# Installez le plug-in SnapCenter pour Microsoft Windows

SnapCenter Software 4.6

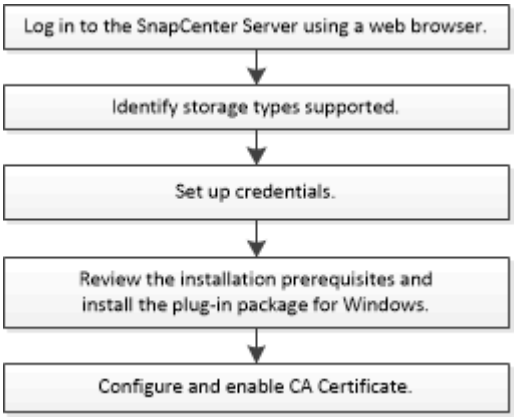
NetApp
September 29, 2025

# Sommaire

# Installez le plug-in SnapCenter pour Microsoft Windows

## Workflow d'installation du plug-in SnapCenter pour Microsoft Windows

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




## Conditions d'installation requises pour le plug-in SnapCenter pour Microsoft Windows

Avant d'installer le plug-in pour Windows, vous devez connaître certaines conditions d'installation.

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 un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Si vous souhaitez sauvegarder la réplication, vous devez configurer SnapMirror et SnapVault.

### Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows

Avant d'installer le package de plug-ins SnapCenter pour Windows, vous devez connaître les exigences en matière d'espace système hôte de base et de dimensionnement.

| Élément | De formation |
| --- | --- |
| Systèmes d'exploitation | Microsoft Windows<br><br>Pour obtenir les dernières informations sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp". |
| RAM minimale pour le plug-in SnapCenter sur l'hôte | 1 GO |
| Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte | 5 GO<br><br>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation 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 récentes. |
| Packs logiciels requis | • Microsoft .NET Framework 4.5.2 ou version ultérieure<br>• Windows Management Framework (WMF) 4.0 ou version ultérieure<br>• PowerShell 4.0 ou version ultérieure<br><br>Pour obtenir les dernières informations sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp". |

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

SnapCenter utilise des identifiants pour authentifier les utilisateurs pour les opérations SnapCenter. Vous devez créer des informations d'identification pour l'installation des plug-ins SnapCenter, ainsi que des informations d'identification supplémentaires pour exécuter les 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 les 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 affecter au moins le groupe de ressources et les privilèges de sauvegarde à l'utilisateur.

**Étapes**

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

| Pour ce champ… | Procédez comme ça… |
| --- | --- |
| Nom d'identification | Saisissez un nom pour les informations d'identification. |
| Nom d'utilisateur/Mot de passe | Entrez le nom d'utilisateur et le mot de passe utilisés pour l'authentification.<br>• Administrateur de domaine ou tout membre du groupe d'administrateurs<br>Spécifiez l'administrateur de domaine ou tout membre du groupe d'administrateurs sur le système sur lequel vous installez le plug-in SnapCenter. Les formats valides pour le champ Nom d'utilisateur sont les suivants :<br>◦ `NetBIOS\UserName`<br>◦ `Domain FQDN\UserName`<br>◦ `UserName@upn`<br>• Administrateur local (groupes de travail uniquement)<br>Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré sur le système sur lequel vous installez le plug-in SnapCenter. Vous pouvez spécifier un compte d'utilisateur local appartenant au groupe d'administrateurs locaux si le compte d'utilisateur dispose de privilèges élevés ou si la fonction de contrôle d'accès utilisateur est désactivée sur le système hôte. Le format du champ Nom d'utilisateur est le suivant : `UserName`<br>N'utilisez pas de guillemets (") ou de contre-coches (") dans les mots de passe. Vous ne devez pas utiliser moins de (<) et un point d'exclamation (!) symboles ensemble dans les mots de passe. Par exemple, moins<!10, moins dix<!, contre-recul 12. |

| Pour ce champ… | Procédez comme ça… |
| --- | --- |
| Mot de passe | Entrez le mot de passe utilisé pour l'authentification. |

5. Cliquez sur **OK**.

   Une fois que vous avez terminé la configuration des informations d'identification, vous pouvez affecter la maintenance des informations d'identification à un utilisateur ou à un groupe d'utilisateurs sur la page utilisateur et accès.

## Configurez GMSA sur Windows Server 2012 ou version ultérieure

Windows Server 2012 ou version ultérieure vous permet de créer un compte de service géré de groupe (GMSA) qui fournit une gestion automatisée des mots de passe de compte de service à partir d'un compte de domaine géré.

**Ce dont vous aurez besoin**

- Vous devez disposer d'un contrôleur de domaine Windows Server 2012 ou version ultérieure.
- Vous devez disposer d'un hôte Windows Server 2012 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 -EffectiveImmediely
3. Créez et configurez votre GMSA :
   a. Créez un compte de groupe d'utilisateurs au format suivant :

```
 domainName\accountName$
.. Ajouter des objets d'ordinateur 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,…>
.. Courez `Get-ADServiceAccount` 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 lancer 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 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 d'administration au GMSA configuré sur l'hôte.
6. Ajoutez l'hôte Windows en spécifiant le compte GMSA configuré dans le serveur SnapCenter.

   Le serveur SnapCenter installe les plug-ins sélectionnés sur l'hôte et le GMSA spécifié sera utilisé comme compte de journal de service lors de l'installation du plug-in.

# Configurez GMSA sur Windows Server 2012 ou version ultérieure

Windows Server 2012 ou version ultérieure vous permet de créer un compte de service géré de groupe (GMSA) qui fournit une gestion automatisée des mots de passe de compte de service à partir d'un compte de domaine géré.

**Ce dont vous aurez besoin**

- Vous devez disposer d'un contrôleur de domaine Windows Server 2012 ou version ultérieure.
- Vous devez disposer d'un hôte Windows Server 2012 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 -EffectiveImmediely

3. Créez et configurez votre GMSA :
   a. Créez un compte de groupe d'utilisateurs au format suivant :

```
 domainName\accountName$
.. Ajouter des objets d'ordinateur 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,…>
.. Courez `Get-ADServiceAccount` 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 lancer 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 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 d'administration au GMSA configuré sur l'hôte.
6. Ajoutez l'hôte Windows en spécifiant le compte GMSA configuré dans le serveur SnapCenter.

   Le serveur SnapCenter installe les plug-ins sélectionnés sur l'hôte et le GMSA spécifié sera utilisé comme compte de journal de service lors de 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 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 installer les plug-ins. Vous pouvez ajouter un hôte et installer un plug-in pour un hôte individuel ou un cluster.

**Ce dont vous aurez besoin**

- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation du plug-in, comme le rôle d'administrateur SnapCenter.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré 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 le compte de service géré de groupe (GMSA), vous devez configurer GMSA avec des privilèges d'administration.

  "Configurez le compte de service géré par groupe sur Windows Server 2012 ou version ultérieure pour Windows File System"

**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.
- Plug-ins Windows
  - Microsoft Windows
  - Microsoft Exchange Server
  - Microsoft SQL Server
  - SAP HANA
  - Plug-ins personnalisés
- Installation des 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 noeuds du cluster.

- Stockage E-Series

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

**Étapes**

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

| **Pour ce champ…** | **Procédez comme ça…** |
| --- | --- |
| Type d'hôte | Sélectionnez le type d'hôte **Windows**.<br><br>Le serveur SnapCenter 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.<br><br>SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le nom de domaine complet (FQDN).<br><br>Vous pouvez entrer les adresses IP ou FQDN de l'un des éléments suivants :<br><br>• Hôte autonome<br>• Windows Server Failover Clustering (WSFC)<br><br>Si vous ajoutez un hôte à l'aide de SnapCenter et qu'il fait partie d'un sous-domaine, vous devez fournir le FQDN. |

| Pour ce champ… | Procédez comme ça… |
| --- | --- |
| Informations d'identification | Sélectionnez le nom d'identification que vous avez créé ou créez les nouvelles informations d'identification.<br><br>Les informations d'identification doivent disposer de droits d'administration sur l'hôte distant. Pour plus d'informations, reportez-vous à la section informations sur la création d'informations d'identification.<br><br>Les informations d'identification, notamment le nom d'utilisateur, le domaine et le type d'hôte, s'affichent en plaçant votre curseur sur le nom d'identification fourni.<br><br>Le mode d'authentification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajout d'hôte. |

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

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

6. (Facultatif) cliquez sur **plus d'options**.

| Pour ce champ… | Procédez comme ça… |
| --- | --- |
| Port | Conservez le numéro de port par défaut ou spécifiez le numéro de port.<br><br>Le numéro de port par défaut est 8145. Si le serveur SnapCenter a été installé sur un port personnalisé, ce numéro de port est affiché comme port par défaut.<br><br>Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Dans le cas contraire, l'opération échoue. |

| Pour ce champ… | Procédez comme ça… |
| --- | --- |
| Chemin d'installation | Le chemin par défaut est C:\Program Files\NetApp\SnapCenter.<br><br>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. Toutefois, si vous le souhaitez, vous pouvez personnaliser le chemin par défaut. |
| Ajoutez tous les hôtes du cluster | Cochez cette case pour ajouter tous les nœuds du 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 vérifier si l'hôte répond aux exigences d'installation du plug-in. |
| Utilisez le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in | Cochez cette case si vous souhaitez utiliser le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in.<br><br>Indiquez le nom GMSA dans le format suivant : *domainName\accountName$*.<br><br>GMSA sera utilisé comme compte de service de connexion uniquement pour le plug-in SnapCenter pour Windows. |

7. Cliquez sur **soumettre**.

   Si vous n'avez pas coché la case **Skip précontrôles**, l'hôte est validé pour vérifier s'il répond aux conditions requises pour installer le plug-in. L'espace disque, la RAM, la version PowerShell, la version .NET et l'emplacement sont validés par rapport aux exigences minimales. Si la configuration minimale requise n'est pas respectée, 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 `C:\Program Files\NetApp\SnapCenter` WebApp pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez corriger le problème.

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

8. Surveillez la progression de l'installation.

# Installation du plug-in SnapCenter pour Microsoft Windows sur plusieurs hôtes distants à l'aide d'applets de commande PowerShell

Si vous souhaitez installer le plug-in SnapCenter pour Microsoft Windows sur plusieurs hôtes simultanément, vous pouvez le faire en utilisant le `Install-SmHostPackage` Cmdlet PowerShell.

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

**Étapes**

1. Lancer PowerShell.
2. Sur l'hôte du serveur SnapCenter, établissez une session à l'aide de `Open-SmConnection` cmdlet, puis saisissez vos informations d'identification.
3. Ajoutez l'hôte autonome ou le cluster au système SnapCenter à l'aide du `Add-SmHost` cmdlet et les paramètres requis.

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

   Vous pouvez utiliser le `-skipprecheck` option lorsque vous avez installé les plug-ins manuellement et ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.

# Installez le plug-in SnapCenter pour Microsoft Windows silencieusement 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 pouvez pas 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.

**Ce dont vous aurez besoin**

- Vous devez avoir installé Microsoft .Net 4.5.2 ou une version ultérieure.
- Vous devez avoir installé PowerShell 4.0 ou une version ultérieure.
- Vous devez avoir activé la mise en file d'attente des messages Windows.
- 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 à partir de 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. Entrez 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 de Plug-in pour Windows sont sensibles à la casse.

   Entrez les valeurs des variables suivantes :

| Variable | Valeur |
|---|---|
| */debuglog »<Debug_Log_Path>* | 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. |
| SUITE_INSTALLDIR | Spécifiez le répertoire d'installation du module de plug-in hôte. |
| BI_SERVICEACCOUNT | Spécifiez le compte de service Web SnapCenter Plug-in pour Microsoft Windows. |
| BI_SERVICEPWD | Spécifiez le mot de passe du compte de service Web SnapCenter Plug-in pour Microsoft Windows. |

| Variable | Valeur |
| --- | --- |
| Installation de ISFeatureInstall | Spécifier la solution à déployer par SnapCenter sur un hôte distant |

Le paramètre *debulog* inclut le chemin du fichier journal pour SnapCenter. L'écriture dans ce fichier journal est la méthode recommandée 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 trouverez des informations de dépannage supplémentaires dans le fichier journal du package SnapCenter pour Windows. Les fichiers journaux du package sont répertoriés (le plus ancien d'abord) 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 de SnapCenter ou de l'applet de commande PowerShell. Une fois l'hôte ajouté, le plug-in est automatiquement découvert.

# Contrôler l'état d'installation du module d'extension SnapCenter

Vous pouvez contrôler la progression de l'installation du module d'extension SnapCenter à l'aide de la page travaux. Vous pouvez 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 travaux et indiquent l'état de l'opération :

- En cours
- Terminé avec succès
- Échec
- Terminé avec des avertissements ou impossible de 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 **travaux**.
3. Dans la page travaux, pour filtrer la liste de manière à ce que seules les opérations d'installation du plug-in soient répertoriées, procédez comme suit :
   a. Cliquez sur **Filtrer**.
   b. Facultatif : spécifiez les dates 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 le travail d'installation et cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

# 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.

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 Nom alternatif du sujet (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 **Oui**, importez la clé privée, puis cliquez sur **Suivant**. |
| Importer le format de fichier | N'apportez aucune modification ; cliquez sur **Suivant**. |
| Sécurité | Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur **Suivant**. |
| Exécution de l'assistant d'importation de certificat | Vérifiez le résumé, puis cliquez sur **Terminer** pour lancer l'importation. |

L'importation du certificat doit être groupée avec la clé privée (les formats pris en charge sont : *.pfx, *.p12, *.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"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
   appid="$guid"
   ```

## 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.

**Ce dont vous aurez besoin**

- 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**.

**Après la fin**

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



## Informations sur les marques commerciales