# Configurer le certificat CA pour l'hôte Windows

SnapCenter software

NetApp
November 06, 2025

# Sommaire

# Configurer le certificat CA pour l'hôte Windows

## 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 avec le site SnapCenter

Vous devez configurer le certificat CA avec le site SnapCenter sur l'hôte Windows.

**Mesures**

1. Ouvrez le Gestionnaire IIS sur le serveur Windows sur lequel SnapCenter est installé.
2. Dans le volet de navigation de gauche, cliquez sur **Connexions**.
3. Développez le nom du serveur et **Sites**.
4. Sélectionnez le site Web SnapCenter sur lequel vous souhaitez installer le certificat SSL.
5. Accédez à **Actions** > **Modifier le site**, cliquez sur **Liaisons**.
6. Dans la page Liaisons, sélectionnez **liaison pour https**.
7. Cliquez sur **Modifier**.
8. Dans la liste déroulante Certificat SSL, sélectionnez le certificat SSL récemment importé.

9. Cliquez sur **OK**.

> Le site SnapCenter Scheduler (port par défaut : 8154, HTTPS) est configuré avec un certificat auto-signé. Ce port communique avec l'hôte SnapCenter Server et il n'est pas obligatoire de le configurer avec un certificat CA. Toutefois, si votre environnement vous oblige à utiliser un certificat CA, répétez les étapes 5 à 9 à l'aide du site SnapCenter Scheduler.

> Si le certificat CA récemment déployé n'est pas répertorié dans le menu déroulant, vérifiez si le certificat CA est associé à la clé privée.

> Assurez-vous que le certificat est ajouté à l'aide du chemin suivant : **Racine de la console > Certificats – Ordinateur local > Autorités de certification racines de confiance > Certificats**.

# Activer les certificats CA pour SnapCenter

Vous devez configurer les certificats CA et activer la validation du certificat CA pour le serveur SnapCenter .

**Avant de commencer**

- Vous pouvez activer ou désactiver les certificats d'autorité de certification à l'aide de l'applet de commande Set-SmCertificateSettings.
- Vous pouvez afficher l'état du certificat du serveur SnapCenter à l'aide de l'applet de commande 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 vous référer à la "Guide de référence de l'applet de commande du logiciel SnapCenter" .

**Mesures**

1. Dans la page Paramètres, accédez à **Paramètres** > **Paramètres globaux** > **Paramètres du certificat CA**.
2. Sélectionnez **Activer la validation du certificat**.
3. Cliquez sur **Appliquer**.

**Après avoir fini**

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 qu'aucun certificat CA n'est activé ou 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