



# **Configurer le certificat CA**

## **SnapCenter Software 4.9**

NetApp  
March 20, 2024

# Sommaire

Configurer le certificat CA .....	1
Générer le fichier CSR de certificat CA .....	1
Importer des certificats CA .....	1
Obtenez le certificat CA imprimé .....	2
Configurez le certificat d'autorité de certification avec les services de plug-in d'hôte Windows .....	2
Configurez le certificat d'autorité de certification pour le service de plug-ins personnalisés SnapCenter sur l'hôte Linux .....	3
Configurez le certificat d'autorité de certification pour le service de plug-ins personnalisés SnapCenter sur l'hôte Windows .....	6
Activez les certificats CA pour les plug-ins .....	8

# Configurer le certificat CA

## Générer le fichier CSR de certificat CA

Vous pouvez générer une requête 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 RSC générée. Une clé privée sera associée au certificat.

CSR est un bloc de texte codé donné à un fournisseur de certificats autorisé pour obtenir le certificat d'autorité de certification signé.



La longueur de la clé RSA du certificat CA doit être d'au moins 3072 bits.

Pour plus d'informations sur la génération d'une RSC, reportez-vous à la section "[Comment générer un fichier CSR de certificat CA](#)".



Si vous possédez le certificat de l'autorité de certification pour votre domaine (\*.domain.company.com) ou votre système (machine1.domain.company.com), vous pouvez ignorer la génération du fichier CSR du certificat de l'autorité de certification. Vous pouvez déployer le certificat d'autorité de certification existant avec SnapCenter.

Pour les configurations de cluster, le nom de cluster (FQDN du cluster virtuel) et les noms d'hôte correspondants doivent être mentionnés dans le certificat de l'autorité de certification. Le certificat peut être mis à jour en remplissant le champ Subject alternative Name (SAN) avant d'obtenir le certificat. Pour un certificat de type Wild card (\*.domain.company.com), le certificat contiendra implicitement tous les noms d'hôte du domaine.

## Importer des certificats CA

Vous devez importer les certificats d'autorité de certification 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 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 > autorités de certification racines de confiance > certificats**.
5. Cliquez avec le bouton droit de la souris sur le dossier "autorités de certification racine de confiance", puis sélectionnez **toutes les tâches > Importer** pour lancer l'assistant d'importation.
6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Importer une clé privée	Sélectionnez l'option <b>Oui</b> , importez la clé privée, puis cliquez sur <b>Suivant</b> .

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Importer le format de fichier	N'apportez aucune modification ; cliquez sur <b>Suivant</b> .
Sécurité	Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur <b>Suivant</b> .
Exécution de l'assistant d'importation de certificat	Vérifiez le résumé, puis cliquez sur <b>Terminer</b> pour lancer 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 ».

## Obtenez le certificat CA imprimé

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

### 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 **Thumbprint**.
  - d. Copiez les caractères hexadécimaux de la zone.
  - e. Supprimez les espaces entre les nombres hexadécimaux.

Par exemple, si l'empreinte est : "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", après avoir retiré les espaces, il sera : "a909502dd82a41433e6f83886b00d4277a32a7b".

2. Effectuer les opérations suivantes à partir de PowerShell :
  - a. Exécutez la commande suivante pour lister l'empreinte du certificat installé et identifier le certificat récemment installé par le nom de l'objet.

```
Get-ChildItem -Path Cert:\Localmachine\My
```

- b. Copiez l'empreinte.

## Configurez le certificat d'autorité de certification avec les services de plug-in d'hôte Windows

Vous devez configurer le certificat d'autorité de certification avec les services de plug-in d'hôte Windows pour activer le certificat numérique installé.

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

## Étapes

1. Supprimez la liaison du certificat existant 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
. Associez le certificat récemment 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"
```

## Configurez le certificat d'autorité de certification pour le service de plug-ins personnalisés SnapCenter sur l'hôte Linux

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

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

## Gérer le mot de passe pour le magasin de clés de plug-in personnalisé et l'alias de la paire de clés signée par l'autorité de certification utilisée

### Étapes

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

C'est la valeur correspondant à la clé 'KEYSTORE\_PASS'.

2. Modifiez le mot de passe du magasin de clés :

```
keytool -storepasswd -keystore keystore.jks  
. Remplacez le mot de passe de tous les alias des entrées de clé privée  
du magasin de clés par le même mot de passe que celui utilisé pour le  
magasin de clés :
```

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

Procédez de même 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 de plug-in personnalisé et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

## Configurez les certificats racine ou intermédiaire sur le magasin de confiance du plug-in personnalisé

Vous devez configurer les certificats racine ou intermédiaire sans la clé privée sur le magasin de confiance du plug-in personnalisé.

### Étapes

1. Naviguez jusqu'au dossier contenant le keystore de plug-in personnalisé : `/opt/NetApp/snapcenter/scc/etc`
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
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  
intermédiaire sur le magasin de confiance personnalisé du plug-in.
```



Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

## Configurez la paire de clés signée CA sur un plug-in de stockage en confiance personnalisé

Vous devez configurer la paire de clés signées CA dans le magasin de confiance personnalisé du plug-in.

### Étapes

1. Accédez au dossier contenant le magasin de clés personnalisé du plug-in `/opt/NetApp/snapcenter/scc/etc`
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

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

4. Ajoutez le certificat de l'autorité de certification ayant 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 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 de magasin de clés personnalisé par défaut est la valeur du FICHIER `KEYSTORE_PASS` dans le fichier `agent.properties`.

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

. 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 "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 cette valeur à jour 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 dans le magasin de confiance personnalisé du plug-in.

## Configurez la liste de révocation de certificats (CRL) pour les plug-ins personnalisés SnapCenter

### Description de la tâche

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

### Étapes

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

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

## Configurez le certificat d'autorité de certification pour le service de plug-ins personnalisés SnapCenter sur l'hôte Windows

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

Les plug-ins personnalisés utilisent le fichier `keystore.jks`, qui se trouve à l'adresse `C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc` comme magasin de confiance et magasin de clés.

## Gérer le mot de passe pour le magasin de clés de plug-in personnalisé et l'alias de la paire de clés signée par l'autorité de certification utilisée

### Étapes

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

C'est la valeur correspondant à la clé `KEYSTORE_PASS`.

2. Modifiez le mot de passe du magasin de clés :

```
keytool -storepasswd -keystore keystore.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\<jdk_version>\bin\keytool.exe » -storepasswd -keystore.jks
```

3. Remplacez le mot de passe de tous les alias des entrées de clé privée du magasin de clés par le même mot de passe que celui utilisé pour le magasin de clés :



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

Procédez de même 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 de plug-in personnalisé et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

## Configurez les certificats racine ou intermédiaire sur le magasin de confiance du plug-in personnalisé

Vous devez configurer les certificats racine ou intermédiaire sans la clé privée sur le magasin de confiance du plug-in personnalisé.

### Étapes

1. Naviguez jusqu'au dossier contenant le magasin de clés de plug-in personnalisé *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc*
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

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

4. Ajouter un certificat racine ou intermédiaire :

```
Keytool -import -truacts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore.jks
```

5. Redémarrez le service après avoir configuré les certificats racine ou intermédiaire sur le magasin de confiance personnalisé du plug-in.



Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

## Configurez la paire de clés signée CA sur un plug-in de stockage en fiducie personnalisé

Vous devez configurer la paire de clés signées CA dans le magasin de confiance personnalisé du plug-in.

### Étapes

1. Accédez au dossier contenant le magasin de clés personnalisé 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 magasin de clés :

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

4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.

```
Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore.jks -desstoretype JKS
```

5. Répertorier 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 de magasin de clés personnalisé par défaut est la valeur du FICHER KEystore\_PASS dans le fichier agent.properties.

```
Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks
```

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

Mettez cette valeur à jour 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 dans le magasin de confiance personnalisé du plug-in.

## Configurez la liste de révocation de certificats (CRL) pour les plug-ins personnalisés SnapCenter

### Description de la tâche

- Pour télécharger le fichier CRL le plus récent pour le certificat d'autorité de certification associé, reportez-vous à la section ["Comment mettre à jour le fichier de liste de révocation de certificats dans le certificat d'autorité de certification SnapCenter"](#).
- Les plug-ins personnalisés SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins personnalisés 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 du 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 pour chaque CRL.

## Activez les certificats CA pour les plug-ins

Vous devez configurer les certificats d'autorité de certification et déployer les certificats d'autorité de certification dans le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat de l'autorité de certification pour les plug-ins.

### Avant de commencer

- Vous pouvez activer ou désactiver les certificats CA à l'aide de l'applet de commande run *set-SmCertificateSettings*.

- Vous pouvez afficher l'état du certificat pour les plug-ins à l'aide de *get-SmCertificateSettings*.





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 au "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Sélectionnez des hôtes à un ou plusieurs plug-ins.
4. Cliquez sur **plus d'options**.
5. Sélectionnez **Activer la validation de certificat**.

### Une fois que vous avez terminé

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

-  Indique que le certificat CA n'est ni activé ni affecté à l'hôte du plug-in.
-  Indique que le certificat CA a été 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 l'état est jaune ou vert, les opérations de protection des données s'achève correctement.

## Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

## Informations sur les marques commerciales

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