outils ONTAP. Ces utilisateurs ne peuvent pas exécuter d'actions ONTAP Tools for VMware vSphere contrôlées par accès.
Outils NetApp ONTAP pour le provisionnement VMware vSphere	Fournit certains privilèges vCenter Server natifs et certains privilèges spécifiques aux outils ONTAP requis pour provisionner le stockage. Vous pouvez effectuer les tâches suivantes : • Créer de nouveaux datastores • Gérer les datastores

Le rôle admin du gestionnaire d'outils ONTAP n'est pas enregistré auprès de vCenter Server. Ce rôle est spécifique au gestionnaire d'outils ONTAP.

Si votre entreprise exige la mise en œuvre de rôles plus restrictifs que les outils ONTAP standard pour les rôles VMware vSphere, vous pouvez utiliser les outils ONTAP pour les rôles VMware vSphere pour créer de nouveaux rôles.

Dans ce cas, vous allez cloner les outils ONTAP nécessaires pour les rôles VMware vSphere, puis modifier le rôle cloné de sorte qu'il ne dispose que des privilèges dont votre utilisateur a besoin.

Autorisations pour les systèmes ONTAP back-end et les objets vSphere

Si l'autorisation vCenter Server est suffisante, les outils ONTAP pour VMware vSphere vérifient ensuite les privilèges RBAC ONTAP (votre rôle ONTAP) associés aux informations d'identification du système back-end

de stockage (le nom d'utilisateur et le mot de passe). déterminer si vous disposez des privilèges suffisants pour effectuer les opérations de stockage requises par la tâche ONTAP Tools for VMware vSphere sur ce back-end. Si vous disposez des privilèges ONTAP appropriés, vous pouvez accéder au Systèmes back-end de stockage et exécution des outils ONTAP pour les tâches VMware vSphere. Les rôles ONTAP déterminent les outils ONTAP pour les tâches VMware vSphere que vous pouvez effectuer sur le back-end de stockage.

Composants des autorisations de vCenter Server

VCenter Server reconnaît les autorisations et non les privilèges. Chaque autorisation vCenter Server comprend trois composants.

VCenter Server dispose des composants suivants :

- Un ou plusieurs privilèges (le rôle)

  Les privilèges définissent les tâches qu'un utilisateur peut effectuer.

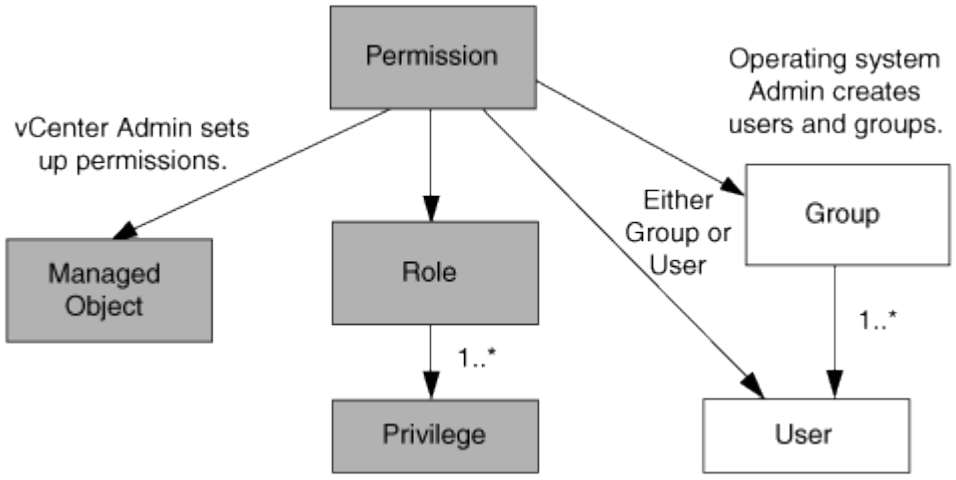
- Un objet vSphere

  L'objet est la cible des tâches.

- Un utilisateur ou un groupe

  L'utilisateur ou le groupe définit qui peut effectuer la tâche.

Dans ce diagramme, les cases grises indiquent les composants qui existent dans vCenter Server et les cases blanches indiquent les composants qui existent dans le système d'exploitation où le serveur vCenter est exécuté.



Privilèges

Deux types de privilèges sont associés aux outils ONTAP pour VMware vSphere :

- Privilèges de serveur vCenter natif

  Ces privilèges sont fournis avec vCenter Server.

- Privilèges spécifiques aux outils ONTAP

  Ces privilèges sont définis pour des outils ONTAP spécifiques pour les tâches VMware vSphere. Elles sont spécifiques aux outils ONTAP pour VMware vSphere.

Les outils ONTAP pour les tâches VMware vSphere requièrent à la fois des privilèges spécifiques aux outils ONTAP et des privilèges natifs du serveur vCenter. Ces privilèges constituent le « rôle » pour l'utilisateur. Une autorisation peut avoir plusieurs privilèges. Ces privilèges concernent un utilisateur connecté à vCenter Server.

> Pour simplifier l'utilisation de vCenter Server RBAC, les outils ONTAP pour VMware vSphere fournissent plusieurs rôles standard qui contiennent tous les privilèges natifs et spécifiques aux outils ONTAP nécessaires à l'exécution des outils ONTAP pour les tâches VMware vSphere.

Si vous modifiez les privilèges dans une autorisation, l'utilisateur associé à cette autorisation doit se déconnecter, puis se connecter pour activer l'autorisation mise à jour.

Objets vSphere

Les autorisations sont associées aux objets vSphere, tels que vCenter Server, les hôtes ESXi, les machines virtuelles, les datastores, les data centers, et les dossiers. Vous pouvez attribuer des autorisations à n'importe quel objet vSphere. En fonction de l'autorisation attribuée à un objet vSphere, vCenter Server détermine qui peut effectuer les tâches sur cet objet. Pour les tâches spécifiques aux outils ONTAP pour VMware vSphere, les autorisations sont attribuées et validées uniquement au niveau du dossier racine (serveur vCenter) et non sur une autre entité. À l'exception de l'opération de plug-in VAAI, où les autorisations sont validées par rapport à l'hôte ESXi concerné.

Utilisateurs et groupes

Vous pouvez utiliser Active Directory (ou la machine vCenter Server locale) pour configurer des utilisateurs et des groupes d'utilisateurs. Vous pouvez ensuite utiliser les autorisations vCenter Server pour accorder l'accès à ces utilisateurs ou groupes afin de leur permettre d'exécuter des outils ONTAP spécifiques pour les tâches VMware vSphere.

> Ces autorisations vCenter Server s'appliquent aux outils ONTAP pour les utilisateurs de VMware vSphere vCenter, et non aux outils ONTAP pour les administrateurs VMware vSphere. Par défaut, les outils ONTAP pour les administrateurs VMware vSphere bénéficient d'un accès complet au produit et ne nécessitent pas d'autorisations qui leur sont attribuées.

Les utilisateurs et les groupes n'ont pas de rôles qui leur sont attribués. Ils ont accès à un rôle en faisant partie de l'autorisation vCenter Server.

Attribuer et modifier des autorisations pour vCenter Server

Lorsque vous travaillez avec des autorisations vCenter Server, vous devez garder à l'esprit plusieurs points clés. La réussite d'une tâche d'outils ONTAP pour VMware vSphere peut dépendre de l'endroit où vous avez attribué une autorisation ou des actions qu'un utilisateur a effectuées après la modification d'une autorisation.

Attribution d’autorisations

Vous n’avez besoin de configurer les autorisations vCenter Server que si vous souhaitez limiter l’accès aux objets et aux tâches vSphere. Sinon, vous pouvez vous connecter en tant qu’administrateur. Cette connexion vous permet automatiquement d’accéder à tous les objets vSphere.

L’emplacement où vous attribuez des autorisations détermine les outils ONTAP pour les tâches VMware vSphere qu’un utilisateur peut effectuer.

Parfois, pour garantir l’exécution d’une tâche, vous devez attribuer une autorisation à un niveau supérieur, tel que l’objet racine. C’est le cas lorsqu’une tâche nécessite un privilège qui ne s’applique pas à un objet vSphere spécifique (par exemple, le suivi de la tâche) ou lorsqu’un privilège requis s’applique à un objet non vSphere (par exemple, un système de stockage).

Dans ce cas, vous pouvez configurer une autorisation de sorte qu’elle soit héritée par les entités enfants. Vous pouvez également attribuer d’autres autorisations aux entités enfants. La permission attribuée à une entité enfant remplace toujours l’autorisation héritée de l’entité parent. Cela signifie que vous pouvez donner des autorisations à une entité enfant pour restreindre la portée d’une autorisation attribuée à un objet racine et héritée par l’entité enfant.

À moins que les règles de sécurité de votre entreprise ne nécessitent des autorisations plus restrictives, il est conseillé d’attribuer des autorisations à l’objet racine (également appelé dossier racine).

Autorisations et objets non vSphere

L’autorisation que vous créez est appliquée à un objet non vSphere. Par exemple, un système de stockage n’est pas un objet vSphere. Si un privilège s’applique à un système de stockage, vous devez attribuer l’autorisation contenant ce privilège aux outils ONTAP pour l’objet racine VMware vSphere car il n’existe aucun objet vSphere auquel vous pouvez l’attribuer.

Par exemple, toute autorisation qui inclut un privilège tel que le privilège Outils ONTAP pour VMware vSphere « Ajouter/Modifier/Ignorer les systèmes de stockage » doit être attribuée au niveau de l’objet racine.

Modification des autorisations

Vous pouvez modifier une autorisation à tout moment.

Si vous modifiez les privilèges dans une autorisation, l’utilisateur associé à cette autorisation doit se déconnecter puis se reconnecter pour activer l’autorisation mise à jour.

Privilèges requis pour les outils ONTAP pour les tâches VMware vSphere

Différents outils ONTAP pour les tâches VMware vSphere requièrent différentes combinaisons de privilèges spécifiques aux outils ONTAP pour VMware vSphere et aux privilèges vCenter Server natifs.

Pour accéder aux outils ONTAP de l’interface utilisateur graphique de VMware vSphere, vous devez disposer du privilège de vue spécifique aux outils ONTAP au niveau du produit, attribué au niveau d’objet vSphere approprié. Si vous vous connectez sans ce privilège, ONTAP Tools for VMware vSphere affiche un message d’erreur lorsque vous cliquez sur l’icône NetApp et vous empêche d’accéder aux outils ONTAP.

Avec le privilège **View**, vous pouvez accéder aux outils ONTAP pour VMware vSphere. Ce privilège ne vous permet pas d'effectuer des tâches dans les outils ONTAP pour VMware vSphere. Pour exécuter des tâches ONTAP Tools for VMware vSphere, vous devez disposer des privilèges vCenter Server natifs et spécifiques aux outils ONTAP pour ces tâches.

Le niveau d'affectation détermine les parties de l'interface utilisateur que vous pouvez voir. L'attribution du privilège d'affichage à l'objet racine (dossier) vous permet d'accéder aux outils ONTAP pour VMware vSphere en cliquant sur l'icône NetApp.

Vous pouvez attribuer le privilège View à un autre niveau d'objet vSphere. Cependant, cela limite les outils ONTAP pour les menus VMware vSphere que vous pouvez voir et utiliser.

L'objet racine est l'endroit recommandé pour attribuer une autorisation contenant le privilège d'affichage.

Rôles ONTAP recommandés pour les outils ONTAP pour VMware vSphere

Vous pouvez définir plusieurs rôles ONTAP recommandés pour l'utilisation des outils ONTAP pour VMware vSphere et le contrôle d'accès basé sur des rôles (RBAC). Ces rôles contiennent les privilèges ONTAP requis pour effectuer les opérations de stockage exécutées par les outils ONTAP pour les tâches VMware vSphere.

Pour créer de nouveaux rôles utilisateur, vous devez vous connecter en tant qu'administrateur des systèmes de stockage exécutant ONTAP. Vous pouvez créer des rôles ONTAP à l'aide de ONTAP System Manager 9.8P1 ou version ultérieure.

Chaque rôle ONTAP est associé à une paire nom d'utilisateur et mot de passe, qui constituent les informations d'identification du rôle. Si vous ne vous connectez pas à l'aide de ces informations d'identification, vous ne pouvez pas accéder aux opérations de stockage associées au rôle.

Par mesure de sécurité, les outils ONTAP pour les rôles ONTAP spécifiques à VMware vSphere sont classés de manière hiérarchique. Cela signifie que le premier rôle est le plus restrictif et ne dispose que des privilèges associés à l'ensemble d'outils ONTAP le plus basique pour les opérations de stockage VMware vSphere. Le rôle suivant comprend ses propres privilèges et tous les privilèges associés au rôle précédent. Chaque rôle supplémentaire est moins restrictif quant aux opérations de stockage prises en charge.

Voici quelques-uns des rôles ONTAP RBAC recommandés lors de l'utilisation des outils ONTAP pour VMware vSphere. Après avoir créé ces rôles, vous pouvez les attribuer à des utilisateurs qui doivent effectuer des tâches liées au stockage, telles que le provisionnement de machines virtuelles.

Rôle	**privilèges**
Détection	Il permet donc d'ajouter des systèmes de stockage.
Créer un stockage	Grâce à ce rôle, vous pouvez créer du stockage. Ce rôle inclut également tous les privilèges associés au rôle découverte.
Modifier le stockage	Ce rôle vous permet de modifier le stockage. Ce rôle inclut également tous les privilèges associés au rôle découverte et au rôle Créer un stockage.

Détruire le stockage	Vous pouvez ainsi détruire le stockage. Ce rôle inclut également tous les privilèges associés au rôle découverte, au rôle Créer un stockage et au rôle Modifier le stockage.

Si vous utilisez les outils ONTAP pour VMware vSphere, vous devez également configurer un rôle de gestion basée sur des règles (PBM). Il permet de gérer le stockage à l'aide de règles de stockage. Ce rôle requiert également que vous ayez défini le rôle « questions à poser ».

Informations sur le copyright

Informations sur les marques commerciales