Configurer le certificat CA

SnapCenter software

NetApp
November 06, 2025

Sommaire

Configurer le certificat CA

Générer le fichier CSR du certificat CA

Vous pouvez générer une demande de signature de certificat (CSR) et importer le certificat qui peut être obtenu auprès d'une autorité de certification (CA) à l'aide de la CSR générée. Le certificat aura une clé privée associée.

Le CSR est un bloc de texte codé qui est remis à un fournisseur de certificats autorisé pour obtenir le certificat CA signé.

La longueur de la clé RSA du certificat CA doit être d'au moins 3 072 bits.

Pour plus d'informations sur la génération d'un CSR, voir "Comment générer un fichier CSR de certificat CA" .

Si vous possédez le certificat CA pour votre domaine (*.domain.company.com) ou votre système (machine1.domain.company.com), vous pouvez ignorer la génération du fichier CSR du certificat CA. Vous pouvez déployer le certificat CA existant avec SnapCenter.

Pour les configurations de cluster, le nom du cluster (FQDN du cluster virtuel) et les noms d'hôtes respectifs doivent être mentionnés dans le certificat CA. Le certificat peut être mis à jour en remplissant le champ Nom alternatif du sujet (SAN) avant d'obtenir le certificat. Pour un certificat générique (*.domain.company.com), le certificat contiendra implicitement tous les noms d'hôtes du domaine.

Importer des certificats CA

Vous devez importer les certificats CA sur le serveur SnapCenter et les plug-ins hôtes Windows à l'aide de la console de gestion Microsoft (MMC).

Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **Fichier** > **Ajouter/Supprimer un composant logiciel enfichable**.
2. Dans la fenêtre Ajouter ou supprimer des composants logiciels enfichables, sélectionnez **Certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable Certificats, sélectionnez l'option **Compte d'ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Racine de la console** > **Certificats – Ordinateur local** > **Autorités de certification racines de confiance** > **Certificats**.
5. Cliquez avec le bouton droit sur le dossier « Autorités de certification racines de confiance », puis sélectionnez **Toutes les tâches** > **Importer** pour démarrer l'assistant d'importation.
6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant…	Procédez comme suit…
Importer la clé privée	Sélectionnez l'option **Oui**, importez la clé privée, puis cliquez sur **Suivant**.

Dans cette fenêtre de l'assistant…	Procédez comme suit…
Format de fichier d'importation	N'effectuez aucune modification ; cliquez sur **Suivant**.
Sécurité	Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur **Suivant**.
Terminer l'assistant d'importation de certificat	Consultez le résumé, puis cliquez sur **Terminer** pour démarrer l'importation.

Le certificat d'importation doit être fourni avec la clé privée (les formats pris en charge sont : *.pfx, *.p12 et *.p7b).

7. Répétez l'étape 5 pour le dossier « Personnel ».

Obtenir l'empreinte numérique du certificat CA

Une empreinte de certificat est une chaîne hexadécimale qui identifie un certificat. Une empreinte numérique est calculée à partir du contenu du certificat à l'aide d'un algorithme d'empreinte numérique.

Étapes

1. Effectuez les opérations suivantes sur l'interface graphique :
   a. Double-cliquez sur le certificat.
   b. Dans la boîte de dialogue Certificat, cliquez sur l'onglet **Détails**.
   c. Faites défiler la liste des champs et cliquez sur **Empreinte digitale**.
   d. Copiez les caractères hexadécimaux de la boîte.
   e. Supprimez les espaces entre les nombres hexadécimaux.

      Par exemple, si l'empreinte digitale est : « a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b », après avoir supprimé les espaces, elle sera : « a909502dd82ae41433e6f83886b00d4277a32a7b ».

2. Effectuez les opérations suivantes à partir de PowerShell :
   a. Exécutez la commande suivante pour répertorier l'empreinte numérique du certificat installé et identifier le certificat récemment installé par le nom du sujet.

      Get-ChildItem -Chemin Cert:\LocalMachine\Mon

   b. Copiez l'empreinte digitale.

Configurer le certificat CA avec les services de plug-in hôte Windows

Vous devez configurer le certificat CA avec les services de plug-in hôte Windows pour

activer le certificat numérique installé.

Effectuez les étapes suivantes sur le serveur SnapCenter et tous les hôtes de plug-in sur lesquels les certificats CA sont déjà déployés.

Étapes

1. Supprimez la liaison de certificat existante avec le port par défaut SMCore 8145, en exécutant la commande suivante :

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Par exemple:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Liez le certificat nouvellement installé aux services du plug-in hôte
   Windows, en exécutant les commandes suivantes :
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Par exemple:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

Configurer le certificat CA pour le service de plug-ins pris en charge par NetApp sur l'hôte Linux

Vous devez gérer le mot de passe du magasin de clés des plug-ins et son certificat, configurer le certificat de l'autorité de certification, configurer les certificats racine ou intermédiaires dans le magasin de clés de confiance des plug-ins et configurer la paire de clés signée par l'autorité de certification dans le magasin de clés de confiance des plug-ins avec le service de plug-ins SnapCenter pour activer le certificat numérique installé.

Les plug-ins utilisent le fichier « keystore.jks », qui se trouve dans */opt/ NetApp/snapcenter/scc/etc* à la fois comme magasin de confiance et comme magasin de clés.

Gérer le mot de passe du magasin de clés du plug-in et l'alias de la paire de clés signée par l'autorité de certification en cours d'utilisation

Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés du plug-in à partir du fichier de propriétés de l'agent du plug-in.

   Il s'agit de la valeur correspondant à la clé 'KEYSTORE_PASS'.

2. Modifier le mot de passe du keystore :

```
 keytool -storepasswd -keystore keystore.jks
. Modifiez le mot de passe de tous les alias des entrées de clés privées dans le magasin de clés avec le même mot de passe que celui utilisé pour le magasin de clés :
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

   Mettez à jour la même chose pour la clé KEYSTORE_PASS dans le fichier *agent.properties*.

3. Redémarrez le service après avoir modifié le mot de passe.

> Le mot de passe du magasin de clés du plug-in et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

Configurer les certificats racine ou intermédiaires pour le plug-in trust-store

Vous devez configurer les certificats racine ou intermédiaires sans la clé privée pour connecter le trust-store.

Étapes

1. Accédez au dossier contenant le keystore du plug-in : /opt/ NetApp/snapcenter/scc/etc.
2. Localisez le fichier « keystore.jks ».
3. Répertoriez les certificats ajoutés dans le keystore :

```
keytool -list -v -keystore keystore.jks
```

4. Ajouter un certificat racine ou intermédiaire :

```
 keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
. Redémarrez le service après avoir configuré les certificats racine ou intermédiaires pour connecter le magasin de confiance.
```

> Vous devez ajouter le certificat CA racine, puis les certificats CA intermédiaires.

Configurer la paire de clés signée par l'autorité de certification pour le plug-in trust-store

Vous devez configurer la paire de clés signée par l'autorité de certification dans le magasin de clés de confiance du plug-in.

Étapes

1. Accédez au dossier contenant le keystore du plug-in /opt/ NetApp/snapcenter/scc/etc.
2. Localisez le fichier « keystore.jks ».
3. Répertoriez les certificats ajoutés dans le keystore :

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Ajoutez le certificat CA contenant à la fois une clé privée et une clé publique.

   ```
   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
   -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```

5. Répertoriez les certificats ajoutés dans le keystore.

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat CA, 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 du magasin de clés du plug-in est la valeur de la clé KEYSTORE_PASS dans le fichier agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Si le nom d'alias dans le certificat CA est long et contient des
   espaces ou des caractères spéciaux (« * », « », « ), remplacez le nom
   d'alias par un nom simple :
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Configurez le nom d'alias à partir du certificat CA dans le fichier
   agent.properties.
   ```

   Mettez à jour cette valeur par rapport à la clé SCC_CERTIFICATE_ALIAS.

8. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification pour le plug-in trust-store.

Configurer la liste de révocation des certificats (CRL) pour les plug-ins

À propos de cette tâche

- Les plug-ins SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins SnapCenter est « opt/ NetApp/snapcenter/scc/etc/crl ».

Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut dans le fichier agent.properties par rapport à la clé CRL_PATH.

   Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés par rapport à chaque CRL.

Configurer le certificat CA pour le service de plug-ins pris en charge par NetApp sur l'hôte Windows

Vous devez gérer le mot de passe du magasin de clés des plug-ins et son certificat, configurer le certificat de l'autorité de certification, configurer les certificats racine ou intermédiaires dans le magasin de clés de confiance des plug-ins et configurer la paire de clés signée par l'autorité de certification dans le magasin de clés de confiance des plug-ins avec le service de plug-ins SnapCenter pour activer le certificat numérique installé.

Les plug-ins utilisent le fichier *keystore.jks*, qui se trouve dans *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* à la fois comme magasin de confiance et comme magasin de clés.

Gérer le mot de passe du magasin de clés du plug-in et l'alias de la paire de clés signée par l'autorité de certification en cours d'utilisation

Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés du plug-in à partir du fichier de propriétés de l'agent du plug-in.

   Il s'agit de la valeur correspondant à la clé *KEYSTORE_PASS*.

2. Modifier le mot de passe du keystore :

   keytool -storepasswd -keystore magasin de clés.jks

   > Si la commande « keytool » n'est pas reconnue sur l'invite de commande Windows, remplacez la commande keytool par son chemin complet.

   C:\Program Files\Java\<version_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks

3. Modifiez le mot de passe de tous les alias des entrées de clés privées dans le magasin de clés avec le même mot de passe que celui utilisé pour le magasin de clés :

   keytool -keypasswd -alias "nom_d'alias_dans_cert" -keystore keystore.jks

Mettez à jour la même chose pour la clé KEYSTORE_PASS dans le fichier *agent.properties*.

4. Redémarrez le service après avoir modifié le mot de passe.

> Le mot de passe du magasin de clés du plug-in et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

Configurer les certificats racine ou intermédiaires pour le plug-in trust-store

Vous devez configurer les certificats racine ou intermédiaires sans la clé privée pour connecter le trust-store.

Étapes

1. Accédez au dossier contenant le keystore du plug-in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localisez le fichier « keystore.jks ».
3. Répertoriez les certificats ajoutés dans le keystore :

   keytool -list -v -keystore keystore.jks

4. Ajouter un certificat racine ou intermédiaire :

   keytool -import -trustcacerts -alias myRootCA -fichier /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. Redémarrez le service après avoir configuré les certificats racine ou intermédiaires pour connecter le magasin de confiance.

> Vous devez ajouter le certificat CA racine, puis les certificats CA intermédiaires.

Configurer la paire de clés signée par l'autorité de certification pour le plug-in trust-store

Vous devez configurer la paire de clés signée par l'autorité de certification dans le magasin de clés de confiance du plug-in.

Étapes

1. Accédez au dossier contenant le keystore du plug-in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localisez le fichier *keystore.jks*.
3. Répertoriez les certificats ajoutés dans le keystore :

   keytool -list -v -keystore keystore.jks

4. Ajoutez le certificat CA contenant à la fois une clé privée et une clé publique.

   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS

5. Répertoriez les certificats ajoutés dans le keystore.

   keytool -list -v -keystore keystore.jks

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat CA, 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 du magasin de clés du plug-in est la valeur de la clé KEYSTORE_PASS dans le fichier agent.properties.

   keytool -keypasswd -alias "nom_d'alias_dans_CA_cert" -keystore keystore.jks

8. Configurez le nom d'alias à partir du certificat CA dans le fichier *agent.properties*.

   Mettez à jour cette valeur par rapport à la clé SCC_CERTIFICATE_ALIAS.

9. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification pour le plug-in trust-store.

Configurer la liste de révocation des certificats (CRL) pour les plug-ins SnapCenter

À propos de cette tâche

- Pour télécharger le dernier fichier CRL pour le certificat CA associé, voir "Comment mettre à jour le fichier de liste de révocation de certificats dans SnapCenter CA Certificate" .
- Les plug-ins SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins SnapCenter est *'C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut dans le fichier *agent.properties* par rapport à la clé CRL_PATH.
2. Vous pouvez placer plusieurs fichiers CRL dans ce répertoire.

   Les certificats entrants seront vérifiés par rapport à chaque CRL.

Activer les certificats CA pour les plug-ins

Vous devez configurer les certificats CA et déployer les certificats CA sur le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat CA pour les plug-ins.

Avant de commencer

- Vous pouvez activer ou désactiver les certificats d'autorité de certification à l'aide de l'applet de commande run *Set-SmCertificateSettings*.
- Vous pouvez afficher l'état du certificat des plug-ins à l'aide de *Get-SmCertificateSettings*.

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

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Hôtes gérés**.
3. Sélectionnez un ou plusieurs hôtes de plug-in.
4. Cliquez sur **Plus d'options**.
5. Sélectionnez **Activer la validation du certificat**.

Après avoir terminé

L'onglet Hôtes gérés affiche un cadenas et la couleur du cadenas indique l'état de la connexion entre SnapCenter Server et l'hôte du plug-in.

- *  * indique que le certificat CA n'est ni activé ni attribué à l'hôte du plug-in.
- *  * indique que le certificat CA est validé avec succès.
- *  * indique que le certificat CA n'a pas pu être validé.
- *  * indique que les informations de connexion n'ont pas pu être récupérées.

Lorsque le statut est jaune ou vert, les opérations de protection des données se terminent avec succès.

Informations sur le copyright

Informations sur les marques commerciales