Préparez-vous à installer le plug-in SnapCenter pour PostgreSQL

SnapCenter software

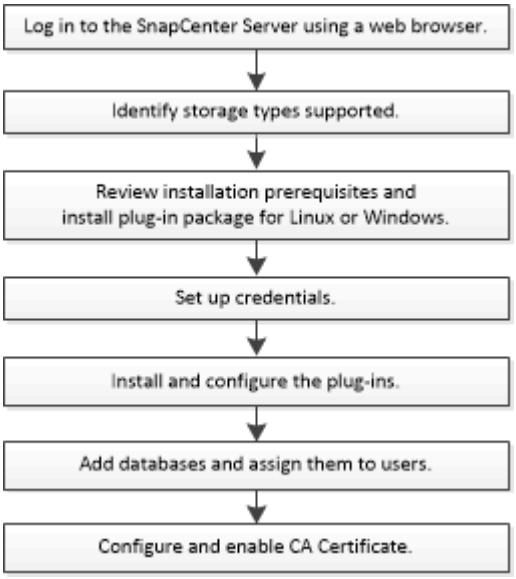
NetApp
November 06, 2025

Sommaire

Préparez-vous à installer le plug-in SnapCenter pour PostgreSQL

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

Vous devez installer et configurer le plug-in SnapCenter pour PostgreSQL si vous souhaitez protéger les clusters PostgreSQL.



Conditions préalables pour ajouter des hôtes et installer le plug-in SnapCenter pour PostgreSQL

Avant d'ajouter un hôte et d'installer les packages de plug-ins, vous devez remplir toutes les conditions requises. Le plug-in SnapCenter pour PostgreSQL est disponible dans les environnements Windows et Linux.

- Vous devez avoir installé Java 11 sur votre hôte.

  IBM Java n'est pas pris en charge sur les hôtes Windows et Linux.

- Pour Windows, le service de création de plug-in doit être exécuté à l'aide de l'utilisateur Windows « LocalSystem », qui est le comportement par défaut lorsque le plug-in pour PostgreSQL est installé en tant qu'administrateur de domaine.
- 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. Le plug-in SnapCenter pour Microsoft Windows sera déployé par défaut avec le plug-in PostgreSQL sur les hôtes Windows.
- SnapCenter Server doit avoir accès au port 8145 ou au port personnalisé de l'hôte Plug-in pour PostgreSQL.

hôtes Windows

- Vous devez disposer d'un utilisateur de domaine avec des privilèges d'administrateur local avec des autorisations de connexion locales sur l'hôte distant.
- Lors de l'installation du plug-in pour PostgreSQL sur un hôte Windows, le plug-in SnapCenter pour Microsoft Windows est installé automatiquement.
- Vous devez avoir activé la connexion SSH basée sur un mot de passe pour l'utilisateur root ou non root.
- Vous devez avoir installé Java 11 sur votre hôte Windows.

  "Télécharger JAVA pour tous les systèmes d'exploitation"

  "Outil de matrice d'interopérabilité NetApp"

Hôtes Linux

- Vous devez avoir activé la connexion SSH basée sur un mot de passe pour l'utilisateur root ou non root.
- Vous devez avoir installé Java 11 sur votre hôte Linux.

  "Télécharger JAVA pour tous les systèmes d'exploitation"

  "Outil de matrice d'interopérabilité NetApp"

- Pour les clusters PostgreSQL exécutés sur un hôte Linux, lors de l'installation du plug-in pour PostgreSQL, le plug-in SnapCenter pour UNIX est installé automatiquement.
- Vous devriez avoir **bash** comme shell par défaut pour l'installation du plug-in.

Commandes supplémentaires

Pour exécuter une commande supplémentaire sur le plug-in SnapCenter pour PostgreSQL, vous devez l'inclure dans le fichier *allowed_commands.config*.

- Emplacement par défaut sur l'hôte Windows : *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Emplacement par défaut sur l'hôte Linux : */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Pour autoriser les commandes supplémentaires sur l'hôte du plug-in, ouvrez le fichier *allowed_commands.config* dans un éditeur. Saisissez chaque commande sur une ligne distincte et les commandes ne sont pas sensibles à la casse. Assurez-vous de spécifier le chemin d'accès complet et de placer le chemin d'accès entre guillemets (") s'il contient des espaces.

Par exemple:

commande : mount commande : umount commande : "C:\Program Files\ NetApp\SnapCreator commands\sdcli.exe" commande : myscript.bat

Si le fichier *allowed_commands.config* n'est pas présent, l'exécution des commandes ou du script sera bloquée et le workflow échouera avec l'erreur suivante :

"[/mnt/mount -a] exécution non autorisée. Autoriser en ajoutant la commande dans le fichier %s sur l'hôte du plugin."

Si la commande ou le script n'est pas présent dans *allowed_commands.config*, l'exécution de la commande ou

du script sera bloquée et le workflow échouera avec l'erreur suivante :

"[/mnt/mount -a] exécution non autorisée. Autoriser en ajoutant la commande dans le fichier %s sur l'hôte du plugin."

Vous ne devez pas utiliser d'entrée générique (*) pour autoriser toutes les commandes.

Configurer les privilèges sudo pour les utilisateurs non root pour l'hôte Linux

SnapCenter permet à un utilisateur non root d'installer le package de plug-ins SnapCenter pour Linux et de démarrer le processus de plug-in. Les processus du plug-in s'exécuteront en tant qu'utilisateur non root effectif. Vous devez configurer les privilèges sudo pour l'utilisateur non root afin de fournir l'accès à plusieurs chemins.

Ce dont vous aurez besoin

- Sudo version 1.8.7 ou ultérieure.
- Si le masque est 0027, assurez-vous que le dossier Java et tous les fichiers qu'il contient doivent avoir l'autorisation 555. Dans le cas contraire, l'installation du plug-in risque d'échouer.
- Pour l'utilisateur non root, assurez-vous que le nom de l'utilisateur non root et le groupe de l'utilisateur doivent être identiques.
- Modifiez le fichier */etc/ssh/sshd_config* pour configurer les algorithmes de code d'authentification des messages : MAC hmac-sha2-256 et MAC hmac-sha2-512.

  Redémarrez le service sshd après avoir mis à jour le fichier de configuration.

  Exemple:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

À propos de cette tâche

Vous devez configurer les privilèges sudo pour l'utilisateur non root afin de fournir l'accès aux chemins suivants :

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /emplacement_personnalisé/ NetApp/snapcenter/spl/bin/spl

Mesures

1. Connectez-vous à l'hôte Linux sur lequel vous souhaitez installer le package de plug-ins SnapCenter pour Linux.
2. Ajoutez les lignes suivantes au fichier /etc/sudoers en utilisant l'utilitaire Linux visudo.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

LINUX_USER est le nom de l'utilisateur non root que vous avez créé.

Vous pouvez obtenir la *valeur de somme de contrôle* à partir du fichier **sc_unix_plugins_checksum.txt**, qui se trouve à :

- _C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt _ si SnapCenter Server est installé sur l'hôte Windows.
- _/opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ si SnapCenter Server est installé sur un hôte Linux.

L'exemple doit être utilisé uniquement comme référence pour la création de vos propres données.

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" .
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."

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

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

Article	Exigences
Systèmes d'exploitation	• Red Hat Enterprise Linux • Serveur d'entreprise SUSE Linux (SLES) Pour obtenir les dernières informations sur les versions prises en charge, consultez le "Outil de matrice d'interopérabilité NetApp" .
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	2 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	Java 11 Oracle Java et OpenJDK Si vous avez mis à niveau JAVA vers la dernière version, vous devez vous assurer que l'option JAVA_HOME située dans /var/opt/snapcenter/spl/etc/spl.properties est définie sur la version JAVA correcte et le chemin correct. Pour obtenir les dernières informations sur les versions prises en charge, consultez le "Outil de matrice d'interopérabilité NetApp" .

Configurer les informations d'identification pour le plug-in SnapCenter pour PostgreSQL

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 des clusters ou des systèmes de fichiers Windows.

À propos de cette tâche

- Hôtes Linux

Vous devez configurer les informations d'identification pour l'installation des plug-ins sur les hôtes Linux.

Vous devez configurer les informations d'identification pour l'utilisateur root ou pour un utilisateur non root disposant de privilèges sudo pour installer et démarrer le processus du plug-in.

Meilleure pratique : bien que vous soyez autorisé à créer des informations d'identification pour Linux après avoir déployé des hôtes et installé des plug-ins, la meilleure pratique consiste à créer des informations d'identification après avoir ajouté des SVM, avant de déployer des hôtes et d'installer des plug-ins.

- hôtes Windows

  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 des droits d'administrateur sur l'hôte distant.

Si vous configurez des informations d'identification pour des groupes de ressources individuels et que le nom d'utilisateur ne dispose pas de privilèges d'administrateur complets, vous devez attribuer au moins les privilèges de groupe de ressources et de sauvegarde au nom d'utilisateur.

Étapes

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, spécifiez les informations requises pour la configuration des informations d'identification :

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

Pour ce domaine…	Fais ceci…
Nom d'utilisateur	Saisissez le nom d'utilisateur et le mot de passe qui doivent être 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 : ◦ *NetBIOS\Nom d'utilisateur* ◦ *Domaine FQDN\Nom d'utilisateur* • 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 : *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.
Mode d'authentification	Sélectionnez le mode d'authentification que vous souhaitez utiliser.
Utiliser les privilèges sudo	Cochez la case **Utiliser les privilèges sudo** si vous créez des informations d'identification pour un utilisateur non root. Applicable uniquement aux utilisateurs Linux.

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 dans 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.

Installer le plug-in SnapCenter pour PostgreSQL

Ajouter des hôtes et installer des packages de plug-ins sur des hôtes distants

Vous devez utiliser la page Ajouter un hôte de SnapCenter pour ajouter des hôtes, puis installer les packages de plug-ins. Les plug-ins sont automatiquement installés sur les hôtes distants. Vous pouvez ajouter l'hôte et installer des packages de plug-ins pour un hôte individuel.

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.
- Vous devez vous assurer que le service de mise en file d'attente des messages est en cours d'exécution.
- La documentation d'administration contient des informations sur la gestion des hôtes.
- 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 PostgreSQL"

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 .

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Vérifiez que l'onglet **Hôtes gérés** est sélectionné en haut.
3. Cliquez sur **Ajouter**.
4. Dans la page Hôtes, effectuez les actions suivantes :

Pour ce domaine…	Fais ceci…
Type d'hôte	Sélectionnez le type d'hôte : • Windows • Linux Le plug-in pour PostgreSQL est installé sur l'hôte client PostgreSQL, et cet hôte peut être sur un système Windows ou un système Linux.
Nom d'hôte	Entrez le nom de l'hôte de communication. 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 FQDN.

Pour ce domaine…	Fais ceci…
Informations d'identification	Sélectionnez le nom des informations d'identification que vous avez créées ou créez de 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. Vous pouvez afficher les détails des informations d'identification en positionnant votre curseur sur le nom des informations d'identification que vous avez fournies. Le mode d'authentification des informations d'identification 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.

   Lors de l'utilisation de l'API REST pour installer le plug-in pour PostgreSQL, vous devez transmettre la version 3.0. Par exemple, PostgreSQL:3.0

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.

Pour ce domaine…	Fais ceci…
Chemin d'installation	Le plug-in pour PostgreSQL est installé sur l'hôte client PostgreSQL, et cet hôte peut être sur un système Windows ou un système Linux. • Pour le package de plug-ins SnapCenter pour Windows, le chemin par défaut est C:\Program Files\ NetApp\ SnapCenter. En option, vous pouvez personnaliser le chemin. • Pour le package de plug-ins SnapCenter pour Linux, le chemin par défaut est /opt/ NetApp/snapcenter. En option, vous pouvez personnaliser le chemin.
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.
Ajouter tous les hôtes du cluster	Cochez cette case pour ajouter tous les nœuds du cluster.
Utiliser un compte de service géré de groupe (gMSA) pour exécuter les services du plug-in	Pour l'hôte Windows, 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 de .NET, l'emplacement (pour les plug-ins Windows) et la version de Java (pour les plug-ins Linux) sont validés par rapport à la configuration minimale requise. 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 dans 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. Si le type d'hôte est Linux, vérifiez l'empreinte digitale, puis cliquez sur **Confirmer et soumettre**.

   Dans une configuration de cluster, vous devez vérifier l'empreinte digitale de chacun des nœuds du cluster.

   La vérification des empreintes digitales est obligatoire même si le même hôte a été ajouté précédemment à SnapCenter et que l'empreinte digitale a été confirmée.

9. Surveiller la progression de l'installation.
   - Pour le plug-in Windows, les journaux d'installation et de mise à niveau se trouvent à : *C:\Windows\SnapCenter plugin\Install*<JOBID>_
   - Pour le plug-in Linux, les journaux d'installation se trouvent à : */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log_ et les journaux de mise à niveau se trouvent à : */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log_

Installer les packages de plug-ins SnapCenter pour Linux ou Windows sur plusieurs hôtes distants à l'aide d'applets de commande

Vous pouvez installer les packages de plug-in SnapCenter pour Linux ou Windows sur plusieurs hôtes simultanément à l'aide de l'applet de commande PowerShell Install-SmHostPackage.

Avant de commencer

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 le package de plug-in.

Étapes

1. Lancez PowerShell.
2. Sur l'hôte SnapCenter Server, établissez une session à l'aide de l'applet de commande Open-SmConnection, puis entrez vos informations d'identification.
3. Installez le plug-in sur plusieurs hôtes à l'aide de l'applet de commande Install-SmHostPackage et des 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" .

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

4. Saisissez vos informations d'identification pour l'installation à distance.

Installez le plug-in SnapCenter pour PostgreSQL sur les hôtes Linux à l'aide de l'interface de ligne de commande

Vous devez installer le plug-in SnapCenter pour le cluster PostgreSQL à l'aide de l'interface utilisateur (UI) de SnapCenter . Si votre environnement ne permet pas

l'installation à distance du plug-in à partir de l'interface utilisateur SnapCenter , vous pouvez installer le plug-in pour le cluster PostgreSQL en mode console ou en mode silencieux à l'aide de l'interface de ligne de commande (CLI).

Avant de commencer

- Vous devez installer le plug-in pour le cluster PostgreSQL sur chacun des hôtes Linux sur lesquels réside le client PostgreSQL.
- L'hôte Linux sur lequel vous installez le plug-in SnapCenter pour le cluster PostgreSQL doit répondre aux exigences logicielles, de cluster et de système d'exploitation dépendantes.

  L'outil de matrice d'interopérabilité (IMT) contient les informations les plus récentes sur les configurations prises en charge.

  "Outil de matrice d'interopérabilité NetApp"

- Le plug-in SnapCenter pour le cluster PostgreSQL fait partie du package de plug-ins SnapCenter pour Linux. Avant d'installer le package de plug-ins SnapCenter pour Linux, vous devez déjà avoir installé SnapCenter sur un hôte Windows.

Étapes

1. Copiez le fichier d'installation du package de plug-ins SnapCenter pour Linux (snapcenter_linux_host_plugin.bin) depuis C:\ProgramData\ NetApp\ SnapCenter\Package Repository vers l'hôte sur lequel vous souhaitez installer le plug-in pour PostgreSQL.

   Vous pouvez accéder à ce chemin à partir de l'hôte sur lequel le serveur SnapCenter est installé.

2. À partir de l'invite de commande, accédez au répertoire dans lequel vous avez copié le fichier d'installation.
3. Installer le plug-in : `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`

   - -DPORT spécifie le port de communication HTTPS SMCore.
   - -DSERVER_IP spécifie l'adresse IP du serveur SnapCenter .
   - -DSERVER_HTTPS_PORT spécifie le port HTTPS du serveur SnapCenter .
   - -DUSER_INSTALL_DIR spécifie le répertoire dans lequel vous souhaitez installer le package de plug-ins SnapCenter pour Linux.
   - DINSTALL_LOG_NAME spécifie le nom du fichier journal.

   ```
   /tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
   -DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
   -DUSER_INSTALL_DIR=/opt
   -DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
   -DCHOSEN_FEATURE_LIST=CUSTOM
   ```

4. Modifiez le fichier /<répertoire d'installation>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties, puis ajoutez le paramètre PLUGINS_ENABLED = PostgreSQL:3.0.
5. Ajoutez l'hôte au serveur SnapCenter à l'aide de l'applet de commande Add-Smhost et des paramètres

requis.

Les informations concernant les paramètres pouvant être utilisés avec la 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" .

Surveiller l'état d'installation du plug-in pour PostgreSQL

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"
```

Configurer le certificat CA pour le service de plug-ins SnapCenter PostgreSQL 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 SnapCenter PostgreSQL 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.