Configurer le serveur SnapCenter

SnapCenter software

NetApp
January 09, 2026

Sommaire

Configurer le serveur SnapCenter

Ajouter et provisionner le système de stockage

Ajout de systèmes de stockage

Vous devez configurer le système de stockage qui donne à SnapCenter un accès au stockage ONTAP, aux systèmes ASA r2 ou à Amazon FSX pour NetApp ONTAP afin d'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 pour NetApp ONTAP, vous pouvez soit ajouter une LIF d'administration FSX composée de plusieurs SVM à l'aide d'un compte fsxadmin, soit ajouter un SVM FSX dans SnapCenter.

Avant de commencer

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

  Les installations de plug-ins hôtes ne doivent pas être en cours d'ajout d'une connexion au système de stockage, car le cache hôte n'est pas nécessairement mis à jour et l'état des bases de données peut être affiché dans l'interface utilisateur graphique de SnapCenter sous la forme « non disponible pour la sauvegarde » ou « non 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 des clusters différents. Chaque système de stockage pris en charge par SnapCenter doit disposer d'un nom unique et d'une adresse IP de LIF de données unique.

À propos de cette tâche

- Lorsque vous configurez des systèmes de stockage, vous pouvez également activer les fonctionnalités EMS (Event Management System) et AutoSupport. L'outil AutoSupport collecte des données relatives à l'état de santé de votre système et les envoie automatiquement au support technique NetApp. Les données y sont ainsi envoyées pour résoudre le problème de votre système.

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

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

> Si vous modifiez le mot de passe du système de stockage, les tâches planifiées, les opérations de sauvegarde à la demande et 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.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Systems**.
2. Dans la page systèmes de stockage, cliquez sur **Nouveau**.
3. Dans la page Add Storage System, fournissez les informations suivantes :

Pour ce champ…	Procédez comme ça…
System de stockage	Entrez le nom ou l'adresse IP du système de stockage. Les noms de système de stockage, sans inclure le nom de domaine, doivent comporter 15 caractères ou moins et les noms doivent être résolus. Pour créer des connexions de système de stockage avec des noms comportant plus de 15 caractères, vous pouvez utiliser l'applet de commande Add-SmStorageConnectionPowerShell. Pour les systèmes de stockage avec configuration MetroCluster (MCC), il est recommandé d'enregistrer des clusters locaux et homologues pour garantir la continuité de l'activité. SnapCenter ne prend pas en charge plusieurs SVM de même nom sur différents clusters. Chaque SVM pris en charge par SnapCenter doit avoir un nom unique. Après avoir ajouté la connexion de stockage à SnapCenter, vous ne devez pas renommer le SVM ou le cluster en utilisant ONTAP. Si un SVM est ajouté avec un nom court ou un nom de domaine complet, il doit être résolu à la fois à partir du serveur SnapCenter et de l'hôte du plug-in.
Nom d'utilisateur/Mot de passe	Entrez les informations d'identification de l'utilisateur de stockage disposant des privilèges requis pour accéder au système de stockage.

Pour ce champ…	Procédez comme ça…
Système de gestion des événements (EMS) et paramètres AutoSupport	Pour envoyer des messages EMS au syslog du système de stockage ou pour que des messages AutoSupport soient envoyés au système de stockage à des fins de protection appliquée, de restauration terminée ou d'échec, cochez la case appropriée. Lorsque vous cochez la case **Envoyer la notification AutoSupport pour les opérations ayant échoué sur le système de stockage**, la case **Enregistrer les événements du serveur SnapCenter sur syslog** est également cochée 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 plate-forme, au protocole, au port et au délai d'attente.

   a. Dans plate-forme, sélectionnez l'une des options dans la liste déroulante.

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

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

   a. Dans Protocol, sélectionnez le protocole configuré lors de la configuration du SVM ou du Cluster, en général HTTPS.
   b. Saisissez 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 60 secondes.

   d. Si le SVM possède 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 Storage Systems (systèmes de stockage), dans la liste déroulante **Type**, effectuez l'une des opérations suivantes :

- Sélectionnez **ONTAP SVM** si vous souhaitez afficher tous les SVM ajoutés.

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

- Sélectionnez **clusters ONTAP** si vous souhaitez afficher tous les clusters 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, tous les SVM qui font partie du cluster sont affichés dans la section Storage Virtual machines.

  Si un nouveau SVM est ajouté au cluster ONTAP à l'aide de l'interface graphique de ONTAP, cliquez sur **redécouvrez** pour afficher le nouveau SVM ajouté.

Après la fin

Un administrateur de cluster doit activer AutoSupport sur chaque nœud du 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 depuis 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 SVM (Storage Virtual machine) n'a pas accès à AutoSupport.

Connexions de stockage et identifiants

Avant d'effectuer les opérations de protection des données, configurez les connexions de stockage et ajoutez les identifiants que le serveur SnapCenter et les plug-ins SnapCenter utiliseront.

Connexions de stockage

Les connexions de stockage permettent au serveur SnapCenter et aux plug-ins SnapCenter d'accéder au système de stockage ONTAP. La configuration de ces connexions implique également la configuration des fonctions AutoSupport et EMS.

Informations d'identification

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

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

  - *NetBIOS\username*
  - *Domain FQDN\username*
  - *Username@upn*
- Administrateur local (groupes de travail uniquement)

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

Le format valide du champ Nom d'utilisateur est : *username*

- Informations d'identification pour des 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 affecter au moins le groupe de ressources et les privilèges de sauvegarde au nom d'utilisateur.

Provisionnement du stockage sur les hôtes Windows

Création et gestion des igroups

Vous créez des groupes initiateurs pour spécifier les hôtes pouvant accéder à une LUN donnée sur le système de stockage. SnapCenter permet de créer, renommer, modifier ou supprimer un groupe initiateur sur un hôte Windows.

Créer un groupe initiateur

Vous pouvez utiliser SnapCenter pour créer un groupe initiateur sur un hôte Windows. Le groupe initiateur sera disponible dans l'assistant de création de disque ou de connexion de disque lorsque vous mappez le groupe initiateur sur une LUN.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
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 le groupe initiateur :

Dans ce champ…	Procédez comme ça…
System de stockage	Sélectionnez le SVM pour la LUN que vous allez mapper sur le groupe initiateur.
Hôte	Sélectionnez l'hôte sur lequel vous souhaitez créer le groupe initiateur.
Nom d'igroup	Indiquez le nom du groupe initiateur.
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 le groupe initiateur sur le système de stockage.

Renommer un groupe initiateur

Vous pouvez utiliser SnapCenter pour renommer un groupe initiateur existant.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **igroup**.
3. Sur la page groupes initiateurs, cliquez dans le champ **Storage Virtual machine** pour afficher la liste des SVM disponibles, puis sélectionnez la SVM du groupe initiateur que vous souhaitez renommer.
4. Dans la liste des igroups pour la SVM, sélectionnez le groupe initiateur que vous souhaitez renommer, puis cliquez sur **Renommer**.
5. Dans la boîte de dialogue Renommer le groupe initiateur, saisissez le nouveau nom du groupe initiateur, puis cliquez sur **Renommer**.

Modifier un groupe initiateur

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

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **igroup**.
3. Sur la page groupes initiateurs, cliquez dans le champ **Storage Virtual machine** pour afficher la liste déroulante des SVM disponibles, puis sélectionnez le SVM du groupe initiateur que vous souhaitez modifier.
4. Dans la liste des groupes initiateurs, sélectionnez un groupe initiateur, puis cliquez sur **Ajouter un initiateur au groupe initiateur**.
5. Sélectionnez un hôte.
6. Sélectionnez les initiateurs et cliquez sur **OK**.

Supprimez un groupe initiateur

Lorsque vous n'en avez plus besoin, vous pouvez utiliser SnapCenter pour supprimer un groupe initiateur.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **igroup**.
3. Sur la page groupes initiateurs, cliquez dans le champ **Storage Virtual machine** pour afficher la liste déroulante des SVM disponibles, puis sélectionnez le SVM du groupe initiateur que vous souhaitez supprimer.
4. Dans la liste des igroups pour la SVM, sélectionnez le groupe initiateur que vous souhaitez supprimer, puis cliquez sur **Delete**.
5. Dans la boîte de dialogue Supprimer un groupe initiateur, cliquez sur **OK**.

   SnapCenter supprime le groupe initiateur.

Création et gestion des disques

L'hôte Windows considère que des LUN de votre système de stockage sont des disques virtuels. Vous pouvez utiliser SnapCenter pour créer et configurer une LUN connectée via FC ou connectée via iSCSI.

- SnapCenter ne prend en charge que 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 primaire est autorisée, dont un volume est formaté avec NTFS ou CSVFS et possède 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

> La SnapCenter ne prend pas en charge la modification du nom d'un disque. Le changement de nom d'un disque géré par SnapCenter permet d'effectuer les opérations SnapCenter sans succès.

Afficher les disques d'un hôte

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

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **disques**.
3. Sélectionnez l'hôte dans la liste déroulante **Host**.

   Les disques sont répertoriés.

Afficher les disques en cluster

Vous pouvez afficher les disques en cluster sur le cluster que vous gérez à l'aide de SnapCenter. Les disques en cluster sont affichés uniquement lorsque vous sélectionnez le cluster dans la liste déroulante hôtes.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **disques**.
3. Sélectionnez le cluster dans la liste déroulante **Host**.

   Les disques sont répertoriés.

Établir une session iSCSI

Si vous utilisez iSCSI pour vous connecter à une LUN, vous devez établir une session iSCSI avant de créer la 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. "En savoir plus >>"

À propos de cette tâche

Vous pouvez établir une session iSCSI uniquement entre les mêmes versions IP, soit d'IPv6 vers IPv6, soit d'IPv4 vers IPv4.

Vous pouvez utiliser une adresse IPv6 lien-local 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 l'initiateur a accès afin qu'il puisse 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 vers 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 autre adresse IP.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **session iSCSI**.
3. Dans la liste déroulante **Storage Virtual machine**, sélectionnez la machine virtuelle de stockage (SVM) pour la cible iSCSI.
4. Dans la liste déroulante **Host**, sélectionnez l'hôte de la session.
5. Cliquez sur **établir session**.

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

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

Dans ce champ…	Entrer…
Nom du nœud cible	Nom du nœud de la cible iSCSI S'il existe un nom de nœud cible existant, le nom est affiché en lecture seule.
Adresse du portail cible	L'adresse IP du portail réseau cible
Port du portail cible	Port TCP du portail réseau cible
Adresse du portail de l'initiateur	L'adresse IP du portail réseau de l'initiateur

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

   SnapCenter établit la session iSCSI.

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

Créer des disques ou des LUN connectés via 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 une LUN connectée via FC ou connectée via 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 les LUN uniquement, et seules les LUN créées avec SnapCenter.

  > Vous ne pouvez pas créer de 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 module 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 une LUN à plusieurs hôtes, sauf si celle-ci est partagée par les hôtes d'un cluster de basculement Windows Server.
- Si un LUN est partagé par les hôtes d'un cluster de basculement Windows Server qui utilise CSV (Cluster Shared volumes), vous devez créer le disque sur l'hôte qui possède le groupe de clusters.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **disques**.
3. Sélectionnez l'hôte dans la liste déroulante **Host**.
4. Cliquez sur **Nouveau**.

   L'assistant de création de disque s'ouvre.

5. Dans la page Nom de la LUN, identifiez la LUN :

Dans ce champ…	Procédez comme ça…
System de stockage	Sélectionnez le SVM pour la LUN.
Chemin de LUN	Cliquez sur **Parcourir** pour sélectionner le chemin d'accès complet du dossier contenant la LUN.
Nom de la LUN	Indiquez le nom de la LUN.

Dans ce champ…	Procédez comme ça…
Taille du cluster	Sélectionnez la taille d'allocation des blocs de LUN pour le cluster. La taille du cluster dépend du système d'exploitation et des applications.
Étiquette de LUN	Si vous le souhaitez, entrez un texte descriptif pour la LUN.

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

Sélectionner…	Si…
Disque dédié	La LUN n'est accessible qu'à un seul hôte. Ignorez le champ **Groupe de ressources**.
Disque partagé	Le LUN est partagé par les hôtes d'un cluster de basculement Windows Server. Entrez le nom du groupe de ressources du cluster dans le champ **Groupe de ressources**. Vous devez créer le disque sur un seul hôte du cluster de basculement.
CSV (Cluster Shared Volume)	La LUN est partagée par les hôtes d'un cluster de basculement Windows Server qui utilise CSV. Entrez 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 clusters.

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

Propriété	Description
Attribuer automatiquement un point de montage	SnapCenter attribue automatiquement un point de montage de volume en fonction du lecteur du système. Par exemple, si votre lecteur système est C:, l'affectation automatique crée un point de montage de volume sous votre lecteur C: (C:\scmnpt\). L'affectation automatique n'est pas prise en charge pour les disques partagés.

Propriété	Description
Attribuer une lettre de lecteur	Montez le disque sur le lecteur sélectionné dans la liste déroulante adjacente.
Utiliser un point de montage de volume	Montez le disque sur le chemin d'accès que vous spécifiez dans le champ adjacent. 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 ou de point de montage de volume	Choisissez cette option si vous préférez monter le disque manuellement sous Windows.
Taille de la LUN	Spécifiez la taille de LUN ; 150 Mo minimum. Sélectionnez Mo, Go ou TB dans la liste déroulante adjacente.
Utilisez l'allocation dynamique pour le volume hébergeant cette LUN	Provisionnement fin de la LUN. Le provisionnement fin n'alloue qu'autant d'espace de stockage que nécessaire en même temps, ce qui permet à la LUN d'évoluer efficacement jusqu'à la capacité maximale disponible. Assurez-vous que l'espace disponible sur le volume est suffisant pour prendre en charge l'ensemble du stockage de LUN dont vous pensez avoir besoin.
Choisissez le type de partition	Sélectionnez partition GPT pour une table de partitions GUID ou partition MBR pour un enregistrement de démarrage maître. Les partitions MBR peuvent causer des problèmes d'alignement dans les clusters de basculement Windows Server. Les disques de partition UEFI ne sont pas pris en charge.

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

Dans ce champ…	Procédez comme ça…
Hôte	Double-cliquez sur le nom du groupe de clusters pour afficher la liste déroulante des hôtes appartenant au cluster, puis sélectionnez l'hôte de l'initiateur. Ce champ s'affiche uniquement si la LUN est partagée par les hôtes d'un cluster de basculement Windows Server.
Choisissez l'initiateur hôte	Sélectionnez **Fibre Channel** ou **iSCSI**, puis sélectionnez l'initiateur sur l'hôte. Vous pouvez sélectionner plusieurs initiateurs FC si vous utilisez FC avec des E/S multivoies (MPIO).

9. Sur la page Type de groupe, indiquez si vous souhaitez mapper un groupe initiateur existant sur la LUN ou en créer un nouveau :

Sélectionner…	Si…
Créez un nouveau groupe initiateur pour les initiateurs sélectionnés	Vous souhaitez créer un nouveau groupe initiateur pour les initiateurs sélectionnés.
Sélectionnez un groupe initiateur existant ou spécifiez un nouveau groupe initiateur pour les initiateurs sélectionnés	Vous souhaitez indiquer un groupe initiateur existant pour les initiateurs sélectionnés ou créer un nouveau groupe initiateur avec le nom que vous spécifiez. Saisissez le nom du groupe initiateur dans le champ **igroup name**. Saisissez les premières lettres du nom du groupe initiateur 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 disque ou au chemin de disque spécifié sur l'hôte.

Redimensionner un disque

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

À propos de cette tâche

- Pour la LUN à provisionnement fin, la taille de la géométrie de la lun ONTAP est indiquée comme taille maximale.
- Pour les LUN thick provisionnées, la taille extensible (taille disponible dans le volume) est indiquée comme taille maximale.
- Les LUN avec partitions de style MBR ont une taille limite de 2 To.

- Les LUN avec des partitions de type GPT ont une taille de système de stockage limite de 16 To.
- Avant de redimensionner une LUN, il est recommandé de créer une copie Snapshot.
- Si vous devez restaurer une LUN à partir d'une copie Snapshot effectuée avant le redimensionnement de la LUN, SnapCenter redimensionne automatiquement la LUN en fonction de sa taille.

  Après l'opération de restauration, les données ajoutées à la LUN après son redimensionnement doivent être restaurées à partir d'une copie Snapshot effectuée après son redimensionnement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
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 à redimensionner, puis cliquez sur **Redimensionner**.
5. Dans la boîte de dialogue Redimensionner le disque, utilisez le 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 pour que le bouton réduire ou développer soit activé de manière appropriée. Vous devez également cliquer sur MB, GB ou TB pour spécifier l'unité de mesure.

6. Lorsque vous êtes satisfait de vos entrées, cliquez sur **réduire** ou **développer**, selon les besoins.

   SnapCenter redimensionne le disque.

Connectez un disque

Vous pouvez utiliser l'assistant de connexion de disque pour connecter une LUN existante à un hôte ou pour reconnecter une LUN qui a été déconnectée.

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 une LUN à plusieurs hôtes, sauf si celle-ci est partagée par les hôtes d'un cluster de basculement Windows Server.
- Si la LUN est partagée par les hôtes d'un cluster de basculement Windows Server qui utilise CSV (Cluster Shared volumes), vous devez connecter le disque sur l'hôte qui possède le groupe de clusters.
- Le plug-in pour Windows doit être installé uniquement sur l'hôte sur lequel vous connectez le disque.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **disques**.
3. Sélectionnez l'hôte dans la liste déroulante **Host**.
4. Cliquez sur **connexion**.

L’assistant de connexion au disque s’ouvre.

5. Dans la page Nom de LUN, identifiez la LUN à connecter sur :

Dans ce champ…	Procédez comme ça…
System de stockage	Sélectionnez le SVM pour la LUN.
Chemin de LUN	Cliquez sur **Browse** pour sélectionner le chemin d’accès complet du volume contenant la LUN.
Nom de la LUN	Indiquez le nom de la LUN.
Taille du cluster	Sélectionnez la taille d’allocation des blocs de LUN pour le cluster. La taille du cluster dépend du système d’exploitation et des applications.
Étiquette de LUN	Si vous le souhaitez, entrez un texte descriptif pour la LUN.

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

Sélectionner…	Si…
Disque dédié	La LUN n’est accessible qu’à un seul hôte.
Disque partagé	Le LUN est partagé par les hôtes d’un cluster de basculement Windows Server. Vous n’avez besoin de connecter le disque qu’à un hôte du cluster de basculement.
CSV (Cluster Shared Volume)	La LUN est partagée par les hôtes d’un cluster de basculement Windows Server qui utilise CSV. Assurez-vous que l’hôte sur lequel vous vous connectez au disque est le propriétaire du groupe de clusters.

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 du système. Par exemple, si votre lecteur système est C:, la propriété affectation automatique crée un point de montage de volume sous votre lecteur C: (C:\scmnpt\). La propriété affectation automatique n'est pas prise en charge pour les disques partagés.
Attribuer une lettre de lecteur	Montez le disque sur le lecteur sélectionné dans la liste déroulante adjacente.
Utiliser un point de montage de volume	Montez le disque sur le chemin de lecteur que vous spécifiez dans le champ adjacent. 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 ou de point de montage de volume	Choisissez cette option si vous préférez monter le disque manuellement sous Windows.

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

Dans ce champ…	Procédez comme ça…
Hôte	Double-cliquez sur le nom du groupe de clusters pour afficher la liste déroulante des hôtes appartenant au cluster, puis sélectionnez l'hôte de l'initiateur. Ce champ s'affiche uniquement si la LUN est partagée par les hôtes d'un cluster de basculement Windows Server.
Choisissez l'initiateur hôte	Sélectionnez **Fibre Channel** ou **iSCSI**, puis sélectionnez l'initiateur sur l'hôte. Vous pouvez sélectionner plusieurs initiateurs FC si vous utilisez FC avec MPIO.

9. Sur la page Type de groupe, indiquez si vous souhaitez mapper un groupe initiateur existant sur la LUN ou en créer un nouveau :

Sélectionner…	Si…
Créez un nouveau groupe initiateur pour les initiateurs sélectionnés	Vous souhaitez créer un nouveau groupe initiateur pour les initiateurs sélectionnés.
Sélectionnez un groupe initiateur existant ou spécifiez un nouveau groupe initiateur pour les initiateurs sélectionnés	Vous souhaitez indiquer un groupe initiateur existant pour les initiateurs sélectionnés ou créer un nouveau groupe initiateur avec le nom que vous spécifiez. Saisissez le nom du groupe initiateur dans le champ **igroup name**. Saisissez les premières lettres du nom du groupe initiateur existant pour compléter automatiquement le champ.

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

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

Déconnectez un disque

Vous pouvez déconnecter une LUN d'un hôte sans affecter le contenu de la LUN, à une exception près : si vous déconnectez un clone avant sa mise hors service, vous perdez le contenu du clone.

Avant de commencer

- Assurez-vous que la LUN n'est utilisée par aucune application.
- Vérifiez que la LUN n'est pas surveillée avec le logiciel de surveillance.
- Si la LUN est partagée, assurez-vous de supprimer les dépendances liées aux ressources du cluster de la LUN et vérifiez que tous les nœuds du cluster sont sous tension, fonctionnent correctement et disponibles pour SnapCenter.

À propos de cette tâche

Si vous déconnectez une LUN d'un volume FlexClone que SnapCenter a créé et qu'aucune autre LUN du volume n'est connectée, SnapCenter supprime le volume. Avant de déconnecter la LUN, SnapCenter affiche un message vous informant que le volume FlexClone peut être supprimé.

Pour éviter la suppression automatique du volume FlexClone, vous devez renommer le volume avant de déconnecter la dernière LUN. Lorsque vous renommez le volume, assurez-vous de changer plusieurs caractères plutôt que le dernier caractère du nom.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **disques**.
3. Sélectionnez l'hôte dans la liste déroulante **Host**.

   Les disques sont répertoriés.

4. Sélectionnez le disque à déconnecter, puis cliquez sur **déconnecter**.
5. Dans la boîte de dialogue Disconnect Disk (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 plus le supprimer.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **disques**.
3. Sélectionnez l'hôte dans la liste déroulante **Host**.

   Les disques sont répertoriés.

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

   SnapCenter supprime le disque.

Création et gestion de partages SMB

Pour configurer un partage SMB3 sur un 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 encapsulent les meilleures pratiques pour la configuration des volumes et des partages. Vous trouverez les modèles dans le dossier modèles du dossier d'installation du module de plug-ins SnapCenter pour Windows.

Si vous vous sentez à l'aise de le faire, vous pouvez créer vos propres modèles en suivant les modèles fournis. Avant de créer un modèle personnalisé, vérifiez les paramètres dans la documentation de l'applet de commande.

Créez un partage SMB

La page partages SnapCenter permet de créer un partage SMB3 sur un 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.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **partages**.
3. Sélectionnez la SVM dans la liste déroulante **Storage Virtual machine**.
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 champ…	Procédez comme ça…
Description	Entrez un texte descriptif pour le partage.
Nom de partage	Entrez le nom du partage, par exemple test_Share. Le nom que vous saisissez pour le partage sera également utilisé comme nom de volume. Le nom du partage : • Doit être une chaîne UTF-8. • Ne doit pas inclure les caractères suivants : les caractères de contrôle de 0x00 à 0x1F (tous les deux compris), 0x22 (guillemets doubles) et les caractères spéciaux `\ / [ ] : (vertical bar) < > + = ; , ?`
Chemin du partage	• Cliquez dans le champ pour entrer un nouveau chemin d'accès au système de fichiers, par exemple, /. • Double-cliquez dans le champ pour sélectionner un chemin de système de fichiers existant.

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

   SnapCenter crée le partage SMB sur le SVM.

Supprime un partage SMB

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

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **partages**.
3. Sur la page partages, cliquez dans le champ **Storage Virtual machine** pour afficher une liste déroulante avec la liste des SVM disponibles, puis sélectionnez le SVM pour le partage que vous souhaitez supprimer.
4. Dans la liste des partages du SVM, sélectionnez le partage que vous souhaitez supprimer et cliquez sur **Delete**.
5. Dans la boîte de dialogue Supprimer le partage, cliquez sur **OK**.

   SnapCenter supprime le partage SMB du SVM.

Récupération de l’espace sur le système de stockage

Bien que NTFS surveille l’espace disponible sur une 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 du plug-in pour Windows afin de vous assurer que les blocs récemment 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 la LUN est partagée par les hôtes d’un cluster de basculement Windows Server, vous devez effectuer la récupération d’espace sur l’hôte qui possède le groupe de clusters.
- Pour un stockage optimal en termes de performances, nous vous conseillons d’assurer la récupération d’espace aussi souvent que possible.

  Assurez-vous que l’intégralité du système de fichiers NTFS a été numérisée.

À propos de cette tâche

- La récupération de l’espace étant chronophage et consommatrice en ressources système, il est généralement préférable d’exécuter les opérations lorsque le système de stockage et l’utilisation des hôtes Windows sont faibles.
- La récupération d’espace désaline l’espace disponible, mais pas 100 %.
- Vous ne devez pas exécuter la défragmentation du disque en même temps que vous effectuez la récupération d’espace.

  Cela peut ralentir le processus de récupération.

Étape

Dans l’invite de commandes PowerShell du serveur d’applications, saisissez la commande suivante :

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

Chemin_lecteur correspond au chemin d’accès du disque mappé sur la LUN.

Provisionnement du stockage avec les applets de commande PowerShell

Si vous ne souhaitez pas utiliser l’interface graphique 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 relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter à la "Guide de référence de l'applet de commande du logiciel SnapCenter".

Si les applets de commande SnapCenter PowerShell sont cassés afin de supprimer SnapDrive pour Windows du serveur, reportez-vous à "Les applets de commande SnapCenter sont cassés lors de la désinstallation de SnapDrive pour Windows".

Provisionnement du 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 de Windows Server prises en charge
- Configurations en cluster Microsoft

  Prise en charge jusqu'à 16 nœuds pris en charge sur VMware lors de l'utilisation de l'initiateur logiciel Microsoft iSCSI, 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 un plug-in VMware VM MSCS Box-to-box pour configuration Windows

  Prend en charge le contrôleur SCSI paravirtuel VMware. 256 disques peuvent être pris en charge sur des disques RDM.

Limitations liées au serveur VMware ESXi

- L'installation du plug-in pour Windows sur un cluster Microsoft sur des machines virtuelles utilisant 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 une LUN RDM en dehors du plug-in pour Windows, vous devez redémarrer le service du plug-in pour lui permettre de reconnaître le nouveau disque créé.
- Vous ne pouvez pas utiliser simultanément des initiateurs iSCSI et FC sur un système d'exploitation invité VMware.

Privilèges vCenter minimum 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 :

- Datastore : supprimer le fichier
- Hôte : configuration > Configuration de la partition de stockage

- Ordinateur virtuel : configuration

Vous devez attribuer ces privilèges à un rôle au niveau du serveur Virtual Center. Le rôle auquel vous attribuez ces privilèges ne peut être attribué à aucun 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 RDM FC, 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.

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

De formation

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

- Les machines virtuelles doivent exécuter la même version de Windows Server.
- Les versions des serveurs ESX ou ESXi doivent être identiques pour chaque hôte parent VMware.
- Chaque hôte parent doit disposer d'au moins deux cartes réseau.
- Au moins un datastore VMware Virtual machine File System (VMFS) doit être partagé entre les deux serveurs ESX ou ESXi.
- VMware recommande de créer le datastore partagé sur un SAN FC.

  Si nécessaire, le datastore partagé peut également être créé via iSCSI.

- La LUN RDM partagée 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 requiert la configuration du contrôleur SCSI SAS LSI Logic sur chaque machine virtuelle. Les LUN partagées ne peuvent pas utiliser le contrôleur SAS LSI Logic existant si seul un de son type existe et 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 une LUN partagée 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 VMware Infrastructure client.

- 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 groupe initiateur unique avec des initiateurs à partir de plusieurs hôtes.

  Le groupe initiateur 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.

- Veillez à créer une LUN RDM sur ESXi 5.0 à l'aide d'un initiateur FC.

  Lorsque vous créez une LUN RDM, un groupe initiateur est créé avec ALUA.

Limites

Le plug-in pour Windows prend en charge les clusters Microsoft à l'aide de LUN RDM FC/iSCSI 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 datastores iSCSI et NFS ESX.
- 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 iSCSI ESX et les HBA ne sont pas pris en charge sur les disques partagés d'un cluster Microsoft.
- Le plug-in pour Windows ne prend pas en charge la migration des machines virtuelles avec vMotion si l'ordinateur virtuel fait partie d'un cluster Microsoft.
- Le plug-in pour Windows ne prend pas en charge MPIO sur des machines virtuelles d'un cluster Microsoft.

Créer une LUN FC RDM partagée

Avant de pouvoir utiliser des LUN RDM FC 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 "Machines virtuelles de clusters sur des hôtes physiques".

Ajout de licences SnapCenter standard basées sur le contrôleur

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

La licence basée sur le contrôleur présente les caractéristiques suivantes :

- Droits SnapCenter Standard inclus dans l'achat des bundles Premium ou Flash (non inclus dans le pack de base)

- Utilisation illimitée du stockage
- 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 pour le numéro de série du contrôleur

Pour plus d'informations sur les licences requises, reportez-vous à la section "Licences SnapCenter".

Étape 1 : vérifiez si la licence de la suite SnapManager 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 Storage Systems (systèmes de stockage), dans le menu déroulant **Type**, indiquez si vous souhaitez afficher tous les SVM ou clusters ajoutés :
   - Pour afficher tous les SVM ajoutés, sélectionnez **ONTAP SVM**.
   - Pour afficher tous les clusters ajoutés, sélectionnez **ONTAP clusters**.

     Lorsque vous sélectionnez le nom du cluster, tous les SVM faisant partie du cluster s'affichent dans la section Storage Virtual machines.
3. Dans la liste connexions de stockage, recherchez la colonne Licence de contrôleur.

   La colonne Controller License affiche l'état 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 de la suite SnapManager n'est pas applicable, car le contrôleur de stockage se trouve sur Amazon FSX pour les plateformes de stockage NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select ou secondaires.

Étape 2 : identifier les licences installées sur le contrôleur

Vous pouvez utiliser la ligne de commandes de ONTAP pour afficher toutes les licences installées sur votre contrôleur. Vous devez être administrateur du 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 SnapManager Suite est installée. Par conséquent, aucune opération 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 vérifiez les valeurs de 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. Notez les numéros de série.

Étape 4 : récupérez 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

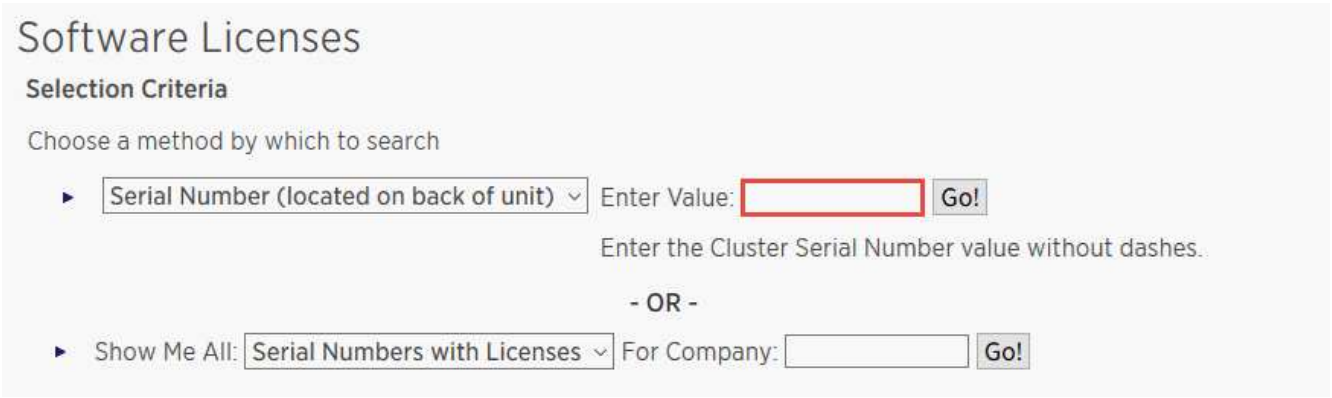
- Vous devez disposer d'identifiants de connexion valides au site du support NetApp.

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

- Vous devez disposer du numéro de série du contrôleur.

Étapes

1. Connectez-vous au "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, saisissez le numéro de série du contrôleur, puis sélectionnez **Go!**.



   La liste des licences du contrôleur spécifié s'affiche.

4. Recherchez et enregistrez la licence SnapCenter Standard ou SnapManager Suite.

Étape 5 : ajoutez 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 du cluster sur le système FAS, AFF ou ASA.
- Vous devez disposer de la licence SnapCenter Standard ou SnapManager Suite.

Description de la tâche

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

Si vous souhaitez installer SnapCenter sous forme d'essai, contactez votre ingénieur commercial pour obtenir une licence d'évaluation du pack Premium pour l'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 de SnapManager Suite :

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

   Cette commande est disponible au niveau de privilège admin.

3. Vérifiez que la licence SnapManager Suite est installée :

   ```
   license show
   ```

Étape 6 : supprimez 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 nécessaire que si vous utilisez une licence basée sur le 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 le mot de passe 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 invite à saisir le mot de passe. Saisissez les informations d'identification fournies lors de la réinitialisation du mot de passe.

3. Supprimez la licence d'évaluation de la base de données :

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

Configuration de la haute disponibilité

Configurez les serveurs SnapCenter pour la haute disponibilité

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

Vous pouvez également configurer l'équilibrage de la charge réseau (NLB) pour configurer la haute disponibilité SnapCenter. Vous devez configurer manuellement NLB hors de l'installation SnapCenter pour la haute disponibilité.

Pour les environnements cloud, vous pouvez configurer la haute disponibilité à l'aide d'Amazon Web Services (AWS) Elastic Load Balancing (ELB) et d'Azure load balancer.

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 la 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 :

- Add-SmServerCluster
- Add-SmServer
- Remove-SmServerCluster

  Pour plus d'informations, reportez-vous "Guide de référence de l'applet de commande du logiciel SnapCenter"à .

Informations supplémentaires

- Après avoir installé et configuré SnapCenter pour la haute disponibilité, modifiez le raccourci du bureau SnapCenter pour pointer 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 hôte SnapCenter bascule fréquemment entre les hôtes en panne et en cours d'exécution. Pour résoudre ce problème, vous devez vous assurer que les deux hôtes SnapCenter sont en mesure de résoudre l'hôte dans NLB ou F5.
- Les commandes SnapCenter pour les paramètres MFA doivent être exécutées sur tous les hôtes. La configuration des parties utilisatrices doit être effectuée dans 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 après l'activation de l'authentification multifacteur.
- Pendant le basculement, les paramètres du journal d'audit ne s'y reflètent pas sur le second hôte. Par conséquent, vous devez répéter manuellement les paramètres du journal d'audit sur l'hôte passif F5 lorsqu'il devient actif.

Configuration de 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 la haute disponibilité SnapCenter. Vous devez configurer manuellement NLB hors de l'installation SnapCenter pour la haute disponibilité.

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

Configuration de 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 distinctes (AZ) et en les configurant pour un 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. Configurez l'IP de superposition privée virtuelle dans AWS. Pour plus d'informations, reportez-vous à "Configurer l'IP de superposition privée virtuelle"la .
2. Préparez votre hôte Windows
   a. Forcer la priorité IPv4 au-dessus d'IPv6 :
      - Emplacement : HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
      - Clé : DisabledComponents
      - Tapez : REG_DWORD
      - Valeur : 0x20
   b. Assurez-vous que les noms de domaine complets peuvent être résolus via DNS ou via la configuration de l'hôte local vers les adresses IPv4.
   c. Assurez-vous qu'aucun proxy système n'est configuré.
   d. Assurez-vous que le mot de passe administrateur est le même sur le serveur Windows lorsque vous utilisez une configuration sans Active Directory et que les serveurs ne se trouvent pas dans un domaine.
   e. Ajoutez une adresse IP virtuelle sur les deux serveurs Windows.
3. Créez le cluster SnapCenter.
   a. Démarrez PowerShell et connectez-vous à SnapCenter. `Open-SmConnection`
   b. Création du 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. Découvrez tous les détails sur la haute disponibilité. `Get-SmServerConfig`
4. Créez la fonction Lamda pour ajuster la table de routage en cas d'indisponibilité du point de terminaison IP privé virtuel, contrôlé par AWS CloudWatch. Pour plus d'informations, reportez-vous à "Créer une fonction Lambda"la .
5. Créez un moniteur dans CloudWatch pour contrôler la disponibilité du terminal SnapCenter. Une alarme est configurée pour déclencher une fonction Lambda si le point final 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 Canaries synthétiques"la .
6. Implémenter un flux de travail en utilisant une fonction STEP comme alternative à la surveillance CloudWatch, ce qui réduit les temps de basculement. Le flux de travail comprend une fonction de sonde Lambda pour tester l'URL SnapCenter, une table DynamoDB pour le stockage des nombres de défaillances et la fonction pas à pas elle-même.
   a. Utilisez une fonction lambda pour sonder l'URL SnapCenter. Pour plus d'informations, reportez-vous à "Création de la fonction Lambda"la .
   b. Créez une table DynamoDB pour stocker le nombre de pannes entre deux itérations de fonction Step. Pour plus d'informations, reportez-vous à "Commencez avec la table DynamoDB"la .
   c. Créer la fonction pas à pas. Pour plus d'informations, reportez-vous à "Documentation des fonctions STEP"la .
   d. Testez une seule étape.
   e. Tester le fonctionnement complet.

f. Créer un rôle IAM et ajuster les autorisations à autoriser à exécuter la fonction Lambda.

g. Créer un programme pour déclencher la fonction pas à pas. Pour plus d'informations, reportez-vous à "Utilisation d'Amazon EventBridge Scheduler pour démarrer des fonctions Step"la .

Configurez 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. Création de machines virtuelles dans un ensemble d'échelles à l'aide du portail Azure L'ensemble d'échelle des machines virtuelles Azure vous permet de créer et de gérer un groupe de machines virtuelles à charge équilibrée. Le nombre d'instances de machines virtuelles peut augmenter ou diminuer automatiquement en réponse à la demande ou à un planning défini. Pour plus d'informations, reportez-vous à "Création de machines virtuelles dans un ensemble d'échelles à l'aide du portail Azure"la .
2. Après avoir configuré les machines virtuelles, connectez-vous à chaque machine virtuelle dans le jeu de machines virtuelles et installez le serveur SnapCenter sur les deux nœuds.
3. Créer 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. Consultez les détails sur la haute disponibilité. `Get-SmServerConfig`
6. Si nécessaire, reconstruisez l'hôte secondaire. `Set-SmRepositoryConfig -RebuildSlave -Verbose`
7. Basculement vers le second hôte. `Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose`

== passer de NLB à F5 pour la haute disponibilité

Vous pouvez modifier votre configuration SnapCenter HA à partir de l'équilibrage de la charge du réseau (NLB) pour utiliser F5 Load Balancer.

Étapes

1. Configurez les serveurs SnapCenter pour une haute disponibilité à l'aide de F5. "En savoir plus >>".
2. Sur l'hôte SnapCenter Server, lancez PowerShell.
3. Démarrez une session à l'aide de la cmdlet Open-SmConnection, puis saisissez 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 relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter à la "Guide de référence de l'applet de commande du logiciel SnapCenter".

Haute disponibilité pour le référentiel SnapCenter MySQL

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 la haute disponibilité uniquement sur deux nœuds NLB (Network Load Balancing-Enabled).

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

Si vous souhaitez utiliser la fonction haute disponibilité MySQL (HA), 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 second nœud, vous devez rejoindre la F5 du premier nœud et créer une copie du référentiel MySQL sur le second nœud.

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

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter à la "Guide de référence de l'applet de commande du logiciel SnapCenter".

Vous devez connaître les 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 SnapCenter à une installation NLB ou vice versa et le passage d'une configuration autonome MySQL à 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 le serveur MySQL ou SnapCenter est en panne, alors les travaux en cours d'exécution risquent d'échouer. Après le basculement vers le second nœud, toutes les tâches suivantes s'exécutent correctement.

Pour plus d'informations sur la configuration de la haute disponibilité, reportez-vous à la section "Comment configurer NLB et ARR avec SnapCenter".

Configuration du contrôle d'accès basé sur des 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 sur .
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. Select **tous les membres de ce rôle peuvent voir les objets d'autres membres** pour permettre aux autres membres du rôle d'afficher 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 les autres membres sont affectés.

   Lorsque cette option est activée, il n'est pas nécessaire d'attribuer aux utilisateurs un accès aux objets ou aux ressources 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**.

Ajoutez un rôle NetApp ONTAP RBAC à l'aide de commandes de connexion de sécurité

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

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 répertoires de commandes et/ou de commandes.

  Il existe deux niveaux d'accès pour chaque répertoire de commande/commande : All-Access et read-only.

  Vous devez toujours attribuer les privilèges All-Access en premier.

- Attribuez 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.

Description de la 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 for NetApp ONTAP ajoute automatiquement le Privileges dans le bon ordre afin que le Privileges tout accès apparaisse en premier. Si vous ajoutez d'abord les privilèges en lecture seule, puis ajoutez les privilèges All-Access, ONTAP marque les privilèges All-Access en tant que doublons et les ignore.

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

Plus d'informations sur la configuration des rôles RBAC ONTAP, consultez le "Guide de l'authentification de l'administrateur ONTAP 9 et de l'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 ne renseignez pas ce champ, l'administrateur de cluster est défini par défaut.
   - nom_rôle est le nom que vous spécifiez pour le rôle.
   - La commande correspond à la fonctionnalité ONTAP.

     > Vous devez répéter cette commande pour chaque autorisation. N'oubliez pas que les commandes All-Access doivent être répertoriées avant les commandes read-only.

   Pour plus d'informations sur la liste des autorisations, reportez-vous à la section "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"
   ```

   - nom_utilisateur 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 ce 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\>
   ```

   - <nom_utilisateur> 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.
   - <nom_rôle> 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\>
```

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

Créez des rôles de SVM avec des privilèges minimaux

Il existe plusieurs commandes CLI ONTAP 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 qu'ils soient utilisés avec SnapCenter et que vous ne souhaitez pas utiliser le rôle vsadmin.

Étapes

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-lui le rôle.

```
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 créer des rôles SVM et attribuer des autorisations

Vous devez exécuter plusieurs commandes ONTAP CLI 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`

Création de 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.

Étapes

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-lui le rôle.

   ```
   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 créer des rôles SVM et attribuer des autorisations

Vous devez exécuter plusieurs commandes ONTAP CLI 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`

Créez 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 de l'interface de ligne de commandes ONTAP pour créer le rôle de cluster ONTAP et attribuer des privilèges minimaux.

Étapes

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-lui le rôle.

   ```
   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 permettant de créer des rôles de cluster et d'attribuer des autorisations

Vous devez exécuter plusieurs commandes CLI ONTAP 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

Créez 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 de l'interface de ligne de commandes ONTAP pour créer le rôle de cluster ONTAP et attribuer des privilèges minimaux.

Étapes

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-lui le rôle.

   ```
   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 permettant de créer des rôles de cluster et d'attribuer des autorisations

Vous devez exécuter plusieurs commandes CLI ONTAP 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 des rôles pour les utilisateurs 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 avoir ouvert une session en tant que rôle « SnapCenterAdmin ».
- Vous devez avoir créé les comptes utilisateur ou 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 de groupe : espace ( ), tiret (-), trait de soulignement (_) et deux-points (:).

- SnapCenter inclut plusieurs rôles prédéfinis.

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

- Les utilisateurs AD et les groupes AD qui sont ajoutés au RBAC SnapCenter doivent disposer de l'autorisation DE LECTURE sur le conteneur d'utilisateurs et le conteneur d'ordinateurs dans Active Directory.
- Après avoir affecté un rôle à un utilisateur ou à un groupe qui contient les autorisations appropriées, vous devez attribuer l'accès de l'utilisateur aux ressources SnapCenter, telles que les hôtes et les connexions de stockage.

Cela permet aux utilisateurs d'effectuer les actions pour lesquelles ils ont des autorisations sur les ressources qui leur sont assignées.

- Vous devez à un moment ou à un autre attribuer un rôle à l'utilisateur ou au groupe afin de tirer profit des autorisations et des fonctionnalités d'efficacité RBAC.
- Vous pouvez affecter des ressources comme hôte, groupes de ressources, stratégie, connexion au stockage, 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 affecter à un utilisateur pour effectuer certaines opérations sont les suivantes :

Fonctionnement	Affectation des ressources
Protéger les ressources	hôte, règle
Sauvegarde	hôte, groupe de ressources, stratégie
Restaurer	hôte, groupe de ressources
Clonage	hôte, groupe de ressources, stratégie
Cycle de vie des clones	hôte
Créer un groupe de ressources	hôte

- Lorsqu'un nouveau nœud est ajouté à un cluster Windows ou à un actif DAG (Groupe de disponibilité de la base de données Exchange Server) et si ce nouveau nœud est affecté à un utilisateur, vous devez réassigner le bien à l'utilisateur ou au groupe pour inclure le nouveau nœud à l'utilisateur ou au groupe.

  Vous devez réassigner 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 avez un cluster à deux nœuds et avez affecté un utilisateur ou un groupe RBAC au cluster. Lorsque vous ajoutez un autre nœud au cluster, vous devez réattribuer l'utilisateur ou le groupe RBAC au cluster afin d'inclure le nouveau nœud pour l'utilisateur ou le groupe RBAC.

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

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

Si vous utilisez le plug-in SnapCenter pour les fonctions VMware vSphere pour protéger les machines virtuelles, les VMDK ou les datastores, vous devez utiliser l'interface graphique de VMware vSphere pour ajouter un utilisateur vCenter à un rôle de plug-in SnapCenter pour VMware vSphere. Pour plus d'informations sur les rôles VMware vSphere, reportez-vous à la section "Rôles prédéfinis avec le plug-in SnapCenter pour VMware vSphere".

Étapes

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 Workgroup :

Pour ce champ…	Procédez comme ça…
Type d'accès	Sélectionnez domaine ou groupe de travail 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. Par défaut, il est pré-rempli avec le nom de domaine connecté. Vous devez enregistrer le domaine non approuvé dans la page **Paramètres** > **Paramètres globaux** > **Paramètres de domaine**.
Type	Sélectionnez utilisateur ou Groupe SnapCenter prend uniquement en charge le groupe de sécurité, et non le groupe de distribution.
Nom d'utilisateur	a. Saisissez le nom d'utilisateur partiel, puis cliquez sur **Ajouter**. Le nom d'utilisateur est sensible à la casse. b. Sélectionnez le nom d'utilisateur dans la liste de recherche. Lorsque vous ajoutez des utilisateurs d'un domaine différent ou d'un domaine non fiable, vous devez saisir le nom d'utilisateur entièrement car il n'existe aucune liste de recherche pour les utilisateurs d'un domaine à l'autre. Répétez cette étape pour ajouter d'autres utilisateurs ou groupes au rôle sélectionné.
Rôles	Sélectionnez le rôle auquel vous souhaitez ajouter l'utilisateur.

4. Cliquez sur **attribuer**, puis sur la page affecter des ressources :

a. Sélectionnez le type de ressource dans la liste déroulante **Asset**.
b. Dans le tableau actif, sélectionnez l'actif.

   Les ressources sont répertoriées uniquement si l'utilisateur a ajouté les ressources 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 affecté 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 à l'emplacement d'installation par défaut *C:\Program Files\NetApp\SnapCenter WebApp\audit*\.

Les journaux d'audit sont sécurisés par la génération d'un résumé signé numériquement pour chaque événement d'audit afin de les protéger contre les modifications non autorisées. Les données de résumé générées sont conservées dans le fichier de somme de contrôle d'audit distinct et l'intégrité est soumise à des contrôles périodiques pour assurer l'intégrité du contenu.

Vous devriez avoir ouvert une session en tant que rôle « SnapCenterAdmin ».

Description de la tâche

- Les alertes sont envoyées dans les scénarios suivants :
  - Le programme de vérification de l'intégrité du journal d'audit ou le serveur Syslog est activé ou désactivé
  - Vérification de l'intégrité du journal d'audit, journal d'audit ou échec du journal du serveur Syslog
  - Espace disque faible
- L'e-mail est envoyé uniquement en cas d'échec du contrôle d'intégrité.
- Vous devez modifier les chemins d'accès du répertoire du journal d'audit et du répertoire du journal de la somme de contrôle d'audit ensemble. Vous ne pouvez modifier qu'une seule d'entre elles.
- Lorsque les chemins du répertoire du journal d'audit et du répertoire du journal de la 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 du répertoire du journal d'audit et du répertoire du journal de la somme de contrôle d'audit doivent se trouver sur le disque local du serveur SnapCenter.

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

- Si le protocole UDP est utilisé dans les paramètres du serveur Syslog, les erreurs dues au port sont en panne ou 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 la cmdlet et leurs descriptions peuvent être obtenues en exécutant Get-Help nom_commande. 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, entrez les détails.
3. Entrez le répertoire **Audit log** et le répertoire **Audit checksum log**
   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) Activer **Log UTC Time**.
5. (Facultatif) activez **Audit Log Integrity Check Schedule** et cliquez sur **Start Integrity Check** pour vérifier l'intégrité à la demande.

   Vous pouvez également exécuter la commande **Start-SmAuditIntegrityCheck** pour lancer le contrôle d'intégrité à la demande.
6. (Facultatif) activez les journaux d'audit transmis au serveur syslog distant et entrez les détails du serveur Syslog.

   Vous devez importer le certificat depuis le serveur Syslog vers 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 des audits et les vérifications de l'espace disque en cliquant sur **Monitor** > **Jobs**.

Configurez les connexions MySQL sécurisées avec le serveur SnapCenter

Vous pouvez générer des certificats SSL (Secure Sockets Layer) et des fichiers clés si vous souhaitez sécuriser la communication entre le serveur SnapCenter et le serveur MySQL dans des configurations autonomes ou dans des configurations NLB (Network Load Balancing).

Configurez des connexions MySQL sécurisées pour des configurations serveur SnapCenter autonomes

Vous pouvez générer des certificats SSL (Secure Sockets Layer) et des fichiers de clés, si vous souhaitez sécuriser la communication entre le serveur SnapCenter et le serveur MySQL. Vous devez configurer les certificats et les fichiers de clé 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 et fichier de clé privée du client

Étapes

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

   Pour plus d'informations, reportez-vous à la section "MySQL version 5.7 : création de certificats et de clés SSL à l'aide d'openssl"

   > La valeur de nom commune utilisée pour le certificat de serveur, le certificat client et les fichiers de clé doit être différente de la valeur de nom commune utilisée pour le certificat de l'autorité de certification. Si les valeurs de nom communes 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 de serveur.

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

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

3. Mettez à jour le certificat CA, le certificat public du serveur, le certificat public du client, la clé privée du serveur et les chemins de 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 le certificat CA, le certificat public du serveur et les chemins de clé privée du serveur dans la section [mysqld] du fichier de configuration du serveur MySQL (my.ini).

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

   L'exemple suivant montre les certificats et les fichiers de clé 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 du serveur SnapCenter 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 du serveur SnapCenter dans IIS.

Configurez les connexions MySQL sécurisées pour les configurations haute disponibilité

Si vous souhaitez sécuriser la communication entre le serveur SnapCenter et les serveurs MySQL, vous pouvez générer des certificats SSL (Secure Sockets Layer) et des fichiers clés pour les nœuds HA (High Availability). Vous devez configurer les certificats et les fichiers de clé dans les serveurs MySQL et sur les nœuds HA.

Les certificats suivants sont générés :

- Certificat CA

  Un certificat d'autorité de certification est généré sur l'un des nœuds HA, et ce certificat est copié sur l'autre nœud HA.

- Les fichiers de clés privées de serveur et de certificat public pour les deux nœuds HA
- Certificat public du client et fichiers de clé privée du client pour les deux nœuds HA

Étapes

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

   Pour plus d'informations, reportez-vous à la section "MySQL version 5.7 : création de certificats et de clés SSL à l'aide d'openssl"

   La valeur de nom commune utilisée pour le certificat de serveur, le certificat client et les fichiers de clé doit être différente de la valeur de nom commune utilisée pour le certificat de l'autorité de certification. Si les valeurs de nom communes 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 de serveur.

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

   Le chemin par défaut du dossier MySQL Data est C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\.

3. Mettez à jour le certificat CA, le certificat public du serveur, le certificat public du client, la clé privée du serveur et les chemins de 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 le certificat CA, le certificat public du serveur et les chemins de clé privée du serveur dans la section [mysqld] du fichier de configuration du serveur MySQL (my.ini).

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

   L'exemple suivant montre les certificats et les fichiers de clé 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 second nœud HA, copiez le certificat de l'autorité de certification et générez le certificat public du serveur, les fichiers de clé privée du serveur, le certificat public client et les fichiers de clé privée du client. effectuez les opérations suivantes :

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

      Le chemin par défaut du dossier MySQL Data est C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\.

      > Vous ne devez pas créer de nouveau un certificat CA. Vous ne devez créer que 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 clés pour les serveurs et les clients MySQL sur Windows à l'aide de la commande openssl.

      "MySQL version 5.7 : création de certificats et de clés SSL à l'aide d'openssl"

La valeur de nom commune utilisée pour le certificat de serveur, le certificat client et les fichiers de clé doit être différente de la valeur de nom commune utilisée pour le certificat de l'autorité de certification. Si les valeurs de nom communes 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 FQDN du serveur comme nom commun pour le certificat du serveur.

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

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

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

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

L'exemple suivant montre les certificats et les fichiers de clé 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 du serveur SnapCenter 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 du serveur SnapCenter dans IIS sur les deux nœuds HA.
10. Utilisez l'applet de commande Set-SmRepositoryConfig -Rebuildesclave -Force PowerShell 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.