Installer le plug-in SnapCenter pour Microsoft Windows

SnapCenter software

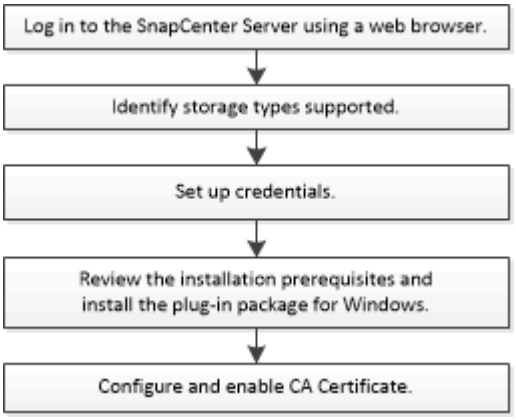
NetApp
November 06, 2025

Sommaire

Installer le plug-in SnapCenter pour Microsoft Windows

Flux de travail d'installation du plug-in SnapCenter pour Microsoft Windows

Vous devez installer et configurer SnapCenter Plug-in pour Microsoft Windows si vous souhaitez protéger les fichiers Windows qui ne sont pas des fichiers de base de données.



Configuration requise pour l'installation du plug-in SnapCenter pour Microsoft Windows

Vous devez connaître certaines exigences d'installation avant d'installer le plug-in pour Windows.

Avant de commencer à utiliser le plug-in pour Windows, l'administrateur SnapCenter doit installer et configurer SnapCenter Server et effectuer les tâches préalables.

- Vous devez disposer des privilèges d'administrateur SnapCenter pour installer le plug-in pour Windows.

  Le rôle d'administrateur SnapCenter doit disposer de privilèges d'administrateur.

- Vous devez avoir installé et configuré le serveur SnapCenter .
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez des informations d'identification qui ne sont pas intégrées ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Vous devez configurer SnapMirror et SnapVault si vous souhaitez une réplication de sauvegarde.

Configuration requise pour l'installation du package de plug-ins SnapCenter pour Windows

Avant d'installer le package de plug-ins SnapCenter pour Windows, vous devez vous familiariser avec certaines exigences de base en matière d'espace et de taille du système hôte.

Article	Exigences
Systèmes d'exploitation	Microsoft Windows Pour obtenir les dernières informations sur les versions prises en charge, consultez le "Outil de matrice d'interopérabilité NetApp" . Si vous utilisez une configuration de cluster Windows, vous devez également installer et configurer la gestion à distance Windows (WinRM).
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 Go
Espace minimum d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	5 Go Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace journal requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récemment exécutées.
Logiciels requis	• Pack d'hébergement ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x ultérieurs) • PowerShell Core 7.4.2 Pour obtenir les dernières informations sur les versions prises en charge, consultez le "Outil de matrice d'interopérabilité NetApp" . Pour obtenir des informations de dépannage spécifiques à .NET, consultez "La mise à niveau ou l'installation de SnapCenter échoue pour les systèmes hérités qui ne disposent pas de connectivité Internet."

Configurez vos informations d'identification pour le plug-in pour Windows

SnapCenter utilise des informations d'identification pour authentifier les utilisateurs pour les opérations SnapCenter . Vous devez créer des informations d'identification pour l'installation des plug-ins SnapCenter et des informations d'identification supplémentaires pour effectuer des opérations de protection des données sur les systèmes de fichiers Windows.

Ce dont vous aurez besoin

- Vous devez configurer les informations d'identification Windows avant d'installer les plug-ins.
- Vous devez configurer les informations d'identification avec des privilèges d'administrateur, y compris les droits d'administrateur, sur l'hôte distant.
- Si vous configurez des informations d'identification pour des groupes de ressources individuels et que l'utilisateur ne dispose pas de privilèges d'administrateur complets, vous devez attribuer au moins les privilèges de groupe de ressources et de sauvegarde à l'utilisateur.

Mesures

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Informations d'identification**.
3. Cliquez sur **Nouveau**.
4. Dans la page Informations d'identification, procédez comme suit :

Pour ce domaine…	**Fais ceci…**
Nom d'identification	Entrez un nom pour les informations d'identification.

Pour ce domaine…	Fais ceci…
Nom d'utilisateur/Mot de passe	Saisissez le nom d'utilisateur et le mot de passe utilisés pour l'authentification. • Administrateur de domaine ou tout membre du groupe d'administrateurs Indiquez l'administrateur du domaine ou tout membre du groupe d'administrateurs du 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 (pour les groupes de travail uniquement) Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré du système sur lequel vous installez le plug-in SnapCenter . Vous pouvez spécifier un compte utilisateur local appartenant au groupe des administrateurs locaux si ce compte dispose de privilèges élevés ou si la fonctionnalité de contrôle d'accès utilisateur est désactivée sur le système hôte. Le format valide pour le champ Nom d'utilisateur est le suivant : `UserName` N'utilisez pas de guillemets doubles (") ou de backtick (`) dans les mots de passe. Vous ne devez pas utiliser les symboles inférieur à (<) et d'exclamation (!) ensemble dans les mots de passe. Par exemple, lessthan<!10, lessthan10<!, backtick`12.
Mot de passe	Entrez le mot de passe utilisé pour l'authentification.

5. Cliquez sur **OK**.

   Une fois que vous avez terminé de configurer les informations d'identification, vous souhaiterez peut-être attribuer la maintenance des informations d'identification à un utilisateur ou à un groupe d'utilisateurs sur la page Utilisateur et accès.

Configurer gMSA sur Windows Server 2016 ou version ultérieure

Windows Server 2016 ou version ultérieure vous permet de créer un compte de service géré de groupe (gMSA) qui fournit une gestion automatisée des mots de passe des comptes de service à partir d'un compte

de domaine géré.

Avant de commencer

- Vous devez disposer d'un contrôleur de domaine Windows Server 2016 ou version ultérieure.
- Vous devez disposer d'un hôte Windows Server 2016 ou version ultérieure, qui est membre du domaine.

Étapes

1. Créez une clé racine KDS pour générer des mots de passe uniques pour chaque objet de votre gMSA.
2. Pour chaque domaine, exécutez la commande suivante à partir du contrôleur de domaine Windows : Add-KDSRootKey -EffectiveImmediately
3. Créez et configurez votre gMSA :
   a. Créez un compte de groupe d'utilisateurs au format suivant :

```
 domainName\accountName$
.. Ajoutez des objets informatiques au groupe.
.. Utilisez le groupe d'utilisateurs que vous venez de créer pour
créer le gMSA.
```

   Par exemple,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Courir `Get-ADServiceAccount` commande pour vérifier le compte de
service.
```

4. Configurez le gMSA sur vos hôtes :
   a. Activez le module Active Directory pour Windows PowerShell sur l'hôte sur lequel vous souhaitez utiliser le compte gMSA.

   Pour ce faire, exécutez la commande suivante depuis PowerShell :

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install State
------------                            ----                -------------
[ ] Active Directory Domain Services    AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. Redémarrez votre hôte.

b. Installez le gMSA sur votre hôte en exécutant la commande suivante à partir de l'invite de commande PowerShell : `Install-AdServiceAccount <gMSA>`

c. Vérifiez votre compte gMSA en exécutant la commande suivante : `Test-AdServiceAccount <gMSA>`

5. Attribuez les privilèges administratifs au gMSA configuré sur l'hôte.
6. Ajoutez l'hôte Windows en spécifiant le compte gMSA configuré dans le serveur SnapCenter .

   SnapCenter Server installera les plug-ins sélectionnés sur l'hôte et le gMSA spécifié sera utilisé comme compte de connexion au service pendant l'installation du plug-in.

Ajoutez des hôtes et installez le plug-in SnapCenter pour Microsoft Windows

Vous pouvez utiliser la page Ajouter un hôte de SnapCenter pour ajouter des hôtes Windows. Le plug-in SnapCenter pour Microsoft Windows est automatiquement installé sur l'hôte spécifié. Il s'agit de la méthode recommandée pour l'installation des plug-ins. Vous pouvez ajouter un hôte et installer un plug-in pour un hôte individuel ou un cluster.

Avant de commencer

- Si le système d'exploitation de l'hôte SnapCenter Server est Windows 2019 et que le système d'exploitation de l'hôte du plug-in est Windows 2022, vous devez effectuer les opérations suivantes :
  - Mise à niveau vers Windows Server 2019 (build du système d'exploitation 17763.5936) ou version ultérieure
  - Mise à niveau vers Windows Server 2022 (build du système d'exploitation 20348.2402) ou version ultérieure

- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation de plug-in, tel que le rôle Administrateur SnapCenter .
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez des informations d'identification qui ne sont pas intégrées ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- L'utilisateur SnapCenter doit être ajouté au rôle « Se connecter en tant que service » du serveur Windows.
- Vous devez vous assurer que le service de mise en file d'attente des messages est en cours d'exécution.
- Si vous utilisez un compte de service géré de groupe (gMSA), vous devez configurer gMSA avec des privilèges administratifs.

  "Configurer un compte de service géré de groupe sur Windows Server 2016 ou version ultérieure pour le système de fichiers Windows"

À propos de cette tâche

- Vous ne pouvez pas ajouter un serveur SnapCenter en tant qu'hôte de plug-in à un autre serveur SnapCenter .
- Plugins Windows
  - Microsoft Windows
  - Serveur Microsoft Exchange
  - Microsoft SQL Server
  - SAP HANA
- Installation de plug-ins sur un cluster

  Si vous installez des plug-ins sur un cluster (WSFC, Oracle RAC ou Exchange DAG), ils sont installés sur tous les nœuds du cluster.
- Stockage de la série E

  Vous ne pouvez pas installer le plug-in pour Windows sur un hôte Windows connecté au stockage de la série E.

> SnapCenter ne prend pas en charge l'ajout du même hôte (hôte plug-in) à SnapCenter si l'hôte fait déjà partie d'un groupe de travail et a été modifié vers un autre domaine ou vice versa. Si vous souhaitez ajouter le même hôte, vous devez supprimer l'hôte de SnapCenter et l'ajouter à nouveau.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Assurez-vous que **Hôtes gérés** est sélectionné en haut.
3. Cliquez sur **Ajouter**.
4. Dans la page Hôtes, procédez comme suit :

Pour ce domaine…	Fais ceci…
Type d'hôte	Sélectionnez le type d'hôte **Windows**. SnapCenter Server ajoute l'hôte, puis installe le plug-in pour Windows s'il n'est pas déjà installé sur l'hôte.
Nom d'hôte	Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte. SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le nom de domaine complet (FQDN). Vous pouvez saisir les adresses IP ou le FQDN de l'un des éléments suivants : • Hôte autonome • Clustering de basculement Windows Server (WSFC) Si vous ajoutez un hôte à l'aide de SnapCenter et qu'il fait partie d'un sous-domaine, vous devez fournir le nom de domaine complet.
Informations d'identification	Sélectionnez le nom des informations d'identification que vous avez créées ou créez les nouvelles informations d'identification. L'identifiant doit disposer de droits administratifs sur l'hôte distant. Pour plus de détails, consultez les informations sur la création d'informations d'identification. Les détails sur les informations d'identification, y compris le nom d'utilisateur, le domaine et le type d'hôte, s'affichent en plaçant votre curseur sur le nom d'informations d'identification que vous avez fourni. Le mode d'authentification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajouter un hôte.

5. Dans la section Sélectionner les plug-ins à installer, sélectionnez les plug-ins à installer.

   Pour les nouveaux déploiements, aucun package de plug-in n'est répertorié.

6. (Facultatif) Cliquez sur **Plus d'options**.

Pour ce domaine…	Fais ceci…
Port	Conservez le numéro de port par défaut ou spécifiez le numéro de port. Le numéro de port par défaut est 8145. Si le serveur SnapCenter a été installé sur un port personnalisé, ce numéro de port sera affiché comme port par défaut. Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Sinon, l'opération échoue.
Chemin d'installation	Le chemin par défaut est C:\Program Files\ NetApp\ SnapCenter. Vous pouvez éventuellement personnaliser le chemin. Pour le package de plug-ins SnapCenter pour Windows, le chemin par défaut est C:\Program Files\ NetApp\ SnapCenter. Cependant, si vous le souhaitez, vous pouvez personnaliser le chemin par défaut.
Ajouter tous les hôtes du cluster	Cochez cette case pour ajouter tous les nœuds de cluster dans un WSFC.
Ignorer les vérifications de préinstallation	Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas valider si l'hôte répond aux exigences d'installation du plug-in.
Utiliser un compte de service géré de groupe (gMSA) pour exécuter les services du plug-in	Cochez cette case si vous souhaitez utiliser un compte de service géré de groupe (gMSA) pour exécuter les services de plug-in. Fournissez le nom gMSA au format suivant : *domainName\accountName$*. gMSA sera utilisé comme compte de service de connexion uniquement pour le service SnapCenter Plug-in pour Windows.

7. Cliquez sur **Soumettre**.

   Si vous n'avez pas coché la case « Ignorer les pré-vérifications », l'hôte est validé afin de vérifier s'il répond aux exigences d'installation du plug-in. L'espace disque, la RAM, la version de PowerShell, la version .NET et l'emplacement sont vérifiés par rapport aux exigences minimales. Si les exigences

minimales ne sont pas respectées, des messages d'erreur ou d'avertissement appropriés s'affichent.

Si l'erreur est liée à l'espace disque ou à la RAM, vous pouvez mettre à jour le fichier web.config situé à l'adresse `C:\Program Files\NetApp\SnapCenter` WebApp pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez résoudre le problème.

> Dans une configuration HA, si vous mettez à jour le fichier web.config, vous devez mettre à jour le fichier sur les deux nœuds.

8. Surveiller la progression de l'installation.

Installer le plug-in SnapCenter pour Microsoft Windows sur plusieurs hôtes distants à l'aide des applets de commande PowerShell

Si vous souhaitez installer SnapCenter Plug-in pour Microsoft Windows sur plusieurs hôtes à la fois, vous pouvez le faire en utilisant le `Install-SmHostPackage` Applet de commande PowerShell.

Vous devez vous être connecté à SnapCenter en tant qu'utilisateur de domaine avec des droits d'administrateur local sur chaque hôte sur lequel vous souhaitez installer des plug-ins.

Étapes

1. Lancez PowerShell.
2. Sur l'hôte SnapCenter Server, établissez une session à l'aide de `Open-SmConnection` applet de commande, puis entrez vos informations d'identification.
3. Ajoutez l'hôte autonome ou le cluster à SnapCenter à l'aide de l' `Add-SmHost` applet de commande et les paramètres requis.

   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" .

4. Installez le plug-in sur plusieurs hôtes à l'aide du `Install-SmHostPackage` applet de commande et les paramètres requis.

   Vous pouvez utiliser le `-skipprecheck` option lorsque vous avez installé les plug-ins manuellement et que vous ne souhaitez pas valider si l'hôte répond aux exigences pour installer le plug-in.

Installez le plug-in SnapCenter pour Microsoft Windows en mode silencieux à partir de la ligne de commande

Vous pouvez installer le plug-in SnapCenter pour Microsoft Windows localement sur un hôte Windows si vous ne parvenez pas à installer le plug-in à distance à partir de l'interface graphique SnapCenter . Vous pouvez exécuter le programme d'installation du plug-in SnapCenter pour Microsoft Windows sans surveillance, en mode silencieux, à partir de la ligne de commande Windows.

Avant de commencer

- Vous devez avoir installé le bundle d'hébergement ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x ultérieurs).
- Vous devez avoir installé PowerShell 7.4.2 ou une version ultérieure.
- Vous devez être un administrateur local sur l'hôte.

Étapes

1. Téléchargez le plug-in SnapCenter pour Microsoft Windows à partir de votre emplacement d'installation.

   Par exemple, le chemin d'installation par défaut est C:\ProgramData\ NetApp\ SnapCenter\Package Repository.

   Ce chemin est accessible depuis l'hôte sur lequel le serveur SnapCenter est installé.

2. Copiez le fichier d'installation sur l'hôte sur lequel vous souhaitez installer le plug-in.
3. À partir de l'invite de commande, accédez au répertoire dans lequel vous avez téléchargé le fichier d'installation.
4. Saisissez la commande suivante en remplaçant les variables par vos données :

   ```
   "snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""
   BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
   ISFeatureInstall=SCW
   ```

   Par exemple:

   ```
   `"C:\ProgramData\NetApp\SnapCenter\Package Repository
   \snapcenter_windows_host_plugin.exe"/silent /debuglog"C:
   \HPPW_SCW_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
   SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
   BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
   ISFeatureInstall=SCW`
   ```

   Tous les paramètres transmis lors de l'installation du Plug-in pour Windows sont sensibles à la casse.

   Saisissez les valeurs des variables suivantes :

Variable	Valeur
/debuglog"<Chemin_du_journal_de_débogage>	Spécifiez le nom et l'emplacement du fichier journal du programme d'installation de la suite, comme dans l'exemple suivant : Setup.exe /debuglog"C:\PathToLog\setupexe.log".
BI_SNAPCENTER_PORT	Spécifiez le port sur lequel SnapCenter communique avec SMCore.

Variable	Valeur
SUITE_INSTALLDIR	Spécifiez le répertoire d'installation du package du plug-in hôte.
BI_SERVICEACCOUNT	Spécifiez le plug-in SnapCenter pour le compte de service Web Microsoft Windows.
BI_SERVICEPWD	Spécifiez le mot de passe du compte de service Web SnapCenter Plug-in pour Microsoft Windows.
Installation de la fonctionnalité ISFeature	Spécifiez la solution à déployer par SnapCenter sur l'hôte distant.

Le paramètre *debuglog* inclut le chemin du fichier journal pour SnapCenter. L'écriture dans ce fichier journal est la méthode préférée pour obtenir des informations de dépannage, car le fichier contient les résultats des vérifications effectuées par l'installation pour les prérequis du plug-in.

Si nécessaire, vous pouvez trouver des informations de dépannage supplémentaires dans le fichier journal du package SnapCenter pour Windows. Les fichiers journaux du package sont répertoriés (du plus ancien au plus ancien) dans le dossier *%Temp%*, par exemple, *C:\temp*\.

L'installation du plug-in pour Windows enregistre le plug-in sur l'hôte et non sur le serveur SnapCenter . Vous pouvez enregistrer le plug-in sur le serveur SnapCenter en ajoutant l'hôte à l'aide de l'interface graphique SnapCenter ou de l'applet de commande PowerShell. Une fois l'hôte ajouté, le plug-in est automatiquement découvert.

Surveiller l'état d'installation du package de plug-in SnapCenter

Vous pouvez surveiller la progression de l'installation du package de plug-in SnapCenter à l'aide de la page Tâches. Vous souhaiterez peut-être vérifier la progression de l'installation pour déterminer quand elle est terminée ou s'il y a un problème.

À propos de cette tâche

Les icônes suivantes apparaissent sur la page Tâches et indiquent l'état de l'opération :

- En cours
- Terminé avec succès
- Échoué
- Terminé avec des avertissements ou n'a pas pu démarrer en raison d'avertissements
- En file d'attente

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Moniteur**.

2. Dans la page **Moniteur**, cliquez sur **Tâches**.
3. Dans la page **Tâches**, pour filtrer la liste afin que seules les opérations d'installation de plug-ins soient répertoriées, procédez comme suit :
   a. Cliquez sur **Filtre**.
   b. Facultatif : précisez la date de début et de fin.
   c. Dans le menu déroulant Type, sélectionnez **Installation du plug-in**.
   d. Dans le menu déroulant État, sélectionnez l'état de l'installation.
   e. Cliquez sur **Appliquer**.
4. Sélectionnez la tâche d'installation et cliquez sur **Détails** pour afficher les détails de la tâche.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

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**.
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"
   ```

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.