# Configurer le serveur SnapCenter

SnapCenter software

NetApp
November 06, 2025

# Sommaire

# Configurer le serveur SnapCenter

## Ajouter et provisionner le système de stockage

### Ajouter des systèmes de stockage

Vous devez configurer le système de stockage qui donne à SnapCenter l'accès au stockage ONTAP , aux systèmes ASA r2 ou à Amazon FSx for NetApp ONTAP pour effectuer des opérations de protection et de provisionnement des données.

Vous pouvez ajouter un SVM autonome ou un cluster comprenant plusieurs SVM. Si vous utilisez Amazon FSx for NetApp ONTAP, vous pouvez soit ajouter un LIF d'administration FSx comprenant plusieurs SVM à l'aide du compte fsxadmin, soit ajouter un SVM FSx dans SnapCenter.

**Avant de commencer**

- Vous devez disposer des autorisations requises dans le rôle d'administrateur d'infrastructure pour créer des connexions de stockage.
- Vous devez vous assurer que les installations de plug-ins ne sont pas en cours.

  Les installations de plug-ins hôtes ne doivent pas être en cours lors de l'ajout d'une connexion au système de stockage, car le cache hôte peut ne pas être mis à jour et l'état des bases de données peut s'afficher dans l'interface graphique SnapCenter comme « Non disponible pour la sauvegarde » ou « Pas sur le stockage NetApp ».

- Les noms des systèmes de stockage doivent être uniques.

  SnapCenter ne prend pas en charge plusieurs systèmes de stockage portant le même nom sur différents clusters. Chaque système de stockage pris en charge par SnapCenter doit avoir un nom unique et une adresse IP LIF de données unique.

**À propos de cette tâche**

- Lorsque vous configurez des systèmes de stockage, vous pouvez également activer les fonctionnalités du système de gestion des événements (EMS) et AutoSupport . L'outil AutoSupport collecte des données sur l'état de votre système et envoie automatiquement les données au support technique NetApp , leur permettant de dépanner votre système.

  Si vous activez ces fonctionnalités, SnapCenter envoie des informations AutoSupport au système de stockage et des messages EMS au syslog du système de stockage lorsqu'une ressource est protégée, qu'une opération de restauration ou de clonage se termine avec succès ou qu'une opération échoue.

- Si vous prévoyez de répliquer des snapshots vers une destination SnapMirror ou SnapVault , vous devez configurer des connexions au système de stockage pour le SVM ou le cluster de destination ainsi que pour le SVM ou le cluster source.

> Si vous modifiez le mot de passe du système de stockage, les tâches planifiées, les sauvegardes à la demande et les opérations de restauration peuvent échouer. Après avoir modifié le mot de passe du système de stockage, vous pouvez mettre à jour le mot de passe en cliquant sur **Modifier** dans l'onglet Stockage.

**Mesures**

1. Dans le volet de navigation de gauche, cliquez sur **Systèmes de stockage**.
2. Dans la page Systèmes de stockage, cliquez sur **Nouveau**.
3. Sur la page Ajouter un système de stockage, fournissez les informations suivantes :

| Pour ce domaine… | Fais ceci… |
| --- | --- |
| Système de stockage | Saisissez le nom du système de stockage ou l'adresse IP.<br><br>Les noms des systèmes de stockage, à l'exclusion du nom de domaine, doivent comporter 15 caractères ou moins et doivent pouvoir être résolus. Pour créer des connexions au système de stockage avec des noms comportant plus de 15 caractères, vous pouvez utiliser l'applet de commande Add-SmStorageConnectionPowerShell.<br><br>Pour les systèmes de stockage avec configuration MetroCluster (MCC), il est recommandé d'enregistrer les clusters locaux et homologues pour des opérations sans interruption.<br><br>SnapCenter ne prend pas en charge plusieurs SVM portant le même nom sur différents clusters. Chaque SVM pris en charge par SnapCenter doit avoir un nom unique.<br><br>Après avoir ajouté la connexion de stockage à SnapCenter, vous ne devez pas renommer le SVM ou le cluster à l'aide d' ONTAP.<br><br>Si SVM est ajouté avec un nom court ou un nom de domaine complet, il doit pouvoir être résolu à la fois depuis SnapCenter et depuis l'hôte du plug-in. |
| Nom d'utilisateur/Mot de passe | Saisissez les informations d'identification de l'utilisateur de stockage disposant des privilèges requis pour accéder au système de stockage. |

| Pour ce domaine… | Fais ceci… |
| --- | --- |
| Système de gestion des événements (EMS) et paramètres AutoSupport | Si vous souhaitez envoyer des messages EMS au syslog du système de stockage ou si vous souhaitez que les messages AutoSupport soient envoyés au système de stockage pour la protection appliquée, les opérations de restauration terminées ou les opérations ayant échoué, cochez la case appropriée.<br><br>Lorsque vous sélectionnez la case à cocher **Envoyer une notification AutoSupport pour les opérations ayant échoué au système de stockage**, la case à cocher **Consigner les événements SnapCenter Server dans syslog** est également sélectionnée, car la messagerie EMS est requise pour activer les notifications AutoSupport . |

4. Cliquez sur **Plus d'options** si vous souhaitez modifier les valeurs par défaut attribuées à la plateforme, au protocole, au port et au délai d'expiration.

   a. Dans Plateforme, sélectionnez l'une des options dans la liste déroulante.

      Si le SVM est le système de stockage secondaire dans une relation de sauvegarde, cochez la case **Secondaire**. Lorsque l'option **Secondaire** est sélectionnée, SnapCenter n'effectue pas de vérification de licence immédiatement.

   Si vous avez ajouté SVM dans SnapCenter , l'utilisateur doit sélectionner manuellement le type de plateforme dans la liste déroulante.

   a. Dans Protocole, sélectionnez le protocole qui a été configuré lors de la configuration de SVM ou du cluster, généralement HTTPS.
   b. Entrez le port accepté par le système de stockage.

      Le port par défaut 443 fonctionne généralement.

   c. Saisissez le temps en secondes qui doit s'écouler avant que les tentatives de communication ne soient interrompues.

      La valeur par défaut est de 60 secondes.

   d. Si le SVM dispose de plusieurs interfaces de gestion, cochez la case **IP préférée**, puis saisissez l'adresse IP préférée pour les connexions SVM.
   e. Cliquez sur **Enregistrer**.
5. Cliquez sur **Soumettre**.

**Résultat**

Dans la page Systèmes de stockage, à partir de la liste déroulante **Type**, effectuez l'une des actions suivantes :

- Sélectionnez * ONTAP SVMs* si vous souhaitez afficher tous les SVM qui ont été ajoutés.

Si vous avez ajouté des SVM FSx, les SVM FSx sont répertoriés ici.

- Sélectionnez * Clusters ONTAP * si vous souhaitez afficher tous les clusters qui ont été ajoutés.

  Si vous avez ajouté des clusters FSx à l'aide de fsxadmin, les clusters FSx sont répertoriés ici.

  Lorsque vous cliquez sur le nom du cluster, toutes les SVM qui font partie du cluster s'affichent dans la section Machines virtuelles de stockage.

  Si une nouvelle SVM est ajoutée au cluster ONTAP à l'aide de l'interface graphique utilisateur ONTAP , cliquez sur **Redécouvrir** pour afficher la SVM nouvellement ajoutée.

**Après avoir fini**

Un administrateur de cluster doit activer AutoSupport sur chaque nœud de système de stockage pour envoyer des notifications par e-mail à partir de tous les systèmes de stockage auxquels SnapCenter a accès, en exécutant la commande suivante à partir de la ligne de commande du système de stockage :

```
autosupport trigger modify -node nodename -autosupport-message client.app.info
-to enable -noteto enable
```

L'administrateur de la machine virtuelle de stockage (SVM) n'a pas accès à AutoSupport.

## Connexions de stockage et informations d'identification

Avant d'effectuer des opérations de protection des données, vous devez configurer les connexions de stockage et ajouter les informations d'identification que le serveur SnapCenter et les plug-ins SnapCenter utiliseront.

### Connexions de stockage

Les connexions de stockage donnent au serveur SnapCenter et aux plug-ins SnapCenter accès au stockage ONTAP . La configuration de ces connexions implique également la configuration des fonctionnalités AutoSupport et du système de gestion des événements (EMS).

### Informations d'identification

- Administrateur de domaine ou tout membre du groupe d'administrateurs

  Indiquez l'administrateur du domaine ou tout membre du groupe d'administrateurs du système sur lequel vous installez le plug-in SnapCenter . Les formats valides pour le champ Nom d'utilisateur sont :

  - *NetBIOS\Nom d'utilisateur*
  - *Domaine FQDN\Nom d'utilisateur*
  - *Nom d'utilisateur@upn*
- Administrateur local (pour les groupes de travail uniquement)

  Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré du système sur lequel vous installez le plug-in SnapCenter . Vous pouvez spécifier un compte utilisateur local appartenant au groupe des administrateurs locaux si ce compte dispose de privilèges élevés ou si la fonctionnalité de contrôle d'accès utilisateur est désactivée sur le système hôte.

Le format valide pour le champ Nom d'utilisateur est : *UserName*

- Informations d'identification pour les groupes de ressources individuels

  Si vous configurez des informations d'identification pour des groupes de ressources individuels et que le nom d'utilisateur ne dispose pas de privilèges d'administrateur complets, vous devez attribuer au moins les privilèges de groupe de ressources et de sauvegarde au nom d'utilisateur.

## Provisionner le stockage sur les hôtes Windows

### Créer et gérer des igroups

Vous créez des groupes d'initiateurs (igroups) pour spécifier quels hôtes peuvent accéder à un LUN donné sur le système de stockage. Vous pouvez utiliser SnapCenter pour créer, renommer, modifier ou supprimer un igroup sur un hôte Windows.

#### Créer un igroup

Vous pouvez utiliser SnapCenter pour créer un igroup sur un hôte Windows. L'igroup sera disponible dans l'assistant Créer un disque ou Connecter un disque lorsque vous mappez l'igroup à un LUN.

**Mesures**

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Igroup**.
3. Dans la page Groupes d'initiateurs, cliquez sur **Nouveau**.
4. Dans la boîte de dialogue Créer un igroup, définissez l'igroup :

| Dans ce domaine… | Fais ceci… |
|---|---|
| Système de stockage | Sélectionnez le SVM pour le LUN que vous allez mapper au igroup. |
| Hôte | Sélectionnez l'hôte sur lequel vous souhaitez créer l'igroup. |
| Nom du groupe I | Entrez le nom du groupe i. |
| Initiateurs | Sélectionnez l'initiateur. |
| Type | Sélectionnez le type d'initiateur, iSCSI, FCP ou mixte (FCP et iSCSI). |

5. Lorsque vous êtes satisfait de vos entrées, cliquez sur **OK**.

   SnapCenter crée l'igroup sur le système de stockage.

#### Renommer un igroup

Vous pouvez utiliser SnapCenter pour renommer un igroup existant.

### Mesures

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Igroup**.
3. Dans la page Groupes d'initiateurs, cliquez dans le champ **Machine virtuelle de stockage** pour afficher une liste des SVM disponibles, puis sélectionnez la SVM pour l'igroup que vous souhaitez renommer.
4. Dans la liste des igroups pour le SVM, sélectionnez l'igroup que vous souhaitez renommer et cliquez sur **Renommer**.
5. Dans la boîte de dialogue Renommer le groupe i, entrez le nouveau nom du groupe i et cliquez sur **Renommer**.

#### Modifier un igroup

Vous pouvez utiliser SnapCenter pour ajouter des initiateurs igroup à un igroup existant. Lors de la création d'un igroup, vous ne pouvez ajouter qu'un seul hôte. Si vous souhaitez créer un igroup pour un cluster, vous pouvez modifier l'igroup pour ajouter d'autres nœuds à cet igroup.

### Mesures

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Igroup**.
3. Dans la page Groupes d'initiateurs, cliquez dans le champ **Machine virtuelle de stockage** pour afficher une liste déroulante des SVM disponibles, puis sélectionnez la SVM pour l'igroup que vous souhaitez modifier.
4. Dans la liste des igroups, sélectionnez un igroup et cliquez sur **Ajouter un initiateur à l'igroup**.
5. Sélectionnez un hôte.
6. Sélectionnez les initiateurs et cliquez sur **OK**.

#### Supprimer un igroup

Vous pouvez utiliser SnapCenter pour supprimer un igroup lorsque vous n'en avez plus besoin.

### Mesures

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Igroup**.
3. Dans la page Groupes d'initiateurs, cliquez dans le champ **Machine virtuelle de stockage** pour afficher une liste déroulante des SVM disponibles, puis sélectionnez la SVM pour le groupe d'initiateurs que vous souhaitez supprimer.
4. Dans la liste des igroups du SVM, sélectionnez l'igroup que vous souhaitez supprimer et cliquez sur **Supprimer**.
5. Dans la boîte de dialogue Supprimer le groupe i, cliquez sur **OK**.

   SnapCenter supprime le groupe i.

### Créer et gérer des disques

L'hôte Windows voit les LUN sur votre système de stockage comme des disques virtuels. Vous pouvez utiliser SnapCenter pour créer et configurer un LUN connecté FC ou iSCSI.

- SnapCenter prend en charge uniquement les disques de base. Les disques dynamiques ne sont pas pris en charge.
- Pour GPT, une seule partition de données et pour MBR, une partition principale est autorisée, dotée d'un volume formaté avec NTFS ou CSVFS et d'un chemin de montage.
- Styles de partition pris en charge : GPT, MBR ; dans une machine virtuelle VMware UEFI, seuls les disques iSCSI sont pris en charge

SnapCenter ne prend pas en charge le changement de nom d'un disque. Si un disque géré par SnapCenter est renommé, les opérations SnapCenter échoueront.

#### Afficher les disques sur un hôte

Vous pouvez afficher les disques sur chaque hôte Windows que vous gérez avec SnapCenter.

**Mesures**

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Disques**.
3. Sélectionnez l'hôte dans la liste déroulante **Hôte**.

   Les disques sont répertoriés.

#### Afficher les disques en cluster

Vous pouvez afficher les disques en cluster sur le cluster que vous gérez avec SnapCenter. Les disques en cluster s'affichent uniquement lorsque vous sélectionnez le cluster dans la liste déroulante Hôtes.

**Mesures**

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Disques**.
3. Sélectionnez le cluster dans la liste déroulante **Hôte**.

   Les disques sont répertoriés.

#### Établir une session iSCSI

Si vous utilisez iSCSI pour vous connecter à un LUN, vous devez établir une session iSCSI avant de créer le LUN pour activer la communication.

**Avant de commencer**

- Vous devez avoir défini le nœud du système de stockage comme cible iSCSI.
- Vous devez avoir démarré le service iSCSI sur le système de stockage. "Apprendre encore plus"

**À propos de cette tâche**

Vous ne pouvez établir une session iSCSI qu'entre les mêmes versions IP, soit d'IPv6 à IPv6, soit d'IPv4 à IPv4.

Vous pouvez utiliser une adresse IPv6 locale pour la gestion des sessions iSCSI et pour la communication entre un hôte et une cible uniquement lorsque les deux se trouvent dans le même sous-réseau.

Si vous modifiez le nom d'un initiateur iSCSI, l'accès aux cibles iSCSI est affecté. Après avoir modifié le nom, vous devrez peut-être reconfigurer les cibles auxquelles accède l'initiateur afin qu'elles puissent reconnaître le nouveau nom. Vous devez vous assurer de redémarrer l'hôte après avoir modifié le nom d'un initiateur iSCSI.

Si votre hôte dispose de plusieurs interfaces iSCSI, une fois que vous avez établi une session iSCSI sur SnapCenter à l'aide d'une adresse IP sur la première interface, vous ne pouvez pas établir de session iSCSI à partir d'une autre interface avec une adresse IP différente.

**Mesures**

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Session iSCSI**.
3. Dans la liste déroulante **Machine virtuelle de stockage**, sélectionnez la machine virtuelle de stockage (SVM) pour la cible iSCSI.
4. Dans la liste déroulante **Hôte**, sélectionnez l'hôte de la session.
5. Cliquez sur **Établir une session**.

   L'assistant d'établissement de session s'affiche.

6. Dans l'assistant Établir une session, identifiez la cible :

| Dans ce domaine… | Entrer… |
|---|---|
| Nom du nœud cible | Le nom du nœud de la cible iSCSI<br><br>S'il existe un nom de nœud cible existant, le nom est affiché au format lecture seule. |
| Adresse du portail cible | L'adresse IP du portail réseau cible |
| Port du portail cible | Le port TCP du portail réseau cible |
| Adresse du portail initiateur | L'adresse IP du portail réseau initiateur |

7. Lorsque vous êtes satisfait de vos entrées, cliquez sur **Connecter**.

   SnapCenter établit la session iSCSI.

8. Répétez cette procédure pour établir une session pour chaque cible.

#### Créer des LUN ou des disques connectés FC ou iSCSI

L'hôte Windows voit les LUN de votre système de stockage comme des disques virtuels. Vous pouvez utiliser SnapCenter pour créer et configurer un LUN connecté FC ou iSCSI.

Si vous souhaitez créer et formater des disques en dehors de SnapCenter, seuls les systèmes de fichiers NTFS et CSVFS sont pris en charge.

**Avant de commencer**

- Vous devez avoir créé un volume pour le LUN sur votre système de stockage.

  Le volume doit contenir uniquement des LUN, et uniquement des LUN créés avec SnapCenter.

  > Vous ne pouvez pas créer un LUN sur un volume clone créé par SnapCenter, sauf si le clone a déjà été divisé.

- Vous devez avoir démarré le service FC ou iSCSI sur le système de stockage.
- Si vous utilisez iSCSI, vous devez avoir établi une session iSCSI avec le système de stockage.
- Le package de plug-ins SnapCenter pour Windows doit être installé uniquement sur l'hôte sur lequel vous créez le disque.

**À propos de cette tâche**

- Vous ne pouvez pas connecter un LUN à plusieurs hôtes, sauf si le LUN est partagé par des hôtes dans un cluster de basculement Windows Server.
- Si un LUN est partagé par des hôtes dans un cluster de basculement Windows Server qui utilise CSV (Cluster Shared Volumes), vous devez créer le disque sur l'hôte propriétaire du groupe de cluster.

**Mesures**

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Disques**.
3. Sélectionnez l'hôte dans la liste déroulante **Hôte**.
4. Cliquez sur **Nouveau**.

   L'assistant de création de disque s'ouvre.

5. Dans la page Nom du LUN, identifiez le LUN :

| **Dans ce domaine…** | **Fais ceci…** |
|---|---|
| Système de stockage | Sélectionnez le SVM pour le LUN. |
| Chemin LUN | Cliquez sur **Parcourir** pour sélectionner le chemin complet du dossier contenant le LUN. |
| Nom du LUN | Entrez le nom du LUN. |
| Taille du cluster | Sélectionnez la taille d'allocation du bloc LUN pour le cluster.<br><br>La taille du cluster dépend du système d'exploitation et des applications. |

| Dans ce domaine… | Fais ceci… |
| --- | --- |
| Étiquette LUN | Vous pouvez également saisir un texte descriptif pour le LUN. |

6. Dans la page Type de disque, sélectionnez le type de disque :

| Sélectionner… | Si… |
| --- | --- |
| Disque dédié | Le LUN n'est accessible que par un seul hôte.<br><br>Ignorez le champ **Groupe de ressources**. |
| Disque partagé | Le LUN est partagé par les hôtes d'un cluster de basculement Windows Server.<br><br>Saisissez le nom du groupe de ressources du cluster dans le champ **Groupe de ressources**. Vous devez créer le disque sur un seul hôte dans le cluster de basculement. |
| Volume partagé de cluster (CSV) | Le LUN est partagé par les hôtes d'un cluster de basculement Windows Server qui utilise CSV.<br><br>Saisissez le nom du groupe de ressources du cluster dans le champ **Groupe de ressources**. Assurez-vous que l'hôte sur lequel vous créez le disque est le propriétaire du groupe de cluster. |

7. Dans la page Propriétés du lecteur, spécifiez les propriétés du lecteur :

| Propriété | Description |
| --- | --- |
| Attribution automatique du point de montage | SnapCenter attribue automatiquement un point de montage de volume en fonction du lecteur système.<br><br>Par exemple, si votre lecteur système est C:, l'attribution automatique crée un point de montage de volume sous votre lecteur C: (C:\scmnpt\). L'attribution automatique n'est pas prise en charge pour les disques partagés. |
| Attribuer une lettre de lecteur | Montez le disque sur le lecteur que vous sélectionnez dans la liste déroulante adjacente. |
| Utiliser le point de montage du volume | Montez le disque sur le chemin d'accès au lecteur que vous spécifiez dans le champ adjacent.<br><br>La racine du point de montage du volume doit appartenir à l'hôte sur lequel vous créez le disque. |

| Propriété | Description |
| --- | --- |
| N’attribuez pas de lettre de lecteur ni de point de montage de volume | Choisissez cette option si vous préférez monter le disque manuellement sous Windows. |
| Taille du LUN | Spécifiez la taille du LUN ; 150 Mo minimum.<br><br>Sélectionnez Mo, Go ou To dans la liste déroulante adjacente. |
| Utiliser le provisionnement léger pour le volume hébergeant ce LUN | Provisionnement fin du LUN.<br><br>Le provisionnement léger alloue uniquement l’espace de stockage nécessaire à un moment donné, ce qui permet au LUN de croître efficacement jusqu’à la capacité maximale disponible.<br><br>Assurez-vous qu’il y a suffisamment d’espace disponible sur le volume pour accueillir tout le stockage LUN dont vous pensez avoir besoin. |
| Choisissez le type de partition | Sélectionnez la partition GPT pour une table de partition GUID ou la partition MBR pour un enregistrement de démarrage principal.<br><br>Les partitions MBR peuvent provoquer des problèmes de désalignement dans les clusters de basculement Windows Server.<br><br>Les disques de partition d’interface de micrologiciel extensible unifié (UEFI) ne sont pas pris en charge. |

8. Dans la page Map LUN, sélectionnez l’initiateur iSCSI ou FC sur l’hôte :

| Dans ce domaine… | Fais ceci… |
| --- | --- |
| Hôte | Double-cliquez sur le nom du groupe de clusters pour afficher une liste déroulante indiquant les hôtes appartenant au cluster, puis sélectionnez l’hôte pour l’initiateur.<br><br>Ce champ s’affiche uniquement si le LUN est partagé par des hôtes dans un cluster de basculement Windows Server. |

| Dans ce domaine… | Fais ceci… |
| --- | --- |
| Choisir l'initiateur hôte | Sélectionnez **Fibre Channel** ou **iSCSI**, puis sélectionnez l'initiateur sur l'hôte.<br><br>Vous pouvez sélectionner plusieurs initiateurs FC si vous utilisez FC avec E/S multi-chemins (MPIO). |

9. Dans la page Type de groupe, indiquez si vous souhaitez mapper un igroup existant au LUN ou créer un nouveau igroup :

| Sélectionner… | Si… |
| --- | --- |
| Créer un nouveau groupe pour les initiateurs sélectionnés | Vous souhaitez créer un nouveau igroup pour les initiateurs sélectionnés. |
| Choisissez un igroup existant ou spécifiez un nouveau igroup pour les initiateurs sélectionnés | Vous souhaitez spécifier un igroup existant pour les initiateurs sélectionnés ou créer un nouvel igroup avec le nom que vous spécifiez.<br><br>Tapez le nom du groupe i dans le champ **nom du groupe i**. Tapez les premières lettres du nom du groupe i existant pour compléter automatiquement le champ. |

10. Dans la page Résumé, vérifiez vos sélections, puis cliquez sur **Terminer**.

    SnapCenter crée le LUN et le connecte au lecteur ou au chemin de lecteur spécifié sur l'hôte.

#### Redimensionner un disque

Vous pouvez augmenter ou diminuer la taille d'un disque en fonction de l'évolution des besoins de votre système de stockage.

### À propos de cette tâche

- Pour les LUN à provisionnement dynamique, la taille de la géométrie LUN ONTAP est affichée comme taille maximale.
- Pour les LUN à provisionnement épais, la taille extensible (taille disponible dans le volume) est affichée comme taille maximale.
- Les LUN avec des partitions de style MBR ont une limite de taille de 2 To.
- Les LUN avec des partitions de style GPT ont une limite de taille de système de stockage de 16 To.
- C'est une bonne idée de faire un instantané avant de redimensionner un LUN.
- Si vous devez restaurer un LUN à partir d'un snapshot réalisé avant le redimensionnement du LUN, SnapCenter redimensionne automatiquement le LUN à la taille du snapshot.

  Après l'opération de restauration, les données ajoutées au LUN après son redimensionnement doivent être restaurées à partir d'un instantané réalisé après son redimensionnement.

### Mesures

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Disques**.
3. Sélectionnez l'hôte dans la liste déroulante Hôte.

   Les disques sont répertoriés.

4. Sélectionnez le disque que vous souhaitez redimensionner, puis cliquez sur **Redimensionner**.
5. Dans la boîte de dialogue Redimensionner le disque, utilisez l'outil curseur pour spécifier la nouvelle taille du disque ou entrez la nouvelle taille dans le champ Taille.

   Si vous entrez la taille manuellement, vous devez cliquer en dehors du champ Taille avant que le bouton Réduire ou Développer ne soit activé de manière appropriée. Vous devez également cliquer sur Mo, Go ou To pour spécifier l'unité de mesure.

6. Lorsque vous êtes satisfait de vos entrées, cliquez sur **Réduire** ou **Agrandir**, selon le cas.

   SnapCenter redimensionne le disque.

#### Connecter un disque

Vous pouvez utiliser l'assistant Connect Disk pour connecter un LUN existant à un hôte ou pour reconnecter un LUN qui a été déconnecté.

**Avant de commencer**

- Vous devez avoir démarré le service FC ou iSCSI sur le système de stockage.
- Si vous utilisez iSCSI, vous devez avoir établi une session iSCSI avec le système de stockage.
- Vous ne pouvez pas connecter un LUN à plusieurs hôtes, sauf si le LUN est partagé par des hôtes dans un cluster de basculement Windows Server.
- Si le LUN est partagé par des hôtes dans un cluster de basculement Windows Server qui utilise CSV (Cluster Shared Volumes), vous devez connecter le disque sur l'hôte propriétaire du groupe de clusters.
- Le plug-in pour Windows doit être installé uniquement sur l'hôte sur lequel vous connectez le disque.

**Mesures**

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Disques**.
3. Sélectionnez l'hôte dans la liste déroulante **Hôte**.
4. Cliquez sur **Connecter**.

   L'assistant Connect Disk s'ouvre.

5. Dans la page Nom du LUN, identifiez le LUN auquel vous souhaitez vous connecter :

| Dans ce domaine… | Fais ceci… |
| --- | --- |
| Système de stockage | Sélectionnez le SVM pour le LUN. |

| Dans ce domaine… | Fais ceci… |
| --- | --- |
| Chemin LUN | Cliquez sur **Parcourir** pour sélectionner le chemin complet du volume contenant le LUN. |
| Nom du LUN | Entrez le nom du LUN. |
| Taille du cluster | Sélectionnez la taille d'allocation du bloc LUN pour le cluster.<br><br>La taille du cluster dépend du système d'exploitation et des applications. |
| Étiquette LUN | Vous pouvez également saisir un texte descriptif pour le LUN. |

6. Dans la page Type de disque, sélectionnez le type de disque :

| Sélectionner… | Si… |
| --- | --- |
| Disque dédié | Le LUN n'est accessible que par un seul hôte. |
| Disque partagé | Le LUN est partagé par les hôtes d'un cluster de basculement Windows Server.<br><br>Il vous suffit de connecter le disque à un seul hôte du cluster de basculement. |
| Volume partagé de cluster (CSV) | Le LUN est partagé par les hôtes d'un cluster de basculement Windows Server qui utilise CSV.<br><br>Assurez-vous que l'hôte sur lequel vous vous connectez au disque est le propriétaire du groupe de cluster. |

7. Dans la page Propriétés du lecteur, spécifiez les propriétés du lecteur :

| Propriété | Description |
| --- | --- |
| Attribution automatique | Laissez SnapCenter attribuer automatiquement un point de montage de volume en fonction du lecteur système.<br><br>Par exemple, si votre lecteur système est C:, la propriété d'attribution automatique crée un point de montage de volume sous votre lecteur C: (C:\scmnpt\). La propriété d'attribution automatique n'est pas prise en charge pour les disques partagés. |

| Propriété | Description |
| --- | --- |
| Attribuer une lettre de lecteur | Montez le disque sur le lecteur que vous sélectionnez dans la liste déroulante adjacente. |
| Utiliser le point de montage du volume | Montez le disque sur le chemin d'accès au lecteur que vous spécifiez dans le champ adjacent.<br><br>La racine du point de montage du volume doit appartenir à l'hôte sur lequel vous créez le disque. |
| N'attribuez pas de lettre de lecteur ni de point de montage de volume | Choisissez cette option si vous préférez monter le disque manuellement sous Windows. |

8. Dans la page Map LUN, sélectionnez l'initiateur iSCSI ou FC sur l'hôte :

| Dans ce domaine… | Fais ceci… |
| --- | --- |
| Hôte | Double-cliquez sur le nom du groupe de clusters pour afficher une liste déroulante indiquant les hôtes appartenant au cluster, puis sélectionnez l'hôte pour l'initiateur.<br><br>Ce champ s'affiche uniquement si le LUN est partagé par des hôtes dans un cluster de basculement Windows Server. |
| Choisir l'initiateur hôte | Sélectionnez **Fibre Channel** ou **iSCSI**, puis sélectionnez l'initiateur sur l'hôte.<br><br>Vous pouvez sélectionner plusieurs initiateurs FC si vous utilisez FC avec MPIO. |

9. Dans la page Type de groupe, indiquez si vous souhaitez mapper un igroup existant au LUN ou créer un nouveau igroup :

| Sélectionner… | Si… |
| --- | --- |
| Créer un nouveau groupe pour les initiateurs sélectionnés | Vous souhaitez créer un nouveau igroup pour les initiateurs sélectionnés. |
| Choisissez un igroup existant ou spécifiez un nouveau igroup pour les initiateurs sélectionnés | Vous souhaitez spécifier un igroup existant pour les initiateurs sélectionnés ou créer un nouvel igroup avec le nom que vous spécifiez.<br><br>Tapez le nom du groupe i dans le champ **nom du groupe i**. Tapez les premières lettres du nom du groupe i existant pour compléter automatiquement le champ. |

10. Dans la page Résumé, vérifiez vos sélections et cliquez sur **Terminer**.

    SnapCenter connecte le LUN au lecteur ou au chemin de lecteur spécifié sur l'hôte.

#### Déconnecter un disque

Vous pouvez déconnecter un LUN d'un hôte sans affecter le contenu du LUN, à une exception près : si vous déconnectez un clone avant qu'il ne soit divisé, vous perdez le contenu du clone.

**Avant de commencer**

- Assurez-vous que le LUN n'est utilisé par aucune application.
- Assurez-vous que le LUN n'est pas surveillé par un logiciel de surveillance.
- Si le LUN est partagé, assurez-vous de supprimer les dépendances des ressources du cluster du LUN et vérifiez que tous les nœuds du cluster sont sous tension, fonctionnent correctement et sont disponibles pour SnapCenter.

### À propos de cette tâche

Si vous déconnectez un LUN dans un volume FlexClone créé par SnapCenter et qu'aucun autre LUN sur le volume n'est connecté, SnapCenter supprime le volume. Avant de déconnecter le LUN, SnapCenter affiche un message vous avertissant que le volume FlexClone pourrait être supprimé.

Pour éviter la suppression automatique du volume FlexClone , vous devez renommer le volume avant de déconnecter le dernier LUN. Lorsque vous renommez le volume, assurez-vous de modifier plusieurs caractères et pas seulement le dernier caractère du nom.

### Mesures

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Disques**.
3. Sélectionnez l'hôte dans la liste déroulante **Hôte**.

   Les disques sont répertoriés.

4. Sélectionnez le disque que vous souhaitez déconnecter, puis cliquez sur **Déconnecter**.
5. Dans la boîte de dialogue Déconnecter le disque, cliquez sur **OK**.

   SnapCenter déconnecte le disque.

#### Supprimer un disque

Vous pouvez supprimer un disque lorsque vous n'en avez plus besoin. Après avoir supprimé un disque, vous ne pouvez pas le restaurer.

### Mesures

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Disques**.
3. Sélectionnez l'hôte dans la liste déroulante **Hôte**.

   Les disques sont répertoriés.

4. Sélectionnez le disque que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
5. Dans la boîte de dialogue Supprimer le disque, cliquez sur **OK**.

   SnapCenter supprime le disque.

### Créer et gérer des partages SMB

Pour configurer un partage SMB3 sur une machine virtuelle de stockage (SVM), vous pouvez utiliser l'interface utilisateur SnapCenter ou les applets de commande PowerShell.

**Meilleure pratique :** l'utilisation des applets de commande est recommandée car elle vous permet de tirer parti des modèles fournis avec SnapCenter pour automatiser la configuration du partage.

Les modèles résument les meilleures pratiques en matière de configuration du volume et du partage. Vous pouvez trouver les modèles dans le dossier Modèles du dossier d'installation du package de plug-ins SnapCenter pour Windows.

Si vous vous sentez à l'aise, vous pouvez créer vos propres modèles en suivant les modèles fournis. Vous devez consulter les paramètres dans la documentation de l'applet de commande avant de créer un modèle personnalisé.

#### Créer un partage SMB

Vous pouvez utiliser la page Partages SnapCenter pour créer un partage SMB3 sur une machine virtuelle de stockage (SVM).

Vous ne pouvez pas utiliser SnapCenter pour sauvegarder des bases de données sur des partages SMB. Le support SMB est limité au provisionnement uniquement.

**Mesures**

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Partages**.
3. Sélectionnez la SVM dans la liste déroulante **Machine virtuelle de stockage**.
4. Cliquez sur **Nouveau**.

   La boîte de dialogue Nouveau partage s'ouvre.

5. Dans la boîte de dialogue Nouveau partage, définissez le partage :

| Dans ce domaine… | Fais ceci… |
| --- | --- |
| Description | Saisissez un texte descriptif pour le partage. |

| Dans ce domaine… | Fais ceci… |
| --- | --- |
| Nom de partage | Saisissez le nom du partage, par exemple, test_share.<br><br>Le nom que vous entrez pour le partage sera également utilisé comme nom de volume.<br><br>Le nom de l'action :<br><br>• Doit être une chaîne UTF-8.<br>• Ne doit pas inclure les caractères suivants : caractères de contrôle de 0x00 à 0x1F (tous deux inclus), 0x22 (guillemets doubles) et les caractères spéciaux `\ / [ ] : (vertical bar) < > + = ; , ?` |
| Partager le chemin | • Cliquez dans le champ pour saisir un nouveau chemin d'accès au système de fichiers, par exemple, /.<br>• Double-cliquez dans le champ pour sélectionner parmi une liste de chemins de système de fichiers existants. |

6. Lorsque vous êtes satisfait de vos entrées, cliquez sur **OK**.

   SnapCenter crée le partage SMB sur le SVM.

#### Supprimer un partage SMB

Vous pouvez supprimer un partage SMB lorsque vous n'en avez plus besoin.

**Mesures**

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Partages**.
3. Dans la page Partages, cliquez dans le champ **Machine virtuelle de stockage** pour afficher une liste déroulante contenant une liste des machines virtuelles de stockage (SVM) disponibles, puis sélectionnez la SVM du partage que vous souhaitez supprimer.
4. Dans la liste des partages sur le SVM, sélectionnez le partage que vous souhaitez supprimer et cliquez sur **Supprimer**.
5. Dans la boîte de dialogue Supprimer le partage, cliquez sur **OK**.

   SnapCenter supprime le partage SMB du SVM.

#### Récupérer de l'espace sur le système de stockage

Bien que NTFS suive l'espace disponible sur un LUN lorsque des fichiers sont supprimés ou modifiés, il ne signale pas les nouvelles informations au système de stockage. Vous

pouvez exécuter l'applet de commande PowerShell de récupération d'espace sur l'hôte Plug-in pour Windows pour garantir que les blocs nouvellement libérés sont marqués comme disponibles dans le stockage.

Si vous exécutez l'applet de commande sur un hôte de plug-in distant, vous devez avoir exécuté l'applet de commande SnapCenterOpen-SMConnection pour ouvrir une connexion au serveur SnapCenter .

**Avant de commencer**

- Vous devez vous assurer que le processus de récupération d'espace est terminé avant d'effectuer une opération de restauration.
- Si le LUN est partagé par des hôtes dans un cluster de basculement Windows Server, vous devez effectuer une récupération d'espace sur l'hôte propriétaire du groupe de clusters.
- Pour des performances de stockage optimales, vous devez effectuer une récupération d'espace aussi souvent que possible.

  Vous devez vous assurer que l'ensemble du système de fichiers NTFS a été analysé.

**À propos de cette tâche**

- La récupération d'espace prend du temps et consomme beaucoup de ressources processeur. Il est donc généralement préférable d'exécuter l'opération lorsque l'utilisation du système de stockage et de l'hôte Windows est faible.
- La récupération d'espace récupère presque tout l'espace disponible, mais pas 100 pour cent.
- Vous ne devez pas exécuter la défragmentation du disque en même temps que vous effectuez une récupération d'espace.

  Cela peut ralentir le processus de récupération.

**Étape**

À partir de l'invite de commande PowerShell du serveur d'applications, entrez la commande suivante :

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

drive_path est le chemin du lecteur mappé au LUN.

**Provisionner le stockage à l'aide des applets de commande PowerShell**

Si vous ne souhaitez pas utiliser l'interface graphique utilisateur SnapCenter pour effectuer des tâches de provisionnement d'hôte et de récupération d'espace, vous pouvez utiliser les applets de commande PowerShell. Vous pouvez utiliser les applets de commande directement ou les ajouter aux scripts.

Si vous exécutez les applets de commande sur un hôte de plug-in distant, vous devez exécuter l'applet de commande SnapCenter Open-SMConnection pour ouvrir une connexion au serveur SnapCenter .

Les informations concernant les paramètres pouvant être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant *Get-Help command_name*. Alternativement, vous pouvez également vous référer à la "Guide de référence de l'applet de commande du logiciel SnapCenter" .

Si les applets de commande SnapCenter PowerShell sont endommagées en raison de la suppression de

SnapDrive pour Windows du serveur, reportez-vous à "Les applets de commande SnapCenter sont défectueuses lors de la désinstallation de SnapDrive pour Windows" .

## Provisionner le stockage dans les environnements VMware

Vous pouvez utiliser le plug-in SnapCenter pour Microsoft Windows dans les environnements VMware pour créer et gérer des LUN et gérer des snapshots.

#### Plateformes de système d'exploitation invité VMware prises en charge

- Versions prises en charge de Windows Server
- Configurations de cluster Microsoft

  Prise en charge jusqu'à un maximum de 16 nœuds pris en charge sur VMware lors de l'utilisation de Microsoft iSCSI Software Initiator, ou jusqu'à deux nœuds utilisant FC

- LUN RDM

  Prise en charge d'un maximum de 56 LUN RDM avec quatre contrôleurs SCSI LSI Logic pour RDMS normal, ou 42 LUN RDM avec trois contrôleurs SCSI LSI Logic sur une configuration VMware VM MSCS box-to-box Plug-in pour Windows

  Prend en charge le contrôleur VMware ParaVirtual SCSI. 256 disques peuvent être pris en charge sur les disques RDM.

Pour obtenir les dernières informations sur les versions prises en charge, consultez "Outil de matrice d'interopérabilité NetApp" .

##### Limitations liées au serveur VMware ESXi

- L'installation du plug-in pour Windows sur un cluster Microsoft sur des machines virtuelles à l'aide des informations d'identification ESXi n'est pas prise en charge.

  Vous devez utiliser vos informations d'identification vCenter lors de l'installation du plug-in pour Windows sur des machines virtuelles en cluster.

- Tous les nœuds en cluster doivent utiliser le même ID cible (sur l'adaptateur SCSI virtuel) pour le même disque en cluster.
- Lorsque vous créez un LUN RDM en dehors du plug-in pour Windows, vous devez redémarrer le service du plug-in pour lui permettre de reconnaître le disque nouvellement créé.
- Vous ne pouvez pas utiliser les initiateurs iSCSI et FC en même temps sur un système d'exploitation invité VMware.

##### Privilèges vCenter minimaux requis pour les opérations SnapCenter RDM

Vous devez disposer des privilèges vCenter suivants sur l'hôte pour effectuer des opérations RDM dans un système d'exploitation invité :

- Magasin de données : supprimer le fichier
- Hôte : Configuration > Configuration de la partition de stockage
- Machine virtuelle : configuration

Vous devez attribuer ces privilèges à un rôle au niveau du serveur Virtual Center. Le rôle auquel vous attribuez ces privilèges ne peut pas être attribué à un utilisateur sans privilèges root.

Après avoir attribué ces privilèges, vous pouvez installer le plug-in pour Windows sur le système d'exploitation invité.

### Gérer les LUN FC RDM dans un cluster Microsoft

Vous pouvez utiliser le plug-in pour Windows pour gérer un cluster Microsoft à l'aide de LUN FC RDM, mais vous devez d'abord créer le quorum RDM partagé et le stockage partagé en dehors du plug-in, puis ajouter les disques aux machines virtuelles du cluster.

À partir d'ESXi 5.5, vous pouvez également utiliser le matériel ESX iSCSI et FCoE pour gérer un cluster Microsoft. Le plug-in pour Windows inclut une prise en charge prête à l'emploi pour les clusters Microsoft.

#### Exigences

Le plug-in pour Windows prend en charge les clusters Microsoft utilisant des LUN FC RDM sur deux machines virtuelles différentes appartenant à deux serveurs ESX ou ESXi différents, également appelés cluster sur plusieurs boîtes, lorsque vous répondez à des exigences de configuration spécifiques.

- Les machines virtuelles (VM) doivent exécuter la même version de Windows Server.
- Les versions du serveur ESX ou ESXi doivent être identiques pour chaque hôte parent VMware.
- Chaque hôte parent doit disposer d'au moins deux adaptateurs réseau.
- Il doit y avoir au moins une banque de données VMware Virtual Machine File System (VMFS) partagée entre les deux serveurs ESX ou ESXi.
- VMware recommande que le magasin de données partagé soit créé sur un SAN FC.

  Si nécessaire, le magasin de données partagé peut également être créé via iSCSI.

- Le LUN RDM partagé doit être en mode de compatibilité physique.
- Le LUN RDM partagé doit être créé manuellement en dehors du plug-in pour Windows.

  Vous ne pouvez pas utiliser de disques virtuels pour le stockage partagé.

- Un contrôleur SCSI doit être configuré sur chaque machine virtuelle du cluster en mode de compatibilité physique :

  Windows Server 2008 R2 nécessite que vous configuriez le contrôleur SCSI SAS LSI Logic sur chaque machine virtuelle. Les LUN partagés ne peuvent pas utiliser le contrôleur SAS LSI Logic existant si un seul de son type existe et qu'il est déjà connecté au lecteur C :.

  Les contrôleurs SCSI de type paravirtuel ne sont pas pris en charge sur les clusters VMware Microsoft.

  > Lorsque vous ajoutez un contrôleur SCSI à un LUN partagé sur une machine virtuelle en mode de compatibilité physique, vous devez sélectionner l'option **Mappages de périphériques bruts** (RDM) et non l'option **Créer un nouveau disque** dans le client VMware Infrastructure.

- Les clusters de machines virtuelles Microsoft ne peuvent pas faire partie d'un cluster VMware.
- Vous devez utiliser les informations d'identification vCenter et non les informations d'identification ESX ou ESXi lorsque vous installez le plug-in pour Windows sur des machines virtuelles appartenant à un cluster

Microsoft.

- Le plug-in pour Windows ne peut pas créer un seul igroup avec des initiateurs provenant de plusieurs hôtes.

  Le groupe igroup contenant les initiateurs de tous les hôtes ESXi doit être créé sur le contrôleur de stockage avant de créer les LUN RDM qui seront utilisés comme disques de cluster partagés.

- Assurez-vous de créer un LUN RDM sur ESXi 5.0 à l'aide d'un initiateur FC.

  Lorsque vous créez un LUN RDM, un groupe d'initiateurs est créé avec ALUA.

#### Limites

Le plug-in pour Windows prend en charge les clusters Microsoft utilisant des LUN FC/iSCSI RDM sur différentes machines virtuelles appartenant à différents serveurs ESX ou ESXi.

Cette fonctionnalité n'est pas prise en charge dans les versions antérieures à ESX 5.5i.

- Le plug-in pour Windows ne prend pas en charge les clusters sur les banques de données ESX iSCSI et NFS.
- Le plug-in pour Windows ne prend pas en charge les initiateurs mixtes dans un environnement de cluster.

  Les initiateurs doivent être FC ou Microsoft iSCSI, mais pas les deux.

- Les initiateurs et HBA iSCSI ESX ne sont pas pris en charge sur les disques partagés dans un cluster Microsoft.
- Le plug-in pour Windows ne prend pas en charge la migration de machine virtuelle avec vMotion si la machine virtuelle fait partie d'un cluster Microsoft.
- Le plug-in pour Windows ne prend pas en charge MPIO sur les machines virtuelles d'un cluster Microsoft.

#### Créer un LUN FC RDM partagé

Avant de pouvoir utiliser les LUN FC RDM pour partager le stockage entre les nœuds d'un cluster Microsoft, vous devez d'abord créer le disque quorum partagé et le disque de stockage partagé, puis les ajouter aux deux machines virtuelles du cluster.

Le disque partagé n'est pas créé à l'aide du plug-in pour Windows. Vous devez créer puis ajouter le LUN partagé à chaque machine virtuelle du cluster. Pour plus d'informations, voir "Regrouper des machines virtuelles sur des hôtes physiques" .

# Ajouter des licences basées sur le contrôleur SnapCenter Standard

Une licence basée sur un contrôleur SnapCenter Standard est requise si vous utilisez des contrôleurs de stockage FAS, AFF ou ASA .

La licence basée sur le contrôleur présente les caractéristiques suivantes :

- Le droit à SnapCenter Standard est inclus avec l'achat de Premium ou Flash Bundle (pas avec le pack de base)

- Utilisation de stockage illimitée
- Ajouté directement au contrôleur de stockage FAS, AFF ou ASA à l'aide d' ONTAP System Manager ou de l' ONTAP CLI.

> Vous n'entrez aucune information de licence dans l'interface utilisateur de SnapCenter pour les licences basées sur le contrôleur SnapCenter .

- Verrouillé sur le numéro de série du contrôleur

Pour plus d'informations sur les licences requises, voir"Licences SnapCenter" .

## Étape 1 : Vérifiez si la licence SnapManager Suite est installée

Vous pouvez utiliser l'interface utilisateur de SnapCenter pour vérifier si une licence SnapManager Suite est installée sur les systèmes de stockage principaux FAS, AFF ou ASA et identifier les systèmes qui ont besoin de licences. Les licences SnapManager Suite s'appliquent uniquement aux SVM ou clusters FAS, AFF et ASA sur les systèmes de stockage principaux.

> Si vous disposez déjà d'une licence SnapManager Suite sur votre contrôleur, SnapCenter fournit automatiquement le droit de licence standard basé sur le contrôleur. Les noms de licence SnapManagerSuite et de licence basée sur le contrôleur SnapCenter Standard sont utilisés de manière interchangeable, mais ils font référence à la même licence.

**Étapes**

1. Dans le volet de navigation de gauche, sélectionnez **Systèmes de stockage**.
2. Dans la page Systèmes de stockage, dans la liste déroulante **Type**, sélectionnez si vous souhaitez afficher tous les SVM ou clusters qui ont été ajoutés :
   - Pour afficher tous les SVM qui ont été ajoutés, sélectionnez * ONTAP SVM*.
   - Pour afficher tous les clusters qui ont été ajoutés, sélectionnez * Clusters ONTAP *.

     Lorsque vous sélectionnez le nom du cluster, toutes les SVM qui font partie du cluster s'affichent dans la section Machines virtuelles de stockage.
3. Dans la liste Connexions de stockage, recherchez la colonne Licence du contrôleur.

   La colonne Licence du contrôleur affiche le statut suivant :

   - ✔ indique qu'une licence SnapManager Suite est installée sur un système de stockage principal FAS, AFF ou ASA .
   - ⊘ indique qu'une licence SnapManager Suite n'est pas installée sur un système de stockage principal FAS, AFF ou ASA .
   - Non applicable indique qu'une licence SnapManager Suite n'est pas applicable car le contrôleur de stockage se trouve sur Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select ou des plates-formes de stockage secondaires.

## Étape 2 : Identifier les licences installées sur le contrôleur

Vous pouvez utiliser la ligne de commande ONTAP pour afficher toutes les licences installées sur votre contrôleur. Vous devez être administrateur de cluster sur le système FAS, AFF ou ASA .

> Le contrôleur affiche la licence basée sur le contrôleur SnapCenter Standard comme licence SnapManagerSuite.

**Étapes**

1. Connectez-vous au contrôleur NetApp à l'aide de la ligne de commande ONTAP .
2. Entrez la commande license show, puis affichez la sortie pour voir si la licence SnapManagerSuite est installée.

**Exemple de sortie**

```
cluster1::> license show
(system license show)

Serial Number: 1-80-0000xx
Owner: cluster1
Package           Type     Description             Expiration
----------------- -------- ---------------------   ---------------
Base              site     Cluster Base License    -

Serial Number: 1-81-00000000000000000000000xx
Owner: cluster1-01
Package           Type     Description             Expiration
----------------- -------- ---------------------   ---------------
NFS               license  NFS License             -
CIFS              license  CIFS License            -
iSCSI             license  iSCSI License           -
FCP               license  FCP License             -
SnapRestore       license  SnapRestore License     -
SnapMirror        license  SnapMirror License      -
FlexClone         license  FlexClone License       -
SnapVault         license  SnapVault License       -
SnapManagerSuite  license  SnapManagerSuite License -
```

Dans l'exemple, la licence SnapManagerSuite est installée, par conséquent, aucune action de licence SnapCenter supplémentaire n'est requise.

## Étape 3 : Récupérer le numéro de série du contrôleur

Obtenez le numéro de série du contrôleur à l'aide de la ligne de commande ONTAP . Vous devez être administrateur de cluster sur le système FAS, AFF ou ASA pour obtenir votre numéro de série de licence basé sur le contrôleur.

**Étapes**

1. Connectez-vous au contrôleur à l'aide de la ligne de commande ONTAP .
2. Entrez la commande system show -instance, puis examinez la sortie pour localiser le numéro de série du contrôleur.

   **Exemple de sortie**

```
cluster1::> system show -instance

Node: fasxxxx-xx-xx-xx
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false

Node: fas8080-41-42-02
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234512
Asset Tag: -
Uptime: 144 days 00:08
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. Enregistrez les numéros de série.

## Étape 4 : Récupérer le numéro de série de la licence basée sur le contrôleur

Si vous utilisez un stockage FAS, ASA ou AFF , vous pouvez récupérer la licence basée sur le contrôleur

SnapCenter à partir du site de support NetApp avant de l'installer à l'aide de la ligne de commande ONTAP .

**Avant de commencer**

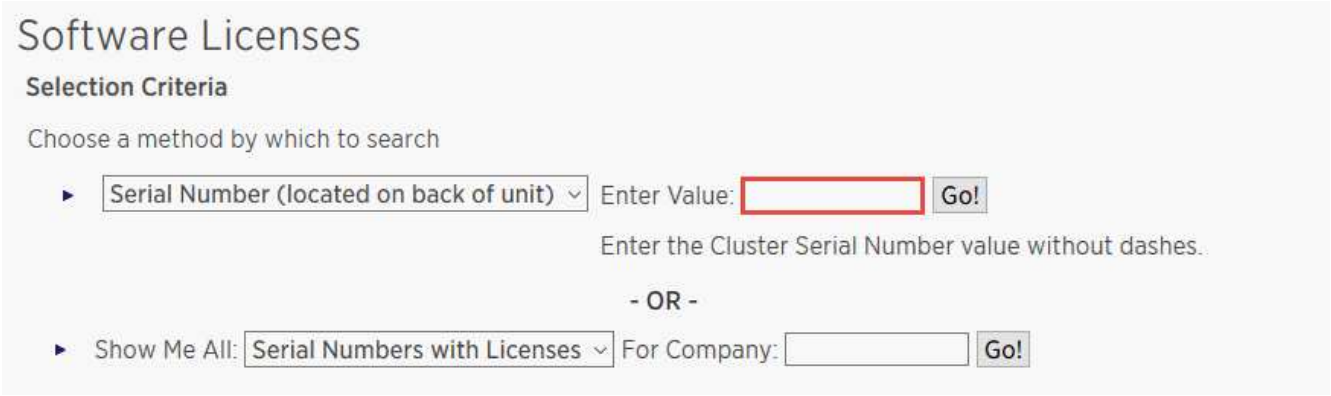
- Vous devez disposer d'informations de connexion valides au site de support NetApp .

  Si vous ne saisissez pas d'informations d'identification valides, le système ne renvoie aucune information pour votre recherche.

- Vous devriez avoir le numéro de série du contrôleur.

**Étapes**

1. Connectez-vous à la "Site de support NetApp" .
2. Accédez à **Systèmes** > **Licences logicielles**.
3. Dans la zone Critères de sélection, assurez-vous que le numéro de série (situé à l'arrière de l'unité) est sélectionné, entrez le numéro de série du contrôleur, puis sélectionnez **Go!**.




   Une liste de licences pour le contrôleur spécifié s'affiche.

4. Localisez et enregistrez la licence SnapCenter Standard ou SnapManagerSuite.

## Étape 5 : Ajouter une licence basée sur le contrôleur

Vous pouvez utiliser la ligne de commande ONTAP pour ajouter une licence basée sur un contrôleur SnapCenter lorsque vous utilisez des systèmes FAS, AFF ou ASA et que vous disposez d'une licence SnapCenter Standard ou SnapManagerSuite.

**Avant de commencer**

- Vous devez être administrateur de cluster sur le système FAS, AFF ou ASA .
- Vous devez disposer de la licence SnapCenter Standard ou SnapManagerSuite.

**À propos de cette tâche**

Si vous souhaitez installer SnapCenter à titre d'essai avec un stockage FAS, AFF ou ASA , vous pouvez obtenir une licence d'évaluation Premium Bundle à installer sur votre contrôleur.

Si vous souhaitez installer SnapCenter à titre d'essai, vous devez contacter votre représentant commercial pour obtenir une licence d'évaluation Premium Bundle à installer sur votre contrôleur.

**Étapes**

1. Connectez-vous au cluster NetApp à l'aide de la ligne de commande ONTAP .

2. Ajoutez la clé de licence SnapManagerSuite :

   ```
   system license add -license-code license_key
   ```

   Cette commande est disponible au niveau de privilège administrateur.

3. Vérifiez que la licence SnapManagerSuite est installée :

   ```
   license show
   ```

### Étape 6 : Supprimer la licence d'essai

Si vous utilisez une licence SnapCenter Standard basée sur un contrôleur et que vous devez supprimer la licence d'essai basée sur la capacité (numéro de série se terminant par « 50 »), vous devez utiliser les commandes MySQL pour supprimer la licence d'essai manuellement. La licence d'essai ne peut pas être supprimée à l'aide de l'interface utilisateur de SnapCenter .

> La suppression manuelle d'une licence d'essai n'est requise que si vous utilisez une licence basée sur un contrôleur SnapCenter Standard.

**Étapes**

1. Sur le serveur SnapCenter , ouvrez une fenêtre PowerShell pour réinitialiser le mot de passe MySQL.
   a. Exécutez l'applet de commande Open-SmConnection pour établir une connexion avec le serveur SnapCenter pour un compte SnapCenterAdmin.
   b. Exécutez Set-SmRepositoryPassword pour réinitialiser le mot de passe MySQL.

      Pour plus d'informations sur les applets de commande, voir "Guide de référence de l'applet de commande du logiciel SnapCenter" .

2. Ouvrez l'invite de commande et exécutez mysql -u root -p pour vous connecter à MySQL.

   MySQL vous demande le mot de passe. Saisissez les informations d'identification que vous avez fournies lors de la réinitialisation du mot de passe.

3. Supprimer la licence d'essai de la base de données :

   ```
   use nsm;DELETE FROM nsm_License WHERE nsm_License_Serial_Number='510000050';
   ```

# Configurer la haute disponibilité

## Configurer les serveurs SnapCenter pour une haute disponibilité

Pour prendre en charge la haute disponibilité (HA) dans SnapCenter exécuté sous Windows ou sous Linux, vous pouvez installer l'équilibreur de charge F5. F5 permet au serveur SnapCenter de prendre en charge les configurations actives-passives dans un maximum de deux hôtes situés au même emplacement. Pour utiliser l'équilibreur de charge F5 dans SnapCenter, vous devez configurer les serveurs SnapCenter et configurer l'équilibreur de charge F5.

Vous pouvez également configurer l'équilibrage de la charge réseau (NLB) pour configurer SnapCenter High Availability. Vous devez configurer manuellement NLB en dehors de l'installation de SnapCenter pour une haute disponibilité.

Pour l'environnement cloud, vous pouvez configurer la haute disponibilité à l'aide d'Amazon Web Services (AWS) Elastic Load Balancing (ELB) et de l'équilibreur de charge Azure.

**Configurer la haute disponibilité à l'aide de F5**

Pour obtenir des instructions sur la configuration des serveurs SnapCenter pour une haute disponibilité à l'aide de l'équilibreur de charge F5, reportez-vous à "Comment configurer les serveurs SnapCenter pour une haute disponibilité à l'aide de F5 Load Balancer" .

Vous devez être membre du groupe Administrateurs locaux sur les serveurs SnapCenter (en plus d'être affecté au rôle SnapCenterAdmin) pour utiliser les applets de commande suivantes pour ajouter et supprimer des clusters F5 :

- Ajouter-SmServerCluster
- Ajouter-SmServer
- Supprimer-SmServerCluster

  Pour plus d'informations, consultez "Guide de référence de l'applet de commande du logiciel SnapCenter" .

Informations Complémentaires

- Après avoir installé et configuré SnapCenter pour une haute disponibilité, modifiez le raccourci du bureau SnapCenter pour qu'il pointe vers l'adresse IP du cluster F5.
- Si un basculement se produit entre les serveurs SnapCenter et s'il existe également une session SnapCenter existante, vous devez fermer le navigateur et vous reconnecter à SnapCenter .
- Dans la configuration de l'équilibreur de charge (NLB ou F5), si vous ajoutez un hôte partiellement résolu par l'hôte NLB ou F5 et si l'hôte SnapCenter n'est pas en mesure d'atteindre cet hôte, la page de l'hôte SnapCenter bascule fréquemment entre les états d'arrêt et d'exécution des hôtes. Pour résoudre ce problème, vous devez vous assurer que les deux hôtes SnapCenter sont en mesure de résoudre l'hôte dans l'hôte NLB ou F5.
- Les commandes SnapCenter pour les paramètres MFA doivent être exécutées sur tous les hôtes. La configuration de la partie de confiance doit être effectuée sur le serveur Active Directory Federation Services (AD FS) à l'aide des détails du cluster F5. L'accès à l'interface utilisateur SnapCenter au niveau de l'hôte sera bloqué une fois l'authentification multifacteur activée.
- Lors du basculement, les paramètres du journal d'audit ne seront pas reflétés sur le deuxième hôte. Par conséquent, vous devez répéter manuellement les paramètres du journal d'audit sur l'hôte passif F5 lorsqu'il devient actif.

**Configurer la haute disponibilité à l'aide de l'équilibrage de la charge réseau (NLB)**

Vous pouvez configurer l'équilibrage de la charge réseau (NLB) pour configurer SnapCenter High Availability. Vous devez configurer manuellement NLB en dehors de l'installation de SnapCenter pour une haute disponibilité.

Pour plus d'informations sur la configuration de l'équilibrage de la charge réseau (NLB) avec SnapCenter , reportez-vous à "Comment configurer NLB avec SnapCenter" .

**Configurer la haute disponibilité à l'aide d'AWS Elastic Load Balancing (ELB)**

Vous pouvez configurer un environnement SnapCenter haute disponibilité dans Amazon Web Services (AWS) en configurant deux serveurs SnapCenter dans des zones de disponibilité (AZ) distinctes et en les configurant pour le basculement automatique. L'architecture comprend des adresses IP privées virtuelles, des tables de routage et la synchronisation entre les bases de données MySQL actives et de secours.

**Étapes**

1. Configurer une IP de superposition privée virtuelle dans AWS. Pour plus d'informations, reportez-vous à "Configurer une IP de superposition privée virtuelle" .
2. Préparez votre hôte Windows
   a. Forcer IPv4 à être prioritaire sur IPv6 :
      - Emplacement : HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
      - Clé : DisabledComponents
      - Type : REG_DWORD
      - Valeur : 0x20
   b. Assurez-vous que les noms de domaine entièrement qualifiés peuvent être résolus via DNS ou via la configuration de l'hôte local vers les adresses IPv4.
   c. Assurez-vous que vous n'avez pas de proxy système configuré.
   d. Assurez-vous que le mot de passe administrateur est le même sur les deux serveurs Windows lorsque vous utilisez une configuration sans Active Directory et que les serveurs ne se trouvent pas dans le même domaine.
   e. Ajoutez une IP virtuelle sur les deux serveurs Windows.
3. Créez le cluster SnapCenter .
   a. Démarrez Powershell et connectez-vous à SnapCenter. `Open-SmConnection`
   b. Créer le cluster. `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator`
   c. Ajoutez le serveur secondaire. `Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator`
   d. Obtenez les détails de haute disponibilité. `Get-SmServerConfig`
4. Créez la fonction Lamda pour ajuster la table de routage au cas où le point de terminaison IP privé virtuel deviendrait indisponible, surveillé par AWS CloudWatch. Pour plus d'informations, reportez-vous à "Créer une fonction Lambda" .
5. Créez un moniteur dans CloudWatch pour surveiller la disponibilité du point de terminaison SnapCenter . Une alarme est configurée pour déclencher une fonction Lambda si le point de terminaison est inaccessible. La fonction Lambda ajuste la table de routage pour rediriger le trafic vers le serveur SnapCenter actif. Pour plus d'informations, reportez-vous à "Créer des canaris synthétiques" .
6. Implémentez un flux de travail à l'aide d'une fonction d'étape comme alternative à la surveillance CloudWatch, offrant des temps de basculement plus courts. Le flux de travail comprend une fonction de sonde Lambda pour tester l'URL SnapCenter , une table DynamoDB pour stocker les nombres d'échecs et la fonction Step elle-même.
   a. Utilisez une fonction lambda pour sonder l'URL SnapCenter . Pour plus d'informations, reportez-vous à "Créer une fonction Lambda" .
   b. Créez une table DynamoDB pour stocker le nombre d'échecs entre deux itérations de fonction Step. Pour plus d'informations, reportez-vous à "Démarrer avec la table DynamoDB" .
   c. Créez la fonction Step. Pour plus d'informations, reportez-vous à "Documentation de la fonction Step" .
   d. Tester une seule étape.
   e. Tester la fonction complète.

f. Créez un rôle IAM et ajustez les autorisations pour être autorisé à exécuter la fonction Lambda.

g. Créez un calendrier pour déclencher la fonction Step. Pour plus d'informations, reportez-vous à "Utilisation d'Amazon EventBridge Scheduler pour démarrer une fonction Step Functions" .

**Configurer la haute disponibilité à l'aide de l'équilibreur de charge Azure**

Vous pouvez configurer un environnement SnapCenter haute disponibilité à l'aide de l'équilibreur de charge Azure.

**Étapes**

1. Créez des machines virtuelles dans un groupe identique à l'aide du portail Azure. L'ensemble de machines virtuelles identiques Azure vous permet de créer et de gérer un groupe de machines virtuelles à charge équilibrée. Le nombre d'instances de machine virtuelle peut augmenter ou diminuer automatiquement en réponse à la demande ou à une planification définie. Pour plus d'informations, reportez-vous à "Créer des machines virtuelles dans un groupe identique à l'aide du portail Azure" .
2. Après avoir configuré les machines virtuelles, connectez-vous à chaque machine virtuelle de l'ensemble de machines virtuelles et installez SnapCenter Server sur les deux nœuds.
3. Créez le cluster dans l'hôte 1. `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>`
4. Ajoutez le serveur secondaire. `Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>`
5. Obtenez les détails de haute disponibilité. `Get-SmServerConfig`
6. Si nécessaire, reconstruisez l'hôte secondaire. `Set-SmRepositoryConfig -RebuildSlave -Verbose`
7. Basculement vers le deuxième hôte. `Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose`

== Passer de NLB à F5 pour une haute disponibilité

Vous pouvez modifier votre configuration SnapCenter HA de Network Load Balancing (NLB) pour utiliser F5 Load Balancer.

**Mesures**

1. Configurez les serveurs SnapCenter pour une haute disponibilité à l'aide de F5. "Apprendre encore plus" .
2. Sur l'hôte SnapCenter Server, lancez PowerShell.
3. Démarrez une session en utilisant l'applet de commande Open-SmConnection, puis entrez vos informations d'identification.
4. Mettez à jour le serveur SnapCenter pour qu'il pointe vers l'adresse IP du cluster F5 à l'aide de l'applet de commande Update-SmServerCluster.

   Les informations concernant les paramètres pouvant être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant *Get-Help command_name*. Alternativement, vous pouvez également vous référer à la "Guide de référence de l'applet de commande du logiciel SnapCenter" .

### Haute disponibilité pour le référentiel MySQL SnapCenter

La réplication MySQL est une fonctionnalité de MySQL Server qui vous permet de répliquer des données d'un serveur de base de données MySQL (maître) vers un autre serveur de base de données MySQL (esclave). SnapCenter prend en charge la réplication MySQL pour une haute disponibilité uniquement sur deux nœuds compatibles NLB (Network Load Balancing).

SnapCenter effectue des opérations de lecture ou d'écriture sur le référentiel maître et achemine sa connexion vers le référentiel esclave en cas de panne sur le référentiel maître. Le référentiel esclave devient alors le référentiel maître. SnapCenter prend également en charge la réplication inverse, qui est activée uniquement lors du basculement.

Si vous souhaitez utiliser la fonctionnalité de haute disponibilité (HA) de MySQL, vous devez configurer Network Load Balancer (NLB) sur le premier nœud. Le référentiel MySQL est installé sur ce nœud dans le cadre de l'installation. Lors de l'installation de SnapCenter sur le deuxième nœud, vous devez vous connecter au F5 du premier nœud et créer une copie du référentiel MySQL sur le deuxième nœud.

SnapCenter fournit les applets de commande PowerShell *Get-SmRepositoryConfig* et *Set-SmRepositoryConfig* pour gérer la réplication MySQL.

Les informations concernant les paramètres pouvant être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant *Get-Help command_name*. Alternativement, vous pouvez également vous référer à la "Guide de référence de l'applet de commande du logiciel SnapCenter" .

Vous devez être conscient des limitations liées à la fonctionnalité MySQL HA :

- NLB et MySQL HA ne sont pas pris en charge au-delà de deux nœuds.
- Le passage d'une installation autonome de SnapCenter à une installation NLB ou vice versa et le passage d'une configuration autonome MySQL à MySQL HA ne sont pas pris en charge.
- Le basculement automatique n'est pas pris en charge si les données du référentiel esclave ne sont pas synchronisées avec les données du référentiel maître.

  Vous pouvez lancer un basculement forcé à l'aide de l'applet de commande *Set-SmRepositoryConfig*.

- Lorsque le basculement est lancé, les tâches en cours d'exécution peuvent échouer.

  Si le basculement se produit parce que MySQL Server ou SnapCenter Server est en panne, toutes les tâches en cours d'exécution peuvent échouer. Après le basculement vers le deuxième nœud, toutes les tâches suivantes s'exécutent avec succès.

Pour plus d'informations sur la configuration de la haute disponibilité, voir "Comment configurer NLB et ARR avec SnapCenter" .

# Configurer le contrôle d'accès basé sur les rôles (RBAC)

### Créer un rôle

En plus d'utiliser les rôles SnapCenter existants, vous pouvez créer vos propres rôles et personnaliser les autorisations.

Pour créer vos propres rôles, il est nécessaire de vous connecter en tant que rôle « SnapCenterAdmin ».

**Étapes**

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Rôles**.
3. Cliquez + .
4. Spécifiez un nom et une description pour le nouveau rôle.

   Seuls les caractères spéciaux suivants peuvent être utilisés dans les noms d'utilisateur et les noms de groupe : espace ( ), trait d'union (-), trait de soulignement (_) et deux points (:).

5. Sélectionnez **Tous les membres de ce rôle peuvent voir les objets des autres membres** pour permettre aux autres membres du rôle de voir les ressources telles que les volumes et les hôtes après avoir actualisé la liste des ressources.

   Vous devez désélectionner cette option si vous ne souhaitez pas que les membres de ce rôle voient les objets auxquels d'autres membres sont affectés.

   Lorsque cette option est activée, l'attribution d'un accès utilisateur aux objets ou aux ressources n'est pas requise si les utilisateurs appartiennent au même rôle que l'utilisateur qui a créé les objets ou les ressources.

6. Dans la page Autorisations, sélectionnez les autorisations que vous souhaitez attribuer au rôle ou cliquez sur **Sélectionner tout** pour accorder toutes les autorisations au rôle.
7. Cliquez sur **Soumettre**.

## Ajouter un rôle RBAC NetApp ONTAP à l'aide des commandes de connexion de sécurité

Vous pouvez utiliser les commandes de connexion de sécurité pour ajouter un rôle RBAC NetApp ONTAP lorsque vos systèmes de stockage exécutent ONTAP en cluster.

**Avant de commencer**

- Identifiez la tâche (ou les tâches) que vous souhaitez effectuer et les privilèges requis pour effectuer ces tâches.
- Accorder des privilèges aux commandes et/ou aux répertoires de commandes.

  Il existe deux niveaux d'accès pour chaque commande/répertoire de commandes : accès total et lecture seule.

  Vous devez toujours attribuer d'abord les privilèges d'accès complet.

- Attribuer des rôles aux utilisateurs.
- Identifiez votre configuration selon que vos plug-ins SnapCenter sont connectés à l'IP de l'administrateur de cluster pour l'ensemble du cluster ou directement connectés à une SVM au sein du cluster.

**À propos de cette tâche**

Pour simplifier la configuration de ces rôles sur les systèmes de stockage, vous pouvez utiliser l'outil RBAC User Creator pour NetApp ONTAP , publié sur le forum des communautés NetApp .

Cet outil gère automatiquement la configuration correcte des privilèges ONTAP . Par exemple, l'outil RBAC User Creator pour NetApp ONTAP ajoute automatiquement les privilèges dans l'ordre correct afin que les privilèges d'accès complet apparaissent en premier. Si vous ajoutez d'abord les privilèges en lecture seule, puis les privilèges d'accès complet, ONTAP marque les privilèges d'accès complet comme des doublons et les ignore.

> Si vous mettez à niveau ultérieurement SnapCenter ou ONTAP, vous devez réexécuter l'outil RBAC User Creator pour NetApp ONTAP pour mettre à jour les rôles d'utilisateur que vous avez créés précédemment. Les rôles d'utilisateur créés pour une version antérieure de SnapCenter ou ONTAP ne fonctionnent pas correctement avec les versions mises à niveau. Lorsque vous réexécutez l'outil, il gère automatiquement la mise à niveau. Vous n'avez pas besoin de recréer les rôles.

Pour plus d'informations sur la configuration des rôles ONTAP RBAC, consultez le "Guide d'authentification de l'administrateur ONTAP 9 et d'alimentation RBAC" .

**Étapes**

1. Sur le système de stockage, créez un nouveau rôle en entrant la commande suivante :

   ```
   security login role create <role_name\> -cmddirname "command" -access all
   -vserver <svm_name\>
   ```

   - svm_name est le nom du SVM. Si vous laissez ce champ vide, la valeur par défaut est l'administrateur du cluster.
   - role_name est le nom que vous spécifiez pour le rôle.
   - la commande est la capacité ONTAP .

     > Vous devez répéter cette commande pour chaque autorisation. N'oubliez pas que toutes les commandes d'accès doivent être répertoriées avant les commandes en lecture seule.

   Pour plus d'informations sur la liste des autorisations, voir"Commandes CLI ONTAP pour la création de rôles et l'attribution d'autorisations" .

2. Créez un nom d'utilisateur en entrant la commande suivante :

   ```
   security login create -username <user_name\> -application ontapi -authmethod
   <password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment
   "user_description"
   ```

   - user_name est le nom de l'utilisateur que vous créez.
   - <password> est votre mot de passe. Si vous ne spécifiez pas de mot de passe, le système vous en demandera un.
   - svm_name est le nom du SVM.

3. Attribuez le rôle à l'utilisateur en entrant la commande suivante :

   ```
   security login modify username <user_name\> -vserver <svm_name\> -role
   <role_name\> -application ontapi -application console -authmethod <password\>
   ```

   - <user_name> est le nom de l'utilisateur que vous avez créé à l'étape 2. Cette commande vous permet de modifier l'utilisateur pour l'associer au rôle.

- <svm_name> est le nom du SVM.
- <role_name> est le nom du rôle que vous avez créé à l'étape 1.
- <password> est votre mot de passe. Si vous ne spécifiez pas de mot de passe, le système vous en demandera un.

4. Vérifiez que l'utilisateur a été créé correctement en entrant la commande suivante :

   ```
   security login show –vserver <svm_name\> -user-or-group-name <user_name\>
   ```

   user_name est le nom de l'utilisateur que vous avez créé à l'étape 3.

## Créer des rôles SVM avec des privilèges minimaux

Il existe plusieurs commandes ONTAP CLI que vous devez exécuter lorsque vous créez un rôle pour un nouvel utilisateur SVM dans ONTAP. Ce rôle est requis si vous configurez des SVM dans ONTAP pour les utiliser avec SnapCenter et que vous ne souhaitez pas utiliser le rôle vsadmin.

**Mesures**

1. Sur le système de stockage, créez un rôle et attribuez toutes les autorisations au rôle.

   ```
   security login role create –vserver <svm_name\>- role <SVM_Role_Name\>
   -cmddirname <permission\>
   ```

   Vous devez répéter cette commande pour chaque autorisation.

2. Créez un utilisateur et attribuez le rôle à cet utilisateur.

   ```
   security login create -user <user_name\> -vserver <svm_name\> -application
   ontapi -authmethod password -role <SVM_Role_Name\>
   ```

3. Déverrouiller l'utilisateur.

   ```
   security login unlock -user <user_name\> -vserver <svm_name\>
   ```

### Commandes CLI ONTAP pour la création de rôles SVM et l'attribution d'autorisations

Il existe plusieurs commandes ONTAP CLI que vous devez exécuter pour créer des rôles SVM et attribuer des autorisations.

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"lun show" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"vserver cifs share show" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all`

## Créer des rôles SVM pour les systèmes ASA r2

Il existe plusieurs commandes ONTAP CLI que vous devez exécuter pour créer un rôle pour un nouvel utilisateur SVM dans les systèmes ASA r2. Ce rôle est requis si vous configurez des SVM dans des systèmes ASA r2 pour les utiliser avec SnapCenter et que vous ne souhaitez pas utiliser le rôle vsadmin.

**Mesures**

1. Sur le système de stockage, créez un rôle et attribuez toutes les autorisations au rôle.

   ```
   security login role create –vserver <svm_name\>- role <SVM_Role_Name\>
   -cmddirname <permission\>
   ```

   Vous devez répéter cette commande pour chaque autorisation.

2. Créez un utilisateur et attribuez le rôle à cet utilisateur.

   ```
   security login create -user <user_name\> -vserver <svm_name\> -application
   http -authmethod password -role <SVM_Role_Name\>
   ```

3. Déverrouiller l'utilisateur.

   ```
   security login unlock -user <user_name\> -vserver <svm_name\>
   ```

**Commandes CLI ONTAP pour la création de rôles SVM et l'attribution d'autorisations**

Il existe plusieurs commandes ONTAP CLI que vous devez exécuter pour créer des rôles SVM et attribuer des autorisations.

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname`

"network interface" -access readonly

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"vserver cifs show" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "storage-unit show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "consistency-group" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror protect" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume delete" -access all`
- `security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name`
- `security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name`

## Créer des rôles de cluster ONTAP avec des privilèges minimaux

Vous devez créer un rôle de cluster ONTAP avec des privilèges minimaux afin de ne pas avoir à utiliser le rôle d'administrateur ONTAP pour effectuer des opérations dans SnapCenter. Vous pouvez exécuter plusieurs commandes ONTAP CLI pour créer le rôle de cluster ONTAP et attribuer des privilèges minimaux.

**Mesures**

1. Sur le système de stockage, créez un rôle et attribuez toutes les autorisations au rôle.

   ```
   security login role create –vserver <cluster_name\>- role <role_name\>
   -cmddirname <permission\>
   ```

   Vous devez répéter cette commande pour chaque autorisation.

2. Créez un utilisateur et attribuez le rôle à cet utilisateur.

   ```
   security login create -user <user_name\> -vserver <cluster_name\> -application
   ontapi http -authmethod password -role <role_name\>
   ```

3. Déverrouiller l'utilisateur.

   ```
   security login unlock -user <user_name\> -vserver <cluster_name\>
   ```

**Commandes CLI ONTAP pour la création de rôles de cluster et l'attribution d'autorisations**

Il existe plusieurs commandes ONTAP CLI que vous devez exécuter pour créer des rôles de cluster et attribuer des autorisations.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

"lun mapping create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"snapmirror update-ls-set" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```
"vserver cifs modify" -access all
```

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all`

### Créer des rôles de cluster ONTAP pour les systèmes ASA r2

Vous devez créer un rôle de cluster ONTAP avec des privilèges minimaux afin de ne pas avoir à utiliser le rôle d'administrateur ONTAP pour effectuer des opérations dans SnapCenter. Vous pouvez exécuter plusieurs commandes ONTAP CLI pour créer le rôle de cluster ONTAP et attribuer des privilèges minimaux.

### Mesures

1. Sur le système de stockage, créez un rôle et attribuez toutes les autorisations au rôle.

   ```
   security login role create –vserver <cluster_name\>- role <role_name\>
   -cmddirname <permission\>
   ```

   Vous devez répéter cette commande pour chaque autorisation.

2. Créez un utilisateur et attribuez le rôle à cet utilisateur.

   ```
   security login create -user <user_name\> -vserver <cluster_name\> -application
   http -authmethod password -role <role_name\>
   ```

3. Déverrouiller l'utilisateur.

   ```
   security login unlock -user <user_name\> -vserver <cluster_name\>
   ```

### Commandes CLI ONTAP pour la création de rôles de cluster et l'attribution d'autorisations

Il existe plusieurs commandes ONTAP CLI que vous devez exécuter pour créer des rôles de cluster et attribuer des autorisations.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

"lun create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"snapmirror policy delete" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"volume snapshot rename" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "storage-unit show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "consistency-group" show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror protect" show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume delete" show" -access all`

## Ajoutez un utilisateur ou un groupe et attribuez un rôle et des ressources

Pour configurer le contrôle d'accès basé sur les rôles pour les utilisateurs de SnapCenter , vous pouvez ajouter des utilisateurs ou des groupes et attribuer un rôle. Le rôle détermine les options auxquelles les utilisateurs de SnapCenter peuvent accéder.

**Avant de commencer**

- Vous devez vous être connecté en tant que rôle « SnapCenterAdmin ».
- Vous devez avoir créé les comptes d'utilisateur ou de groupe dans Active Directory dans le système d'exploitation ou la base de données. Vous ne pouvez pas utiliser SnapCenter pour créer ces comptes.

  Vous ne pouvez inclure que les caractères spéciaux suivants dans les noms d'utilisateur et les noms de groupe : espace ( ), trait d'union (-), trait de soulignement (_) et deux points (:).

- SnapCenter comprend plusieurs rôles prédéfinis.

  Vous pouvez soit attribuer ces rôles à l'utilisateur, soit créer de nouveaux rôles.

- Les utilisateurs AD et les groupes AD ajoutés à SnapCenter RBAC doivent disposer de l'autorisation LECTURE sur le conteneur Utilisateurs et le conteneur Ordinateurs dans Active Directory.
- Après avoir attribué un rôle à un utilisateur ou à un groupe contenant les autorisations appropriées, vous devez attribuer à l'utilisateur l'accès aux ressources SnapCenter , telles que les hôtes et les connexions de stockage.

  Cela permet aux utilisateurs d'effectuer les actions pour lesquelles ils disposent d'autorisations sur les

actifs qui leur sont attribués.

- Vous devez attribuer un rôle à l'utilisateur ou au groupe à un moment donné pour profiter des autorisations et de l'efficacité du RBAC.
- Vous pouvez attribuer des ressources telles que l'hôte, les groupes de ressources, la politique, la connexion de stockage, le plug-in et les informations d'identification à l'utilisateur lors de la création de l'utilisateur ou du groupe.
- Les ressources minimales que vous devez attribuer à un utilisateur pour effectuer certaines opérations sont les suivantes :

| Opération | Cession des actifs |
|---|---|
| Protéger les ressources | hôte, politique |
| Sauvegarde | hôte, groupe de ressources, politique |
| Restaurer | hôte, groupe de ressources |
| Cloner | hôte, groupe de ressources, politique |
| Cycle de vie du clone | hôte |
| Créer un groupe de ressources | hôte |

- Lorsqu'un nouveau nœud est ajouté à un cluster Windows ou à une ressource DAG (Exchange Server Database Availability Group) et si ce nouveau nœud est attribué à un utilisateur, vous devez réattribuer la ressource à l'utilisateur ou au groupe pour inclure le nouveau nœud à l'utilisateur ou au groupe.

  Vous devez réaffecter l'utilisateur ou le groupe RBAC au cluster ou au DAG pour inclure le nouveau nœud à l'utilisateur ou au groupe RBAC. Par exemple, vous disposez d'un cluster à deux nœuds et vous avez attribué un utilisateur ou un groupe RBAC au cluster. Lorsque vous ajoutez un autre nœud au cluster, vous devez réaffecter l'utilisateur ou le groupe RBAC au cluster pour inclure le nouveau nœud pour l'utilisateur ou le groupe RBAC.

- Si vous prévoyez de répliquer des instantanés, vous devez attribuer la connexion de stockage pour le volume source et le volume de destination à l'utilisateur effectuant l'opération.

  Vous devez ajouter des ressources avant d'attribuer l'accès aux utilisateurs.

Si vous utilisez les fonctions SnapCenter Plug-in for VMware vSphere pour protéger des machines virtuelles, des VMDK ou des banques de données, vous devez utiliser l'interface graphique utilisateur VMware vSphere pour ajouter un utilisateur vCenter à un rôle SnapCenter Plug-in for VMware vSphere . Pour plus d'informations sur les rôles VMware vSphere, consultez "Rôles prédéfinis fournis avec le SnapCenter Plug-in for VMware vSphere" .

**Mesures**

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Utilisateurs et accès** > * *.

3. Dans la page Ajouter des utilisateurs/groupes à partir d'Active Directory ou d'un groupe de travail :

| Pour ce domaine… | Fais ceci… |
| --- | --- |
| Type d'accès | Sélectionnez un domaine ou un groupe de travail<br><br>Pour le type d'authentification de domaine, vous devez spécifier le nom de domaine de l'utilisateur ou du groupe auquel vous souhaitez ajouter l'utilisateur à un rôle.<br><br>Par défaut, il est pré-rempli avec le nom de domaine connecté.<br><br>Vous devez enregistrer le domaine non approuvé dans la page **Paramètres** > **Paramètres globaux** > **Paramètres du domaine**. |
| Type | Sélectionnez Utilisateur ou Groupe<br><br>SnapCenter prend en charge uniquement le groupe de sécurité et non le groupe de distribution. |
| Nom d'utilisateur | a. Saisissez le nom d'utilisateur partiel, puis cliquez sur **Ajouter**.<br><br>Le nom d'utilisateur est sensible à la casse.<br><br>b. Sélectionnez le nom d'utilisateur dans la liste de recherche.<br><br>Lorsque vous ajoutez des utilisateurs d'un domaine différent ou d'un domaine non approuvé, vous devez saisir le nom d'utilisateur dans son intégralité, car il n'existe pas de liste de recherche pour les utilisateurs inter-domaines.<br><br>Répétez cette étape pour ajouter des utilisateurs ou des groupes supplémentaires au rôle sélectionné. |
| Rôles | Sélectionnez le rôle auquel vous souhaitez ajouter l'utilisateur. |

4. Cliquez sur **Attribuer**, puis sur la page Attribuer des actifs :
   a. Sélectionnez le type d'actif dans la liste déroulante **Actif**.

b. Dans le tableau Actif, sélectionnez l'actif.

   Les actifs sont répertoriés uniquement si l'utilisateur a ajouté les actifs à SnapCenter.

c. Répétez cette procédure pour tous les actifs requis.

d. Cliquez sur **Enregistrer**.

5. Cliquez sur **Soumettre**.

Après avoir ajouté des utilisateurs ou des groupes et attribué des rôles, actualisez la liste des ressources.

# Configurer les paramètres du journal d'audit

Des journaux d'audit sont générés pour chaque activité du serveur SnapCenter . Par défaut, les journaux d'audit sont sécurisés dans l'emplacement d'installation par défaut *C:\Program Files\ NetApp\ SnapCenter WebApp\audit*.

Les journaux d'audit sont sécurisés au moyen de la génération d'un condensé signé numériquement pour chaque événement d'audit afin de le protéger contre toute modification non autorisée. Les résumés générés sont conservés dans le fichier de somme de contrôle d'audit séparé et sont soumis à des contrôles d'intégrité périodiques pour garantir l'intégrité du contenu.

Vous devez vous être connecté avec le rôle « SnapCenterAdmin ».

**À propos de cette tâche**

- Les alertes sont envoyées dans les scénarios suivants :
  - La planification de la vérification de l'intégrité du journal d'audit ou du serveur Syslog est activée ou désactivée
  - Vérification de l'intégrité du journal d'audit, journal d'audit ou échec du journal du serveur Syslog
  - Faible espace disque
- Le courrier électronique est envoyé uniquement lorsque le contrôle d'intégrité échoue.
- Vous devez modifier simultanément les chemins d'accès au répertoire du journal d'audit et au répertoire du journal de somme de contrôle d'audit. Vous ne pouvez pas en modifier un seul.
- Lorsque les chemins d'accès au répertoire du journal d'audit et au répertoire du journal de somme de contrôle d'audit sont modifiés, la vérification d'intégrité ne peut pas être effectuée sur les journaux d'audit présents à l'emplacement précédent.
- Les chemins d'accès au répertoire du journal d'audit et au répertoire du journal de somme de contrôle d'audit doivent se trouver sur le lecteur local de SnapCenter Server.

  Les lecteurs partagés ou montés en réseau ne sont pas pris en charge.

- Si le protocole UDP est utilisé dans les paramètres du serveur Syslog, les erreurs dues à un port hors service ou indisponible ne peuvent pas être capturées comme une erreur ou une alerte dans SnapCenter.
- Vous pouvez utiliser les commandes Set-SmAuditSettings et Get-SmAuditSettings pour configurer les journaux d'audit.

  Les informations concernant les paramètres pouvant être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant Get-Help command_name. Alternativement, vous pouvez également vous référer au "Guide de référence de l'applet de commande du logiciel SnapCenter" .

**Étapes**

1. Dans la page **Paramètres**, accédez à **Paramètres** > **Paramètres globaux** > **Paramètres du journal d'audit**.
2. Dans la section Journal d'audit, saisissez les détails.
3. Accédez au **répertoire du journal d'audit** et au **répertoire du journal de somme de contrôle d'audit**
   a. Entrez la taille maximale du fichier
   b. Entrez le nombre maximal de fichiers journaux
   c. Entrez le pourcentage d'utilisation de l'espace disque pour envoyer une alerte
4. (Facultatif) Activez **Enregistrer l'heure UTC**.
5. (Facultatif) Activez **Planification de vérification de l'intégrité du journal d'audit** et cliquez sur **Démarrer la vérification de l'intégrité** pour une vérification de l'intégrité à la demande.

   Vous pouvez également exécuter la commande **Start-SmAuditIntegrityCheck** pour démarrer la vérification d'intégrité à la demande.

6. (Facultatif) Activez les journaux d'audit transférés vers le serveur Syslog distant et entrez les détails du serveur Syslog.

   Vous devez importer le certificat du serveur Syslog dans la « racine de confiance » pour le protocole TLS 1.2.

   a. Entrez l'hôte du serveur Syslog
   b. Entrez le port du serveur Syslog
   c. Entrez le protocole du serveur Syslog
   d. Entrez le format RFC
7. Cliquez sur **Enregistrer**.
8. Vous pouvez voir les vérifications d'intégrité d'audit et les vérifications d'espace disque en cliquant sur **Surveiller** > **Tâches**.

# Configurer des connexions MySQL sécurisées avec SnapCenter Server

Vous pouvez générer des certificats Secure Sockets Layer (SSL) et des fichiers de clés si vous souhaitez sécuriser la communication entre SnapCenter Server et MySQL Server dans des configurations autonomes ou des configurations d'équilibrage de charge réseau (NLB).

## Configurer des connexions MySQL sécurisées pour les configurations SnapCenter Server autonomes

Vous pouvez générer des certificats et des fichiers de clés Secure Sockets Layer (SSL) si vous souhaitez sécuriser la communication entre SnapCenter Server et MySQL Server. Vous devez configurer les certificats et les fichiers de clés dans le serveur MySQL et le serveur SnapCenter .

Les certificats suivants sont générés :

- Certificat CA
- Certificat public du serveur et fichier de clé privée
- Certificat public client et fichier de clé privée

**Mesures**

1. Configurez les certificats SSL et les fichiers de clés pour les serveurs et clients MySQL sous Windows à l'aide de la commande openssl.

   Pour plus d'informations, voir "MySQL version 5.7 : Création de certificats et de clés SSL avec OpenSSL"

   > La valeur du nom commun utilisée pour le certificat du serveur, le certificat client et les fichiers de clés doit être différente de la valeur du nom commun utilisée pour le certificat de l'autorité de certification. Si les valeurs de nom commun sont les mêmes, les fichiers de certificat et de clé échouent pour les serveurs compilés à l'aide d'OpenSSL.

   **Meilleure pratique :** vous devez utiliser le nom de domaine complet (FQDN) du serveur comme nom commun pour le certificat du serveur.

2. Copiez les certificats SSL et les fichiers clés dans le dossier MySQL Data.

   Le chemin d'accès par défaut du dossier de données MySQL est `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`.

3. Mettez à jour les chemins d'accès au certificat CA, au certificat public du serveur, au certificat public du client, à la clé privée du serveur et à la clé privée du client dans le fichier de configuration du serveur MySQL (my.ini).

   Le chemin par défaut du fichier de configuration du serveur MySQL (my.ini) est `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`.

   > Vous devez spécifier les chemins d'accès au certificat CA, au certificat public du serveur et à la clé privée du serveur dans la section [mysqld] du fichier de configuration du serveur MySQL (my.ini).

   Vous devez spécifier les chemins d'accès au certificat CA, au certificat public client et à la clé privée client dans la section [client] du fichier de configuration du serveur MySQL (my.ini).

   L'exemple suivant montre les certificats et les fichiers de clés copiés dans la section [mysqld] du fichier my.ini dans le dossier par défaut `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data`.

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
   ```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-
key.pem"
```

L'exemple suivant montre les chemins mis à jour dans la section [client] du fichier my.ini.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-
key.pem"
```

4. Arrêtez l'application Web SnapCenter Server dans Internet Information Server (IIS).
5. Redémarrez le service MySQL.
6. Mettez à jour la valeur de la clé MySQLProtocol dans le fichier SnapManager.Web.UI.dll.config.

   L'exemple suivant montre la valeur de la clé MySQLProtocol mise à jour dans le fichier SnapManager.Web.UI.dll.config.

```
<add key="MySQLProtocol" value="SSL" />
```

7. Mettez à jour le fichier SnapManager.Web.UI.dll.config avec les chemins fournis dans la section [client] du fichier my.ini.

   L'exemple suivant montre les chemins mis à jour dans la section [client] du fichier my.ini.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

8. Démarrez l'application Web SnapCenter Server dans IIS.

## Configurer des connexions MySQL sécurisées pour les configurations HA

Vous pouvez générer des certificats Secure Sockets Layer (SSL) et des fichiers de clés pour les deux nœuds haute disponibilité (HA) si vous souhaitez sécuriser la communication entre SnapCenter Server et les serveurs MySQL. Vous devez configurer les certificats et les fichiers de clés dans les serveurs MySQL et sur les nœuds HA.

Les certificats suivants sont générés :

- Certificat CA

  Un certificat CA est généré sur l'un des nœuds HA et ce certificat CA est copié sur l'autre nœud HA.

- Fichiers de certificat public et de clé privée du serveur pour les deux nœuds HA
- Fichiers de certificat public client et de clé privée client pour les deux nœuds HA

**Mesures**

1. Pour le premier nœud HA, configurez les certificats SSL et les fichiers de clés pour les serveurs et clients MySQL sous Windows à l'aide de la commande openssl.

   Pour plus d'informations, voir "MySQL version 5.7 : Création de certificats et de clés SSL avec OpenSSL"

   > La valeur du nom commun utilisée pour le certificat du serveur, le certificat client et les fichiers de clés doit être différente de la valeur du nom commun utilisée pour le certificat de l'autorité de certification. Si les valeurs de nom commun sont les mêmes, les fichiers de certificat et de clé échouent pour les serveurs compilés à l'aide d'OpenSSL.

   **Meilleure pratique :** vous devez utiliser le nom de domaine complet (FQDN) du serveur comme nom commun pour le certificat du serveur.

2. Copiez les certificats SSL et les fichiers clés dans le dossier MySQL Data.

   Le chemin d'accès par défaut au dossier de données MySQL est C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\Data\.

3. Mettez à jour les chemins d'accès au certificat CA, au certificat public du serveur, au certificat public du client, à la clé privée du serveur et à la clé privée du client dans le fichier de configuration du serveur MySQL (my.ini).

   Le chemin d'accès par défaut du fichier de configuration du serveur MySQL (my.ini) est C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\my.ini.

   > Vous devez spécifier les chemins d'accès au certificat CA, au certificat public du serveur et à la clé privée du serveur dans la section [mysqld] du fichier de configuration du serveur MySQL (my.ini).

   Vous devez spécifier les chemins d'accès au certificat CA, au certificat public client et à la clé privée client dans la section [client] du fichier de configuration du serveur MySQL (my.ini).

   L'exemple suivant montre les certificats et les fichiers de clés copiés dans la section [mysqld] du fichier my.ini dans le dossier par défaut C:/ProgramData/ NetApp/ SnapCenter/MySQL Data/Data.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

L'exemple suivant montre les chemins mis à jour dans la section [client] du fichier my.ini.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
```

4. Pour le deuxième nœud HA, copiez le certificat CA et générez le certificat public du serveur, les fichiers de clé privée du serveur, le certificat public du client et les fichiers de clé privée du client. Procédez comme suit :

   a. Copiez le certificat CA généré sur le premier nœud HA dans le dossier MySQL Data du deuxième nœud NLB.

      Le chemin d'accès par défaut au dossier de données MySQL est C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\Data\.

      > Vous ne devez pas créer à nouveau un certificat CA. Vous devez créer uniquement le certificat public du serveur, le certificat public du client, le fichier de clé privée du serveur et le fichier de clé privée du client.

   b. Pour le premier nœud HA, configurez les certificats SSL et les fichiers de clés pour les serveurs et clients MySQL sous Windows à l'aide de la commande openssl.

      "MySQL version 5.7 : Création de certificats et de clés SSL avec OpenSSL"

      > La valeur du nom commun utilisée pour le certificat du serveur, le certificat client et les fichiers de clés doit être différente de la valeur du nom commun utilisée pour le certificat de l'autorité de certification. Si les valeurs de nom commun sont les mêmes, les fichiers de certificat et de clé échouent pour les serveurs compilés à l'aide d'OpenSSL.

Il est recommandé d'utiliser le nom de domaine complet du serveur comme nom commun pour le certificat du serveur.

c. Copiez les certificats SSL et les fichiers clés dans le dossier MySQL Data.

d. Mettez à jour les chemins d'accès au certificat CA, au certificat public du serveur, au certificat public du client, à la clé privée du serveur et à la clé privée du client dans le fichier de configuration du serveur MySQL (my.ini).

> Vous devez spécifier les chemins d'accès au certificat CA, au certificat public du serveur et à la clé privée du serveur dans la section [mysqld] du fichier de configuration du serveur MySQL (my.ini).

Vous devez spécifier les chemins d'accès au certificat CA, au certificat public client et à la clé privée client dans la section [client] du fichier de configuration du serveur MySQL (my.ini).

L'exemple suivant montre les certificats et les fichiers de clés copiés dans la section [mysqld] du fichier my.ini dans le dossier par défaut C:/ProgramData/ NetApp/ SnapCenter/MySQL Data/Data.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

L'exemple suivant montre les chemins mis à jour dans la section [client] du fichier my.ini.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

+

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

+

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

5. Arrêtez l'application Web SnapCenter Server dans Internet Information Server (IIS) sur les deux nœuds HA.

6. Redémarrez le service MySQL sur les deux nœuds HA.
7. Mettez à jour la valeur de la clé MySQLProtocol dans le fichier SnapManager.Web.UI.dll.config pour les deux nœuds HA.

   L'exemple suivant montre la valeur de la clé MySQLProtocol mise à jour dans le fichier SnapManager.Web.UI.dll.config.

   ```
   <add key="MySQLProtocol" value="SSL" />
   ```

8. Mettez à jour le fichier SnapManager.Web.UI.dll.config avec les chemins que vous avez spécifiés dans la section [client] du fichier my.ini pour les deux nœuds HA.

   L'exemple suivant montre les chemins mis à jour dans la section [client] des fichiers my.ini.

   ```
   <add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
   Data/Data/client-cert.pem" />
   ```

   ```
   <add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
   Data/Data/client-key.pem" />
   ```

   ```
   <add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
   Data/Data/ca.pem" />
   ```

9. Démarrez l'application Web SnapCenter Server dans IIS sur les deux nœuds HA.
10. Utilisez l'applet de commande PowerShell Set-SmRepositoryConfig -RebuildSlave -Force avec l'option -Force sur l'un des nœuds HA pour établir une réplication MySQL sécurisée sur les deux nœuds HA.

    Même si l'état de réplication est sain, l'option -Force vous permet de reconstruire le référentiel esclave.