Configurer l'authentification basée sur certificat

SnapCenter Software 5.0

NetApp
July 18, 2024

Sommaire

Configurer l'authentification basée sur certificat

Exporter des certificats d'autorité de certification (CA) depuis le serveur SnapCenter

Vous devez exporter les certificats d'autorité de certification du serveur SnapCenter vers les hôtes de plug-in à l'aide de la console MMC (Microsoft Management Console).

Avant de commencer

Vous devez avoir configuré le protocole SSL bidirectionnel.

Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier** > **Ajouter/Supprimer Snapin**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root** > **certificats - ordinateur local** > **personnel** > **certificats**.
5. Cliquez avec le bouton droit de la souris sur le certificat CA fourni, qui est utilisé pour le serveur SnapCenter, puis sélectionnez **toutes les tâches** > **Exporter** pour lancer l'assistant d'exportation.
6. Effectuez les actions suivantes dans l'assistant.

Pour cette option…	Procédez comme suit…
Exporter la clé privée	Sélectionnez **non, ne pas exporter la clé privée**, puis cliquez sur **Suivant**.
Exporter le format de fichier	Cliquez sur **Suivant**.
Nom du fichier	Cliquez sur **Parcourir** et spécifiez le chemin d'accès au fichier pour enregistrer le certificat, puis cliquez sur **Suivant**.
Exécution de l'assistant d'exportation de certificat	Vérifiez le résumé, puis cliquez sur **Terminer** pour lancer l'exportation.

L'authentification basée sur certificat n'est pas prise en charge pour les configurations SnapCenter HA et le plug-in SnapCenter pour VMware vSphere.

Importer le certificat de l'autorité de certification (CA) vers les hôtes du plug-in Windows

Pour utiliser le certificat de l'autorité de certification du serveur SnapCenter exporté, vous devez importer le certificat associé sur les hôtes du plug-in Windows SnapCenter à l'aide de la console MMC (Microsoft Management Console).

Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier** > **Ajouter/Supprimer Snapin**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root** > **certificats - ordinateur local** > **personnel** > **certificats**.
5. Cliquez avec le bouton droit de la souris sur le dossier "personnel", puis sélectionnez **toutes les tâches** > **Importer** pour lancer l'assistant d'importation.
6. Effectuez les actions suivantes dans l'assistant.

Pour cette option…	Procédez comme suit…
Emplacement du magasin	Cliquez sur **Suivant**.
Fichier à importer	Sélectionnez le certificat du serveur SnapCenter qui se termine par l'extension .cer.
Magasin de certificats	Cliquez sur **Suivant**.
Exécution de l'assistant d'exportation de certificat	Vérifiez le résumé, puis cliquez sur **Terminer** pour lancer l'importation.

Importez le certificat CA dans les plug-ins hôtes UNIX et configurez les certificats racine ou intermédiaire dans le magasin de confiance SPL

Importez le certificat CA sur les hôtes du plug-in UNIX

Vous devez importer le certificat de l'autorité de certification sur les hôtes du plug-in UNIX.

À propos de cette tâche

- Vous pouvez gérer le mot de passe de la base de stockage de clés SPL et l'alias de la paire de clés signées CA utilisée.
- Le mot de passe de la base de stockage de clés SPL et de tous les mots de passe alias associés à la clé privée doit être le même.

Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés SPL dans le fichier de propriétés SPL. C'est la valeur correspondant à la clé `SPL_KEYSTORE_PASS`.
2. Modifiez le mot de passe de la base de stockage de clés : `$ keytool -storepasswd -keystore keystore.jks`
3. Remplacez le mot de passe de tous les alias des entrées de clé privée dans la base de stockage de clés

par le même mot de passe que celui utilisé pour la base de stockage de clés : `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`

4. Mettez à jour la même valeur pour la clé SPL_KEYSTORE_PASS dans `spl.properties` le fichier.
5. Redémarrez le service après avoir modifié le mot de passe.

Configurez les certificats racine ou intermédiaire sur le magasin de confiance SPL

Vous devez configurer les certificats racine ou intermédiaire dans le magasin de confiance SPL. Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

Étapes

1. Naviguez jusqu'au dossier contenant le magasin de clés SPL : `/var/opt/snapcenter/spl/etc`.
2. Localisez le fichier `keystore.jks`.
3. Répertoriez les certificats ajoutés dans la base de stockage de clés : `$ keytool -list -v -keystore keystore.jks`
4. Ajouter un certificat racine ou intermédiaire : `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. Redémarrez le service après avoir configuré les certificats racine ou intermédiaire sur le stockage de confiance SPL.

Configurez la paire de clés signée CA sur le magasin de confiance SPL

Vous devez configurer la paire de clés signées par l'autorité de certification dans le magasin de confiance SPL.

Étapes

1. Accédez au dossier contenant le magasin de clés de la SPL `/var/opt/snapcenter/spl/etc`.
2. Localisez le fichier `keystore.jks`.
3. Répertoriez les certificats ajoutés dans la base de stockage de clés : `$ keytool -list -v -keystore keystore.jks`
4. Ajoutez le certificat de l'autorité de certification ayant à la fois une clé privée et une clé publique. `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. Répertorie les certificats ajoutés dans le magasin de clés. `$ keytool -list -v -keystore keystore.jks`
6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.
7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

   Le mot de passe par défaut de la SPL KEYSTORE est la valeur de la clé SPL_KEYSTORE_PASS dans `spl.properties` le fichier.

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks`
```

8. Si le nom d'alias du certificat de l'autorité de certification est long et contient de l'espace ou des caractères spéciaux ("*",","), remplacez le nom d'alias par un nom simple : `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
9. Configurez le nom d'alias à partir du magasin de clés situé dans `spl.properties` le fichier. Mettez à jour cette valeur par rapport à la clé SPL_CERTIFICATE_ALIAS.
10. Redémarrez le service après avoir configuré la paire de clés signée CA dans la boutique de confiance SPL.

Activer l'authentification basée sur un certificat

Pour activer l'authentification basée sur certificat pour le serveur SnapCenter et les hôtes de plug-in Windows, exécutez l'applet de commande PowerShell suivante. Pour les hôtes plug-in Linux, l'authentification basée sur certificat sera activée lorsque vous activez le protocole SSL bidirectionnel.

- Pour activer l'authentification basée sur un certificat client :

```
Set-SmConfigSettings -Agent –configSettings
@{"EnableClientCertificateAuthentication"="true"} -HostName [hostname]
```

- Pour désactiver l'authentification basée sur des certificats client :

```
Set-SmConfigSettings -Agent –configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```

Informations sur le copyright

Informations sur les marques commerciales