# Privilèges requis pour les tâches VSC

VSC, VASA Provider, and SRA 9.7

NetApp
April 01, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/vsc-vasa-provider-sra-97/deploy/reference-product-level-privilege-required-by-vsc-for-vmware-vsphere.html on April 01, 2025. Always check docs.netapp.com for the latest.

# Sommaire


Privilèges requis pour les tâches VSC . . . 1
- Privilèges de niveau produit requis par VSC pour VMware vSphere . . . 1
- Contrôle d’accès basé sur des rôles ONTAP pour l’appliance virtuelle pour VSC, VASA Provider et SRA . . . 1
- Rôles ONTAP recommandés lors de l’utilisation de VSC pour VMware vSphere . . . 3
- Comment configurer le contrôle d’accès basé sur des rôles ONTAP pour VSC pour VMware vSphere . . . 4
  - Rôles VSC . . . 5
  - Rôles de VASA Provider . . . 5
  - Rôles SRA . . . 5
- Configurez les rôles et privilèges utilisateur . . . 5

# Privilèges requis pour les tâches VSC

Les différentes tâches de Virtual Storage Console pour VMware vSphere nécessitent différentes combinaisons de privilèges spécifiques à (VSC) et vCenter Server natif.

Pour plus d'informations sur les privilèges requis pour les tâches VSC, consultez l'article 1032542 de la base de connaissances NetApp.

"Comment configurer le RBAC pour Virtual Storage Console"

## Privilèges de niveau produit requis par VSC pour VMware vSphere

Pour accéder à l'interface graphique Virtual Storage Console pour VMware vSphere, vous devez disposer du privilège VSC-Specific View (vue) au niveau du produit, qui est attribué au niveau de l'objet vSphere approprié. Si vous vous connectez sans ce privilège, VSC affiche un message d'erreur lorsque vous cliquez sur l'icône NetApp et vous empêche d'accéder à VSC.

Les informations suivantes décrivent le privilège VSC Product-Level View :

| Privilège | Description | Niveau d'affectation |
|---|---|---|
| Afficher | Vous pouvez accéder à l'interface graphique de VSC. Ce privilège ne vous permet pas d'effectuer des tâches dans VSC. Pour effectuer toutes les tâches VSC, vous devez disposer des privilèges vCenter Server natifs et spécifiques à VSC pour ces tâches. | Le niveau d'affectation détermine les parties de l'interface utilisateur que vous pouvez voir.<br><br>L'attribution du privilège View (View) à l'objet racine (dossier) vous permet d'entrer dans VSC en cliquant sur l'icône NetApp.<br><br>Vous pouvez attribuer le privilège View à un autre niveau d'objets vSphere. Toutefois, vous pouvez limiter les menus VSC que vous pouvez voir et utiliser.<br><br>L'objet racine est l'endroit recommandé pour attribuer une autorisation contenant le privilège d'affichage. |

## Contrôle d'accès basé sur des rôles ONTAP pour l'appliance virtuelle pour VSC, VASA Provider et SRA

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 Virtual Storage Console pour VMware vSphere, la fonction RBAC d'ONTAP fonctionne avec vCenter Server RBAC pour déterminer quelles tâches VSC (Virtual Storage Console) un utilisateur peut effectuer sur les objets d'un système de stockage spécifique.

VSC utilise les identifiants (nom d'utilisateur et mot de passe) que vous configurez dans VSC afin d'authentifier chaque système de stockage et de déterminer les opérations de stockage pouvant être effectuées sur ce système de stockage. VSC utilise un ensemble d'identifiants pour chaque système de stockage. Ces identifiants déterminent quelles tâches VSC peuvent être effectuées sur ce système de stockage. En d'autres termes, les identifiants sont utilisés pour VSC et non pour un utilisateur VSC.

Le contrôle d'accès basé sur des rôles (RBAC) ONTAP ne s'applique qu'à l'accès aux systèmes de stockage et aux tâches VSC liées au stockage, comme 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 le contrôle d'accès basé sur des rôles ONTAP associé aux privilèges spécifiques de VSC afin de contrôler les tâches VSC que 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 (RBAC) ONTAP avec les privilèges spécifiques de VSC fournit 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 contrôle d'accès basé sur les rôles du serveur vCenter, vous pouvez autoriser l'utilisateur vCenter à provisionner un datastore sur le stockage tout en empêchant l'utilisateur vCenter 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 VSC, VSC vérifie d'abord si vous disposez de l'autorisation vCenter Server appropriée pour cette tâche. Si l'autorisation de vCenter Server n'est pas suffisante pour vous permettre d'effectuer la tâche, VSC n'a pas besoin de vérifier les privilèges ONTAP de ce système de stockage car vous n'avez pas réussi 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, VSC vérifie alors les privilèges RBAC ONTAP (votre rôle ONTAP) associés aux informations d'identification du système de stockage (nom d'utilisateur et mot de passe) Pour déterminer si vous disposez de privilèges suffisants pour exécuter les opérations de stockage requises par la tâche VSC sur ce système de stockage. Si vous disposez des privilèges ONTAP appropriés, vous pouvez accéder au système de stockage et effectuer la tâche VSC. Les rôles ONTAP déterminent les tâches VSC 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, VSC fournit 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 du stockage.

- Facilité d'utilisation

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

# Rôles ONTAP recommandés lors de l'utilisation de VSC pour VMware vSphere

Vous pouvez définir plusieurs rôles ONTAP recommandés pour l'utilisation de la console de stockage virtuel pour VMware vSphere et du contrôle d'accès basé sur des rôles (RBAC). Ces rôles disposent des privilèges ONTAP requis pour effectuer les opérations de stockage requises exécutées par les tâches (VSC).

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 l'une des options suivantes :

- 9.7 ou ultérieure

  "Configurez les rôles et privilèges utilisateur"

- Créateur d'utilisateurs RBAC pour l'outil ONTAP (si vous utilisez ONTAP 9.6 ou une version antérieure)

  "Outil RBAC User Creator pour VSC, VASA Provider et Storage Replication adapter 7.0 pour VMware vSphere"

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.

Par mesure de sécurité, les rôles ONTAP spécifiques à VSC sont classés par ordre hiérarchique. Le premier rôle est donc le rôle le plus restrictif et ne dispose que de privilèges associés à un ensemble d'opérations de stockage VSC de base. 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 certains des rôles RBAC ONTAP recommandés lors de l'utilisation de VSC. 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 ».

# Comment configurer le contrôle d'accès basé sur des rôles ONTAP pour VSC 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 Virtual Storage Console pour VMware vSphere (VSC). Vous pouvez créer un ou plusieurs comptes utilisateur personnalisés avec des privilèges d'accès limités grâce à la fonction RBAC ONTAP.

VSC et SRA sont capables d'accéder aux systèmes de stockage au niveau du cluster ou du système. 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, 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 à VSC au niveau du cluster, même si vous utilisez VSC ou SRA.

Pour créer un utilisateur et connecter un cluster ou un cluster à VSC, VASA Provider et SRA, il est important de procéder comme suit :

- Créez un administrateur de cluster ou un rôle d'administrateur

  Pour créer ces rôles, vous pouvez utiliser l'une des méthodes suivantes :

  - ONTAP System Manager 9.7 ou version ultérieure

  "Configurez les rôles et privilèges utilisateur"

  - Créateur d'utilisateurs RBAC pour l'outil ONTAP (si vous utilisez ONTAP 9.6 ou une version antérieure)

  "Outil RBAC User Creator pour VSC, VASA Provider et Storage Replication adapter 7.0 pour VMware vSphere"

- Créez des utilisateurs avec le rôle attribué et le jeu d'applications approprié à l'aide de ONTAP

  Ces identifiants sont nécessaires pour configurer les systèmes de stockage pour VSC. Vous pouvez configurer les systèmes de stockage pour VSC en saisissant les identifiants dans VSC. Chaque fois que

vous vous connectez à un système de stockage avec ces identifiants, vous disposez d'autorisations pour accéder aux fonctions VSC que vous avez configurées dans ONTAP lors de la création des identifiants.

- Ajoutez le système de stockage à VSC et fournissez les identifiants de l'utilisateur que vous venez de créer

### Rôles VSC

VSC classifie les privilèges ONTAP en fonction de l'ensemble des rôles VSC suivants :

- 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 du niveau. Les utilisateurs peuvent ainsi exécuter des opérations SRM.

Vous devez vous reporter aux articles de la base de connaissances si vous souhaitez configurer manuellement les rôles et les privilèges à l'aide des commandes ONTAP.

- "Configuration du RBAC ONTAP VSC, VASA et SRA 7.0"
- "Synthèse de toutes les commandes pour VSC et SRA pour le niveau du SVM"

Lors de l'ajout du cluster à VSC, VSC procède à une validation initiale des rôles RBAC ONTAP. Si vous avez ajouté une adresse IP de stockage direct, VSC n'effectue pas la validation initiale. VSC vérifie et applique les privilèges plus tard dans le flux de travail des tâches.

# Configurez les rôles et privilèges utilisateur

Vous pouvez configurer de nouveaux rôles utilisateur pour la gestion des systèmes de stockage à l'aide du fichier JSON fourni avec l'appliance virtuelle pour VSC, VASA Provider, SRA et ONTAP System Manager.

**Avant de commencer**

- Vous devez avoir téléchargé le fichier ONTAP Privileges depuis l'appliance virtuelle pour VSC, VASA Provider et SRA à l'aide de `https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip`.
- Vous devez avoir configuré ONTAP 9.7 System Manager.
- Vous devez avoir ouvert une session avec les privilèges d'administrateur pour le système de stockage.

**étapes**

1. Décompressez le fichier téléchargé `https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip` fichier.
2. Accédez à ONTAP System Manager.
3. Cliquez sur **CLUSTER › Paramètres › utilisateurs et rôles**.
4. Cliquez sur **Ajouter un utilisateur**.
5. Dans la boîte de dialogue **Ajouter un utilisateur**, sélectionnez **produits de virtualisation**.
6. Cliquez sur **Parcourir** pour sélectionner et télécharger le fichier JSON de privilèges ONTAP.

   Le champ PRODUIT est rempli automatiquement.

7. Sélectionnez la capacité requise dans le menu déroulant **PRODUCT CAPABILITY**.

   Le champ **ROLE** est renseigné automatiquement en fonction de la capacité du produit sélectionnée.

8. Saisissez le nom d'utilisateur et le mot de passe requis.
9. Sélectionnez les privilèges (Discovery, Create Storage, Modify Storage, Destroy Storage) requis pour l'utilisateur, puis cliquez sur **Add**.

**Résultats**

Le nouveau rôle et l'utilisateur sont ajoutés et vous pouvez voir les privilèges détaillés sous le rôle que vous avez configuré.

**Informations sur le copyright**

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

**Informations sur les marques commerciales**

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.