Contrôle d'accès basé sur des rôles

ONTAP tools for VMware vSphere 9.13

NetApp
December 17, 2025

Sommaire

Contrôle d’accès basé sur des rôles

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

VCenter Server fournit un contrôle d’accès basé sur des rôles (RBAC) qui vous permet de contrôler l’accès aux objets vSphere. Dans les outils ONTAP® pour VMware vSphere, vCenter Server RBAC fonctionne avec ONTAP RBAC pour déterminer les tâches d’outils ONTAP qu’un utilisateur spécifique peut effectuer sur des objets d’un système de stockage spécifique.

Pour réussir une tâche, vous devez disposer des autorisations appropriées pour le contrôle d’accès basé sur les rôles du serveur vCenter. Au cours d’une tâche, les outils ONTAP vérifient les autorisations du serveur vCenter d’un utilisateur avant de vérifier les privilèges ONTAP de l’utilisateur.

Vous pouvez définir les autorisations de vCenter Server sur l’objet racine (également appelé dossier racine). Vous pouvez ensuite affiner la sécurité en limitant les entités enfants qui n’ont pas besoin de ces autorisations.

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

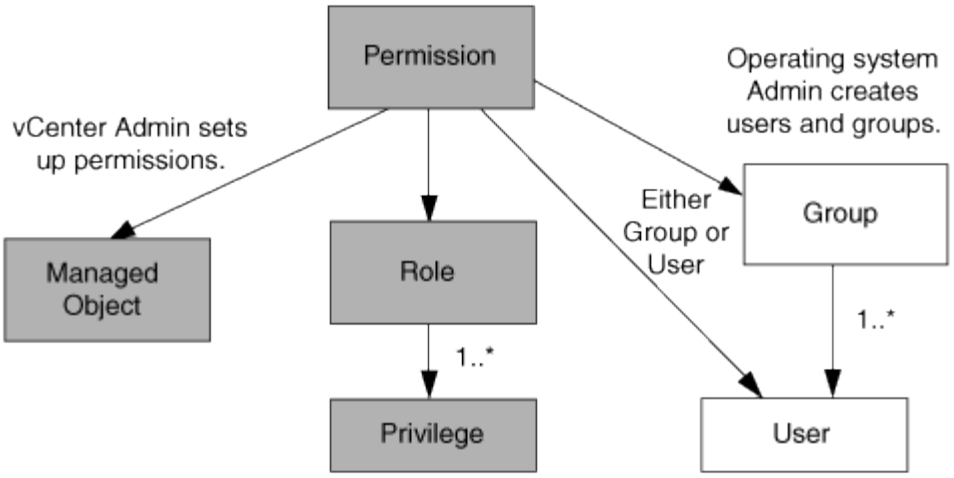
  L’objet est la cible des tâches.

- Un utilisateur ou un groupe

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

Comme le montre le diagramme suivant, vous devez disposer des trois éléments pour avoir une autorisation.

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 tâches spécifiques des outils ONTAP. Ils sont spécifiques aux outils ONTAP.

Les tâches relatives aux outils ONTAP 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 proposent plusieurs rôles standard qui contiennent tous les privilèges natifs et spécifiques aux outils ONTAP requis pour effectuer les tâches des outils ONTAP.

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.

Privilège	Rôles	Tâches
Console des outils NetApp ONTAP > Afficher	• Administrateur VSC • Provisionnement VSC • VSC en lecture seule	Tous les outils ONTAP pour les tâches spécifiques à VMware vSphere et VASA Provider nécessitent le privilège View.
NetApp Virtual Storage Console > gestion basée sur des règles > gestion ou privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label > gestion	Administrateur VSC	Outils ONTAP pour VMware vSphere et tâches VASA Provider liées aux profils de fonctionnalités de stockage et aux paramètres de seuil.

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, les autorisations sont attribuées et validées uniquement au niveau du dossier racine (serveur vCenter) et non sur une autre entité. Sauf pour le fonctionnement du plug-in VAAI, où les autorisations sont validées par rapport à l'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 du serveur vCenter pour accorder l'accès à ces utilisateurs ou groupes afin de leur permettre d'effectuer des tâches spécifiques aux outils ONTAP.

> Ces autorisations vCenter Server s'appliquent aux utilisateurs vCenter des outils ONTAP, 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.

Points clés concernant l'attribution et la modification 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 une autorisation détermine les tâches des outils ONTAP qu'un utilisateur peut effectuer.

Parfois, pour assurer la réalisation d'une tâche, vous devez attribuer l'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 autoriser une entité enfant pour restreindre la portée d'une autorisation qui a été 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 à l'objet racine des outils ONTAP 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 « 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.

Rôles standard fournis avec les outils ONTAP

Pour simplifier l'utilisation des privilèges du serveur vCenter et du contrôle d'accès basé sur les rôles (RBAC), les outils ONTAP fournissent des rôles d'outils ONTAP standard qui vous permettent d'effectuer des tâches clés des outils ONTAP. Il existe également un rôle en lecture seule qui vous permet d'afficher les informations, mais pas d'effectuer des tâches.

Les rôles d'outils ONTAP standard possèdent à la fois les privilèges spécifiques aux outils ONTAP requis et les privilèges de serveur vCenter natif requis pour que les utilisateurs puissent effectuer des tâches d'outils ONTAP. En outre, les rôles sont configurés de manière à disposer des privilèges requis pour toutes les versions prises en charge de vCenter Server.

En tant qu'administrateur, vous pouvez attribuer ces rôles aux utilisateurs selon les besoins.

Lorsque vous mettez à niveau les outils ONTAP vers la dernière version, les rôles standard sont automatiquement mis à niveau pour fonctionner avec la nouvelle version de l'outil.

Vous pouvez afficher les rôles standard des outils ONTAP en cliquant sur **Roles** sur la page d'accueil du client vSphere.

Les rôles fournis par les outils ONTAP vous permettent d'effectuer les tâches suivantes :

Rôle	Description
Administrateur VSC	Fournit tous les privilèges natifs du serveur vCenter et les privilèges spécifiques aux outils ONTAP requis pour effectuer toutes les tâches des outils ONTAP.

VSC 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.
Provisionnement VSC	Fournit tous les privilèges de serveur vCenter natif et les privilèges spécifiques aux outils ONTAP requis pour provisionner le stockage. Vous pouvez effectuer les tâches suivantes : • Créer de nouveaux datastores • Détruire les datastores • Afficher des informations sur les profils de capacité de stockage

Instructions d'utilisation des rôles standard des outils ONTAP

Lorsque vous utilisez les outils ONTAP standard pour les rôles VMware vSphere, vous devez suivre certaines directives.

Vous ne devez pas modifier directement les rôles standard. Si c'est le cas, les outils ONTAP écraseront vos modifications chaque fois que vous effectuez une mise à niveau. Le programme d'installation met à jour les définitions de rôles standard chaque fois que vous mettez à niveau les outils ONTAP. Cela permet de s'assurer que les rôles sont à jour pour votre version des outils ONTAP pour VMware vSphere ainsi que pour toutes les versions prises en charge du serveur vCenter.

Vous pouvez toutefois utiliser les rôles standard pour créer des rôles adaptés à votre environnement. Pour ce faire, vous devez copier le rôle standard des outils ONTAP, puis modifier le rôle copié. En créant un nouveau rôle, vous pouvez conserver ce rôle même lorsque vous redémarrez ou mettez à niveau le service Windows des outils ONTAP.

Vous pouvez utiliser les rôles standard des outils ONTAP de différentes façons :

- Utilisez les rôles d'outils ONTAP standard pour toutes les tâches d'outils ONTAP.

  Dans ce scénario, les rôles standard fournissent tous les privilèges dont un utilisateur a besoin pour effectuer les tâches des outils ONTAP.

- Associer des rôles pour développer les tâches qu'un utilisateur peut effectuer.

  Si les rôles standard des outils ONTAP apportent une granularité excessive à votre environnement, vous pouvez développer les rôles en créant des groupes de niveau supérieur contenant plusieurs rôles.

  Si un utilisateur doit effectuer d'autres tâches d'outils non ONTAP qui nécessitent des privilèges vCenter Server natifs supplémentaires, vous pouvez créer un rôle qui fournit ces privilèges et l'ajouter au groupe.

- Créer des rôles plus précis.

  Si votre entreprise exige que vous mettiez en œuvre des rôles plus restrictifs que les rôles standard pour les outils ONTAP, vous pouvez utiliser les rôles des outils ONTAP pour créer de nouveaux rôles.

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

Privilèges requis pour les tâches des outils ONTAP

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 plus d'informations sur les privilèges requis pour les tâches relatives aux outils ONTAP, consultez l'article 1032542 de la base de connaissances NetApp.

"Outils ONTAP pour VMware vSphere : configuration RBAC"

Privilège au niveau du produit requis par les outils ONTAP pour VMware vSphere

Pour accéder à l'interface graphique ONTAP Tools for 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 affiche un message d'erreur lorsque vous cliquez sur l'icône NetApp et vous empêche d'accéder aux outils ONTAP.

Dans le privilège **Afficher**, vous pouvez accéder à l'interface graphique des outils ONTAP. Ce privilège ne vous permet pas d'effectuer des tâches dans les outils ONTAP. Pour effectuer des tâches d'outils ONTAP, 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 en cliquant sur l'icône NetApp.

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

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

Autorisations pour les systèmes de stockage ONTAP et les objets vSphere

Le contrôle d'accès basé sur des rôles (RBAC) de ONTAP vous permet de contrôler l'accès aux systèmes de stockage spécifiques et de contrôler les actions qu'un utilisateur peut effectuer sur ces systèmes. Dans les outils ONTAP® pour VMware vSphere, ONTAP RBAC fonctionne avec vCenter Server RBAC pour déterminer les tâches d'outils ONTAP qu'un utilisateur spécifique peut effectuer sur les objets d'un système de stockage spécifique.

Les outils ONTAP utilisent les informations d'identification (nom d'utilisateur et mot de passe) que vous configurez dans les outils ONTAP pour authentifier chaque système de stockage et déterminer les opérations de stockage qui peuvent être effectuées sur ce système de stockage. Les outils ONTAP utilisent un ensemble d'informations d'identification pour chaque système de stockage. Ces informations d'identification déterminent les tâches des outils ONTAP qui peuvent être effectuées sur ce système de stockage. En d'autres termes, elles sont destinées aux outils ONTAP et non à un utilisateur individuel des outils ONTAP.

Le contrôle d'accès basé sur des rôles ONTAP s'applique uniquement à l'accès aux systèmes de stockage et à l'exécution de tâches d'outils ONTAP en rapport avec le stockage, telles que le provisionnement de machines virtuelles. Si vous ne disposez pas des privilèges ONTAP RBAC appropriés pour un système de

stockage spécifique, vous ne pouvez pas effectuer de tâches sur un objet vSphere hébergé sur ce système de stockage. Vous pouvez utiliser ONTAP RBAC en association avec les privilèges spécifiques aux outils ONTAP pour contrôler les tâches des outils ONTAP qu'un utilisateur peut effectuer :

- Surveillance et configuration d'objets de stockage ou vCenter Server résidant sur un système de stockage
- Provisionnement d'objets vSphere résidant sur un système de stockage

L'utilisation du contrôle d'accès basé sur des rôles ONTAP avec les privilèges spécifiques aux outils ONTAP offre une couche de sécurité orientée stockage que l'administrateur du stockage peut gérer. Par conséquent, le contrôle d'accès est plus granulaire que ce que vous ne pouvez prendre en charge que le RBAC ONTAP seul ou le RBAC vCenter Server. Par exemple, avec le RBAC de vCenter Server, vous pouvez permettre à vCenter UserB de provisionner un datastore sur le stockage NetApp tout en empêchant vCenter UserA de provisionner des datastores. Si les informations d'identification du système de stockage pour un système de stockage spécifique ne prennent pas en charge la création de stockage, ni vCenter UserB ni vCenter UserA ne peuvent provisionner un datastore sur ce système de stockage.

Lorsque vous lancez une tâche d'outils ONTAP, les outils ONTAP vérifient d'abord si vous disposez de l'autorisation de serveur vCenter appropriée pour cette tâche. Si l'autorisation du serveur vCenter n'est pas suffisante pour vous permettre d'effectuer la tâche, les outils ONTAP n'ont pas besoin de vérifier les privilèges ONTAP pour ce système de stockage car vous n'avez pas passé le contrôle de sécurité initial du serveur vCenter. Dans ce cas, vous ne pouvez pas accéder au système de stockage.

Si l'autorisation vCenter Server est suffisante, les outils ONTAP vérifient ensuite les privilèges RBAC ONTAP (votre rôle ONTAP) associés aux informations d'identification du système 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 sur ce système de stockage. Si vous disposez des privilèges ONTAP appropriés, vous pouvez accéder au système de stockage et effectuer la tâche Outils ONTAP. Les rôles ONTAP déterminent les tâches d'outils ONTAP que vous pouvez effectuer sur le système de stockage.

Chaque système de stockage dispose d'un ensemble de privilèges ONTAP qui lui sont associés.

L'utilisation de RBAC ONTAP et du RBAC vCenter Server offre les avantages suivants :

- Sécurité

  L'administrateur peut déterminer les utilisateurs qui peuvent effectuer les tâches au niveau objet précis de vCenter Server et au niveau du système de stockage.

- Informations d'audit

  Dans de nombreux cas, les outils ONTAP fournissent une piste d'audit sur le système de stockage qui vous permet de suivre les événements vers l'utilisateur vCenter Server qui a effectué les modifications de stockage.

- Facilité d'utilisation

  Vous pouvez conserver toutes les informations d'identification du contrôleur en un seul emplacement.

Rôles ONTAP recommandés pour l'utilisation des outils ONTAP pour VMware vSphere

Vous pouvez configurer plusieurs rôles ONTAP recommandés pour utiliser les outils ONTAP® pour VMware vSphere et le contrôle d'accès basé sur les rôles (RBAC). Ces rôles contiennent les privilèges ONTAP requis pour effectuer les opérations de stockage requises qui sont exécutées par les tâches des outils ONTAP.

Pour créer de nouveaux rôles utilisateur, vous devez vous connecter en tant qu'administrateur sur les systèmes de stockage exécutant ONTAP. Vous pouvez créer des rôles ONTAP à l'aide de ONTAP System Manager 9.8P1 ou version ultérieure. Voir "Configurez les rôles et privilèges utilisateur" pour en savoir plus.

Chaque rôle ONTAP est associé à un nom d'utilisateur et une paire de mots de passe qui constituent les identifiants 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.

À titre de mesure de sécurité, les rôles ONTAP spécifiques aux outils ONTAP sont classés de manière hiérarchique. Cela signifie que le premier rôle est le rôle le plus restrictif et ne dispose que des privilèges associés à l'ensemble le plus basique d'opérations de stockage des outils ONTAP. Le rôle suivant inclut à la fois ses propres privilèges et tous les privilèges associés au rôle précédent. Chaque rôle supplémentaire est moins restrictif en termes de termes de limites au niveau des opérations de stockage prises en charge.

Voici quelques-uns des rôles ONTAP RBAC recommandés lors de l'utilisation d'outils ONTAP. Une fois ces rôles créés, vous pouvez attribuer les rôles aux utilisateurs qui doivent effectuer des tâches associées au stockage, par exemple le provisionnement de machines virtuelles.

1. Détection

   Il permet donc d'ajouter des systèmes de stockage.

2. Créer un stockage

   Grâce à ce rôle, vous pouvez créer du stockage. Ce rôle inclut également l'ensemble des privilèges associés au rôle découverte.

3. 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.

4. 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 VASA Provider pour ONTAP, vous devez également définir 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 ».

Configuration du contrôle d'accès basé sur des rôles ONTAP pour les outils ONTAP pour VMware vSphere

Vous devez configurer le contrôle d'accès basé sur des rôles (RBAC) ONTAP sur le système de stockage si vous souhaitez utiliser le contrôle d'accès basé sur des rôles avec les outils ONTAP pour VMware vSphere. Vous pouvez créer un ou plusieurs comptes utilisateur personnalisés avec des privilèges d'accès limités grâce à la fonction RBAC ONTAP.

Les outils ONTAP pour VMware vSphere et SRA peuvent accéder aux systèmes de stockage au niveau du cluster ou des SVM. Si vous ajoutez des systèmes de stockage au niveau du cluster, vous devez fournir les

identifiants de l'utilisateur admin pour fournir toutes les fonctionnalités requises. Si vous ajoutez des systèmes de stockage en ajoutant directement des détails SVM, vous devez savoir que l'utilisateur « vsadmin » n'a pas tous les rôles et les fonctionnalités nécessaires pour effectuer certaines tâches.

Vasa Provider ne peut accéder aux systèmes de stockage qu'au niveau du cluster. Si VASA Provider est requis pour un contrôleur de stockage spécifique, le système de stockage doit être ajouté aux outils ONTAP pour VMware vSphere au niveau du cluster, même si vous utilisez des outils ONTAP ou SRA.

Pour créer un nouvel utilisateur et connecter un cluster ou un SVM aux outils ONTAP, il faut effectuer les opérations suivantes :

- Créer un rôle d'administrateur de cluster ou SVM à l'aide de ONTAP System Manager 9.8P1 ou version ultérieure. Voir "Configurez les rôles et privilèges utilisateur" pour en savoir plus.
- Créez des utilisateurs avec le rôle attribué et le jeu d'applications approprié à l'aide de ONTAP

  Vous avez besoin de ces informations d'identification pour configurer les systèmes de stockage pour les outils ONTAP. Vous pouvez configurer les systèmes de stockage pour les outils ONTAP en saisissant les informations d'identification dans les outils ONTAP. Chaque fois que vous vous connectez à un système de stockage avec ces informations d'identification, vous disposez des autorisations nécessaires pour accéder aux fonctions des outils ONTAP que vous avez configurées dans ONTAP lors de la création des informations d'identification.

- Ajoutez le système de stockage aux outils ONTAP pour VMware vSphere et fournissez les informations d'identification de l'utilisateur que vous venez de créer

Rôles des outils ONTAP

Les outils ONTAP classifient les privilèges ONTAP en l'ensemble suivant de rôles d'outils ONTAP :

- Détection

  Permet la détection de tous les contrôleurs de stockage connectés

- Créer un stockage

  Création de volumes et de LUN

- Modifier le stockage

  Permet le redimensionnement et la déduplication des systèmes de stockage

- Détruire le stockage

  Permet la destruction de volumes et de LUN

Rôles de VASA Provider

Vous pouvez créer uniquement une gestion basée sur des règles au niveau du cluster. Ce rôle permet la gestion du stockage basée sur des règles à l'aide de profils de fonctions de stockage.

Rôles SRA

SRA classifie les privilèges d'ONTAP en rôle SAN ou NAS au niveau du cluster ou des SVM. Les utilisateurs peuvent ainsi exécuter des opérations SRM.

Les outils ONTAP valident les privilèges initiaux des rôles ONTAP RBAC lorsque vous ajoutez le cluster aux outils ONTAP. Si vous avez ajouté une IP de stockage utilisateur SVM, les outils ONTAP n'effectuent pas la validation initiale. Les outils ONTAP vérifient et appliquent les privilèges ultérieurement dans le flux de travail des tâches.